Enumerative Combinatorics: class notes

Darij Grinberg

March 11, 2023 (unfinished!)

Status: Chapters 1 and 2 finished; Chapter 3 outlined.

Contents

Preface

This is the text accompanying my Math 222 (Enumerative Combinatorics) class at Drexel University in Fall 2019. The website of this class can be found at

`http://www.cip.ifi.lmu.de/~grinberg/t/19fco`

and includes some extra materials (such as homeworks and solutions).

This document is a work in progress. It might become a textbook one day, but for now only parts of it (currently Chapters 1 and 2) are at the level of detail expected from a textbook and can be read on a standalone basis. The later chapters are a construction zone.

Please report any errors you find to `darijgrinberg@gmail.com` **.**

What is this?

These notes cover the basics of enumerative combinatorics, with an emphasis on counting, identities and bijections. We assume that you (the reader) are well familiar with the basics of rigorous mathematics (such as proof methods, the constructions of integers and rationals, and basic properties of finite sets), as covered (for example) in [LeLeMe16, Chapters 1–5], [Day16], [Hammac15], [Newste19, Part I and Appendices A–B] and [Loehr20]. We will not rely on any analysis, linear algebra or abstract algebra except for the little that we introduce ourselves.

In terms of coverage, these notes do not set out to break any new ground.

- The first chapter (Chapter 1) is introductory and begins (in Section 1.1) with a problem (that of counting domino tilings) that is not in itself particularly important, but serves to motivate many basic ideas and notions (such as bijective proofs, the sum rule and the product rule). We continue (in Section 1.2) with another elementary problem (viz., finding closed-form expressions for sums of the form $1^k + 2^k + \cdots + n^k$), which we do not solve at this point (it serves as a teaser for the next chapter) but which prompts us to introduce the finite sum notation and get some passing acquaintance with certain combinatorial numbers that will later become important. The next section (Section 1.3) introduces factorials and binomial coefficients, and proves (mostly algebraically) their most basic properties, such as the recursion, the combinatorial interpretation and the hockey-stick formula. In the sections that follow (Sections 1.4, 1.5, 1.6 and 1.7), we start counting for real: Various problems are considered and solved, counting (certain kinds of) subsets, tuples, maps and permutations. In the process we gradually introduce general strategies (such as the difference rule, the isomorphism principle, or the interchange of summations) as they become useful. Among other things, we also provide brief introductions to the use of modern electronic tools like the Online Encyclopedia of Integer Sequences and the SageMath CAS.

- The second chapter (Chapter 2) focusses on binomial coefficients and related concepts and problems. The first sections revisit some statements made in the previous chapter, proving and re-proving them and demonstrating some further techniques in the process. Section 2.4 answers one of the most basic counting problems, namely that of counting injective maps between two finite sets; the analogous problem for surjective maps has no closed-form answer, but two recurrences are derived. Section 2.5 then proves the formula for $1^k + 2^k + \cdots + n^k$ that was left unproved in Section 1.2. The next section (Section 2.6) states, proves and applies the Vandermonde convolution theorem in several ways, while also explaining the "polynomial identity trick" on which all of the proofs rely and which is a versatile tool in the study of binomial coefficients (despite not being in itself a result of combinatorics). The next sections continue with a re-proof of the combinatorial interpretation of $\binom{n}{k}$ (Section 2.7), a first encounter with the method of generating functions (Section 2.8), and the Principle of Inclusion and Exclusion (Section 2.9). Then, in Section 2.10, we count several kinds and variants of compositions of an integer. In Section 2.11, we introduce multisubsets of a set, count them and show an application to an elementary (but far from simple) counting problem. In Section 2.12, we introduce multinomial coefficients and establish their basic properties.
- ... (Further summaries will be written as the respective chapters will be finished.)

One particular goal of these notes is to develop at least the basics of the theory rigorously – i.e., without handwaving, picture "proofs" and ambiguous terminology like "ways to choose" or vaguely specified "arrangements". This does not mean that we shall avoid such semi-intuitive explanations whatsoever; but we aim to ensure that they will never be used in a load-bearing capacity. Sometimes, a statement will be first proved informally using such explanations, then re-proved in a rigorous language.

These notes have their origin in the handwritten class notes I made for the Math 5705 (Enumerative Combinatorics) class at the UMN in Fall 2018[1]. However, they differ noticeably (both in coverage and in the order of the topics).

0.1. Notations

The following notations will be used throughout the notes:

- The symbol $\mathbb{N}$ means the set of all nonnegative integers, i.e., the set $\{0, 1, 2, 3, \ldots\}$.

[1] `http://www.cip.ifi.lmu.de/~grinberg/t/18f`

- The symbol id denotes the identity map of a set X (that is, the map from X to X that sends each element $x \in X$ to x).
- For any $k \in \mathbb{Z}$, we let $[k]$ denote the set $\{1, 2, \ldots, k\}$ of the first k positive integers. When $k \leq 0$, this set is understood to be empty.
- The notation $|S|$ denotes the size (i.e., the number of elements) of a set S.
- The symbol # stands for "number" (or "the number"), as in "the number of all subsets of $\{1, 2\}$ is 4".

Several further notations will be introduced over the course of these notes. In particular, we will define

- the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ (Definition 1.1.10);
- the summation sign $\sum$ (Definition 1.2.2 and Definition 1.3.26);
- the product sign $\prod$ (Definition 1.2.7);
- the two-line notation for a map (Definition 1.2.11);
- the factorials $n!$ (Definition 1.3.1);
- the binomial coefficients $\binom{n}{k}$ (Definition 1.3.3);
- the truth value $[\mathcal{A}]$ (Definition 1.3.15);
- the notion of a lacunar set of integers (Definition 1.4.2);
- the floor and ceiling of a number ($\lfloor x \rfloor$ and $\lceil x \rceil$) (Definition 1.4.4);
- the notion of a permutation (Definition 1.7.1);
- the notion of a composition (Definition 2.10.2);
- the concept of a multisubset (Definition 2.11.1) and the notation $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ for it, along with various related notions;
- the surjection numbers $\operatorname{sur}(m, n)$ (Definition 2.4.9);
- the multinomial coefficients $\binom{n}{n_1, n_2, \ldots, n_k}$ (Definition 2.12.1);

and several others.

Class of 2019-09-23

1. Introduction

This is a text on *enumerative combinatorics*: the part of mathematics concerned with the sizes of finite sets, particularly their computation and the proof of equalities between them. More precisely, here are what I consider to be the three main threads of enumerative combinatorics:

- **Counting** – i.e., finding formulas for the sizes of certain finite sets. For example, we count the permutations of the set $\{1,2,\ldots,n\}$, or the k-element subsets of $\{1,2,\ldots,n\}$ that contain no two consecutive elements. "Count" means finding a formula that expresses the number of such permutations or k-element subsets in terms of n and k.
- **Proving polynomial identities** (such as the binomial formula $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ or various deeper ones).
- **Finding and studying interesting maps between finite sets**. A basic example of such a map is the "bit-set encoding": the bijection from the set of all subsets of $\{1,2,\ldots,n\}$ (for a fixed positive integer n) to the set of all n-tuples $(i_1,i_2,\ldots,i_n) \in \{0,1\}^n$ (known as "length-n bitstrings") which sends each subset S of $\{1,2,\ldots,n\}$ to the n-tuple $(i_1,i_2,\ldots,i_n)$, where $i_k = \begin{cases} 1, & \text{if } k \in S; \\ 0, & \text{if } k \notin S \end{cases}$. We will care particularly about bijections, since they directly help in counting, but even non-bijective maps are fundamental to enumerative combinatorics.

You will see more examples of each of these three threads all over this text, starting with this introductory chapter.

We will also occasionally see some connections to linear algebra, abstract algebra, number theory and graph theory. There are other threads in enumerative combinatorics that we are not going to encounter (or only tangentially): applications (mostly), connections to representation theory or geometry, asymptotics and many more. A one-semester course needs to have its limits!

First, I will discuss some interesting (if you share my taste) questions, in no particular order. Not all of them will be answered right away.

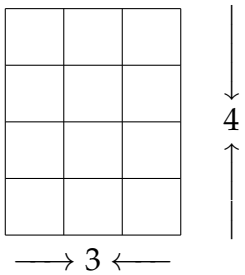
1.1. Domino tilings

1.1.1. The problem

Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Here and in the following, $\mathbb{N}$ means the set $\{0,1,2,\ldots\}$.

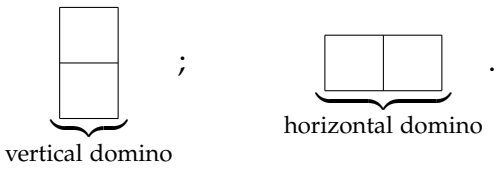
Let $R_{n,m}$ denote an $n \times m$-*rectangle*, i.e., a rectangle with width n and height m. (We imagine a specific such rectangle drawn somewhere in the plane.) For

example, $R_{3,4}$ looks like this:[2]



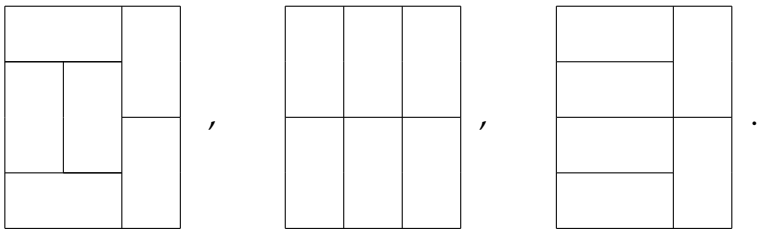
(1)

A *domino* shall mean a 1×2-rectangle or a 2×1-rectangle. More specifically: A *vertical domino* shall mean a 1×2-rectangle; a *horizontal domino* shall mean a 2×1-rectangle. Here is how they look like:



A *domino tiling* of $R_{n,m}$ is a way to cover the rectangle $R_{n,m}$ with non-overlapping dominos.

For example, here are three domino tilings of the rectangle $R_{3,4}$ (which rectangle you have seen in (1)):

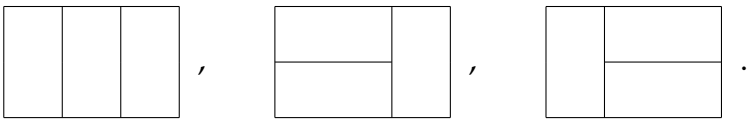


(Now, of course, we are no longer drawing the grid lines, but only the outlines of the dominos.)

We can now state our first enumeration (i.e., counting) problem: How many domino tilings does $R_{n,m}$ have?

As we just saw, $R_{3,4}$ has at least 3 domino tilings, but in fact you can find several more. Counting them all is, at the very least, an unpleasant exercise in carefulness. Let us try a simpler example:

Example 1.1.1. Here are all domino tilings of $R_{3,2}$:



[2]We subdivide it with grid lines just to show its dimensions.

If we are to solve the above problem in general, our first step should be making it rigorous. We said that a domino tiling should be a way to cover the rectangle $R_{n,m}$ with non-overlapping dominos. What does "cover" mean, and what does "non-overlapping" mean? Visually, it is pretty clear, but we do not have bulletproof mathematical definitions yet. There are two ways to create such definitions:

- **The geometric way:** We really define $R_{n,m}$ as a rectangle of width n and height m in the Euclidean plane; for example, let us pick the rectangle with vertices $(0,0)$, $(n,0)$, (n,m) and $(0,m)$ (where we model the Euclidean plane through a Cartesian coordinate system as usual).[3] We say that a set of dominos *covers* $R_{n,m}$ if their union (as sets) is $R_{n,m}$. It is harder to define what it means for a set of dominos to be *non-overlapping*; clearly, this is not quite the same as them being disjoint as sets (because they are allowed to have edges or vertices in common). There are several good ways to define non-overlappingness[4]. Unfortunately, once all these definitions are made, it is still far from clear how to **reason** about them rigorously! For example, it may seem obvious, but why exactly must all the dominos in a domino tiling of $R_{n,m}$ be "snapped to the grid" (i.e., why must their corners be grid points[5])? This is indeed true, but proving this would take serious work. Thus, even our previous observation that $R_{3,2}$ has three domino tilings (shown visually in Example 1.1.1) would become a nontrivial theorem. Thus, we leave this geometric model of domino tilings aside, and instead define things in ...

- **The combinatorial way:** We redefine $R_{n,m}$ as the set $[n] \times [m]$, where we set

$$[k] = \{1, 2, \ldots, k\} \qquad \text{for each } k \in \mathbb{N}.$$

  Its elements thus are the pairs (i,j) with $i \in [n]$ and $j \in [m]$; we call these pairs "*squares*". Thus, $R_{n,m}$ is a **finite** set of size[6] $|R_{n,m}| = nm$.

  A *vertical domino* shall mean a set of the form $\{(i,j),\ (i,j+1)\}$ for some $i, j \in \mathbb{Z}$.

  A *horizontal domino* shall mean a set of the form $\{(i,j),\ (i+1,j)\}$ for some $i, j \in \mathbb{Z}$.

  A *domino* shall mean a set that is either a vertical domino or a horizontal domino.

  If S is a set of squares (for example, $R_{n,m}$), then a *domino tiling* of S shall mean a set $\{S_1, S_2, \ldots, S_k\}$ of **disjoint** dominos whose union is S (that is, $S_1 \cup S_2 \cup \cdots \cup S_k = S$).

[3] This rectangle contains both the points on its boundary and its interior point.

[4] For example, you can say that two dominos are *non-overlapping* if their intersection is either the empty set or a point or a line segment. Then you can say that a set of dominos is *non-overlapping* if any two distinct dominos in it are non-overlapping.

[5] A *grid point* means a point with integer coordinates.

[6] The *size* of a finite set S is the number of elements of S. It is denoted by $|S|$. For example, $|\{1,4,6\}| = 3$ and $|\{-1,1,6,7\}| = 4$ and $|\varnothing| = 0$.

A few words are in order about what this has to do with our visual concept of domino tilings.

First of all, why are we suddenly considering the finite set $R_{n,m}$ to be a "rectangle"? Because we are no longer thinking in terms of all points in the plane, but rather thinking in terms of *grid squares* (as in (1)). Thus, the rectangle $R_{n,m}$ is no longer an (infinite) set of points, but now becomes a (finite) set of grid squares that lie in this rectangle. We label these grid squares by pairs of integers (namely, we label each grid square by the pair (i,j) of Cartesian coordinates of its northeastern corner[7]; thus, the southwesternmost square of $R_{n,m}$ is labeled $(1,1)$, and the eastern neighbor of a square (i,j) is $(i+1,j)$, whereas the northern neighbor of a square (i,j) is $(i,j+1)$). In other words, the square in column i (counted from the left) and row j (counted from the bottom) is labelled by the pair (i,j).

Having thus redefined the rectangle $R_{n,m}$ as a finite set of grid squares, we then do the same for dominos and domino tilings. A domino, too, is not an infinite set any more, but just a set of two adjacent grid squares. It is a vertical domino if these grid squares differ in their y-coordinate (i.e., have the forms (i,j) and $(i,j+1)$ for some $i,j \in \mathbb{Z}$), and it is a horizontal domino if these grid squares differ in their x-coordinate (i.e., have the forms (i,j) and $(i+1,j)$ for some $i,j \in \mathbb{Z}$). From this point of view, two dominos are non-overlapping if they are literally disjoint (because they are sets of grid squares now, and thus disjointness means that they have no grid squares in common; it does not matter if they share an edge).

So we have obtained a new model for domino tilings, with simpler definitions and with all sets involved being finite. This kind of model is called a **discrete model**. It is much more manageable than the geometric one, and in particular, almost everything that is visually obvious is actually straightforward to prove in this model (unlike in the geometric one). For example, it is easy to rigorously reproduce our result from Example 1.1.1 saying that $R_{3,2}$ has 3

[7]Here is how $R_{3,4}$ looks like with each square labeled:

$(1,4)$	$(2,4)$	$(3,4)$
$(1,3)$	$(2,3)$	$(3,3)$
$(1,2)$	$(2,2)$	$(3,2)$
$(1,1)$	$(2,1)$	$(3,1)$

domino tilings. In the discrete model, these domino tilings are[8]

$$\left\{ \underbrace{\{(1,1),(1,2)\}}_{\substack{\text{vertical domino}\\ \text{covering the}\\ \text{leftmost column}}}, \underbrace{\{(2,1),(2,2)\}}_{\substack{\text{vertical domino}\\ \text{covering the}\\ \text{middle column}}}, \underbrace{\{(3,1),(3,2)\}}_{\substack{\text{vertical domino}\\ \text{covering the}\\ \text{rightmost column}}} \right\},$$

$$\left\{ \underbrace{\{(1,1),(2,1)\}}_{\substack{\text{horizontal domino}\\ \text{in the bottom row}}}, \underbrace{\{(1,2),(2,2)\}}_{\substack{\text{horizontal domino}\\ \text{in the top row}}}, \underbrace{\{(3,1),(3,2)\}}_{\substack{\text{vertical domino}\\ \text{covering the}\\ \text{rightmost column}}} \right\},$$

$$\left\{ \underbrace{\{(1,1),(1,2)\}}_{\substack{\text{vertical domino}\\ \text{covering the}\\ \text{leftmost column}}}, \underbrace{\{(2,1),(3,1)\}}_{\substack{\text{horizontal domino}\\ \text{in the bottom row}}}, \underbrace{\{(2,2),(3,2)\}}_{\substack{\text{horizontal domino}\\ \text{in the top row}}} \right\}.$$

You do need a bit of work to verify that no other domino tilings of $R_{3,2}$ exist; but it is very much doable. The surefire (but boring) way is to simply check all possibilities by **brute force**: There are only 7 dominos that lie inside[9] $R_{3,2}$, and clearly any domino tiling must consist of some of these 7 dominos; now, you can check all the 2^7 possible subsets. (This is the most brainless approach; of course, with a bit of thinking, you can save yourself a lot of work.)

From now on, we shall always be using the discrete model when we study domino tilings – i.e., we define $R_{n,m}$, dominos and domino tilings via the combinatorial way.

If $n, m \in \mathbb{N}$, then let us define an integer $d_{n,m}$ by

$$d_{n,m} = (\#\text{ of domino tilings of } R_{n,m}). \tag{2}$$

Here and in the following, the symbol "#" always means "number" (or "the number", depending on context).

Our problem thus asks us to compute $d_{n,m}$. In Example 1.1.1, we have seen that $d_{3,2} = 3$. For any fixed n and m, we can technically compute $d_{n,m}$ by brute force (i.e., trying out all possible subsets of the set of dominoes lying inside $R_{n,m}$, and counting the domino tilings among them). But this becomes forbiddingly slow when n and m get even a little bit large (say, $n = 8$ and $m = 8$). We are looking for something better: for an explicit formula for $d_{n,m}$ if possible, and otherwise at least for faster algorithms that compute $d_{n,m}$.

[8] listed here in the same order in which they appeared in Example 1.1.1

[9] To "lie inside" $R_{3,2}$ means to be a subset of $R_{3,2}$ here.

1.1.2. The odd-by-odd case and the sum rule

We begin with a particularly simple case:

Proposition 1.1.2. Assume that n and m are odd. Then, $d_{n,m} = 0$.

Proof sketch. We have assumed that n and m are odd. Thus, the product nm is odd as well. In other words, the size $|R_{n,m}|$ is odd (since $|R_{n,m}| = nm$).

But each domino has even size (in fact, it has size 2).

If the set $R_{n,m}$ had a domino tiling, then the size $|R_{n,m}|$ of $R_{n,m}$ would equal the sum of the sizes of all the dominos in the tiling (because $R_{n,m}$ is the union of the dominos, and the dominos are disjoint). But the size $|R_{n,m}|$ is odd, whereas the sum of the sizes of all the dominos in the tiling is even (since each domino has even size); thus the former cannot equal the latter. This shows that the set $R_{n,m}$ has no domino tilings. In other words, the # of domino tilings of $R_{n,m}$ is 0. In other words, $d_{n,m} = 0$. □

It is worth being a little bit more detailed once and look under the hood of this proof. We have used the following basic fact:

Theorem 1.1.3 (The sum rule)**.** If a finite set S is the union of k disjoint sets $S_1, S_2, \ldots, S_k$, then

$$|S| = |S_1| + |S_2| + \cdots + |S_k| .$$

Theorem 1.1.3 is known as the *sum rule* or the *addition rule*, and is so fundamental for all of mathematics that you have probably not even noticed us tacitly using it in the proof of Proposition 1.1.2 above. We shall not prove Theorem 1.1.3, since this is a job for "axiomatic foundations of mathematics" courses and depends on the "implementation details" of your mathematical "standard library" (such as: how do you define the size of a finite set?).[10]

We can restate Theorem 1.1.3 as follows: If $S_1, S_2, \ldots, S_k$ are k disjoint finite sets, then the set $S_1 \cup S_2 \cup \cdots \cup S_k$ is finite and satisfies

$$|S_1 \cup S_2 \cup \cdots \cup S_k| = |S_1| + |S_2| + \cdots + |S_k| . \tag{3}$$

(Indeed, this follows from Theorem 1.1.3, applied to $S = S_1 \cup S_2 \cup \cdots \cup S_k$.)

[10] For example, if you define your sets and numbers in the old-fashioned Bourbakist way, then you can find Theorem 1.1.3 with proof in [Bourba68, Chapter III, §3.3, Corollary]. If you are using constructivist foundations, then Theorem 1.1.3 can be proven by induction on k (see [Loehr11, proof of 1.2] for the details of this induction proof), relying on the fact that any two disjoint finite sets A and B of $|A \cup B| = |A| + |B|$. The latter fact (which is, of course, essentially equivalent to the particular case of Theorem 1.1.3 for $k = 2$) can be proven directly by explicitly constructing a bijection $A \cup B \to [n+m]$ out of two bijections $A \to [n]$ and $B \to [m]$ (see [Loehr11, proof of 1.32] for the details of this construction). But we will not dwell on fundamental issues like this here.

Thus, if X and Y are two disjoint finite sets, then the set $X \cup Y$ is finite and satisfies

$$|X \cup Y| = |X| + |Y|. \tag{4}$$

(Indeed, this follows from (3), applied to $k = 2$, $S_1 = X$ and $S_2 = Y$.)

We have also used the visually obvious fact that $|R_{n,m}| = nm$ (that is, $R_{n,m}$ has nm squares). Formally speaking, this is a consequence of another basic fact:

Theorem 1.1.4 (The product rule for two sets)**.** Let X and Y be two finite sets. Then, $X \times Y$ is a finite set with size

$$|X \times Y| = |X| \cdot |Y|. \tag{5}$$

In other words, this theorem is saying that the number of pairs $(x, y) \in X \times Y$ (where X and Y are two given finite sets) is $|X| \cdot |Y|$. This is intuitive, since such a pair (x, y) can be constructed by choosing an element x of X (there are $|X|$ many options for it) and choosing an element y of Y (there are $|Y|$ many options for it); since the two choices are completely independent, it is reasonable that they should lead to $|X| \cdot |Y|$ many options for the whole pair (x, y).

Again, we will not prove Theorem 1.1.4, as it is sufficiently elementary.[11] It is called the *product rule for two sets*, as there is a product rule for k sets as well (Theorem 1.5.3 below).

Let us now restate our above proof of Proposition 1.1.2 in a way that makes the uses of Theorem 1.1.3 and of Theorem 1.1.4 in it explicit:

Proof of Proposition 1.1.2 (detailed version). For each $k \in \mathbb{N}$, we have $[k] = \{1, 2, \ldots, k\}$ and thus $|[k]| = |\{1, 2, \ldots, k\}| = k$. Hence, $|[n]| = n$ and $|[m]| = m$. But $R_{n,m} = [n] \times [m]$ and thus

$$\begin{aligned} |R_{n,m}| &= |[n] \times [m]| = \underbrace{|[n]|}_{=n} \cdot \underbrace{|[m]|}_{=m} \qquad \text{(by (5), applied to } X = [n] \text{ and } Y = [m]) \\ &= nm. \end{aligned}$$

We have assumed that n and m are odd. Thus, the product nm is odd as well. In other words, the size $|R_{n,m}|$ is odd (since $|R_{n,m}| = nm$).

Our next goal is to show that the set $R_{n,m}$ has no domino tilings.

Indeed, let T be a domino tiling of $R_{n,m}$. We will derive a contradiction.

Write T in the form $T = \{S_1, S_2, \ldots, S_k\}$, where $S_1, S_2, \ldots, S_k$ are distinct dominos[12]. Then, the sets $S_1, S_2, \ldots, S_k$ are dominos; thus, their sizes $|S_1|, |S_2|, \ldots, |S_k|$ are even (since

[11] See [Loehr11, 1.5] for a proof (even of a more general statement).

[12] Here, we are tacitly using the fact that T is finite. Why is T finite? Intuitively it is obvious. More rigorously, you can argue this as follows: There are only finitely many dominos that are subsets of $R_{n,m}$. The set T, being a domino tiling of $R_{n,m}$, must consist entirely of such dominos; thus, it must be a subset of the (finite) set of these dominos. Hence, T is itself finite (since a subset of a finite set is always finite).

We trust you to make such arguments whenever necessary; we will not dwell on them in the future.

the size of each domino is even[13]). Hence, the sum $|S_1| + |S_2| + \cdots + |S_k|$ is even (being a sum of even integers).

But the finite set $R_{n,m}$ is a union of the k disjoint sets $S_1, S_2, \ldots, S_k$ (since $\{S_1, S_2, \ldots, S_k\} = T$ is a domino tiling of $R_{n,m}$). Hence, Theorem 1.1.3 (applied to $S = R_{n,m}$) yields $|R_{n,m}| = |S_1| + |S_2| + \cdots + |S_k|$. Hence, $|R_{n,m}|$ is even (since $|S_1| + |S_2| + \cdots + |S_k|$ is even). This contradicts the fact that $|R_{n,m}|$ is odd.

Now, forget that we fixed T. We thus have found a contradiction for each domino tiling T of $R_{n,m}$. This shows that there exists no domino tiling of $R_{n,m}$. In other words, the # of domino tilings of $R_{n,m}$ is 0. In other words, $d_{n,m} = 0$. This proves Proposition 1.1.2. □

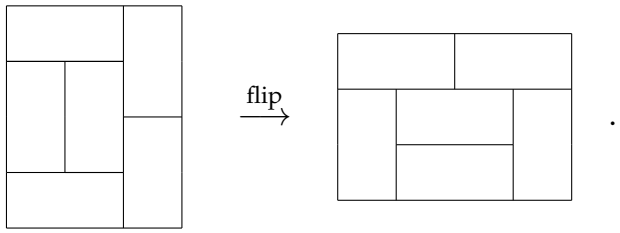
In the future, we will be using the sum rule (Theorem 1.1.3) and the product rule (Theorem 1.1.4) many times, usually without even mentioning it.

1.1.3. The symmetry and the bijection rule

Thus we have handled at least one case of our counting problem: the case when n and m are odd. It remains to handle the case when at least one of n and m is even. More precisely, it suffices to handle the case when n is even, because of the following symmetry in the problem:

Proposition 1.1.5. Let $n, m \in \mathbb{N}$. Then, $d_{n,m} = d_{m,n}$.

Proof sketch. The idea is very simple: The rectangle $R_{m,n}$ can be obtained by "flipping" the rectangle $R_{n,m}$ across the line with equation $x = y$ (in Cartesian coordinates). This "flip" operation turns domino tilings of $R_{m,n}$ into domino tilings of $R_{n,m}$ and vice versa; here is an example:



Thus, the domino tilings of $R_{m,n}$ are in 1-to-1 correspondence with the domino tilings of $R_{n,m}$. This entails that the # of the former equals the # of the latter. Since the # of the former is $d_{m,n}$ (by the definition of $d_{m,n}$), whereas the # of the latter is $d_{n,m}$ (by the definition of $d_{n,m}$), we can rewrite this as follows: $d_{m,n} = d_{n,m}$. This proves Proposition 1.1.5. □

It is worth expanding this proof just to see what exactly we have done; again, the underlying principle is very basic but worth stating at least once. The domino tilings of $R_{m,n}$ are not literally the same as the domino tilings of $R_{n,m}$ (in general[14]);

[13] Indeed, the size of each domino is 2.

[14] The words "in general" here are a pedantic hedge: Of course, the domino tilings of $R_{m,n}$ **are** literally the same as the domino tilings of $R_{n,m}$ when $n = m$ (or when $n = 0$, or when $m = 0$, or when both n and m are odd). But they are not the same, for example, when $n = 2$ and $m = 3$.

yet, we have argued that the former are in 1-to-1 correspondence with the latter, and therefore equinumerous to the latter. Formally, a 1-to-1 correspondence between two sets of objects is given by a map from one set to the other, but it cannot be just any map: It has to be a bijection (i.e., a bijective map)[15]. Thus, what we have used is the fact that if there is a bijection between two sets, then these two sets have the same size. Let us state this a little bit more explicitly:

Theorem 1.1.6 (The bijection principle)**.** If X and Y are two sets, and if $f : X \to Y$ is a bijection (i.e., a bijective map), then

$$|X| = |Y| . \tag{6}$$

We have not required X and Y to be finite in Theorem 1.1.6. The size of an infinite set is a well-defined notion in mathematics (more commonly known as *cardinality*); see, e.g., [LeLeMe16, §8.1] for an introduction to this or [Newste19, Chapter 9] for a more in-depth treatment. We will only use Theorem 1.1.6 in the case when at least one of the sets X and Y is known to be finite (in which case its size is a nonnegative integer). In this case, Theorem 1.1.6 automatically yields that **both** sets X and Y are finite, and have equal size.

Theorem 1.1.6 is known as the *bijection principle* or the *bijection rule*, and is sufficiently basic that some authors consider it part of the definition of the cardinality of a set; we are not going to reference it explicitly every time we use it. But just this one time, let us do so, and while at that, also formalize the definition of the "flip" operation that was used in our proof of Proposition 1.1.5:

Proof of Proposition 1.1.5 (detailed version). Define the map

$$\begin{aligned} F : R_{n,m} &\to R_{m,n}, \\ (i,j) &\mapsto (j,i) . \end{aligned}$$

[15] We refer to places like [LeLeMe16, §4.4–4.5], [Hammac15, §12.2] or [Day16, §3.F] for basic properties of bijections and bijectivity. Here come some brief reminders: A map $f : X \to Y$ between two sets X and Y is said to be

- *injective* if it has the property that $(f(x_1) = f(x_2)) \Longrightarrow (x_1 = x_2)$ for any two elements $x_1, x_2 \in X$ (or, equivalently, if it maps any two distinct elements of X to two distinct elements of Y);
- *surjective* if it has the property that for each $y \in Y$, there exists at least one $x \in X$ satisfying $f(x) = y$ (in other words, every element of Y is a value of f);
- *bijective* if it is both injective and surjective.

It is easy to see that a map is bijective if and only if it is invertible (i.e., has an inverse).

The word "*bijection*" is a shorthand for "bijective map". Likewise, the word "*injection*" is a shorthand for "injective map", whereas the word "*surjection*" is a shorthand for "surjective map".

Bijections are also known as *one-to-one correspondences* or as *1-to-1 correspondences*. The elements of a set X are said to be *in bijection with* (or *in one-to-one correspondence with*) the elements of a set Y if there exists a bijection from X to Y.

(This notation is saying "the map F from $R_{n,m}$ to $R_{m,n}$ that sends each element (i,j) of $R_{n,m}$ to the element (j,i) of $R_{m,n}$". To see why this map is well-defined, just recall that $R_{n,m} = [n] \times [m]$ and $R_{m,n} = [m] \times [n]$, which is why $(i,j) \in R_{n,m}$ will always lead to $(j,i) \in R_{m,n}$.)

Visually speaking, this map F simply flips each square of the rectangle $R_{n,m}$ across the line with equation $x = y$. This yields a square of the rectangle $R_{m,n}$, of course. Thus, it is clear that the map F is a bijection. This can be proved rigorously as follows: The map

$$\begin{aligned} G : R_{m,n} &\to R_{n,m}, \\ (i,j) &\mapsto (j,i) \end{aligned}$$

is well-defined[16] and inverse to F [17]. Thus, the map F is invertible, i.e., is a bijection. Note that its inverse map G was defined in the same way as F, but simply with the roles of n and m interchanged.

The map F is a bijection, but it is not the bijection that we are going to apply Theorem 1.1.6 to. (If we applied Theorem 1.1.6 to $f = F$, then we would conclude that $|R_{n,m}| = |R_{m,n}|$, that is, $nm = mn$, which is reassuring but not what we are trying to prove.)

The map F merely flips the squares of $R_{n,m}$ across the $x = y$ line; we want a map that flips domino tilings. Of course, to flip a domino tiling, we have to flip each domino in it; and to flip a domino, we have to flip each square in it. Thus, we define the following two maps:

- Define the map

$$\begin{aligned} F_{\text{dom}} : \{\text{dominos inside } R_{n,m}\} &\to \{\text{dominos inside } R_{m,n}\}, \\ D &\mapsto \{F(d) \mid d \in D\}. \end{aligned}$$

  (To spell this out: The map F_{dom} sends each domino D to the domino $\{F(d) \mid d \in D\}$, which is obtained from D by flipping each square $d \in D$. In other words, it flips each domino by applying the flip map F to each square of the domino.)

  It is easy to see that this map F_{dom} is a bijection. (Indeed, it has an inverse G_{dom}, which is defined in the same way but with the roles of n and m interchanged.)

- Define the map

$$\begin{aligned} F_{\text{til}} : \{\text{domino tilings of } R_{n,m}\} &\to \{\text{domino tilings of } R_{m,n}\}, \\ T &\mapsto \{F_{\text{dom}}(D) \mid D \in T\}. \end{aligned}$$

  (To spell this out: The map F_{til} sends each domino tiling T to the domino tiling $\{F_{\text{dom}}(D) \mid D \in T\}$, which is obtained from T by flipping each domino $D \in T$. In other words, it flips each domino tiling by applying the flip map F_{dom} to each domino of the tiling.)

  It is easy to see that this map F_{til} is a bijection. (Indeed, it has an inverse G_{til}, which is defined in the same way but with the roles of n and m interchanged.)

[16] This is proved in the same way as we showed that F is well-defined.

[17] since $F \circ G = \text{id}$ (because each $(i,j) \in R_{m,n}$ satisfies $(F \circ G)(i,j) = F\left(\underbrace{G(i,j)}_{=(j,i)}\right) = F(j,i) = (i,j) = \text{id}(i,j)$) and $G \circ F = \text{id}$ (for similar reasons)

To be fully rigorous, we would have to check that these two maps F_{dom} and F_{til} are well-defined (i.e., that flipping a domino inside $R_{n,m}$ really results in a domino inside $R_{m,n}$, and that flipping a domino tiling of $R_{n,m}$ really results in a domino tiling of $R_{m,n}$), but this is intuitively clear, and the formal proof can easily be constructed by just "following your nose"[18], which is why we omit it.

Anyway, we now have constructed a map
$F_{\text{til}} : \{\text{domino tilings of } R_{n,m}\} \to \{\text{domino tilings of } R_{m,n}\}$ and showed that it is a bijection. Hence, (6) (applied to $X = \{\text{domino tilings of } R_{n,m}\}$ and $Y = \{\text{domino tilings of } R_{m,n}\}$ and $f = F_{\text{til}}$) shows that

$$|\{\text{domino tilings of } R_{n,m}\}| = |\{\text{domino tilings of } R_{m,n}\}|. \tag{7}$$

But the definition of $d_{n,m}$ yields

$$d_{n,m} = (\#\text{ of domino tilings of } R_{n,m}) = |\{\text{domino tilings of } R_{n,m}\}|.$$

The same reasoning shows that

$$d_{m,n} = |\{\text{domino tilings of } R_{m,n}\}|.$$

In view of the latter two equalities, we can rewrite (7) as $d_{n,m} = d_{m,n}$. Thus Proposition 1.1.5 is proven. □

For the sake of future use, we observe that Theorem 1.1.6 has a converse:

Theorem 1.1.7. If X and Y are two sets of the same size (that is, $|X| = |Y|$), then there exists a bijection from X to Y.

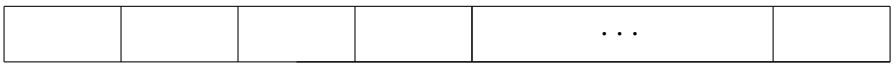
Again, this holds for infinite sets just as it does for finite ones, but we will only use it for finite sets.

1.1.4. The $m = 1$ case

Let us bite another piece off the problem:

Proposition 1.1.8. Assume that $m = 1$ and that n is even. Then, $d_{n,m} = 1$.

Proof of Proposition 1.1.8 (sketched). We must show that there is exactly one domino tiling of $R_{n,m}$. But this is visually obvious: The rectangle $R_{n,m}$ has only one row, and this row has an even number of squares, so we can cover it with horizontal dominos in only one way. Here is how this domino tiling looks like:



.

[18] For example: If D is a horizontal domino $\{(i,j),(i+1,j)\}$, then flipping it yields the vertical domino $\{(j,i),(j,i+1)\}$. Likewise, flipping a vertical domino yields a horizontal domino. Thus, flipping a domino yields a domino. (Note that this would be false if our definition of dominos didn't have the symmetry built in!)

This is not yet a rigorous proof, but it is fairly easy to turn it into one. Rigorously speaking, the domino tiling we just described is[19]

$$\begin{aligned}&\{\{(1,1),(2,1)\},\ \{(3,1),(4,1)\},\ \{(5,1),(6,1)\},\ \ldots,\ \{(n-1,1),(n,1)\}\}\\&=\{\{(2k-1,1),(2k,1)\}\ \mid\ k\in\{1,2,\ldots,n/2\}\}.\end{aligned}\tag{8}$$

It is instantly clear that this is a domino tiling of $R_{n,m}$. In order to show that this is the only domino tiling of $R_{n,m}$, we can let T be any domino tiling of $R_{n,m}$, and then argue as follows:

- The square $(1,1)$ must be contained in some domino $A_1 \in T$ (since T is a domino tiling). This domino A_1 must be either $\{(1,1),(2,1)\}$ or $\{(0,1),(1,1)\}$ or $\{(1,1),(1,2)\}$ or $\{(1,0),(1,1)\}$ (since these are the only dominos that contain $(1,1)$). But out of these four dominos, only $\{(1,1),(2,1)\}$ is a subset of $R_{n,m}$ (since $m=1$). Hence, A_1 must be the domino $\{(1,1),(2,1)\}$. Thus, $(2,1)$ is also contained in A_1.

  Now we know that our tiling T looks like this:

A_1	A_1	?	?	?	?	?	?	?	?	?	?	?	?	?	$\cdots$	?	?	?	?	?	?	?	?	?

  (where we have labeled the leftmost two squares with "A_1" to signify that they are contained in the domino A_1).

- The square $(3,1)$ must be contained in some domino $A_2 \in T$. This domino A_2 must be either $\{(3,1),(4,1)\}$ or $\{(2,1),(3,1)\}$ or $\{(3,1),(3,2)\}$ or $\{(3,0),(3,1)\}$ (since these are the only dominos that contain $(3,1)$). But out of these four dominos, only $\{(3,1),(4,1)\}$ and $\{(2,1),(3,1)\}$ are subsets of $R_{n,m}$ (since $m=1$). Hence, A_2 must be either $\{(3,1),(4,1)\}$ or $\{(2,1),(3,1)\}$. But the dominos in a domino tiling must be disjoint (by definition); hence, A_2 cannot be $\{(2,1),(3,1)\}$ (because if A_2 was $\{(2,1),(3,1)\}$, then it would fail to be disjoint from $A_1=\{(1,1),(2,1)\}$). Thus, A_2 must be $\{(3,1),(4,1)\}$. Hence, $(4,1)$ is also contained in A_2.

  Now we know that our tiling T looks like this:

A_1	A_1	A_2	A_2	?	?	?	?	?	?	?	?	?	?	?	$\cdots$	?	?	?	?	?	?	?	?	?

- The square $(5,1)$ must be contained in some domino $A_3 \in T$. This domino A_3 must be either $\{(5,1),(6,1)\}$ or $\{(4,1),(5,1)\}$ or $\{(5,1),(5,2)\}$ or $\{(5,0),(5,1)\}$ (since these are the only dominos that contain $(5,1)$). But out of these four dominos, only $\{(5,1),(6,1)\}$ and $\{(4,1),(5,1)\}$ are subsets of $R_{n,m}$ (since $m=1$). Hence, A_3 must be either $\{(5,1),(6,1)\}$ or $\{(4,1),(5,1)\}$. But the dominos in a domino tiling must be disjoint (by definition); hence, A_3 cannot be $\{(4,1),(5,1)\}$ (because if A_3 was $\{(4,1),(5,1)\}$, then it would fail to be disjoint from $A_2=\{(3,1),(4,1)\}$). Thus, A_3 must be $\{(5,1),(6,1)\}$. Hence, $(6,1)$ is also contained in A_3.

  Now we know that our tiling T looks like this:

A_1	A_1	A_2	A_2	A_3	A_3	?	?	?	?	?	?	?	?	$\cdots$	?	?	?	?	?	?	?	?

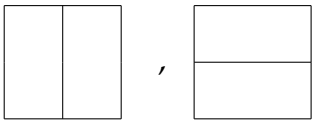
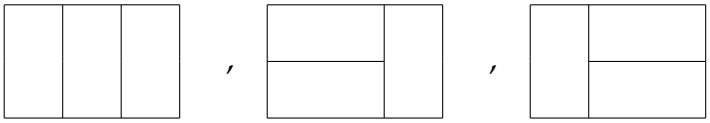
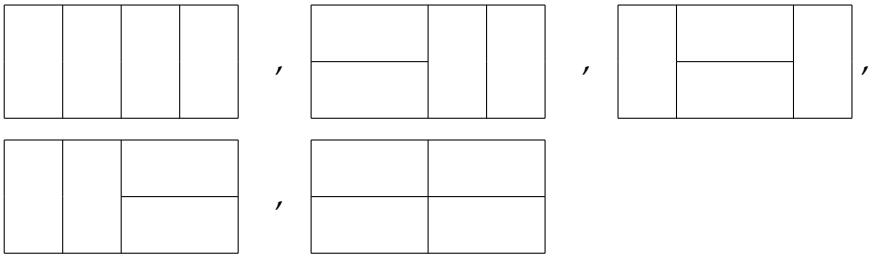
[19] Pay attention to where the set braces are! This is a set of sets of pairs of numbers.

... and so on, proceeding further and further right until you hit the "eastern wall" of $R_{n,m}$ (that is, the square $(n,1)$). Thus, the dominos appearing in T are uniquely determined: They must be $A_1 = \{(1,1),(2,1)\}$, $A_2 = \{(3,1),(4,1)\}$, $A_3 = \{(5,1),(6,1)\}$ and so on. This is precisely the one tiling that we presented in (8). Thus, that one tiling is the only domino tiling of $R_{n,m}$.

To be fully rigorous, this argument should be formalized as an induction proof (feel free to do so!), but even if I wake you up at night, you will know how to construct this argument if necessary, because the idea behind it is glaringly obvious (just walk the rectangle $R_{n,m}$ from its western wall to its eastern wall, and observe that at each step, there is only one possible domino that fits in the rectangle without overlapping with the previous domino). □

1.1.5. The $m = 2$ case and Fibonacci numbers

Between Proposition 1.1.2 and Proposition 1.1.8, we have fully covered the case $m = 1$ of our problem. Let us now move on to the case $m = 2$. We compute $d_{n,m} = d_{n,2}$ for some small values of n simply by listing all domino tilings of $R_{n,m}$:

n	$d_{n,m}$	domino tilings
0	$d_{0,2} = 1$	
1	$d_{1,2} = 1$	
2	$d_{2,2} = 2$	
3	$d_{3,2} = 3$	
4	$d_{4,2} = 5$	

If the $n = 0$ case confuses you, keep in mind that the rectangle $R_{0,2}$ is the empty set (since $R_{0,2} = \underbrace{[0]}_{=\varnothing} \times [2] = \varnothing \times [2] = \varnothing$) and thus has exactly one domino tiling – namely, the tiling that contains no dominos (i.e., the empty set).

Can you find $d_{5,2}$?

Here is a quick way to the answer, at least as far as counting is concerned:

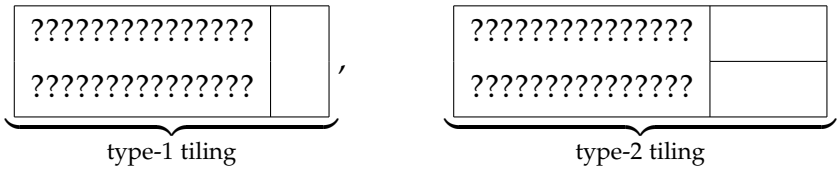
Proposition 1.1.9. For each integer $n \geq 2$, we have $d_{n,2} = d_{n-1,2} + d_{n-2,2}$.

Class of 2019-09-25

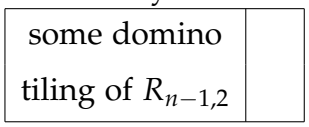
Proof of Proposition 1.1.9 (sketched). Let $n \geq 2$ be an integer. Consider the last[20] column of $R_{n,2}$ (that is, the set $\{(n,1),(n,2)\}$).

In any domino tiling T of $R_{n,2}$, this last column is **either** covered by 1 vertical domino, **or** covered by (parts of) 2 horizontal dominos.

In the former case, we shall call T a *type-1 tiling*; in the latter case, we shall call T a *type-2 tiling*. Visually, these look as follows:



(where the question marks mean an unknown arrangement of dominos).

Let us now analyze type-1 tilings. A type-1 tiling consists of the single vertical domino $\{(n,1),(n,2)\}$ that covers its last column, and a bunch of dominos that cover all the remaining $n-1$ columns. This latter bunch must thus be a domino tiling of $R_{n-1,2}$. Thus, a type-1 tiling consists of the single vertical domino $\{(n,1),(n,2)\}$ and an arbitrary domino tiling of $R_{n-1,2}$. (Visually, this means that it looks as follows: 

.) Hence,[21]

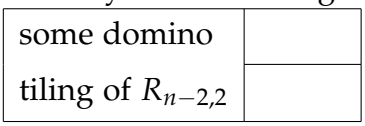
$$(\#\text{ of type-1 tilings}) = (\#\text{ of domino tilings of } R_{n-1,2}) \tag{9}$$
$$= d_{n-1,2} \tag{10}$$

(since $d_{n-1,2}$ was defined as the # of domino tilings of $R_{n-1,2}$).

Let us next analyze type-2 tilings. In a type-2 tiling, the last column is covered by (parts of) 2 horizontal dominos. These 2 dominos must extend to the left (because there is no space for them to extend to the right), and thus also cover the second-to-last column. Explicitly speaking, these 2 dominos must be $\{(n-1,1),(n,1)\}$ and $\{(n-1,2),(n,2)\}$. All the other dominos in the tiling must then cover the remaining $n-2$ columns, i.e., must form a domino tiling of $R_{n-2,2}$. Thus, a type-2 tiling consists of the two horizontal dominos $\{(n-1,1),(n,1)\}$ and $\{(n-1,2),(n,2)\}$

[20] i.e., easternmost

[21] When we say "type-1 tiling", we mean "type-1 tiling of $R_{n,2}$", of course. (The same will apply to "type-2 tiling" later on.)

and an arbitrary domino tiling of $R_{n-2,2}$. (Visually, this means that it looks as follows: 

.) Hence,

$$\begin{aligned}(\#\text{ of type-2 tilings}) &= (\#\text{ of domino tilings of } R_{n-2,2}) && (11)\\ &= d_{n-2,2} && (12)\end{aligned}$$

(since $d_{n-2,2}$ was defined as the # of domino tilings of $R_{n-2,2}$).

Now, recall that each domino tiling of $R_{n,2}$ is either a type-1 tiling or a type-2 tiling (but cannot be both at the same time). Hence,

$$\begin{aligned}&(\#\text{ of domino tilings of } R_{n,2})\\ &= (\#\text{ of type-1 tilings}) + (\#\text{ of type-2 tilings}) && (13)\\ &= d_{n-1,2} + d_{n-2,2} && (14)\end{aligned}$$

(by adding the equalities (10) and (12) together). Now, the definition of $d_{n,2}$ yields

$$d_{n,2} = (\#\text{ of domino tilings of } R_{n,2}) = d_{n-1,2} + d_{n-2,2}$$

(by (14)). This proves Proposition 1.1.9. □

Again, let us analyze what we have actually done in this proof:

1. The equality (9) follows from the bijection principle. Indeed, our argument for it boils down to the (easily established) fact that there is a bijection

   $$f : \{\text{domino tilings of } R_{n-1,2}\} \to \{\text{type-1 tilings}\}$$

   (which takes any domino tiling of $R_{n-1,2}$, and adds the vertical domino $\{(n,1),(n,2)\}$ to it). Once you have convinced yourself of this fact, you can apply Theorem 1.1.6 to $X = \{\text{domino tilings of } R_{n-1,2}\}$ and $Y = \{\text{type-1 tilings}\}$, and conclude that

   $$|\{\text{domino tilings of } R_{n-1,2}\}| = |\{\text{type-1 tilings}\}|.$$

   In other words, (# of domino tilings of $R_{n-1,2}$) = (# of type-1 tilings). Thus, the equality (9) is proven. The equality (11) is obtained similarly.

2. The equality (13) follows from the sum rule. Indeed, the sets {type-1 tilings} and {type-2 tilings} are disjoint, and their union is the set {domino tilings of $R_{n,2}$}. Hence, Theorem 1.1.3 (applied to $S = \{\text{domino tilings of } R_{n,2}\}$, $k = 2$, $S_1 = \{\text{type-1 tilings}\}$ and $S_2 = \{\text{type-2 tilings}\}$) yields

   $$|\{\text{domino tilings of } R_{n,2}\}| = |\{\text{type-1 tilings}\}| + |\{\text{type-2 tilings}\}|.$$

   In other words,

   $$(\#\text{ of domino tilings of } R_{n,2}) = (\#\text{ of type-1 tilings}) + (\#\text{ of type-2 tilings}).$$

   This proves (13).

Proposition 1.1.9 lets us compute the numbers $d_{n,2}$ rather easily, if we compute them in the appropriate order (i.e., start with $d_{0,2}$ and $d_{1,2}$, then compute $d_{2,2}$, then compute $d_{3,2}$, then compute $d_{4,2}$, and so on). For example, we get

$$\begin{aligned} d_{5,2} &= \underbrace{d_{4,2}}_{=5} + \underbrace{d_{3,2}}_{=3} = 5+3 = 8; \\ d_{6,2} &= \underbrace{d_{5,2}}_{=8} + \underbrace{d_{4,2}}_{=5} = 8+5 = 13; \\ d_{7,2} &= \underbrace{d_{6,2}}_{=13} + \underbrace{d_{5,2}}_{=8} = 13+8 = 21; \\ &\cdots. \end{aligned}$$

But what if we want to compute (say) $d_{900,2}$ without having to first compute all the previous numbers $d_{0,2}, d_{1,2}, \ldots, d_{899,2}$? Is there an explicit formula?

Before we answer this question, let us forget for a moment about domino tilings, and define the following sequence of integers:

Definition 1.1.10. The *Fibonacci sequence* is the sequence $(f_0, f_1, f_2, \ldots)$ of nonnegative integers defined recursively by

$$f_0 = 0, \qquad f_1 = 1, \qquad \text{and} \qquad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 2.$$

This is a *recursive definition* – i.e., it tells us how to compute f_n assuming that the previous entries $f_0, f_1, \ldots, f_{n-1}$ of the sequence are already known. Thus, if we want to compute f_5 using this definition, we have to compute f_0, f_1, f_2, f_3, f_4 first. (Let us do this: The definition yields $f_0 = 0$ and $f_1 = 1$ immediately. Furthermore, setting $n = 2$ in the equality $f_n = f_{n-1} + f_{n-2}$, we obtain $f_2 = \underbrace{f_1}_{=1} + \underbrace{f_0}_{=0} = 1+0 = 1$. Next, setting $n = 3$ in the equality $f_n = f_{n-1} + f_{n-2}$, we obtain $f_3 = \underbrace{f_2}_{=1} + \underbrace{f_1}_{=1} = 1+1 = 2$. Likewise, $f_4 = \underbrace{f_3}_{=2} + \underbrace{f_2}_{=1} = 2+1 = 3$. Likewise, $f_5 = \underbrace{f_4}_{=3} + \underbrace{f_3}_{=2} = 5$.)

The entries f_n of the Fibonacci sequence are called *Fibonacci numbers*. Here is a table of the first 10 Fibonacci numbers:

n	0	1	2	3	4	5	6	7	8	9	$\cdots$
f_n	0	1	1	2	3	5	8	13	21	34	$\cdots$

.

The Fibonacci sequence is famous – just look at its Wikipedia page! It also has several books dedicated to it, such as Vorobiev's [Vorobi02] (although, to be fully honest, Vorobiev often uses it as a plug to pivot to other mathematics); there is also a journal called *The Fibonacci Quarterly* (again, however, its actual scope is broader).

Now, we can reduce our problem of computing $d_{n,2}$ to the problem of computing Fibonacci numbers:

Proposition 1.1.11. We have $d_{n,2} = f_{n+1}$ for each $n \in \mathbb{N}$.

Proof of Proposition 1.1.11 (informal version). Here is the main idea of the proof: We must show that the two sequences $(d_{0,2}, d_{1,2}, d_{2,2}, d_{3,2}, \ldots)$ and $(f_1, f_2, f_3, f_4, \ldots)$ are identical. Both of them have the property that their first entries are 1's (that is, $d_{0,2} = 1$ and $f_1 = 1$), their second entries are 1's (that is, $d_{1,2} = 1$ and $f_2 = 1$), and each of their further entries equals the sum of the preceding two entries (because Proposition 1.1.9 shows that the $d_{n,2}$ satisfy $d_{n,2} = d_{n-1,2} + d_{n-2,2}$, whereas the definition of Fibonacci numbers shows that $f_{n+1} = f_n + f_{n-1}$). Thus, to put it in practical terms: Both sequences start with the same two entries, and then are built out of these two entries according to the same rule (namely, each further entry is the sum of the preceding two entries). Hence, the two sequences must be the same. This proves Proposition 1.1.11. □

If you found this proof insufficiently rigorous, here is a formal version of this argument:

Proof of Proposition 1.1.11 (formal version). We shall prove Proposition 1.1.11 by strong induction on n.

A strong induction needs no induction base[22]. Thus, we only do the induction step:

Induction step: Let $m \in \mathbb{N}$. Assume (as the induction hypothesis) that Proposition 1.1.11 holds for each $n < m$. We must prove that Proposition 1.1.11 holds for $n = m$.

Our induction hypothesis says that Proposition 1.1.11 holds for each $n < m$. In other words, we have

$$d_{n,2} = f_{n+1} \qquad \text{for each } n \in \mathbb{N} \text{ satisfying } n < m. \tag{15}$$

Now, we must prove that Proposition 1.1.11 holds for $n = m$. In other words, we must prove that $d_{m,2} = f_{m+1}$. If $m = 0$, then this is true (since $d_{0,2} = 1 = f_1 = f_{0+1}$). If $m = 1$, then this is also true (since $d_{1,2} = 1 = f_2 = f_{1+1}$). Hence, it remains to prove this in the case $m \geq 2$. So let us WLOG[23] assume that $m \geq 2$. Then, $m - 2 \in \mathbb{N}$. Hence, we can apply (15) to $n = m - 2$ (since $m - 2 < m$), and obtain $d_{m-2,2} = f_{(m-2)+1} = f_{m-1}$. Furthermore, $m - 1 \in \mathbb{N}$ (since $m \geq 2 \geq 1$). Thus, we can apply (15) to $n = m - 1$ (since $m - 1 < m$), and obtain $d_{m-1,2} = f_{(m-1)+1} = f_m$. However, Proposition 1.1.9 (applied to $n = m$) shows that

$$d_{m,2} = \underbrace{d_{m-1,2}}_{=f_m} + \underbrace{d_{m-2,2}}_{=f_{m-1}} = f_m + f_{m-1}.$$

Comparing this with

$$\begin{aligned} f_{m+1} &= \underbrace{f_{(m+1)-1}}_{=f_m} + \underbrace{f_{(m+1)-2}}_{=f_{m-1}} \qquad \text{(by the definition of the Fibonacci sequence)} \\ &= f_m + f_{m-1}, \end{aligned}$$

[22] See [Grinbe15, §2.8] for how strong induction works.

[23] "WLOG" means "without loss of generality". We can assume that $m \geq 2$ without loss of generality, since we have already proven our claim (that $d_{m,2} = f_{m+2}$) in all other cases.

we obtain $d_{m,2} = f_{m+1}$. In other words, Proposition 1.1.11 holds for $n = m$. This completes the induction step. Thus, Proposition 1.1.11 is proven. □

So we have identified our numbers $d_{n,2}$ as the famous Fibonacci numbers f_{n+1}. Does this help us compute them directly? Yes, because there is a famous formula for the Fibonacci numbers:

Theorem 1.1.12 (Binet's formula)**.** For each $n \in \mathbb{N}$, we have

$$f_n = \frac{1}{\sqrt{5}} \left(\varphi^n - \psi^n \right),$$

where

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618\ldots \qquad \text{and} \qquad \psi = \frac{1-\sqrt{5}}{2} \approx -0.618\ldots.$$

A few words about this strange formula are in order. On its left hand side is a nonnegative integer, f_n. On its right side is an expression involving irrational numbers like $\sqrt{5}$ as well as minus signs. How could an explicit formula for a sequence of nonnegative integers require irrational numbers and subtraction?

Well, this is the price of asking for explicit formulas!

The numbers φ and ψ in Theorem 1.1.12 are known as the *golden ratios* (although usually only φ is considered "the golden ratio"). They are the two roots of the quadratic polynomial $x^2 - x - 1$, so they satisfy $\varphi^2 = \varphi + 1$ and $\psi^2 = \psi + 1$. If this looks like the Fibonacci recursion $f_n = f_{n-1} + f_{n-2}$, don't be surprised! This is the reason why they show up in the explicit formula for the Fibonacci numbers.

How do you compute f_{900} using Theorem 1.1.12? You may be tempted to just plug $n = 900$ into the formula using your favorite computer algebra system; but there is a subtlety involved: Since $\sqrt{5}$ is irrational, the computer may try to work with approximate values, and then when you take n-th powers, the rounding errors will blow up. You will probably not get an integer as a result, and even if you try to round it to the nearest integer, you may well get the wrong value! Such is the price of blindly trusting floating-point arithmetic. Fortunately, $\sqrt{5}$ is an *algebraic number* (i.e., a root of a polynomial with rational coefficients), and this means that it **is** possible to make **exact** computations with it. You just need to restrict yourself to the "$\sqrt{5}$-rationals" (i.e., the numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$), and instead of approximating them with decimals, you just keep them in the $a + b\sqrt{5}$ form. It is easy to find rules for adding, subtracting, multiplying and

dividing $\sqrt{5}$-rationals by one another[24]; thus you don't need approximate values. Using the "exponentiation by squaring" trick, it is now easy to compute very high powers of φ and ψ, and then Theorem 1.1.12 yields f_n. For example, a computer will readily tell you all the 188 digits of f_{900}, the last six of which are 938800; you would probably have gotten these wrong if you relied on approximate computation.

Theorem 1.1.12 also gives a very easy answer to the question (which we arguably haven't asked) how fast the Fibonacci numbers f_n grow when n gets large. Indeed, $|\psi| < 1$, so that $\psi^n \to 0$ when $n \to \infty$. Hence, for high enough n, we have $f_n \approx \dfrac{1}{\sqrt{5}}\varphi^n$. Of course, the sequence of $\dfrac{1}{\sqrt{5}}\varphi^n$ for $n \in \mathbb{N}$ is a geometric sequence with ratio $\varphi \approx 1.618\ldots$, and grows exponentially. Thus, we see that the Fibonacci numbers f_n grow exponentially – slower than the powers of 2 (since $1.618\ldots < 2$), but still faster than any polynomial. The Fibonacci number f_n will have $\approx \left(\log_{10} \varphi\right) \cdot n \approx 0.209 \cdot n$ many digits.

Theorem 1.1.12 is easy to prove:

Proof of Theorem 1.1.12 (sketched). This can be proven by the same argument that we used for Proposition 1.1.11: We have to show that the sequences $(f_0, f_1, f_2, \ldots)$ and $\left(\dfrac{1}{\sqrt{5}}\left(\varphi^0 - \psi^0\right), \dfrac{1}{\sqrt{5}}\left(\varphi^1 - \psi^1\right), \dfrac{1}{\sqrt{5}}\left(\varphi^2 - \psi^2\right), \ldots\right)$ are identical. Both of them have the property that their first entries are 0's (this is easy to check), their second entries are 1's (this is easy to check), and each of their further entries equals the sum of the preceding two entries[25]. Thus, both sequences start with the same two entries, and then are built out of these two entries according to the same rule. Hence, the two sequences must be the same. This proves Theorem 1.1.12. □

[24]To wit:

$$\left(a + b\sqrt{5}\right) + \left(c + d\sqrt{5}\right) = (a + c) + (b + d)\sqrt{5};$$
$$\left(a + b\sqrt{5}\right) - \left(c + d\sqrt{5}\right) = (a - c) + (b - d)\sqrt{5};$$
$$\left(a + b\sqrt{5}\right)\left(c + d\sqrt{5}\right) = (ac + 5bd) + (ad + bc)\sqrt{5};$$
$$\frac{a + b\sqrt{5}}{c + d\sqrt{5}} = \frac{\left(a + b\sqrt{5}\right)\left(c - d\sqrt{5}\right)}{\left(c + d\sqrt{5}\right)\left(c - d\sqrt{5}\right)} = \frac{(ac - 5bd) + (bc - ad)\sqrt{5}}{c^2 - 5d^2}.$$

Note in particular the last equation: This is why they taught you to rationalize denominators in high school!

[25]Indeed, for the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$, this is clear. For the second sequence, this boils down to proving the identity

$$\frac{1}{\sqrt{5}}\left(\varphi^n - \psi^n\right) = \frac{1}{\sqrt{5}}\left(\varphi^{n-1} - \psi^{n-1}\right) + \frac{1}{\sqrt{5}}\left(\varphi^{n-2} - \psi^{n-2}\right),$$

which however follows by subtracting the two easily verified identities

$$\varphi^n = \varphi^{n-1} + \varphi^{n-2} \qquad \text{and} \qquad \psi^n = \psi^{n-1} + \psi^{n-2}$$

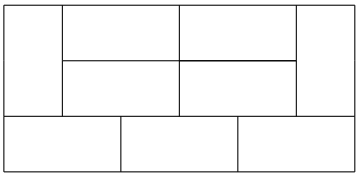
and dividing the result by $\sqrt{5}$.

This proof should convince you that Theorem 1.1.12 holds, but does not explain how you could have come up with Theorem 1.1.12. If time allows, we will later explain this when we explore the concept of *generating functions*.

1.1.6. Kasteleyn's formula (teaser)

Now we have computed $d_{n,2}$ for each $n \in \mathbb{N}$. What about $d_{n,3}$?

Proposition 1.1.2 shows that $d_{n,3} = 0$ when n is odd. But computing $d_{n,3}$ when n is even is a lot harder. You might try to find a recursive formula such as Proposition 1.1.9, but this isn't so easy any more. You can still try to separate the domino tilings of $R_{n,3}$ into types according to how the last column looks like; however, there will be three of these types now, and two of them will not fall into a 1-to-1 correspondence with domino tilings of a smaller rectangle. For example, consider the following domino tiling of $R_{6,3}$:



.

There is no tiling of $R_{5,3}$ anywhere in it, nor of $R_{4,3}$, nor of $R_{3,3}$, nor of $R_{2,3}$, nor of $R_{1,3}$. This thwarts our recursive approach.

Nevertheless, there **is** a nice recursion for $d_{n,3}$:

Proposition 1.1.13. We have $d_{n,3} = 4d_{n-2,3} - d_{n-4,3}$ for each $n \geq 4$.

As I said, there is no proof as easy as the one we gave for Proposition 1.1.9. We will later learn the technique of *generating functions*, which can be used to give a reasonably simple proof (see [Read80] or [21s, §3.12.3]); a tricky combinatorial proof also exists.

What about $d_{n,4}$? There is a recursion, too, according to [Read80, §2]:

$$d_{n,4} = d_{n-1,4} + 5d_{n-2,4} + d_{n-3,4} - d_{n-4,4}.$$

As you see, these are getting more complicated. In theory, recurrence relations like these have explicit formulas like Binet's formula for f_n (Theorem 1.1.12). However, these formulas become more and more complicated as well, and in particular they no longer involve "nice" irrational numbers like $\sqrt{5}$, but rather roots of higher-degree polynomials, which at some point can no longer be expressed using rational numbers, sums, differences, products, quotients and radicals (i.e., $\sqrt[a]{b}$ terms)[26]. This looks like a dead end.

[26]The roots of a quadratic polynomial $x^2 + ax + b$ can be expressed in this way: They are $\frac{-a \pm \sqrt{a^2 - 4b}}{2}$. The roots of a degree-3 or degree-4 polynomial can also be expressed in this way, using complicated formulas due to Tartaglia, Ferrari, Cardano and Descartes. But the *Abel–Ruffini theorem* says that for $k \geq 5$, there is no formula that expresses the roots of a (general) degree-k polynomial using only $+$, $-$, $\cdot$, $/$ and $\sqrt{}$.

In the 20th Century, however, theoretical physicists studying thermodynamics got interested in computing $d_{n,m}$, as they considered a domino tiling to be a (rather idealized) model for a liquid consisting of "dimers" (polymers that take up two adjacent sites in a rectangular lattice; these are exactly our dominos). Even though the 2-dimensionality of a rectangle makes it a somewhat unrealistic approximation for real-world liquids, it found its use as a model for the adsorption of molecules on a surface (see [Kastel61]). In 1961, Kasteleyn found the following surprising formula for $d_{n,m}$:

Theorem 1.1.14 (Kasteleyn's formula)**.** Assume that m is even and $n \geq 1$. Then,

$$d_{n,m} = 2^{mn/2} \prod_{j=1}^{m/2} \prod_{k=1}^{n} \sqrt{\left(\cos \frac{j\pi}{m+1}\right)^2 + \left(\cos \frac{k\pi}{n+1}\right)^2}.$$

(Here, we are using the product sign $\prod$: That is, if $a_1, a_2, \ldots, a_p$ are any numbers, then $\prod_{i=1}^{p} a_i$ means the product $a_1 a_2 \cdots a_p$. The presence of two product signs directly following one another means that we are taking a product of products.)

Actually, "surprising" is an understatement; why cosines of angles would appear in a formula for the integer $d_{n,m}$ is even less transparent than why $\sqrt{5}$ should appear in a formula for Fibonacci numbers!

We won't even get close to proving Theorem 1.1.14. A proof outline appears in [Loehr11, Theorem 12.85], serving as a culmination of a graduate-level combinatorics textbook. A more self-contained exposition of the proof has been given by Stucky in [Stucky15], but even that is only self-contained up to some advanced linear algebra (it requires a good understanding of eigenvectors, Pfaffians and Kronecker products of matrices).

For all its seeming extravagance, Theorem 1.1.14 actually provides a good way of computing $d_{n,m}$. Indeed, cosines like $\cos \frac{j\pi}{m+1}$ and $\cos \frac{k\pi}{n+1}$ are algebraic numbers that lend themselves to exact computation (using cyclotomic polynomials – a piece of abstract algebra we are also not coming close to), and the scary-looking products don't scare a good computer algebra system. For example, Kasteleyn's formula can be used to show that $d_{8,8} = 12\,988\,816$. This wouldn't be so easy to check by a brute force search for domino tilings!

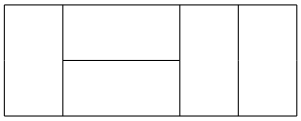
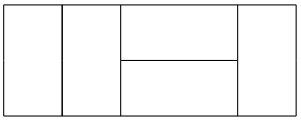
Class of 2019-09-27

1.1.7. Axisymmetric domino tilings

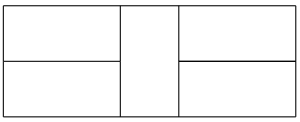
Let us solve a few more counting exercises around domino tilings.

Exercise 1.1.1. Let $n \in \mathbb{N}$. Say that a domino tiling T of $R_{n,2}$ is *axisymmetric* if reflecting it across the vertical axis of symmetry of $R_{n,2}$ leaves it unchanged (i.e., for each domino $\{(i,j),(i',j')\} \in T$, the "mirror domino" $\{(n+1-i,j),(n+1-i',j')\}$ also belongs to T).

For example, the tilings

 and 

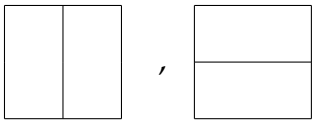
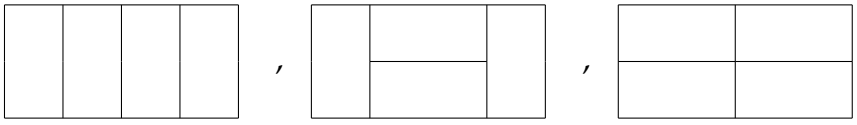
are not axisymmetric (indeed, reflecting them across the vertical line transforms them into one another, and they are not the same), but the tilings

 and 

are axisymmetric.

How many axisymmetric domino tilings does $R_{n,2}$ have?

Example 1.1.15. Let us list the axisymmetric domino tilings for $R_{n,2}$ when n is small:

n	axisymmetric domino tilings	their number
0		1
1		1
2		2
3		1
4		3

Solution sketch to Exercise 1.1.1. Let us only show the main steps; a (more) detailed

solution to Exercise 1.1.1 can be found in [17f-hw1s, Exercise 5].

There are two cases to consider: the case when n is even, and the case when n is odd.

Let us first consider the case when n is even. In this case, I claim that any axisymmetric domino tiling of $R_{n,2}$ has one of the following two forms:

- **Form 1:** a domino tiling J of $R_{n/2,2}$ covering the left half of $R_{n,2}$, and its mirror image across the vertical axis covering the right half:

domino tiling J of $R_{n/2,2}$	mirror image of J

.

(Note that the vertical axis cuts through the middle of this picture.)

- **Form 2:** a domino tiling J of $R_{n/2-1,2}$ covering the leftmost $n/2-1$ columns of $R_{n,2}$, and two horizontal dominos covering the $(n/2)$-th and $(n/2+1)$-th columns[27], and the mirror image of J across the vertical axis covering the rightmost $n/2-1$ columns of $R_{n,2}$:

domino tiling J of $R_{n/2-1,2}$		mirror image of J

.

(Again, the vertical axis cuts through the middle of this picture.)

If you agree with me that these are the only possible forms of an axisymmetric domino tiling of $R_{n,2}$, then it follows (by the same logic as in the proof of Proposition 1.1.9) that the # of axisymmetric domino tilings of $R_{n,2}$ is

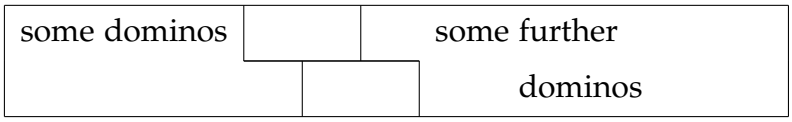
$$\underbrace{(\#\text{ of domino tilings of } R_{n/2,2})}_{\substack{=d_{n/2,2}=f_{n/2+1} \\ \text{(by Proposition 1.1.11, applied to } n/2 \\ \text{instead of } n)}} + \underbrace{(\#\text{ of domino tilings of } R_{n/2-1,2})}_{\substack{=d_{n/2-1,2}=f_{n/2} \\ \text{(by Proposition 1.1.11, applied to } n/2-1 \\ \text{instead of } n)}}$$
$$= f_{n/2+1} + f_{n/2} = f_{n/2+2}$$

(by the recursive definition of the Fibonacci numbers). But why are the above-mentioned two forms the only possible forms of an axisymmetric domino tiling of $R_{n,2}$?

To prove this, we fix an axisymmetric domino tiling T of $R_{n,2}$. We must show that T has one of the above two forms. We can consider what dominos cover the $(n/2)$-th column in T. If this column is covered by one vertical domino, then no domino of T straddles the vertical axis, and thus the tiling T has Form 1 (indeed, the part of T to the right of the vertical axis is a mirror image of the part to the left, since T is axisymmetric). It remains to deal with the case when the $(n/2)$-th

[27] We count columns from the left.

column is covered by two horizontal dominos in T. The question is now where these horizontal dominos fall. If both of them fall into columns $n/2-1$ and $n/2$, then our tiling T has Form 1. If both of them fall into columns $n/2$ and $n/2+1$, then our tiling T has Form 2. What about the remaining "rogue" possibility, that one of them falls into columns $n/2-1$ and $n/2$, while the other falls into columns $n/2$ and $n/2+1$? Here is a picture (which assumes that the former domino is in the top row and the latter domino is in the bottom row; but the argument will be the same in the opposite case):



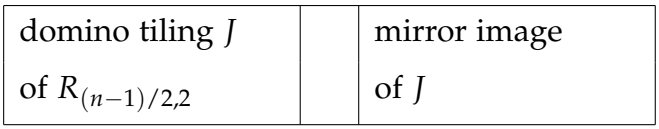
.

Note, however, that the part marked "some dominos" in this picture has an odd number of squares (namely, $2(n/2-1)-1$ many squares), so that it cannot actually be covered by dominos![28] Thus, we obtain a contradiction. Hence, this "rogue" possibility is actually impossible. This shows that every axisymmetric domino tiling T of $R_{n,2}$ either has Form 1 or has Form 2.

Thus, we have proved that the # of axisymmetric domino tilings of $R_{n,2}$ is $f_{n/2+2}$ in the case when n is even.

What about the case when n is odd? In this case, I claim that any axisymmetric domino tiling of $R_{n,2}$ has the following form:

- **Form 1:** a domino tiling J of $R_{(n-1)/2,2}$ covering the leftmost $(n-1)/2$ columns of $R_{n,2}$, and one vertical domino covering the $(n+1)/2$-th column, and the mirror image of J across the vertical axis covering the rightmost $(n-1)/2$ columns of $R_{n,2}$:

  .

  (Again, the vertical axis cuts through the middle of this picture, which in this case means cutting through the middle of the vertical domino.)

This time, there is no Form 2. Again, we need to prove that this is the only possible form. This is even easier than in the previous case; the main idea is the following: If an axisymmetric tiling T of $R_{n,2}$ contained any horizontal domino that intersects its $(n+1)/2$-th column, then it would also contain the mirror image of this domino across the vertical axis (since T is axisymmetric), but then this domino and its mirror image would be distinct but overlapping[29], which would contradict the definition of a domino tiling. Thus, the $(n+1)/2$-th column of any axisymmetric

[28] This is the same logic that we used to prove Proposition 1.1.2.

[29] They would overlap in the $(n+1)/2$-th column.

tiling T of $R_{n,2}$ must be covered by a vertical domino. This shows that Form 1 is the only possible form.

Thus, when n is odd, the # of axisymmetric domino tilings of $R_{n,2}$ equals the # of domino tilings of $R_{(n-1)/2,2}$, which (by Proposition 1.1.11) is $f_{(n-1)/2+1} = f_{(n+1)/2}$.

Thus, the general formula for the # of axisymmetric domino tilings of $R_{n,2}$ is:

$$(\#\text{ of axisymmetric domino tilings of } R_{n,2}) = \begin{cases} f_{n/2+2}, & \text{if } n \text{ is even;} \\ f_{(n+1)/2}, & \text{if } n \text{ is odd} \end{cases}.$$

Exercise 1.1.1 is thus solved. □

1.1.8. Tiling rectangles with k-bricks

Now, let us look at another related problem.

For the rest of Subsection 1.1.8, fix a positive integer k.

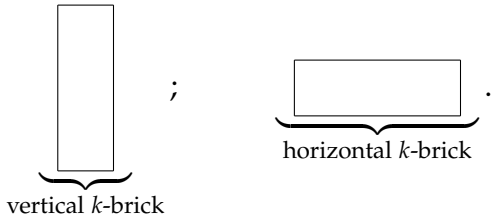
A *k-brick* shall mean a $1 \times k$-rectangle or a $k \times 1$-rectangle. More specifically: A *vertical k-brick* shall mean a $1 \times k$-rectangle (i.e., a set of the form

$$\{(i,j), (i,j+1), (i,j+2), \ldots, (i,j+k-1)\}$$

for some $i, j \in \mathbb{Z}$); a *horizontal k-brick* shall mean a $k \times 1$-rectangle (i.e., a set of the form

$$\{(i,j), (i+1,j), (i+2,j), \ldots, (i+k-1,j)\}$$

for some $i, j \in \mathbb{Z}$). Here is how they look like:



If S is a set of squares, then a *k-brick tiling* of S means a way to cover the set S with non-overlapping k-bricks (i.e., formally speaking: a set of disjoint k-bricks whose union is S).

Thus, k-brick tilings are a generalization of domino tilings. More specifically: If $k = 2$, then k-bricks are the same as dominos, and thus k-brick tilings are the same as domino tilings.

When does a rectangle $R_{n,m}$ have a k-brick tiling? The answer is surprisingly simple:

Proposition 1.1.16. Let $n, m \in \mathbb{N}$, and let k be a positive integer. Then, the rectangle $R_{n,m}$ has a k-brick tiling if and only if we have $k \mid m$ or $k \mid n$.

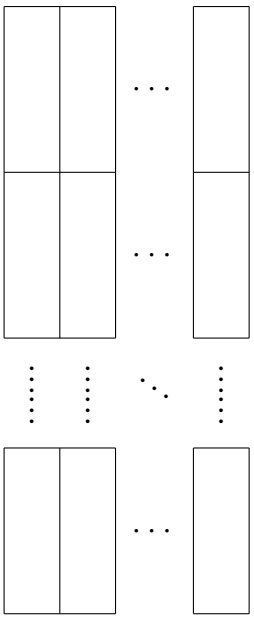
In the case when $k = 2$, Proposition 1.1.16 says that the rectangle $R_{n,m}$ has a domino tiling if and only if we have $2 \mid m$ or $2 \mid n$ (that is, at least one of the numbers m and n is even). This should not be surprising: One direction of this equivalence (namely, the "$\Longrightarrow$" direction: i.e., the direction saying that if $R_{n,m}$ has a domino tiling, then at least one of m and n is even) follows from Proposition 1.1.2, whereas the other direction is easy. We could use a similar argument to prove Proposition 1.1.16 whenever the number k is prime. Indeed, our proof of Proposition 1.1.2 generalizes to show that if the rectangle $R_{n,m}$ has a k-brick tiling, then $k \mid mn$. When k is prime, the divisibility $k \mid mn$ implies that $k \mid m$ or $k \mid n$; thus, the "$\Longrightarrow$" direction of Proposition 1.1.16 would follow immediately in this case. But when k is not prime, we need a better argument.

Proof of Proposition 1.1.16. The claim we want to prove is an "if and only if" claim, so it has two directions: the "$\Longleftarrow$" direction (also known as the "if" direction), and the "$\Longrightarrow$" direction (also known as the "only if" direction). The former direction claims that if we have $k \mid m$ or $k \mid n$, then the rectangle $R_{n,m}$ has a k-brick tiling. The latter claims the converse of this statement.

We shall prove these two directions separately:

$\Longleftarrow$: Assume that $k \mid m$ or $k \mid n$.

If $k \mid m$, then $R_{n,m}$ has a k-brick tiling consisting entirely of vertical k-bricks. It looks as follows:



(with each column being covered by m/k many vertical k-bricks). Similarly, if $k \mid n$, then $R_{n,m}$ has a k-brick tiling consisting entirely of horizontal k-bricks. Thus, in either case, $R_{n,m}$ has a k-brick tiling. This proves the "$\Longleftarrow$" direction of Proposition 1.1.16.

$\Longrightarrow$: Assume that the rectangle $R_{n,m}$ has a k-brick tiling. We must prove that we have $k \mid m$ or $k \mid n$.

Assume the contrary (for the sake of contradiction). Thus, $k \nmid m$ and $k \nmid n$.

We shall use the following notations from elementary number theory: If a is an integer and b is a positive integer, then

- we let $a \mathbin{//} b$ denote the quotient obtained when dividing a by b (in the sense of division with remainder);
- we let $a\%b$ denote the remainder obtained when dividing a by b.

Both of these numbers $a \mathbin{//} b$ and $a\%b$ are integers, and they satisfy $0 \leq a\%b < b$ and $a = (a \mathbin{//} b) \cdot b + (a\%b)$.

Let $r = n\%k$ and $s = m\%k$. We have $r = n\%k \neq 0$ (since $k \nmid n$) and thus $0 < r < k$ (since r is a remainder upon division by k). Likewise, $0 < s < k$.

Now, we are going to color the squares of $R_{n,m}$ with k colors. The k colors we are going to use will be numbered $0, 1, \ldots, k-1$. Each square $(i,j) \in R_{n,m}$ will be colored with the color $(i+j-2)\,\%k$. Here is how this coloring looks like (in the example where $k = 4$, $n = 10$ and $m = 7$):

2	3	0	1	2	3	0	1	2	3
1	2	3	0	1	2	3	0	1	2
0	1	2	3	0	1	2	3	0	1
3	0	1	2	3	0	1	2	3	0
2	3	0	1	2	3	0	1	2	3
1	2	3	0	1	2	3	0	1	2
0	1	2	3	0	1	2	3	0	1

(where we have written the color of each square as a number into this square). Note that if $k = 2$, then there are two colors only, numbered 0 and 1; in this case, our coloring is precisely the usual chessboard coloring (if we regard color 0 as black and color 1 as white).

Let us make a few observations about our coloring:

- The southwesternmost square of $R_{n,m}$ is $(1,1)$, and thus has color $(1+1-2)\,\%k = 0\%k = 0$.
- As we move eastwards, the colors of the squares increase by 1 at each step, until they reach $k-1$, at which point they "fall back down" to 0 at the next step.
- The same happens as we move northwards.
- Along each "northwest-to-southeast" diagonal (i.e., each line with slope -1), the color stays constant.

Let us say that a finite set S of squares is *balanced* if it has equally many squares of each color. In other words, a finite set S of squares is *balanced* if and only if for any color $h \in \{0,1,\ldots,k-1\}$, the # of all squares in S that have color h does not depend on h.

Each horizontal k-brick has exactly 1 square of each color. Indeed, the colors of the k squares in a horizontal k-brick look as follows:

$$\boxed{\begin{array}{cccccccc} u & u+1 & \cdots & k-1 & 0 & 1 & \cdots & u-1 \end{array}}$$

(where u is the color of the leftmost square of the k-brick). Thus, each horizontal k-brick is balanced. Likewise, each vertical k-brick is balanced. Thus, we have shown that each k-brick is balanced.

But we have assumed that the rectangle $R_{n,m}$ has a k-brick tiling. Hence, $R_{n,m}$ must, too, be balanced (by the sum rule)[30].

Let us now subdivide the rectangle $R_{n,m}$ into several (disjoint) *zones* $Z_{u,v}$ by cutting it with several lines[31]. Namely, we cut it with horizontal lines every k squares (counted from the bottom), and with vertical lines every k squares (counted from

[30]Here is the argument in details (albeit using the summation sign, which we won't properly introduce until Definition 1.2.2 below):

We have assumed that the rectangle $R_{n,m}$ has a k-brick tiling. Let T be this k-brick tiling. Write T in the form $T = \{S_1, S_2, \ldots, S_j\}$, where $S_1, S_2, \ldots, S_j$ are distinct k-bricks. Hence, each square in $R_{n,m}$ belongs to exactly one of $S_1, S_2, \ldots, S_j$. Moreover, each of the k-bricks $S_1, S_2, \ldots, S_j$ is balanced (since each k-brick is balanced).

Now, for each color $h \in \{0,1,\ldots,k-1\}$, we have

$$\begin{aligned}
&(\text{\# of all squares in } R_{n,m} \text{ that have color } h) \\
&= (\text{\# of all squares in } R_{n,m} \text{ that belong to } S_1 \text{ and have color } h) \\
&\qquad + (\text{\# of all squares in } R_{n,m} \text{ that belong to } S_2 \text{ and have color } h) \\
&\qquad + \cdots \\
&\qquad + (\text{\# of all squares in } R_{n,m} \text{ that belong to } S_j \text{ and have color } h) \\
&\qquad\qquad \left(\begin{array}{c} \text{by the sum rule, since each square in } R_{n,m} \\ \text{belongs to exactly one of } S_1, S_2, \ldots, S_j \end{array} \right) \\
&= \sum_{i=1}^{j} \underbrace{(\text{\# of all squares in } R_{n,m} \text{ that belong to } S_i \text{ and have color } h)}_{\substack{= (\text{\# of all squares in } S_i \text{ that have color } h) \\ (\text{since } S_i \subseteq R_{n,m})}} \\
&= \sum_{i=1}^{j} \underbrace{(\text{\# of all squares in } S_i \text{ that have color } h)}_{\substack{\text{independent of } h \\ (\text{since } S_i \text{ is balanced})}}.
\end{aligned}$$

Hence, for each $h \in \{0,1,\ldots,k-1\}$, the # of all squares in $R_{n,m}$ that have color h is independent of h (since it is a sum of j numbers that are each independent of h). In other words, $R_{n,m}$ is balanced.

[31]We will give a rigorous definition further below.

the left). Thus, we obtain the following subdivision of $R_{n,m}$:

$Z_{0,2}$	$Z_{1,2}$	$Z_{2,2}$	$Z_{3,2}$
$Z_{0,1}$	$Z_{1,1}$	$Z_{2,1}$	$Z_{3,1}$
$Z_{0,0}$	$Z_{1,0}$	$Z_{2,0}$	$Z_{3,0}$

.

Formally speaking, our zones $Z_{u,v}$ are defined as follows:

$$Z_{u,v} = \{(i,j) \in R_{n,m} \mid (i-1) \,//\, k = u \text{ and } (j-1) \,//\, k = v\}$$
$$\text{for all } u \in \{0,1,\ldots,(n-1) \,//\, k\} \text{ and } v \in \{0,1,\ldots,(m-1) \,//\, k\}.$$

All these zones $Z_{u,v}$ are rectangles. More precisely: Let us call a zone $Z_{u,v}$ (with $u \in \{0,1,\ldots,(n-1) \,//\, k\}$ and $v \in \{0,1,\ldots,(m-1) \,//\, k\}$)

- *generic* if $u < (n-1) \,//\, k$ and $v < (m-1) \,//\, k$;
- *northern* if $u < (n-1) \,//\, k$ and $v = (m-1) \,//\, k$;
- *eastern* if $u = (n-1) \,//\, k$ and $v < (m-1) \,//\, k$;
- *northeastern* if $u = (n-1) \,//\, k$ and $v = (m-1) \,//\, k$.

Then,[32]

- each generic zone is a $k \times k$-rectangle;
- each northern zone is a $k \times s$-rectangle;
- each eastern zone is an $r \times k$-rectangle;
- the northeastern zone is an $r \times s$-rectangle.

Note that all these zones are nonempty, since $r > 0$ and $s > 0$ and $k > 0$.

Each northern zone is a $k \times s$-rectangle, and thus can be tiled with horizontal k-bricks; therefore it is balanced (since each k-brick is balanced). Likewise, each eastern zone is balanced, and each generic zone is balanced. Thus, summarizing, we have shown that each zone Z except for the northeastern zone is balanced. In other words, if Z is a zone that is not the northeastern zone, then, for any color $h \in \{0,1,\ldots,k-1\}$,

$$\text{the \# of all squares in } Z \text{ that have color } h \text{ is independent of } h. \tag{16}$$

[32]Recall that $r = n\%k$ and $s = m\%k$.

But the zones are disjoint and their union is the whole rectangle $R_{n,m}$. Hence, it follows that the northeastern zone is balanced as well[33].

But let us take a closer look at the northeastern zone. We denote this zone by $\mathfrak{Z}$. This zone $\mathfrak{Z}$ is an $r \times s$-rectangle, and (just as for any zone) its southwestern corner has color 0. Thus, the colors of its squares look as follows:

$$\begin{array}{|cccccc|}
\hline
s-1 & s & * & \cdots & * & * \\
s-2 & s-1 & s & \cdots & * & * \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 2 & 3 & \cdots & r-1 & r \\
0 & 1 & 2 & \cdots & r-2 & r-1 \\
\hline
\end{array} \tag{17}$$

(where each asterisk $*$ stands for some entry we don't need to know about).

We shall now show that this northeastern zone is **not** balanced. This will give us a contradiction.

We WLOG assume that $s \leq r$ (since otherwise, the argument is similar[34]). Recall that $0 < r < k$ and $0 < s < k$. From $0 < s$, we obtain $s \geq 1$, so that $s - 1 \leq 0$. Thus,

[33] *Proof.* For any color $h \in \{0, 1, \ldots, k-1\}$, we have

$$\begin{aligned}
&(\#\text{ of all squares in } R_{n,m} \text{ that have color } h) \\
&= \sum_{Z \text{ is a zone}} (\#\text{ of all squares in } Z \text{ that have color } h) \\
&= (\#\text{ of all squares in the northeastern zone that have color } h) \\
&\quad + \sum_{\substack{Z \text{ is a zone;} \\ Z \text{ is not the northeastern zone}}} (\#\text{ of all squares in } Z \text{ that have color } h),
\end{aligned}$$

so that

$$\begin{aligned}
&(\#\text{ of all squares in the northeastern zone that have color } h) \\
&= \underbrace{(\#\text{ of all squares in } R_{n,m} \text{ that have color } h)}_{\substack{\text{independent of } h \\ \text{(since } R_{n,m} \text{ is balanced)}}} \\
&\quad - \sum_{\substack{Z \text{ is a zone;} \\ Z \text{ is not the northeastern zone}}} \underbrace{(\#\text{ of all squares in } Z \text{ that have color } h)}_{\substack{\text{independent of } h \\ \text{(by (16))}}},
\end{aligned}$$

and thus the # of all squares in the northeastern zone that have color h is independent of h. In other words, the northeastern zone is balanced.

[34] More precisely, the same argument applies if we interchange the roles of rows and columns.

$0 \leq \underbrace{s}_{\leq r} - 1 \leq r - 1$. Therefore, each row of $\mathfrak{Z}$ contains at least one square with color $s - 1$. Since $\mathfrak{Z}$ has s rows, we thus conclude that

$$\mathfrak{Z} \text{ contains at least } s \text{ squares with color } s - 1. \tag{18}$$

(We can easily see that $\mathfrak{Z}$ contains exactly s squares with color $s - 1$, but we won't need this.)

On the other hand, the bottommost row of $\mathfrak{Z}$ only contains squares with colors $0, 1, \ldots, r - 1$. Hence, it does not contain a square with color r (since $r > r - 1$). But each row of $\mathfrak{Z}$ has width $r < k$, and thus contains **at most** one square with color r (because if it contained two distinct squares with color r, then these two squares would be a distance of $\geq k$ apart from one another, but the row only has width $r < k$). So we know that the zone $\mathfrak{Z}$ has s rows, one of which (the bottommost one) contains no square with color r, while each of the other $s - 1$ rows contains **at most** one square with color r. Hence, altogether,

$$\mathfrak{Z} \text{ contains at most } s - 1 \text{ squares with color } r. \tag{19}$$

Comparing this with (18), we conclude that the # of squares with color r contained in $\mathfrak{Z}$ is different from the # of squares with color $s - 1$ contained in $\mathfrak{Z}$ (since the former number is $\leq s - 1$, while the latter number is $\geq s$). Hence, $\mathfrak{Z}$ is not balanced. In other words, the northeastern zone is not balanced (since $\mathfrak{Z}$ is the northeastern zone). This contradicts the fact that the northeastern zone is balanced. This contradiction shows that our assumption was false. Hence, the "$\Longrightarrow$" direction of Proposition 1.1.16 is proven. □

This was just a little taste of the theory of tilings of discrete (plane) shapes. See the survey [ArdSta10] by Ardila and Stanley for an introduction to the varied questions and ideas of this theory. See also [18f-hw1s, Exercises 4 and 5] and [19f-hw1s, Exercises 1, 2, 3] for further exercises on counting tilings, and [LeLeMe16, §5.1.5] for a neat exercise in proving existence of tilings. Furthermore, the book [BenQui03] by Benjamin and Quinn provides a lot of applications of tilings to enumerative combinatorics, such as proofs of identities between Fibonacci numbers using their domino-tiling interpretation (Proposition 1.1.11)[35]. (See [BenQui04] for a "best-of" of sorts.)

Class of 2019-09-30

[35] To be more precise, Benjamin and Quinn work not with domino tilings of $R_{n,2}$, but rather with "square-and-domino tilings" of $R_{n,1}$. These objects behave just as domino tilings of $R_{n,2}$ do (there is an easy bijection between the latter and the former), but are easier to argue about.

1.2. Sums of powers

1.2.1. The sum $1+2+...+n$

We now switch the subject and recall a famous result, known colloquially as the *"Little Gauss" formula* due to the anecdote of Gauss inventing it in primary school:[36]

Theorem 1.2.1 ("Little Gauss" formula)**.** Let $n \in \mathbb{N}$. Then,

$$1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Keep in mind that $0 \in \mathbb{N}$ according to our conventions; thus, Theorem 1.2.1 applies to $n = 0$. And indeed, Theorem 1.2.1 holds for $n = 0$, since an *empty sum* (i.e., a sum that consists of no addends) is defined to be 0, and thus we have

$$1+2+\cdots+n = 1+2+\cdots+0 = (\text{empty sum}) = 0 = \frac{0\cdot(0+1)}{2}.$$

First proof of Theorem 1.2.1. Induction on n. The details are completely straightforward and LTTR.

(The abbreviation "LTTR" stands for "left to the reader". I will usually leave arguments to the reader when they are straightforward or easy variations of arguments shown before.) □

Second proof of Theorem 1.2.1. We observe the following fact: If $a_1, a_2, \ldots, a_n$ are n numbers (say, real numbers), and $b_1, b_2, \ldots, b_n$ are n further numbers, then

$$\begin{aligned}&(a_1+a_2+\cdots+a_n)+(b_1+b_2+\cdots+b_n)\\ &= (a_1+b_1)+(a_2+b_2)+\cdots+(a_n+b_n).\end{aligned} \tag{20}$$

(Indeed, both sides of this equality are just two ways to add all the $2n$ numbers $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$. This should convince you that they are the same, although formally speaking, this is not a proof. See Subsection 1.2.2 below for some references to a formal proof.)

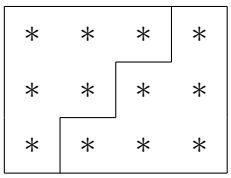
[36] In truth, this formula was known to the Ancient Greeks.

Now,

$$\begin{aligned}
&2 \cdot (1+2+\cdots+n) \\
&= (1+2+\cdots+n) + \underbrace{(1+2+\cdots+n)}_{\substack{=n+(n-1)+\cdots+1 \\ \text{(here, we have just reversed} \\ \text{the order of summation)}}} \\
&= (1+2+\cdots+n) + (n+(n-1)+\cdots+1) \\
&= (1+n) + (2+(n-1)) + \cdots + (n+1) \\
&\qquad \text{(by (20), applied to } a_i = i \text{ and } b_i = n+1-i) \\
&= \underbrace{(n+1)+(n+1)+\cdots+(n+1)}_{n \text{ many addends}} \\
&\qquad \text{(since each of the numbers } 1+n,\ 2+(n-1),\ \ldots,\ n+1 \text{ equals } n+1) \\
&= n\,(n+1)\,.
\end{aligned}$$

Dividing this equality by 2, we obtain $1+2+\cdots+n = \dfrac{n\,(n+1)}{2}$. This proves Theorem 1.2.1 again. □

Third proof of Theorem 1.2.1 (sketched). Here is a picture proof (drawn for the case $n = 3$):



.

This is a 4×3-rectangle[37] (i.e., a rectangle of width 4 and height 3), subdivided into two parts by a broken line which starts in the southwestern corner and winds its way to the northeastern corner, making steps of length 1 eastwards and northwards (by turns). The two parts (the one below and the one above the broken line) have the same area, since they are symmetric to each other with respect to the center of the rectangle.[38] Hence, the area of either part equals half the area of the whole rectangle. Since the area of the whole rectangle is $3 \cdot 4$, we thus conclude that the area of either part equals $\dfrac{3 \cdot 4}{2}$.

On the other hand, here is a different way to compute this area: Let us look at the part below the broken line. This part has 0 squares in the 1-st column[39], 1 square in the 2-nd column, 2 squares in the 3-rd column, and 3 squares in the 4-th

[37] We have put an asterisk into each little square of the rectangle in order to make the squares easier to discern.

[38] Note that "area" is normally a geometric concept, but since both parts consist of full squares, we can redefine it combinatorially as the number of squares in the respective part.

[39] We count columns from the left.

column. Hence, in total, it has $0+1+2+3$ many squares. In other words, its area is $0+1+2+3$.

Now we know that the area of the part of the rectangle below the broken line is $0+1+2+3$, but we also know (from before) that it equals $\dfrac{3\cdot 4}{2}$. Hence, $0+1+2+3=\dfrac{3\cdot 4}{2}$. In view of $0+1+2+3=1+2+3$, this rewrites as $1+2+3=\dfrac{3\cdot 4}{2}$. This is precisely the statement of Theorem 1.2.1 for $n=3$.

The same argument (but using an $(n+1)\times n$-rectangle instead of a 4×3-rectangle) proves Theorem 1.2.1 for arbitrary n.

How can we formalize this argument? Once again (as with domino tilings), it makes sense to think of the $(n+1)\times n$-rectangle as the finite set $[n+1]\times[n]$ (where, as before, we set $[k]=\{1,2,\ldots,k\}$ for each $k\in\mathbb{N}$) rather than a geometric shape in the real plane.[40] The two parts into which this rectangle is divided by the broken line become the two sets

$$A := \{(i,j)\in[n+1]\times[n] \mid i\leq j\} \qquad \text{and}$$
$$B := \{(i,j)\in[n+1]\times[n] \mid i>j\}.$$

(The letters A and B here stand for "above" and "below".)

So let us redo this proof from scratch, using the combinatorial model (i.e., finite sets) throughout it. We consider the finite set $[n+1]\times[n]$, which (according to the product rule) has $(n+1)\cdot n = n(n+1)$ many elements. Define two subsets

$$A := \{(i,j)\in[n+1]\times[n] \mid i\leq j\} \qquad \text{and}$$
$$B := \{(i,j)\in[n+1]\times[n] \mid i>j\}$$

of $[n+1]\times[n]$. These two subsets A and B are disjoint (since no $(i,j)\in[n+1]\times[n]$ can satisfy $i\leq j$ and $i>j$ at the same time), and their union is $[n+1]\times[n]$ (since each $(i,j)\in[n+1]\times[n]$ satisfies either $i\leq j$ or $i>j$). Hence, the sum rule shows that $|[n+1]\times[n]| = |A|+|B|$, so that

$$|A|+|B| = |[n+1]\times[n]| = \underbrace{|[n+1]|}_{=n+1}\cdot\underbrace{|[n]|}_{=n} \qquad \text{(by (5))}$$
$$= (n+1)\cdot n = n(n+1). \tag{21}$$

On the other hand, the map

$$A\to B,$$
$$(i,j)\mapsto(n+2-i,n+1-j)$$

(which, visually, is just the reflection around the center of the $(n+1)\times n$-rectangle) is a bijection[41]. Hence, the bijection rule yields $|A|=|B|$. Thus, $\underbrace{|A|}_{=|B|}+|B| = |B|+|B| = 2\cdot|B|$. Comparing this with (21), we obtain $2\cdot|B| = n(n+1)$, so that

$$|B| = \frac{n(n+1)}{2}. \tag{22}$$

[40] Again, we let (i,j) be the square in column i (counted from the left) and row j (counted from the bottom).

[41] This needs to be proven, but the proof is really straightforward. First, you need to check that this

On the other hand, let us count the squares in B "by column". Recall that, in our combinatorial model, the x-coordinate i of a square (i,j) tells us which column it belongs to. Thus, the squares $c \in B$ in the k-th column (for any given $k \in \{1,2,\ldots,n+1\}$) are precisely the squares $c \in B$ that have x-coordinate k. Hence, we should count the squares in B according to their x-coordinate. Formally speaking, this means applying the sum rule to the set B and its $n+1$ disjoint subsets $\{c \in B \mid c \text{ has x-coordinate } k\}$ for $k \in \{1,2,\ldots,n+1\}$. These $n+1$ subsets are disjoint (since any square $c \in B$ has only one x-coordinate) and their union is B (since each square $c \in B$ has x-coordinate 1 or 2 or $\cdots$ or $n+1$). Hence, the sum rule yields

$$\begin{aligned} |B| &= |\{c \in B \mid c \text{ has x-coordinate } 1\}| + |\{c \in B \mid c \text{ has x-coordinate } 2\}| \\ &\qquad + \cdots + |\{c \in B \mid c \text{ has x-coordinate } n+1\}| \\ &= \sum_{i=1}^{n+1} |\{c \in B \mid c \text{ has x-coordinate } i\}| . \end{aligned} \tag{23}$$

But the addends on the right hand side of this equality are easily computed:[42] For each $i \in \{1,2,\ldots,n+1\}$, we have

$$\begin{aligned} &\{c \in B \mid c \text{ has x-coordinate } i\} \\ &= \{c \in B \mid c = (i,j) \text{ for some } j \in [n]\} \\ &\qquad \left(\begin{array}{c} \text{since a square of } [n+1] \times [n] \text{ has x-coordinate } i \\ \text{if and only if it has the form } (i,j) \text{ for some } j \in [n] \end{array} \right) \\ &= \{(i,j) \mid j \in [n] \text{ such that } (i,j) \in B\} \\ &= \{(i,j) \mid j \in [n] \text{ such that } i > j\} \\ &\qquad \left(\begin{array}{c} \text{since a square } (i,j) \in [n+1] \times [n] \text{ satisfies } (i,j) \in B \\ \text{if and only if } i > j \text{ (by the definition of } B) \end{array} \right) \\ &= \{(i,1), (i,2), \ldots, (i,i-1)\} \end{aligned}$$

and thus

$$\begin{aligned} |\{c \in B \mid c \text{ has x-coordinate } i\}| &= |\{(i,1), (i,2), \ldots, (i,i-1)\}| \\ &= i-1. \end{aligned} \tag{24}$$

---

map is well-defined. This means showing that $(n+2-i, n+1-j) \in B$ for each $(i,j) \in A$. Once this is shown, you can show the bijectivity of this map by explicitly constructing an inverse; namely, the inverse is the map

$$\begin{aligned} B &\to A, \\ (i,j) &\mapsto (n+2-i, n+1-j). \end{aligned}$$

(Don't be surprised that it is given by the same formula: In order to undo a reflection around a point, you have to reflect again around the same point.)

[42] This is just the formalization of our (visually obvious) observation that the part below the broken line (which we are now calling B) has 0 squares in the 1-st column, 1 square in the 2-nd column, 2 squares in the 3-rd column, etc..

Hence, (23) becomes

$$|B| = \sum_{i=1}^{n+1} \underbrace{\left|\{c \in B \mid c \text{ has x-coordinate } i\}\right|}_{\substack{=i-1 \\ \text{(by (24))}}}$$
$$= \sum_{i=1}^{n+1} (i-1) = 0+1+2+\cdots+n = 1+2+\cdots+n.$$

Comparing this with (22), we obtain $1+2+\cdots+n = \dfrac{n(n+1)}{2}$. This finally completes our formalized picture proof of Theorem 1.2.1.

The moral of the story: A picture is worth a thousand words! □

1.2.2. What is a sum, actually?

Throughout Subsection 1.2.1, we have been freely working with expressions like $1+2+\cdots+n$ and (more generally) $a_1+a_2+\cdots+a_n$, where $a_1, a_2, \ldots, a_n$ are n numbers. Looking back, you might wonder: Why are these expressions well-defined? How is "the sum of n numbers" defined to begin with?

Let me explain what I mean by this. Let "number" mean "rational number", just to be specific here (although the same question and the same answer apply to integers, real numbers and complex numbers). I assume you know what the sum of **two** numbers is. Even when two numbers a and b are given without specifying their order, their sum is well-defined, because the *commutativity of addition* (i.e., the rule saying that $a+b = b+a$ for any two numbers a and b) guarantees that the two possible ways of adding them together yield the same result.

Now, suppose you are given **three** numbers a, b and c. To add them all together means to add two of them and then add the third one to the result. How many ways are there to do this? There are 12, as you can easily check, namely

$$\begin{array}{llll} (a+b)+c, & (a+c)+b, & (b+a)+c, & (b+c)+a, \\ (c+a)+b, & (c+b)+a, & a+(b+c), & a+(c+b), \\ b+(a+c), & b+(c+a), & c+(a+b), & c+(b+a). \end{array}$$

If we want to make sense of a "sum of three numbers" without having to specify the precise procedure of summation, we better hope that these 12 ways all lead to the same result! And indeed, they do. This is not hard to derive from the above-mentioned commutativity of addition, combined with the *associativity of addition* (i.e., the rule saying that $(a+b)+c = a+(b+c)$ for any three numbers a, b and

c). For example,

$$\begin{aligned} a+(b+c) &= \underbrace{(a+b)}_{\substack{=b+a \\ \text{(by commutativity)}}} + c \qquad \text{(by associativity)} \\ &= (b+a)+c = b+\underbrace{(a+c)}_{\substack{=c+a \\ \text{(by commutativity)}}} \qquad \text{(by associativity)} \\ &= b+(c+a) = (b+c)+a \qquad \text{(by associativity)} \end{aligned}$$

and so on (in the sense that similar reasoning shows that all 12 ways give equal results). Once we know that these 12 ways all lead to the same result, we can call the result "the sum of the three numbers a, b and c" with a clear conscience, and denote it by $a+b+c$ without specifying the order in which the sum is taken through well-placed parentheses.

Next, suppose you are given **four** numbers a, b, c and d. There are now 120 ways of adding them together, including such ways as

$$((a+b)+c)+d, \qquad (a+b)+(c+d), \qquad (b+d)+(c+a), \qquad (b+(d+a))+c$$

and many others. How can we tell that they all lead to the same result? They do, and this can be proven as for three numbers (we don't need any new rules; commutativity and associativity suffice), but this is of course more laborious than the case of three numbers.

Now, suppose you are given n numbers $a_1, a_2, \ldots, a_n$, and you want to prove that all ways of adding them together give the same result. For example, two of these ways are

$$(\cdots(((a_1+a_2)+a_3)+a_4)+\cdots)+a_n \qquad \text{("left-associative summation")}$$

and

$$a_1+(\cdots+(a_{n-3}+(a_{n-2}+(a_{n-1}+a_n)))\cdots) \qquad \text{("right-associative summation");}$$

how do we know they are equivalent?

Let us close a ring around this problem. As long as we don't know that all ways to add n numbers give the same result, we cannot define "**the** sum" of n numbers. But we can define the **set of all possible sums** of n numbers, i.e., the set of all possible results that can be obtained by adding them together in all possible orders. For example, for three numbers a, b, c, this set will be

$$\{(a+b)+c,\ \ (a+c)+b,\ \ \ldots,\ \ c+(b+a)\}$$

(containing all the 12 ways to add a, b, c together, listed above). This definition can easily be done by recursion:

- There is only one way to add 0 numbers together. Namely, adding 0 numbers always yields 0.
- There is only one way to add 1 number together. Namely, adding 1 number a always yields a itself.
- If $n > 1$, then any way of adding n numbers together is given by splitting them into two (disjoint nonempty) groups[43], then adding the numbers in the first group together (in one of the many possible ways), then adding the numbers in the second group together, and finally adding the two results together.

Thus we can define the **set of all possible sums** of n numbers. Our goal is to prove that there is only one such sum, i.e., that this set is a 1-element set. This is now a rigorously stated claim[44], which we can try to prove! Thus, at the very least, we have formalized our claim that we can add n numbers together in a well-defined way. Proving it is another story, but it can be done with rather elementary tools. See [Grinbe15, §2.14] for a very detailed proof[45] (and [18s, lecture of 7th February 2018, pages 1–7] for a short version). Other proofs can be found in [Warner71, Appendix A] and in [GalQua22, §3.3].

The upshot is that we have a well-defined notion of the sum of any finite family of numbers, even if it is given without specifying an order. For example, "the sum of all prime numbers smaller than 10" is well-defined (and equals $2+3+5+7=17$). Likewise, if you are given a polygon, then "the sum of the sidelengths of the polygon" is well-defined.

It is helpful to have a notation for these kinds of sums, so let us introduce it (although we have already used it to some extent):

Definition 1.2.2. Let S be a finite set. For each $s \in S$, let a_s be a number (e.g., an integer or a rational number or a real number or a complex number).

Then, $\sum_{s \in S} a_s$ shall denote the sum of the numbers a_s for all $s \in S$. This notation is read as "the sum of a_s over all $s \in S$" or "the sum of a_s for s ranging over S" or "the sum of a_s where s runs through S". The "$\sum$" sign in this notation is called the *summation sign*.

Example 1.2.3. **(a)** We have $\sum_{s \in \{1,2,3,4\}} s = 1+2+3+4 = 10$.

(b) We have $\sum_{s \in \{1,2,3,4\}} s^2 = 1^2+2^2+3^2+4^2 = 30$.

[43] "Groups" in the sense of "batches", not in the sense of group theory. For example, if our n numbers are a, b, c, d, e, then the first group may be d, b and the second may be c, a, e.

[44] known as the *general commutativity theorem* ("general" because it applies to any finite number of addends rather than two)

[45] More precisely, the proof is in [Grinbe15, §2.14.1–§2.14.6]. The remaining subsections of [Grinbe15, §2.14] prove properties of sums.

(c) We have $\sum_{s\in\{1,2,3,4\}} \frac{1}{s} = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4} = \frac{25}{12}$.
(d) We have $\sum_{s\in\{3,4,9\}} s = 3+4+9 = 16$.

We need to note a few things about the summation sign:

- The letter "s" in the notation "$\sum_{s\in S} a_s$" is an instance of what is called a *bound variable* (or *running index*, or *dummy variable*): Its only purpose is to mark the "moving part" of the sum. So it plays the same role as the letter "s" in the set-comprehension notation "$\{s \in \mathbb{Z} \mid s > 2\}$", or the letter "$s$" in "the map $\mathbb{Z} \to \mathbb{Z}$, $s \mapsto s+3$", or the letter "s" in the sentence "There exists no $s \in \mathbb{Z}$ such that $s^2 = 2$". Thus, it is perfectly legitimate to replace it by any other symbol (that is not used otherwise). For example, we can rewrite the sum $\sum_{s\in\{1,2,3,4\}} \frac{1}{s}$ as $\sum_{i\in\{1,2,3,4\}} \frac{1}{i}$ or as $\sum_{k\in\{1,2,3,4\}} \frac{1}{k}$ or as $\sum_{\mathfrak{S}\in\{1,2,3,4\}} \frac{1}{\mathfrak{S}}$ or as $\sum_{\spadesuit\in\{1,2,3,4\}} \frac{1}{\spadesuit}$; it will still be the same sum.

- In the notation "$\sum_{s\in S} a_s$", the letter "s" is called the *summation index*; the set S is called the *indexing set* (or *range*) of the sum; and the numbers a_s are called the *addends* of the sum. The whole expression $\sum_{s\in S} a_s$ is called a *finite sum*.

- Our definition of sums forces $\sum_{s\in\varnothing} a_s$ to always be 0. This is called an *empty sum*. Thus, empty sums are 0. If this sounds like an arbitrary convention to you, you should check that it is the only convention that makes (25) hold for one-element sets S.

- Sums can have equal addends. For example,

$$\sum_{s\in\{-2,-1,0,1,2\}} s^2 = (-2)^2+(-1)^2+0^2+1^2+2^2 = 4+1+0+1+4 = 10.$$

However,

$$\sum_{s\in\left\{(-2)^2,(-1)^2,0^2,1^2,2^2\right\}} s = 0^2+1^2+2^2 = 0+1+4 = 5,$$

because the **set** $\left\{(-2)^2,(-1)^2,0^2,1^2,2^2\right\}$ is only a 3-element set (with elements $0^2,1^2,2^2$). Thus, if you want to write down a sum with some of its entries equal, you still need to ensure that each of the addends gets a distinct index in the indexing set. In general, the sum of 5 numbers is not the sum of the elements of the **set** of these 5 numbers, because if some of these 5 numbers are equal, then the set "forgets" that they appear more than once.

- The summation index does not always have to be a single letter. For instance, if S is a set of pairs, then we can write $\sum_{(x,y)\in S} a_{(x,y)}$ (meaning the same as $\sum_{s\in S} a_s$). Here is an example of this notation:

$$\sum_{(x,y)\in\{1,2,3\}^2} \frac{x}{y} = \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{2}{1}+\frac{2}{2}+\frac{2}{3}+\frac{3}{1}+\frac{3}{2}+\frac{3}{3}.$$

Here are some more examples, coming from more combinatorial questions:

Example 1.2.4. **(a)** Let $\mathcal{P}(A)$ denote the powerset of a set A (that is, the set of all subsets of A). Then, we can write the sum of the sizes of all subsets of $\{1,2,3\}$ as follows:

$$\begin{aligned}\sum_{B\in\mathcal{P}(\{1,2,3\})} |B| &= |\varnothing| + |\{1\}| + |\{2\}| + |\{3\}| \\ &\quad + |\{1,2\}| + |\{1,3\}| + |\{2,3\}| + |\{1,2,3\}| \\ &= 0+1+1+1+2+2+2+3 = 12.\end{aligned}$$

(b) If A and B are two sets, then B^A denotes the set of all maps from A to B. For example, let $A=\{1,2\}$ and $B=\{1,2\}$. Then, we can write the sum of the sizes of the images of all maps from A to B as follows:

$$\begin{aligned}&\sum_{f\in B^A} |f(A)| \\ &= \underbrace{|\{1\}|}_{\substack{\text{corresponding to the} \\ \text{map } \left(\begin{smallmatrix}1&2\\1&1\end{smallmatrix}\right)}} + \underbrace{|\{1,2\}|}_{\substack{\text{corresponding to the} \\ \text{map } \left(\begin{smallmatrix}1&2\\1&2\end{smallmatrix}\right)}} + \underbrace{|\{1,2\}|}_{\substack{\text{corresponding to the} \\ \text{map } \left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)}} + \underbrace{|\{2\}|}_{\substack{\text{corresponding to the} \\ \text{map } \left(\begin{smallmatrix}1&2\\2&2\end{smallmatrix}\right)}} \\ &= 1+2+2+1 = 6.\end{aligned}$$

(Here, we have written out each map in two-line notation: That is, the map sending 1 and 2 to a_1 and a_2 has been written as $\begin{pmatrix}1&2\\a_1&a_2\end{pmatrix}$.)

There are several variants of the summation sign:

- The expression $\sum_{\substack{s\in\{1,2,3,4,5,6\};\\ s \text{ is odd}}} s^2$ stands for the sum of the squares of all **odd** elements of $\{1,2,3,4,5,6\}$. In general, if S is a set, and if $\mathcal{A}(s)$ is a logical statement defined for each $s\in S$, then the notation $\sum_{\substack{s\in S;\\ \mathcal{A}(s)}} a_s$ stands for the sum

$\sum\limits_{s \in \{t \in S \mid \mathcal{A}(t)\}} a_s$ (that is, the sum of a_s not over all $s \in S$, but only over the ones which satisfy $\mathcal{A}(s)$). For this sum to be well-defined, we do not need S to be finite; we only need the subset $\{t \in S \mid \mathcal{A}(t)\}$ to be finite (i.e., we need there to only be finitely many $s \in S$ satisfying $\mathcal{A}(s)$).

- The expression $\sum\limits_{i=5}^{8} i^2$ stands for the sum $\sum\limits_{i \in \{5,6,7,8\}} i^2$. In general, if p and q are two integers, then the notation $\sum\limits_{i=p}^{q} a_i$ stands for the sum $\sum\limits_{i \in \{p,p+1,\ldots,q\}} a_i$. Here it should be kept in mind that the set $\{p, p+1, \ldots, q\}$ is understood to be empty if $p > q$. (Be warned that some authors have different conventions for the latter case.)

  In the notation $\sum\limits_{i=p}^{q} a_i$, the integers p and q are called the *bounds* of the summation.

  Note that the summation sign $\sum\limits_{i=1}^{n}$ (for some $n \in \mathbb{N}$) is thus equivalent to $\sum\limits_{i \in \{1,2,\ldots,n\}}$, hence also to $\sum\limits_{i \in [n]}$.

- The summation sign $\sum\limits_{B \subseteq A}$ (where A is a given set) is shorthand for $\sum\limits_{B \in \mathcal{P}(A)}$, where $\mathcal{P}(A)$ stands for the powerset of A (that is, the set of all subsets of A). Thus, the result of Example 1.2.4 **(a)** could be rewritten as $\sum\limits_{B \subseteq \{1,2,3\}} |B| = 12$.

- The summation sign $\sum\limits_{f: A \to B}$ (where A and B are two sets) is shorthand for $\sum\limits_{f \in B^A}$. Thus, the result of Example 1.2.4 **(b)** could be rewritten as $\sum\limits_{f: A \to B} |f(A)| = 6$.

- Statements under the summation sign can be written out in words. For example, "$\sum\limits_{B \text{ is a subset of } A}$" means the same as "$\sum\limits_{B \subseteq A}$".

These notations can be mixed and matched. For example, $\sum\limits_{\substack{f: A \to B; \\ f \text{ is injective}}} |f(A)|$ means the sum of the sizes of the images of all **injective** maps from A to B.

1.2.3. Rules for sums

Finite sums have lots of properties, such as the identity (20) which we have used in the second proof of Theorem 1.2.1. See [Grinbe15, §1.4] for a long list of these properties. Here I shall just list a few:[46]

[46] See [Grinbe15, §1.4.2 and §2.14] for proofs of these properties.

- **Splitting-off:** Let S be a finite set. Let a_s be a number for each $s \in S$. Let $t \in S$. Then,
$$\sum_{s \in S} a_s = a_t + \sum_{s \in S \setminus \{t\}} a_s. \tag{25}$$
In other words, we can always rewrite the sum $\sum_{s \in S} a_s$ as its addend a_t plus the sum of all remaining addends. This is called *splitting off* (or *extracting*) *an addend from a sum*. Particular cases of this identity are the identities
$$\sum_{i=p}^{q} a_i = a_p + \sum_{i=p+1}^{q} a_i \qquad \text{and} \qquad \sum_{i=p}^{q} a_i = a_q + \sum_{i=p}^{q-1} a_i$$
that hold whenever $p \leq q$. (They do not hold for $p > q$, because we cannot extract an addend from an empty sum.)

- **Splitting:** Let S be a finite set. Let X and Y be two subsets of S such that $X \cap Y = \varnothing$ and $X \cup Y = S$. (Equivalently, X and Y are two subsets of S such that each element of S lies in **exactly** one of X and Y.) Let a_s be a number for each $s \in S$. Then,
$$\sum_{s \in S} a_s = \sum_{s \in X} a_s + \sum_{s \in Y} a_s. \tag{26}$$
(The right hand side of this equality has to be understood as $\left(\sum_{s \in X} a_s\right) + \left(\sum_{s \in Y} a_s\right)$. In general, finite sums reach past "$\cdot$" signs but not past "$+$" signs; thus, $\sum_{s \in S} a_s b$ means $\sum_{s \in S} (a_s b)$, but $\sum_{s \in S} a_s + b$ means $\left(\sum_{s \in S} a_s\right) + b$. This is considered to be part of the PEMDAS convention, because finite sums are a form of addition. When in doubt, always use parentheses.)

For example, we can apply (26) to $S = \{1,2,3,4,5\}$ and $X = \{1,3,5\}$ and $Y = \{2,4\}$. We then obtain
$$\sum_{s \in \{1,2,3,4,5\}} a_s = \sum_{s \in \{1,3,5\}} a_s + \sum_{s \in \{2,4\}} a_s, \qquad \text{or, equivalently,}$$
$$a_1 + a_2 + a_3 + a_4 + a_5 = (a_1 + a_3 + a_5) + (a_2 + a_4).$$

More generally, if S is a finite set of integers, then
$$\sum_{s \in S} a_s = \sum_{\substack{s \in S; \\ s \text{ is even}}} a_s + \sum_{\substack{s \in S; \\ s \text{ is odd}}} a_s \tag{27}$$
(by (26), applied to $X = \{s \in S \mid s \text{ is even}\}$ and $Y = \{s \in S \mid s \text{ is odd}\}$).

More generally, let S be a finite set. For each $s \in S$, let $\mathcal{A}(s)$ be a logical statement (which can be either true or false depending on s; for example,

$\mathcal{A}(s)$ could be "s is even" if S is a set of integers, or "s is empty" if S is a set of sets), and let a_s be a number. Then,

$$\sum_{s \in S} a_s = \sum_{\substack{s \in S; \\ \mathcal{A}(s) \text{ is true}}} a_s + \sum_{\substack{s \in S; \\ \mathcal{A}(s) \text{ is false}}} a_s. \tag{28}$$

This follows by applying (26) to $X = \{s \in S \mid \mathcal{A}(s) \text{ is true}\}$ and $Y = \{s \in S \mid \mathcal{A}(s) \text{ is false}\}$. Of course, (27) is the particular case of (28) for $\mathcal{A}(s) = (\text{"}s \text{ is even"})$.

- **Summing equal values:** Let S be a finite set. Let a be a number. Then,

$$\sum_{s \in S} a = |S| \cdot a. \tag{29}$$

(That is, summing n many copies of a number a results in the number na.)

Applying (29) to $a = 1$, we find

$$\sum_{s \in S} 1 = |S| \cdot 1 = |S|. \tag{30}$$

In other words, the size of a finite set is a particular case of a finite sum. This trivial observation will prove rather useful to us below.

- **Splitting an addend:** Let S be a finite set. For every $s \in S$, let a_s and b_s be numbers. Then,

$$\sum_{s \in S} (a_s + b_s) = \sum_{s \in S} a_s + \sum_{s \in S} b_s. \tag{31}$$

When $S = \{1, 2, \ldots, n\}$, this becomes precisely the equality (20).

- **Factoring out:** Let S be a finite set. For every $s \in S$, let a_s be a number. Also, let λ be a number. Then,

$$\sum_{s \in S} \lambda a_s = \lambda \sum_{s \in S} a_s. \tag{32}$$

This is a generalization of the *distributive law* $\lambda(a + b) = \lambda a + \lambda b$.

- **Zeroes sum to zero:** Let S be a finite set. Then,

$$\sum_{s \in S} 0 = 0. \tag{33}$$

- **Renaming the index:** Let S be a finite set. Let a_s be a number for each $s \in S$. Then,

$$\sum_{s \in S} a_s = \sum_{t \in S} a_t.$$

This is called *renaming the summation index*, and is justified by the fact that the summation index is a dummy variable.

- **Substituting the index I:** Let S and T be two finite sets. Let $f : S \to T$ be a bijection. Let a_t be a number for each $t \in T$. Then,

$$\sum_{t \in T} a_t = \sum_{s \in S} a_{f(s)}. \tag{34}$$

The idea here is that the sum $\sum_{s \in S} a_{f(s)}$ contains the same addends as the sum $\sum_{t \in T} a_t$.

When we apply (34), we say that we are *substituting* $f(s)$ for t in the sum $\sum_{t \in T} a_t$.

Applying (34) to $a_t = 1$, we obtain $\sum_{t \in T} 1 = \sum_{s \in S} 1$, which rewrites as $|T| = |S|$ (because of (30)). This is precisely the bijection principle (Theorem 1.1.6). Thus, (34) generalizes the bijection principle.

The equality (34) also shows that we can "turn a sum around", in the sense that we have

$$a_1 + a_2 + \cdots + a_n = a_n + a_{n-1} + \cdots + a_1 \tag{35}$$

for any $n \in \mathbb{N}$ and any n numbers $a_1, a_2, \ldots, a_n$. (This was used in the Second proof of Theorem 1.2.1.) Indeed, the left hand side of (35) can be rewritten as $\sum_{t \in [n]} a_t$, whereas the right hand side can be rewritten as $\sum_{s \in [n]} a_{n+1-s} = \sum_{s \in [n]} a_{f(s)}$, where $f : [n] \to [n]$ is the map that sends each $s \in [n]$ to $n + 1 - s$. Since this latter map $f : [n] \to [n]$ is a bijection, we can use (34) (applied to $S = [n]$ and $T = [n]$) to conclude that $\sum_{t \in [n]} a_t = \sum_{s \in [n]} a_{f(s)}$; but this is precisely the identity (35).

- **Substituting the index II:** Let S and T be two finite sets. Let $f : S \to T$ be a bijection. Let a_s be a number for each $s \in S$. Then,

$$\sum_{s \in S} a_s = \sum_{t \in T} a_{f^{-1}(t)}. \tag{36}$$

This is, of course, just (34) but applied to T, S and f^{-1} instead of S, T and f. We state it as a separate formula because we shall be using both versions.

- **Splitting a sum by a value of a function:** Let S and W be two finite sets. Let $f : S \to W$ be a map. Let a_s be a number for each $s \in S$. Then,

$$\sum_{s \in S} a_s = \sum_{w \in W} \sum_{\substack{s \in S; \\ f(s) = w}} a_s. \tag{37}$$

(There are two summation signs on the right hand side, signifying that we are taking a finite sum of finite sums.) This equality provides a way to split

a sum $\sum_{s \in S} a_s$ into several batches by distributing all possible values of the summation index s into several "bins"[47], and then summing each batch of addends corresponding to a bin together and then summing the "bin totals". For example, let us apply (37) to the 11-element set $S = \{-5, -4, \ldots, 4, 5\}$ and the 6-element set $W = \{0, 1, \ldots, 5\}$ and the map $f : S \to W$ that sends each $s \in S$ to $|s| \in W$. We thus obtain

$$\sum_{s \in \{-5,-4,\ldots,4,5\}} a_s = \sum_{w \in \{0,1,\ldots,5\}} \sum_{\substack{s \in \{-5,-4,\ldots,4,5\}; \\ |s| = w}} a_s.$$

Explicitly, this rewrites as

$$\begin{aligned} &a_{-5} + a_{-4} + \cdots + a_4 + a_5 \\ &= a_0 + (a_{-1} + a_1) + (a_{-2} + a_2) + (a_{-3} + a_3) + (a_{-4} + a_4) + (a_{-5} + a_5). \end{aligned}$$

Here, the "bins" are $\{0\}$, $\{-1, 1\}$, $\{-2, 2\}$, $\{-3, 3\}$, $\{-4, 4\}$ and $\{-5, 5\}$, and the corresponding "bin totals" are a_0, $a_{-1} + a_1$, $a_{-2} + a_2$, $a_{-3} + a_3$, $a_{-4} + a_4$ and $a_{-5} + a_5$.

- **Splitting a sum into subsums:** Let a finite set S be the union of k disjoint sets $S_1, S_2, \ldots, S_k$. Let a_s be a number for each $s \in S$. Then,

$$\sum_{s \in S} a_s = \sum_{w=1}^{k} \sum_{s \in S_w} a_s. \tag{38}$$

(The right hand side can be rewritten in the somewhat more familiar form $\sum_{s \in S_1} a_s + \sum_{s \in S_2} a_s + \cdots + \sum_{s \in S_k} a_s$.)

It is easy to see that (38) follows from (37) (by setting $W = \{1, 2, \ldots, k\}$, and letting $f : S \to W$ be the map that sends each $s \in S$ to the unique $w \in \{1, 2, \ldots, k\}$ for which $s \in S_w$).

Note that if we set $a_s = 1$ for each $s \in S$ and recall the formula (30), then (38) rewrites as $|S| = \sum_{w=1}^{k} |S_w| = |S_1| + |S_2| + \cdots + |S_k|$. Thus, we have recovered the sum rule (Theorem 1.1.3) as a particular case of (38).

There are further rules, such as *Fubini's principle* for the interchange of summation signs. We will not state them yet in order to keep this section reasonably short.

However, let us state an important application of summation signs in counting:

[47] The "bins" are the elements of W here. Each value $s \in S$ goes into bin $f(s)$.

Theorem 1.2.5 (The sum rule, in summation-sign form)**.** Let S and W be two finite sets. Let $f : S \to W$ be a map. Then,

$$|S| = \sum_{w \in W} (\#\text{ of } s \in S \text{ satisfying } f(s) = w).$$

Theorem 1.2.5 is called the *sum rule*, since it is a more flexible version of Theorem 1.1.3. Indeed, both theorems tell us how to compute the size $|S|$ of a set S that has been split into several subsets[48]; but Theorem 1.1.3 requires the latter subsets to be numbered by $1, 2, \ldots, k$, whereas Theorem 1.2.5 only needs them to be indexed by elements w of W.

Example 1.2.6. Assume you have a finite set of socks, and each sock is either red or blue or green. Then,

$$\begin{aligned}(\#\text{ of socks}) &= (\#\text{ of red socks}) + (\#\text{ of blue socks}) + (\#\text{ of green socks}) \\ &= \sum_{w \in \{\text{red,blue,green}\}} (\#\text{ of socks of color } w).\end{aligned}$$

This is a consequence of Theorem 1.2.5, applied to $S = \{\text{socks}\}$, $W = \{\text{red}, \text{blue}, \text{green}\}$ and the map $f : S \to W$ defined by $f(s) = (\text{color of } s)$.

Proof of Theorem 1.2.5. From (30), we obtain

$$|S| = \sum_{s \in S} 1 = \sum_{w \in W} \sum_{\substack{s \in S; \\ f(s) = w}} 1 \tag{39}$$

(by (37), applied to $a_s = 1$).

Now, for each $w \in W$, we have

$$\begin{aligned}\sum_{\substack{s \in S; \\ f(s) = w}} 1 &= \sum_{s \in \{t \in S \mid f(t) = w\}} 1 \\ &\qquad \left(\text{since the sign ``} \sum_{\substack{s \in S; \\ f(s) = w}} \text{'' is shorthand for ``} \sum_{s \in \{t \in S \mid f(t) = w\}} \text{''} \right) \\ &= |\{t \in S \mid f(t) = w\}| \\ &\qquad \text{(by (30), applied to } \{t \in S \mid f(t) = w\} \text{ instead of } S) \\ &= |\{s \in S \mid f(s) = w\}| \qquad \text{(here, we have renamed the index } t \text{ as } s) \\ &= (\#\text{ of } s \in S \text{ satisfying } f(s) = w). \end{aligned} \tag{40}$$

[48] In Theorem 1.1.3, the subsets are $S_1, S_2, \ldots, S_k$; in Theorem 1.2.5, the subsets are $\{s \in S \mid f(s) = w\}$ for various $w \in W$.

Hence, (39) becomes

$$|S| = \sum_{w \in W} \underbrace{\sum_{\substack{s \in S; \\ f(s)=w}} 1}_{\substack{=(\#\text{ of } s \in S \text{ satisfying } f(s)=w) \\ \text{(by (40))}}} = \sum_{w \in W} (\#\text{ of } s \in S \text{ satisfying } f(s) = w)\,.$$

This proves Theorem 1.2.5. □

1.2.4. While at that, what is a finite product?

Similar to the notion of a finite sum is a notion of a finite product:

Definition 1.2.7. Let S be a finite set. For each $s \in S$, let a_s be a number (e.g., an integer or a rational number or a real number or a complex number).

Then, $\prod_{s \in S} a_s$ shall denote the product of the numbers a_s for all $s \in S$. This notation is read as "the product of a_s over all $s \in S$" or "the product of a_s for s ranging over S" or "the product of a_s where s runs through S". The "$\prod$" sign in this notation is called the *product sign*.

This notation is called a *finite product*. For example, $\prod_{s \in \{4,5,7,9\}} s^3 = 4^3 \cdot 5^3 \cdot 7^3 \cdot 9^3$.

Most of what we said about finite sums applies (with the obvious changes) to finite products. In particular, finite products are well-defined (in the sense that all ways to multiply n given numbers together produce the same result) and satisfy analogues of the properties of finite sums listed above (with the obvious changes made: e.g., the equality (29) turns into $\prod_{s \in S} a = a^{|S|}$), except for (30). Notations like $\sum_{\substack{s \in S; \\ \mathcal{A}(s)}} a_s$ and $\sum_{i=p}^{q} a_i$ have their analogues for products, which look exactly the same (that is, $\prod_{\substack{s \in S; \\ \mathcal{A}(s)}} a_s$ and $\prod_{i=p}^{q} a_i$) and are defined in the same way. We only need to be careful in defining empty products correctly: While an empty sum was defined to be 0, we must define an empty product (i.e., a product with no factors[49]) to be 1. This is why, in particular, we have $x^0 = 1$ for each $x \in \mathbb{R}$. (Indeed, x^m is defined as $\underbrace{xx\cdots x}_{m \text{ times}}$ whenever $m \in \mathbb{N}$ and $x \in \mathbb{R}$. Thus, $x^0 = \underbrace{xx\cdots x}_{0 \text{ times}} = (\text{empty product}) = 1$.)

1.2.5. The sums $1^k + 2^k + ... + n^k$

Let us now go back to Theorem 1.2.1. That theorem gave an explicit formula for the sum of the first n positive integers. A similar formula exists for the sum of the squares of the first n positive integers:

[49] The analogue of "addend" in a finite product is "factor".

Proposition 1.2.8. Let $n \in \mathbb{N}$. Then,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n\,(n+1)\,(2n+1)}{6}.$$

Proof of Proposition 1.2.8 (sketched). Again, this can be shown by a straightforward induction (LTTR). □

Is there a picture proof for Proposition 1.2.8 as well, similar to the one we gave for Theorem 1.2.1? Yes, and even several, but they are more complicated. A proof using plane "geometry" can be found in [UspHea39, §I.3], while a "three-dimensional" proof can be found in [Siu84]. In truth, both of these proofs are combinatorial arguments in geometric disguises (thus the quotation marks).

Some more combinatorial proofs of Proposition 1.2.8 can be found in the math.stackexchange thread `https://math.stackexchange.com/questions/95047/` .

Note that a direct imitation of our second proof of Theorem 1.2.1 does not work: The numbers $1^2 + n^2$, $2^2 + (n-1)^2$, $\ldots$, $n^2 + 1^2$ are not equal, and I don't know of a way to reorder the addends in the (expanded) sum $6 \cdot \left(1^2 + 2^2 + \cdots + n^2\right)$ to obtain $n\,(n+1)\,(2n+1)$.

Next, let us sum the cubes of the first n positive integers:

Proposition 1.2.9. Let $n \in \mathbb{N}$. Then,

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2\,(n+1)^2}{4}.$$

Proof of Proposition 1.2.9 (sketched). Again, a straightforward induction does the trick (LTTR). □

Alternatively, a combinatorial proof can be found in `https://math.stackexchange.com/a/95055` . Note that this combinatorial proof relies on counting 4-tuples of numbers. If we tried to visualize this proof as a "picture proof" (along the vein of our third proof of Theorem 1.2.1), then it would require 4-dimensional pictures, which would not be very easy to draw (to put it mildly). But the combinatorics is perfectly clear in any number of dimensions.

Now, a **question** suggests itself: Are Theorem 1.2.1, Proposition 1.2.8 and Proposition 1.2.9 just the first three pieces in a sequence of formulas? In other words, given a positive integer k, is there an explicit formula for $1^k + 2^k + \cdots + n^k$? Having seen the answers for $k = 1$, $k = 2$ and $k = 3$, we would expect the right hand side of such a formula to be a $(k+1)$-st degree polynomial in n.

Let us first reword the question. Recall (from Subsection 1.2.2) that we are using the shorthand notation

$$\sum_{i=p}^{q} a_i \qquad \text{for} \qquad \sum_{i \in \{p, p+1, \ldots, q\}} a_i = a_p + a_{p+1} + \cdots + a_q$$

whenever p and q are two integers and $a_p, a_{p+1}, \ldots, a_q$ are arbitrary numbers. Thus, the sum that we are interested in, namely $1^k + 2^k + \cdots + n^k$, can be rewritten as $\sum_{i=1}^{n} i^k$.

Let us list the answers to our question for small values of k:

$$\sum_{i=1}^{n} i^1 = \frac{n(n+1)}{2} \qquad \text{(by Theorem 1.2.1)};$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \qquad \text{(by Proposition 1.2.8)};$$

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} \qquad \text{(by Proposition 1.2.9)};$$

$$\sum_{i=1}^{n} i^4 = \frac{n(2n+1)(n+1)\left(3n+3n^2-1\right)}{30};$$

$$\sum_{i=1}^{n} i^5 = \frac{n^2(n+1)^2\left(2n+2n^2-1\right)}{12};$$

$$\cdots.$$

(We can prove each of these formulas by induction on n once we know how it looks like.) For now, we don't see much of a pattern. However, there is one – once we rewrite the right hand sides in terms of *binomial coefficients*. We will give a more general definition of binomial coefficients later, but for now let us just set

$$\binom{m}{k} = \frac{m(m-1)(m-2)\cdots(m-k+1)}{k(k-1)(k-2)\cdots 1} \tag{41}$$

for all $m \in \mathbb{R}$ and $k \in \mathbb{N}$. (Here, on the right hand side, the numerator is a product of k factors, the first of which is m and which decrease by 1 from each factor to the next; the denominator is a similar product, but starting at k instead of m.) Furthermore, if k and m are two nonnegative integers, then let us use the notation $\operatorname{sur}(k,i)$ for the # of all surjective maps from $[k]$ to $[i]$. (Recall that $[k]$ stands for $\{1,2,\ldots,k\}$; in particular, $[0] = \varnothing$.) Now, we can answer our question by the following formula:

Theorem 1.2.10. Let $n \in \mathbb{N}$, and let k be a positive integer. Then,

$$\sum_{i=1}^{n} i^k = \sum_{i=0}^{k} \operatorname{sur}(k,i) \cdot \binom{n+1}{i+1}.$$

We will prove this theorem in Section 2.5. For now, let us say a few things about it.

First of all, why does Theorem 1.2.10 answer our question? Why does its right hand side count as an explicit answer? Didn't we just rewrite a finite sum as another finite sum (a more complicated one to boot)? In a sense, yes; however, if k is fixed, then the sum on the right hand side has a fixed number of addends (namely, $k+1$), so it can indeed count as explicit, whereas the left hand side has n addends. To illustrate this point, let us see how Proposition 1.2.8 can be straightforwardly recovered from Theorem 1.2.10.

We will need to know the numbers $\operatorname{sur}(2,i)$ for all $i \in \{0,1,2\}$, so let us agree on a notation for maps between finite sets:

Definition 1.2.11. Let X be a finite set, and let Y be any set. Assume that $X = \{x_1, x_2, \ldots, x_k\}$ for some distinct elements $x_1, x_2, \ldots, x_k$. Let $y_1, y_2, \ldots, y_k$ be any k elements of Y (not necessarily distinct). Then, the map from X to Y that sends $x_1, x_2, \ldots, x_k$ to $y_1, y_2, \ldots, y_k$, respectively, will be called $\begin{pmatrix} x_1 & x_2 & \cdots & x_k \\ y_1 & y_2 & \cdots & y_k \end{pmatrix}$.

This is called the *two-line notation* for maps.

For example, if $X = \{1,2,3\}$ and $Y = \mathbb{Z}$, then the map that sends each $m \in X$ to $m^2 \in \mathbb{Z}$ can be written as $\begin{pmatrix} 1 & 2 & 3 \\ 1^2 & 2^2 & 3^2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix}$ in two-line notation. It can also be written as $\begin{pmatrix} 2 & 1 & 3 \\ 4 & 1 & 9 \end{pmatrix}$ and in four other ways, since we have freedom to decide in which order we list the elements of X.

The two-line notation makes it easy to see whether a map is injective or surjective:

Remark 1.2.12. Let $f : X \to Y$ be a map between two sets X and Y, where X is finite. Assume that $X = \{x_1, x_2, \ldots, x_k\}$ for some distinct elements $x_1, x_2, \ldots, x_k$. Assume that f is written as $\begin{pmatrix} x_1 & x_2 & \cdots & x_k \\ y_1 & y_2 & \cdots & y_k \end{pmatrix}$ in two-line notation. Then:

(a) The map f is injective if and only if $y_1, y_2, \ldots, y_k$ are distinct.

(b) The map f is surjective if and only if $Y = \{y_1, y_2, \ldots, y_k\}$.

With this in hand, we can easily compute $\operatorname{sur}(2,0)$, $\operatorname{sur}(2,1)$ and $\operatorname{sur}(2,2)$:

- There exist no maps $[2] \to [0]$ (since $[0] = \varnothing$ is the empty set, so there is nowhere to map $1 \in [2]$ to). Thus, a fortiori, there exist no surjective maps $[2] \to [0]$. Hence, $\operatorname{sur}(2,0) = 0$. (Similarly, $\operatorname{sur}(k,0) = 0$ for all $k > 0$.)
- There is only one map $[2] \to [1]$, namely the map that sends both 1 and 2 to 1. (In two-line notation, it is written as $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$.) This map is surjective. Hence, there is exactly 1 surjective map $[2] \to [1]$. Hence, $\operatorname{sur}(2,1) = 1$. (Similarly, $\operatorname{sur}(k,1) = 1$ for all $k > 0$.)

- There are four maps $[2] \to [2]$. In two-line notation, they are written as $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$. The second and the third among them are surjective (since $\{1,2\}$ and $\{2,1\}$ both equal $[2]$), whereas the first and the fourth are not. Hence, there are exactly 2 surjective maps $[2] \to [2]$. Hence, $\operatorname{sur}(2,2) = 2$.

Now, we can apply Theorem 1.2.10 to $k = 2$, and conclude that

$$\begin{aligned}
\sum_{i=1}^{n} i^2 &= \sum_{i=0}^{2} \operatorname{sur}(2,i) \cdot \binom{n+1}{i+1} \\
&= \underbrace{\operatorname{sur}(2,0)}_{=0} \cdot \underbrace{\binom{n+1}{0+1}}_{\substack{=\binom{n+1}{1}=\frac{n+1}{1} \\ \text{(by (41), applied} \\ \text{to } m=n+1 \text{ and } k=1)}} + \underbrace{\operatorname{sur}(2,1)}_{=1} \cdot \underbrace{\binom{n+1}{1+1}}_{\substack{=\binom{n+1}{2}=\frac{(n+1)\,n}{2\cdot 1} \\ \text{(by (41), applied} \\ \text{to } m=n+1 \text{ and } k=2)}} \\
&\quad + \underbrace{\operatorname{sur}(2,2)}_{=2} \cdot \underbrace{\binom{n+1}{2+1}}_{\substack{=\binom{n+1}{3}=\frac{(n+1)\,n\,(n-1)}{3\cdot 2\cdot 1} \\ \text{(by (41), applied} \\ \text{to } m=n+1 \text{ and } k=3)}} \\
&= 0 \cdot \frac{n+1}{1} + 1 \cdot \frac{(n+1)\,n}{2\cdot 1} + 2 \cdot \frac{(n+1)\,n\,(n-1)}{3\cdot 2\cdot 1} \\
&= \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n \qquad \text{(after straightforward algebraic manipulations)} \\
&= \frac{n\,(n+1)\,(2n+1)}{6}
\end{aligned}$$

for each $n \in \mathbb{N}$. Thus, Proposition 1.2.8 is proven again. Similarly, we can recover Theorem 1.2.1 and Proposition 1.2.9 and similar formulas for arbitrary values of k.

Theorem 1.2.10 also confirms our suspicion that $1^k + 2^k + \cdots + n^k$ is given by a degree-$(k+1)$ polynomial in n. Indeed, it is easy to see that each of the terms $\binom{n+1}{i+1}$ on the right hand side of Theorem 1.2.10 is a degree-$(i+1)$ polynomial in n (this follows easily from (41)).

Theorem 1.2.10 is likely an old result (18th Century?). Regrettably, I don't know its ultimate origins, since it has been overshadowed by an even more explicit formula for $1^k + 2^k + \cdots + n^k$, the *Faulhaber formula* [Knuth93].

1.3. Factorials and binomial coefficients

1.3.1. Factorials

We now switch from studying sums to studying products.

Definition 1.3.1. For any $n \in \mathbb{N}$, we define a positive integer $n!$ by

$$n! = 1 \cdot 2 \cdot \cdots \cdot n.$$

(Using the product sign as defined in Definition 1.2.7, this rewrites as $n! = \prod_{i=1}^{n} i$.)

We shall refer to $n!$ as "n factorial".

We have agreed that empty products are defined to be 1. Thus, the above definition of 0! yields

$$0! = 1 \cdot 2 \cdot \cdots \cdot 0 = (\text{empty product}) = 1.$$

Definition 1.3.1 yields the following values for the first few factorials:

$$\begin{aligned}
0! &= 1, \\
1! &= 1, \\
2! &= 1 \cdot 2 = 2, \\
3! &= 1 \cdot 2 \cdot 3 = 6, \\
4! &= 1 \cdot 2 \cdot 3 \cdot 4 = 24, \\
5! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120, \\
6! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720, \\
7! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 5\,040, \\
8! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 40\,320.
\end{aligned}$$

Factorials can be computed recursively:

Proposition 1.3.2. If n is a positive integer, then $n! = (n-1)! \cdot n$.

Proof of Proposition 1.3.2. Let n be a positive integer. Then, $n - 1 \in \mathbb{N}$, so that Definition 1.3.1 yields $(n-1)! = 1 \cdot 2 \cdot \cdots \cdot (n-1)$. But Definition 1.3.1 also yields

$$n! = 1 \cdot 2 \cdot \cdots \cdot n = \underbrace{(1 \cdot 2 \cdot \cdots \cdot (n-1))}_{=(n-1)!} \cdot n = (n-1)! \cdot n.$$

This proves Proposition 1.3.2. □

Exercise 1.3.1. Let $n \in \mathbb{N}$. Prove that

$$(2n-1) \cdot (2n-3) \cdot \cdots \cdot 1 = \frac{(2n)!}{2^n n!}.$$

(The left hand side of this equality is understood to be the product of all odd integers from 1 to $2n-1$.)

1.3.2. Definition of binomial coefficients

From now on, the word "number" (as in "Let n be any number", without any further specification) will mean an integer or a rational number or a real number or a complex number, depending on the generality in which you want to work.

Let us now define binomial coefficients.

Definition 1.3.3. Let n and k be any two numbers. We define a number $\binom{n}{k}$ as follows:

- If $k \in \mathbb{N}$, then we set
$$\binom{n}{k} = \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!}. \tag{42}$$
- If $k \notin \mathbb{N}$, then we set
$$\binom{n}{k} = 0. \tag{43}$$

We call $\binom{n}{k}$ a *binomial coefficient*, and we refer to it as "*n choose k*".

This definition is standard across significant parts of the literature; in particular, it is followed in the book [GrKnPa94] (whose entire Chapter 5 is devoted to binomial coefficients), in the book [Comtet74] (one of the classics on enumerative combinatorics and binomial identities), and in [Grinbe15]. Some other authors use other definitions. All definitions I am aware of are equivalent in the "core region" of the binomial coefficients – that is, in the case when $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$. However, some definitions yield values differing from ours when $n < 0$. Many authors prefer to define $\binom{n}{k}$ only for $n \in \mathbb{N}$, or only for $k \in \mathbb{N}$, or even only in the most restrictive case (when $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$). Loehr, in [Loehr11], seems to avoid defining $\binom{n}{k}$ for negative n at all, despite this case being rather useful (as we will see soon).

Some authors use notations like C_k^n or ${}^nC_k$ or ${}_nC_k$ for $\binom{n}{k}$.

We shall later see why the words "binomial coefficient" and "choose" are appropriate for $\binom{n}{k}$.

Definition 1.3.3 does not contradict our earlier definition (41) of binomial coefficients (but merely extends it to a more general setting). Indeed, the product $k\left(k-1\right)\left(k-2\right)\cdots 1$ in the denominator of (41) is precisely the $k!$ in the denominator of (42) (since $k! = 1 \cdot 2 \cdot \cdots \cdot k = k\left(k-1\right)\left(k-2\right)\cdots 1$).

Caution: The notation $\binom{n}{k}$ for a binomial coefficient risks getting confused for the two-line notation for a map (if the domain of the map is a 1-element set) or for a column vector with 2 entries. In practice, this kind of confusion rarely happens, but its possibility should be kept in mind.

Example 1.3.4. Let us see some consequences of Definition 1.3.3.

(a) For any number n, we have

$$\begin{aligned}\binom{n}{0} &= \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-0+1\right)}{0!} \qquad \left(\text{by (42), applied to } k=0\right)\\ &= \frac{1}{1} \qquad \left(\begin{array}{l}\text{since } n\left(n-1\right)\left(n-2\right)\cdots\left(n-0+1\right) = (\text{empty product}) = 1\\ \text{and } 0! = 1\end{array}\right)\\ &= 1. \end{aligned} \tag{44}$$

(b) For any number n, we have

$$\begin{aligned}\binom{n}{1} &= \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-1+1\right)}{1!} \qquad \left(\text{by (42), applied to } k=1\right)\\ &= \frac{n}{1} \qquad \left(\text{since } n\left(n-1\right)\left(n-2\right)\cdots\left(n-1+1\right) = n \text{ and } 1! = 1\right)\\ &= n. \end{aligned} \tag{45}$$

(c) For any number n, we have

$$\begin{aligned}\binom{n}{2} &= \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-2+1\right)}{2!} \qquad \left(\text{by (42), applied to } k=2\right)\\ &= \frac{n\left(n-1\right)}{2}. \end{aligned} \tag{46}$$

(d) For any number n, we have

$$\binom{n}{3} = \frac{n\left(n-1\right)\left(n-2\right)}{3!} = \frac{n\left(n-1\right)\left(n-2\right)}{6} \qquad \left(\text{likewise}\right).$$

(e) The equality (42) (applied to $n=-1$ and $k=5$) yields

$$\begin{aligned}\binom{-1}{5} &= \frac{\left(-1\right)\left(-1-1\right)\left(-1-2\right)\cdots\left(-1-5+1\right)}{5!} = \frac{\left(-1\right)\left(-2\right)\left(-3\right)\left(-4\right)\left(-5\right)}{5!}\\ &= \frac{\left(-1\right)\left(-2\right)\left(-3\right)\left(-4\right)\left(-5\right)}{1\cdot 2\cdot 3\cdot 4\cdot 5} = -1.\end{aligned}$$

(f) More generally, for any $k \in \mathbb{N}$, we have

$$\begin{aligned}\binom{-1}{k} &= \frac{(-1)(-1-1)(-1-2)\cdots(-1-k+1)}{k!} \\ &\qquad \text{(by (42), applied to } n=-1\text{)} \\ &= \frac{(-1)(-2)\cdots(-k)}{k!} = \frac{(-1)(-2)\cdots(-k)}{1\cdot 2\cdot\cdots\cdot k} \\ &= (-1)^k \\ &= \begin{cases} 1, & \text{if } k \text{ is even;} \\ -1, & \text{if } k \text{ is odd} \end{cases}.\end{aligned} \tag{47}$$

(g) The equality (42) (applied to $n=\sqrt{2}$ and $k=2$) yields

$$\binom{\sqrt{2}}{2} = \frac{\sqrt{2}\left(\sqrt{2}-1\right)\left(\sqrt{2}-2\right)\cdots\left(\sqrt{2}-2+1\right)}{2!} = \frac{\sqrt{2}\left(\sqrt{2}-1\right)}{2}.$$

(h) The equality (43) (applied to $n=2$ and $k=\sqrt{2}$) yields

$$\binom{2}{\sqrt{2}} = 0, \qquad \text{since } \sqrt{2} \notin \mathbb{N}.$$

Remark 1.3.5. In [19f-hw0s, Exercise 2], we have introduced the notation $n^{\underline{k}}$ (called a "falling factorial") for the product $n(n-1)(n-2)\cdots(n-k+1)$ whenever n is a number and k is a nonnegative integer. Using this notation, we can rewrite the equality (42) as

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} \qquad \text{for all numbers } n \text{ and all } k \in \mathbb{N}. \tag{48}$$

Class of 2019-10-02

1.3.3. Fundamental properties of the binomial coefficients

The properties of binomial coefficients are one of the major topics in enumerative combinatorics. We shall see many of them in this text. Before we start, let us tabulate the binomial coefficients $\binom{n}{k}$ for all $n \in \{-3,-2,-1,\ldots,6\}$ and some of the $k \in \{0,1,2,3,4,5\}$. In the following table, each row corresponds to a value of

n, while each southwest-northeast diagonal corresponds to a value of k:

												$k{=}0$ ↙		$k{=}1$ ↙		$k{=}2$ ↙		$k{=}3$ ↙						
$n=-3$	$\to$											1		-3		6		-10						
$n=-2$	$\to$										1		-2		3		-4							
$n=-1$	$\to$									1		-1		1		-1		1						
$n=0$	$\to$								1		0		0		0		0							
$n=1$	$\to$							1		1		0		0		0		0						
$n=2$	$\to$						1		2		1		0		0		0							
$n=3$	$\to$					1		3		3		1		0		0		0						
$n=4$	$\to$				1		4		6		4		1		0		0							
$n=5$	$\to$			1		5		10		10		5		1		0		0						
$n=6$	$\to$	1		6		15		20		15		6		1		0								

Just by staring at this table, you will discover many properties of $\binom{n}{k}$. For example, all the zeroes in the right half of it suggest the following fact:

Proposition 1.3.6. Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$ be such that $k > n$. Then, $\binom{n}{k} = 0$.

Proof of Proposition 1.3.6. If $k \notin \mathbb{N}$, then this follows immediately from (43). Thus, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$. Hence, (42) yields

$$\binom{n}{k} = \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!}. \tag{49}$$

But $n \in \{0, 1, \ldots, k-1\}$ (since $n \in \mathbb{N}$ and $k \in \mathbb{N}$ and $k > n$). Hence, one of the factors of the product $n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)$ is $n - n = 0$. Therefore, the product $n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)$ must be 0 (because if one of the factors of a product is 0, then the whole product is 0). Thus, (49) rewrites as $\binom{n}{k} = \frac{0}{k!}$. In other words, $\binom{n}{k} = 0$. This proves Proposition 1.3.6. □

This proof might remind you of the math joke "simplify $\left(x-a\right)\left(x-b\right)\cdots\left(x-z\right)$". [50]

Note that Proposition 1.3.6 no longer holds if we drop the requirement $n \in \mathbb{N}$. For example, $1 > 1/2$, yet $\binom{1/2}{1} = 1/2 \neq 0$. For another example, $1 > -1$, yet $\binom{-1}{1} = -1 \neq 0$.

[50] Answer: 0, because the third factor from the right is $x - x = 0$.

Another pattern that you might guess from the table above is that the binomial coefficients in the "negative rows" (i.e., corresponding to $n = -1$, $n = -2$ and further above) repeat the ones you find in the nonnegative rows up to sign. More precisely:

Proposition 1.3.7 (Upper negation formula)**.** Let $n \in \mathbb{R}$ and $k \in \mathbb{Z}$. Then,

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}. \tag{50}$$

Proof of Proposition 1.3.7. We must be in one of the following two cases:

Case 1: We have $k \notin \mathbb{N}$.

Case 2: We have $k \in \mathbb{N}$.

Let us first consider Case 1. In this case, we have $k \notin \mathbb{N}$. Thus, both binomial coefficients $\binom{-n}{k}$ and $\binom{n+k-1}{k}$ equal 0 (by applying (43)). Hence, the equality (50) rewrites as $0 = (-1)^k \cdot 0$, which is clearly true. Thus, we have proven (50) in Case 1. In other words, Proposition 1.3.7 is proven in Case 1.

Let us now consider Case 2. In this case, we have $k \in \mathbb{N}$. Thus, (42) (applied to $-n$ instead of n) yields

$$\binom{-n}{k} = \frac{(-n)(-n-1)(-n-2)\cdots(-n-k+1)}{k!}. \tag{51}$$

Now, let us rewrite the numerator on the right hand side:

$$\begin{aligned}
&(-n)(-n-1)(-n-2)\cdots(-n-k+1) \\
&= (-1)^k \cdot \underbrace{(n(n+1)(n+2)\cdots(n+k-1))}_{\substack{=(n+k-1)(n+k-2)(n+k-3)\cdots n \\ \text{(here, we have turned the product around)}}} \\
&\qquad \text{(here, we have factored out a } -1 \text{ from each of the } k \text{ factors)} \\
&= (-1)^k \cdot ((n+k-1)(n+k-2)(n+k-3)\cdots n).
\end{aligned}$$

Thus, (51) rewrites as

$$\binom{-n}{k} = \frac{(-1)^k \cdot ((n+k-1)(n+k-2)(n+k-3)\cdots n)}{k!}. \tag{52}$$

On the other hand, (42) (applied to $n+k-1$ instead of n) yields

$$\begin{aligned}
\binom{n+k-1}{k} &= \frac{(n+k-1)(n+k-2)(n+k-3)\cdots(n+k-1-k+1)}{k!} \\
&= \frac{(n+k-1)(n+k-2)(n+k-3)\cdots n}{k!}.
\end{aligned}$$

Multiplying this equality by $(-1)^k$, we find

$$(-1)^k \binom{n+k-1}{k} = (-1)^k \cdot \frac{(n+k-1)(n+k-2)(n+k-3)\cdots n}{k!}$$
$$= \frac{(-1)^k \cdot ((n+k-1)(n+k-2)(n+k-3)\cdots n)}{k!}.$$

Comparing this with (52), we obtain $\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}$. Thus, Proposition 1.3.7 is proven in Case 2. □

Proposition 1.3.7 and Proposition 1.3.6 show that much of our above table of binomial coefficients is redundant. In order to know all $\binom{n}{k}$ with $n \in \mathbb{Z}$ and $k \in \mathbb{N}$, it suffices to tabulate the values $\binom{n}{k}$ for $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$. Let us do this here for $n \in \{0, 1, \ldots, 8\}$:

										$k{=}0$ ↙										
$n=0$	$\to$								1		$k{=}1$ ↙									
$n=1$	$\to$							1		1		$k{=}2$ ↙								
$n=2$	$\to$						1		2		1		$k{=}3$ ↙							
$n=3$	$\to$					1		3		3		1		$k{=}4$ ↙						
$n=4$	$\to$				1		4		6		4		1		$k{=}5$ ↙					
$n=5$	$\to$			1		5		10		10		5		1		$k{=}6$ ↙				
$n=6$	$\to$		1		6		15		20		15		6		1		$k{=}7$ ↙			
$n=7$	$\to$	1		7		21		35		35		21		7		1				
$n=8$	$\to$	1		8		28		56		70		56		28		8		1		

This table is called *Pascal's triangle* due to its triangular form.

One of the most fundamental properties of Pascal's triangle is that each number in it is the sum of the two numbers above it (i.e., the number above-left from it, and the number above-right from it). For example, $56 = 21 + 35$. This holds even for the 1's on the sides of the triangle, if you extend the triangle to include the binomial coefficients $\binom{n}{k}$ with $n < 0$ or $k < 0$ or $k < n$. More generally, this holds for all binomial coefficients $\binom{n}{k}$ – not just for the ones that fit in Pascal's triangle:

Theorem 1.3.8 (Recurrence of the binomial coefficients)**.** Let $n \in \mathbb{R}$ and $k \in \mathbb{R}$. Then,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Proof of Theorem 1.3.8. We are in one of the following three cases:

Case 1: We have $k \in \{1, 2, 3, \ldots\}$.

Case 2: We have $k = 0$.

Case 3: We have $k \notin \mathbb{N}$.

(There are no other cases, because each $k \in \mathbb{N}$ fits either into Case 1 or into Case 2, whereas each $k \notin \mathbb{N}$ fits into Case 3.)

Let us first consider Case 3. In this case, we have $k \notin \mathbb{N}$. Hence, $k-1 \notin \mathbb{N}$. Thus, an application of (43) shows that $\binom{n-1}{k-1} = 0$. Likewise, from $k \notin \mathbb{N}$, we obtain $\binom{n}{k} = 0$ and $\binom{n-1}{k} = 0$. But we must prove the equality $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. In view of the three equalities we just showed ($\binom{n-1}{k-1} = 0$ and $\binom{n}{k} = 0$ and $\binom{n-1}{k} = 0$), this rewrites as $0 = 0 + 0$, which of course is true. Thus, Theorem 1.3.8 is proven in Case 3.

Let us next consider Case 2. In this case, we have $k = 0$. Thus, $\binom{n}{k} = \binom{n}{0} = 1$ (by (44)). Likewise, $\binom{n-1}{k} = 1$. Also, $\underbrace{k}_{=0} - 1 = -1 \notin \mathbb{N}$, and thus $\binom{n-1}{k-1} = 0$ (by an application of (43)). But we must prove the equality $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. In view of the three equalities we just showed ($\binom{n-1}{k-1} = 0$ and $\binom{n}{k} = 1$ and $\binom{n-1}{k} = 1$), this rewrites as $1 = 0 + 1$, which of course is true. Thus, Theorem 1.3.8 is proven in Case 2.

Let us finally consider Case 1. In this case, we have $k \in \{1, 2, 3, \ldots\}$. Hence, Proposition 1.3.2 yields $k! = (k-1)! \cdot k$. Furthermore, both k and $k-1$ belong to $\mathbb{N}$ (since $k \in \{1, 2, 3, \ldots\}$). Hence, all three binomial coefficients $\binom{n}{k}$ and $\binom{n-1}{k}$ and $\binom{n-1}{k-1}$ are defined using the formula (42) (applied to the appropriate num-

bers). Explicitly:

$$\begin{aligned}\binom{n}{k} &= \frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{k!} \\ &= \frac{n\,(n-1)\,(n-2)\cdots(n-k+1)}{(k-1)!\cdot k} \\ &\qquad\qquad (\text{since } k! = (k-1)!\cdot k)\end{aligned} \tag{53}$$

and

$$\begin{aligned}\binom{n-1}{k} &= \frac{(n-1)\,(n-2)\,(n-3)\cdots((n-1)-k+1)}{k!} \\ &= \frac{(n-1)\,(n-2)\,(n-3)\cdots(n-k)}{k!} \\ &= \frac{((n-1)\,(n-2)\,(n-3)\cdots(n-k+1))\cdot(n-k)}{k!} \\ &= \frac{((n-1)\,(n-2)\,(n-3)\cdots(n-k+1))\cdot(n-k)}{(k-1)!\cdot k} \\ &\qquad\qquad (\text{since } k! = (k-1)!\cdot k) \\ &= \frac{(n-1)\,(n-2)\,(n-3)\cdots(n-k+1)}{(k-1)!}\cdot\frac{n-k}{k}\end{aligned} \tag{54}$$

and

$$\begin{aligned}\binom{n-1}{k-1} &= \frac{(n-1)\,(n-2)\,(n-3)\cdots((n-1)-(k-1)+1)}{(k-1)!} \\ &= \frac{(n-1)\,(n-2)\,(n-3)\cdots(n-k+1)}{(k-1)!}.\end{aligned} \tag{55}$$

Adding the equalities (55) and (54) together, we obtain

$$\begin{aligned}
&\binom{n-1}{k-1} + \binom{n-1}{k} \\
&= \frac{(n-1)(n-2)(n-3)\cdots(n-k+1)}{(k-1)!} + \frac{(n-1)(n-2)(n-3)\cdots(n-k+1)}{(k-1)!} \cdot \frac{n-k}{k} \\
&= \frac{(n-1)(n-2)(n-3)\cdots(n-k+1)}{(k-1)!} \underbrace{\left(1 + \frac{n-k}{k}\right)}_{=\frac{n}{k}} \\
&= \frac{(n-1)(n-2)(n-3)\cdots(n-k+1)}{(k-1)!} \cdot \frac{n}{k} \\
&= \frac{n \cdot ((n-1)(n-2)(n-3)\cdots(n-k+1))}{(k-1)! \cdot k} \\
&= \frac{n(n-1)(n-2)(n-3)\cdots(n-k+1)}{(k-1)! \cdot k} \\
&= \frac{n(n-1)(n-2)(n-3)\cdots(n-k+1)}{k!} \qquad (\text{since } (k-1)! \cdot k = k!); \\
&= \binom{n}{k} \qquad (\text{by (53)}).
\end{aligned}$$

Thus, Theorem 1.3.8 is proven in Case 1 as well.

We have thus proven Theorem 1.3.8 in all three Cases 1, 2 and 3. □

The Wikipedia page for Pascal's triangle includes many pictures of Pascal's triangle as well as numerous remarkable properties.

Theorem 1.3.9 (Factorial formula for the binomial coefficients)**.** Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ be such that $k \leq n$. Then,

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Proof of Theorem 1.3.9. Multiplying the equality (42) with $k! \cdot (n-k)!$, we obtain

$$\begin{aligned}
k! \cdot (n-k)! \cdot \binom{n}{k} &= k! \cdot (n-k)! \cdot \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \\
&= \underbrace{(n-k)!}_{\substack{=1\cdot 2\cdot\cdots\cdot(n-k) \\ \text{(by the definition of } (n-k)!)}} \cdot \underbrace{(n(n-1)(n-2)\cdots(n-k+1))}_{\substack{=(n-k+1)\cdot(n-k+2)\cdot\cdots\cdot n \\ \text{(here, we have turned the product around)}}} \\
&= (1 \cdot 2 \cdot \cdots \cdot (n-k)) \cdot ((n-k+1) \cdot (n-k+2) \cdot \cdots \cdot n) \\
&= 1 \cdot 2 \cdot \cdots \cdot n = n!
\end{aligned}$$

(since $n!$ is defined to be $1 \cdot 2 \cdot \cdots \cdot n$). Solving this for $\binom{n}{k}$, we find $\binom{n}{k} = \dfrac{n!}{k! \cdot (n-k)!}$. This proves Theorem 1.3.9. $\square$

Warning: When it applies, Theorem 1.3.9 provides a simple and highly convenient formula for $\binom{n}{k}$. However, Theorem 1.3.9 only applies when $n \in \mathbb{N}$ and $k \in \mathbb{N}$ and $k \leq n$. Thus, you cannot use Theorem 1.3.9 to compute $\binom{-3}{5}$ or $\binom{1/3}{4}$ or $\binom{\pi}{\sqrt{2}}$. (There is a generalization of the factorial called the Gamma function, which does not really alleviate this problem: it would make the right hand side of Theorem 1.3.9 well-defined most of the time, but the equality would still not be true in general.)

Some authors use Theorem 1.3.9 as a **definition** of $\binom{n}{k}$. But, as we just saw, such a definition would only work in the case when $n \in \mathbb{N}$ and $k \in \mathbb{N}$ and $k \leq n$, so it lacks the general applicability of our definition of $\binom{n}{k}$.

Lemma 1.3.10. Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$ be such that $k \notin \{0, 1, \ldots, n\}$. Then, $\binom{n}{k} = 0$.

Proof of Lemma 1.3.10. If $k \notin \mathbb{N}$, then the claim (that $\binom{n}{k} = 0$) follows immediately from (43). Thus, for the rest of this proof, we WLOG assume that we do have $k \in \mathbb{N}$. Combining this with $k \notin \{0, 1, \ldots, n\}$, we obtain $k \in \mathbb{N} \setminus \{0, 1, \ldots, n\} = \{n+1, n+2, n+3, \ldots\}$. Hence, $k \geq n+1 > n$. Thus, Proposition 1.3.6 yields $\binom{n}{k} = 0$. This proves Lemma 1.3.10. $\square$

Theorem 1.3.11 (Symmetry of the binomial coefficients)**.** Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$. Then,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Proof of Theorem 1.3.11. We are in one of the following two cases:

Case 1: We have $k \in \{0, 1, \ldots, n\}$.

Case 2: We have $k \notin \{0, 1, \ldots, n\}$.

Let us first consider Case 1. In this case, we have $k \in \{0, 1, \ldots, n\}$, so that $n - k \in \{0, 1, \ldots, n\}$ as well. Now, Theorem 1.3.9 yields

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Meanwhile, Theorem 1.3.9 (applied to $n-k$ instead of k) yields

$$\binom{n}{n-k} = \frac{n!}{(n-k)! \cdot (n-(n-k))!} \qquad (\text{since } n-k \in \{0,1,\ldots,n\})$$
$$= \frac{n!}{(n-(n-k))! \cdot (n-k)!} = \frac{n!}{k! \cdot (n-k)!}$$

(since $n-(n-k)=k$). Comparing these two equalities, we obtain $\binom{n}{k} = \binom{n}{n-k}$. Thus, Theorem 1.3.11 is proven in Case 1.

Let us now consider Case 2. In this case, we have $k \notin \{0,1,\ldots,n\}$. Hence, we have $n-k \notin \{0,1,\ldots,n\}$ as well[51]. Thus, Lemma 1.3.10 (applied to $n-k$ instead of k) yields $\binom{n}{n-k} = 0$. But Lemma 1.3.10 also yields $\binom{n}{k} = 0$. Comparing these two equalities, we obtain $\binom{n}{k} = \binom{n}{n-k}$. Thus, Theorem 1.3.11 is proven in Case 2.

We have now proven Theorem 1.3.11 in both possible cases. □

Theorem 1.3.11 is known as the *symmetry of binomial coefficients* or the *symmetry of Pascal's triangle*.

Warning: Theorem 1.3.11 does not hold for negative n. For example, $\binom{-1}{1} = -1$ does not equal $\binom{-1}{(-1)-1} = \binom{-1}{-2} = 0$.

Exercise 1.3.2. Let $n \in \mathbb{N}$. Prove that $\binom{n}{n} = 1$.

Class of 2019-10-04

1.3.4. Binomial coefficients count subsets

The following theorem is one of the central properties of binomial coefficients:

Theorem 1.3.12 (Combinatorial interpretation of the binomial coefficients)**.** Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$. Let S be an n-element set. Then,

$$\binom{n}{k} = (\#\text{ of } k\text{-element subsets of } S).$$

[51] because otherwise, we would have $n-k \in \{0,1,\ldots,n\}$ and thus $n-(n-k) \in \{0,1,\ldots,n\}$, which would contradict $n-(n-k) = k \notin \{0,1,\ldots,n\}$

Example 1.3.13. (a) Let $n = 4$ and $k = 2$ and $S = \{1,2,3,4\}$. Then, the 2-element subsets of S are $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$ and $\{3,4\}$. The # of these subsets is $6 = \binom{4}{2}$, which is exactly what Theorem 1.3.12 predicts.

(b) Now, let $k = 5$ instead (while n is still 4, and S is still $\{1,2,3,4\}$). Then, there are no 5-element subsets of S, since S only has 4 elements. Thus, the # of these 5-element subsets is $0 = \binom{4}{5}$, which is exactly what Theorem 1.3.12 predicts.

Theorem 1.3.12 is the reason why $\binom{n}{k}$ is called "n choose k": It is the number of ways to **choose** k distinct elements (without an order) from n given elements. The k-element subsets of S are called the *k-combinations* of S.

Warning: Theorem 1.3.12 says nothing about $\binom{n}{k}$ when $n \notin \mathbb{N}$.

Before we prove Theorem 1.3.12, let us state a simple lemma:

Lemma 1.3.14. Let $k \in \mathbb{R}$. Then, $\binom{0}{k} = [k = 0]$.

Here, we are using the so-called *Iverson bracket notation*:

Definition 1.3.15. If $\mathcal{A}$ is any logical statement, then we define an integer $[\mathcal{A}] \in \{0,1\}$ by

$$[\mathcal{A}] = \begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases}.$$

For example, $[1+1=2] = 1$ (since $1+1=2$ is true), whereas $[1+1=1] = 0$ (since $1+1=1$ is false).

If $\mathcal{A}$ is any logical statement, then the integer $[\mathcal{A}]$ is known as the *truth value* of $\mathcal{A}$.

Proof of Lemma 1.3.14. From (44), we obtain $\binom{0}{0} = 1$. But $[0=0] = 1$ (since $0=0$ is true). Comparing these two equalities, we obtain $\binom{0}{0} = [0=0]$. This shows that Lemma 1.3.14 is true for $k = 0$. Hence, for the rest of this proof, we WLOG assume that $k \neq 0$. Thus, the statement $k = 0$ is false. Hence, $[k=0] = 0$. On the other hand, from $k \neq 0$, we obtain $k \notin \{0\} = \{0,1,\ldots,0\}$. Therefore, Lemma 1.3.10 (applied to $n = 0$) yields $\binom{0}{k} = 0$. Comparing this with $[k=0] = 0$, we obtain $\binom{0}{k} = [k=0]$. This proves Lemma 1.3.14. □

Proof of Theorem 1.3.12. Forget that we fixed n, k and S. (This means that instead of considering n and k as fixed numbers and S as a fixed set, we imagine that Theorem

1.3.12 begins with the words "For all $n \in \mathbb{N}$ and $k \in \mathbb{R}$ and any n-element set S". Thus we are proving the same theorem, but we have the freedom to change our value of k in the proof.)

We proceed by induction on n:

Induction base: If S is a 0-element set, then $S = \varnothing$ and thus

$$\begin{aligned}
&(\#\text{ of } k\text{-element subsets of } S) \\
&= (\#\text{ of } k\text{-element subsets of } \varnothing) \\
&= \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases} \qquad \left(\begin{array}{c} \text{since the empty set } \varnothing \text{ has only one subset,} \\ \text{namely the 0-element subset } \varnothing \end{array} \right) \\
&= [k = 0] \qquad \left(\text{since the definition of } [k = 0] \text{ yields } [k = 0] = \begin{cases} 1, & \text{if } k = 0; \\ 0, & \text{if } k \neq 0 \end{cases} \right) \\
&= \binom{0}{k} \qquad (\text{by Lemma 1.3.14})
\end{aligned}$$

for each $k \in \mathbb{R}$. In other words, for any $k \in \mathbb{R}$ and any 0-element set S, we have $\binom{0}{k} = (\#\text{ of } k\text{-element subsets of } S)$. Thus, Theorem 1.3.12 is proven for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume (as the induction hypothesis) that Theorem 1.3.12 holds for $n = m$. (This means "for $n = m$ and for all values of $k \in \mathbb{R}$ and all n-element sets S", because k and S are not fixed. This is important, since we will later apply the induction hypothesis to two different values of k.)

Let $k \in \mathbb{R}$. Let S be an $(m+1)$-element set. We must prove that

$$\binom{m+1}{k} = (\#\text{ of } k\text{-element subsets of } S)\,.$$

The set S is an $(m+1)$-element set; thus, its size is $|S| = m + 1 \geq 1 > 0$. Hence, the set S is nonempty, i.e., there exists a $t \in S$. Fix such a t.

Now, we shall call a subset of S

- **red** if it contains t, and
- **green** if it does not contain t.

Thus, each subset of S is either red or green (but not both at the same time). Thus, by the sum rule, we have

$$\begin{aligned}
&(\#\text{ of } k\text{-element subsets of } S) \\
&= (\#\text{ of } k\text{-element red subsets of } S) + (\#\text{ of } k\text{-element green subsets of } S)\,.
\end{aligned}$$

We shall now compute the two addends on the right hand side.

The green subsets of S are the subsets of S that don't contain t. In other words, the green subsets of S are exactly the subsets of $S \setminus \{t\}$. Hence,

$$\begin{aligned}&(\#\text{ of } k\text{-element green subsets of } S)\\ &= (\#\text{ of } k\text{-element subsets of } S \setminus \{t\})\,. \end{aligned} \tag{56}$$

But S is an $(m+1)$-element set, and thus $S \setminus \{t\}$ is an m-element set (since $t \in S$). Hence, our induction hypothesis shows that Theorem 1.3.12 can be applied to m and $S \setminus \{t\}$ instead of n and S. We thus obtain

$$\binom{m}{k} = (\#\text{ of } k\text{-element subsets of } S \setminus \{t\})\,.$$

Comparing this with (56), we find

$$(\#\text{ of } k\text{-element green subsets of } S) = \binom{m}{k}. \tag{57}$$

What about the red subsets?

Informally, a similar argument works: The red subsets of S are not exactly the subsets of $S \setminus \{t\}$, but they "correspond to" the latter in a specific way. Namely, since the red subsets of S are required to contain t, the only "information" that a red subset of S really "carries" is what other elements (other than t) it contains. In other words, each red subset R of S "corresponds to" the subset $R \setminus \{t\}$ of $S \setminus \{t\}$. Note that this correspondence changes the size of the subset: Namely, if R was a k-element red subset of S, then $R \setminus \{t\}$ will be a $(k-1)$-element subset of $S \setminus \{t\}$. Thus, the k-element red subsets of S "correspond to" the $(k-1)$-element subsets of $S \setminus \{t\}$.

Formally, this can be restated as follows: The map

$$\begin{aligned} f : \{k\text{-element red subsets of } S\} &\to \{(k-1)\text{-element subsets of } S \setminus \{t\}\}\,,\\ R &\mapsto R \setminus \{t\} \end{aligned}$$

is well-defined and is a bijection. (Indeed, its inverse is

$$\begin{aligned} g : \{(k-1)\text{-element subsets of } S \setminus \{t\}\} &\to \{k\text{-element red subsets of } S\}\,,\\ P &\mapsto P \cup \{t\}\,. \end{aligned}$$

It is easy to verify that both the map f and its alleged inverse g are well-defined[52], and are indeed mutually inverse[53].) Therefore, the bijection principle (applied to

[52] This means proving the following claims:

- If R is any k-element red subset of S, then $R \setminus \{t\}$ is a $(k-1)$-element subset of $S \setminus \{t\}$.
- If P is any $(k-1)$-element subset of $S \setminus \{t\}$, then $P \cup \{t\}$ is a k-element red subset of S.

Both of these are simple exercises in set-theoretic basics.

[53] This means proving the following claims:

the bijection f) yields

$$\begin{aligned}&|\{k\text{-element red subsets of } S\}|\\&= |\{(k-1)\text{-element subsets of } S \setminus \{t\}\}|\,.\end{aligned}$$

In other words,

$$\begin{aligned}&(\#\text{ of } k\text{-element red subsets of } S)\\&= (\#\text{ of } (k-1)\text{-element subsets of } S \setminus \{t\})\,.\end{aligned} \tag{58}$$

But $S \setminus \{t\}$ is an m-element set. Hence, our induction hypothesis shows that Theorem 1.3.12 can be applied to m, $k-1$ and $S \setminus \{t\}$ instead of n, k and S. We thus obtain

$$\binom{m}{k-1} = (\#\text{ of } (k-1)\text{-element subsets of } S \setminus \{t\})\,.$$

Comparing this with (58), we find

$$(\#\text{ of } k\text{-element red subsets of } S) = \binom{m}{k-1}. \tag{59}$$

Now, we can finish our computation of $(\#\text{ of } k\text{-element subsets of } S)$ that we started above:

$$\begin{aligned}&(\#\text{ of } k\text{-element subsets of } S)\\&= \underbrace{(\#\text{ of } k\text{-element red subsets of } S)}_{= \binom{m}{k-1} \text{ (by (59))}} + \underbrace{(\#\text{ of } k\text{-element green subsets of } S)}_{= \binom{m}{k} \text{ (by (57))}}\\&= \binom{m}{k-1} + \binom{m}{k}.\end{aligned} \tag{60}$$

On the other hand, Theorem 1.3.8 (applied to $n = m+1$) yields

$$\binom{m+1}{k} = \binom{(m+1)-1}{k-1} + \binom{(m+1)-1}{k} = \binom{m}{k-1} + \binom{m}{k}$$

(since $(m+1)-1 = m$). Comparing this with (60), we find

$$\binom{m+1}{k} = (\#\text{ of } k\text{-element subsets of } S)\,.$$

- If R is any k-element red subset of S, then $(R \setminus \{t\}) \cup \{t\} = R$.
- If P is any $(k-1)$-element subset of $S \setminus \{t\}$, then $(P \cup \{t\}) \setminus \{t\} = P$.

Both of these are simple exercises in set-theoretic basics.

Now, forget that we fixed k and S. We thus have shown that every $k \in \mathbb{R}$ and every $(m+1)$-element set S satisfy

$$\binom{m+1}{k} = (\#\text{ of } k\text{-element subsets of } S)\,.$$

In other words, Theorem 1.3.12 holds for $n = m+1$. This completes the induction step, and thus the proof of Theorem 1.3.12. □

Exercise 1.3.3. Prove the following rules for truth values:
(a) If $\mathcal{A}$ and $\mathcal{B}$ are two equivalent logical statements, then $[\mathcal{A}] = [\mathcal{B}]$.
(b) If $\mathcal{A}$ is any logical statement, then $[\text{not } \mathcal{A}] = 1 - [\mathcal{A}]$.
(c) If $\mathcal{A}$ and $\mathcal{B}$ are two logical statements, then $[\mathcal{A} \wedge \mathcal{B}] = [\mathcal{A}]\,[\mathcal{B}]$.
(d) If $\mathcal{A}$ and $\mathcal{B}$ are two logical statements, then $[\mathcal{A} \vee \mathcal{B}] = [\mathcal{A}] + [\mathcal{B}] - [\mathcal{A}]\,[\mathcal{B}]$.
(e) If $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are three logical statements, then

$$[\mathcal{A} \vee \mathcal{B} \vee \mathcal{C}] = [\mathcal{A}] + [\mathcal{B}] + [\mathcal{C}] - [\mathcal{A}]\,[\mathcal{B}] - [\mathcal{A}]\,[\mathcal{C}] - [\mathcal{B}]\,[\mathcal{C}] + [\mathcal{A}]\,[\mathcal{B}]\,[\mathcal{C}]\,.$$

(f) If $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k$ are k logical statements (for some $k \in \mathbb{N}$), then

$$[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_k] = [\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_k]\,.$$

(This allows for the possibility of $k = 0$, in which case the conjunction $\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_k$ should be understood as a true statement.)

1.3.5. Integrality and some arithmetic properties

All the numbers we have seen in our tables of binomial coefficients are integers. This is not a coincidence:

Theorem 1.3.16 (Integrality of the binomial coefficients)**.** Let $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$. Then, $\dbinom{n}{k} \in \mathbb{Z}$.

In order to prove this theorem, it is perhaps easiest to start with the case when $n \in \mathbb{N}$, which we can declare a lemma:

Lemma 1.3.17. Let $n \in \mathbb{N}$ and $k \in \mathbb{Z}$. Then, $\dbinom{n}{k} \in \mathbb{N}$.

Proof of Lemma 1.3.17. Let $S = \{1, 2, \ldots, n\}$. Then, S is an n-element set. Hence, Theorem 1.3.12 yields

$$\binom{n}{k} = (\#\text{ of } k\text{-element subsets of } S) = |\{\text{all } k\text{-element subsets of } S\}| \in \mathbb{N}$$

(since the size of any finite set is $\in \mathbb{N}$). This proves Lemma 1.3.17. □

Alternatively, it is not hard to prove Lemma 1.3.17 by induction on n, using Lemma 1.3.14 for the induction base and Theorem 1.3.8 for the induction step:

Exercise 1.3.4. Prove Lemma 1.3.17 without using Theorem 1.3.12.

We can now prove Theorem 1.3.16:

Proof of Theorem 1.3.16. If $n \in \mathbb{N}$, then the claim of Theorem 1.3.16 is true, because Lemma 1.3.17 yields $\binom{n}{k} \in \mathbb{N} \subseteq \mathbb{Z}$ in this case. Thus, for the rest of this proof, we WLOG assume that $n \notin \mathbb{N}$. Hence, n is a **negative** integer (since $n \in \mathbb{Z}$ but $n \notin \mathbb{N}$). Therefore, $n \leq -1$, so that $-n \geq 1$.

If $k \notin \mathbb{N}$, then the claim of Theorem 1.3.16 is true as well (since (43) yields $\binom{n}{k} = 0 \in \mathbb{Z}$ in this case). Thus, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$. Hence, $k \geq 0$.

Now, Proposition 1.3.7 (applied to $-n$ instead of n) yields

$$\binom{-(-n)}{k} = (-1)^k \binom{-n+k-1}{k}.$$

In view of $-(-n) = n$, this rewrites as

$$\binom{n}{k} = (-1)^k \binom{-n+k-1}{k}.$$

But $-n+k-1$ is an integer satisfying $\underbrace{-n}_{\geq 1} + \underbrace{k}_{\geq 0} - 1 \geq 1+0-1 = 0$. Hence, $-n+k-1 \in \mathbb{N}$. Therefore, Lemma 1.3.17 (applied to $-n+k-1$ instead of n) yields $\binom{-n+k-1}{k} \in \mathbb{N} \subseteq \mathbb{Z}$. Hence,

$$\binom{n}{k} = (-1)^k \underbrace{\binom{-n+k-1}{k}}_{\in \mathbb{Z}} \in \mathbb{Z}$$

(since multiplying an integer by $(-1)^k$ clearly results in an integer). Theorem 1.3.16 is thus proven. □

Theorem 1.3.16 tells us that the binomial coefficients $\binom{n}{k}$ are integers, as long as n and k are integers[54]. Thus, it makes sense to ask arithmetical questions about them, such as questions of divisibility and modular congruence[55]. And there is a lot to say about such questions:

[54] Of course, it suffices to assume that n is an integer, since non-integer values of k lead to $\binom{n}{k} = 0$ anyway. But we won't have much use for this generality here.

[55] See, e.g., [Hammac15, §5.2], [LeLeMe16, §9.6] or [Grinbe15, §2.2] for the definition and basic properties of modular congruence ("congruence modulo n").

Theorem 1.3.18. Let p be a prime. Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \binom{p}{k}$.

Theorem 1.3.18 says that if p is a prime, then all entries in the p-th row of Pascal's triangle (i.e., all $\binom{n}{k}$ with $n = p$) are divisible by p, except for the two entries $\binom{p}{0}$ and $\binom{p}{p}$ (which are equal to 1). This property actually characterizes primes: If $n > 1$ is a composite integer (i.e., not a prime), then at least one entry in the n-th row of Pascal's triangle (except for the entries equal to 1) is not divisible by n. For example, $\binom{4}{2} = 6$ is not divisible by 4.

We shall not prove Theorem 1.3.18 here. See, e.g., [Vorobi02, §2.9] or [19s, Theorem 2.17.19] for a proof. We shall likewise not prove the following two propositions, which provide two quick recursive algorithms for telling whether a binomial coefficient is even or odd:

Proposition 1.3.19. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Then:

(a) We have $\binom{2a}{2b} \equiv \binom{a}{b} \bmod 2$.

(b) We have $\binom{2a+1}{2b} \equiv \binom{a}{b} \bmod 2$.

(c) We have $\binom{2a}{2b+1} \equiv 0 \bmod 2$.

(d) We have $\binom{2a+1}{2b+1} \equiv \binom{a}{b} \bmod 2$.

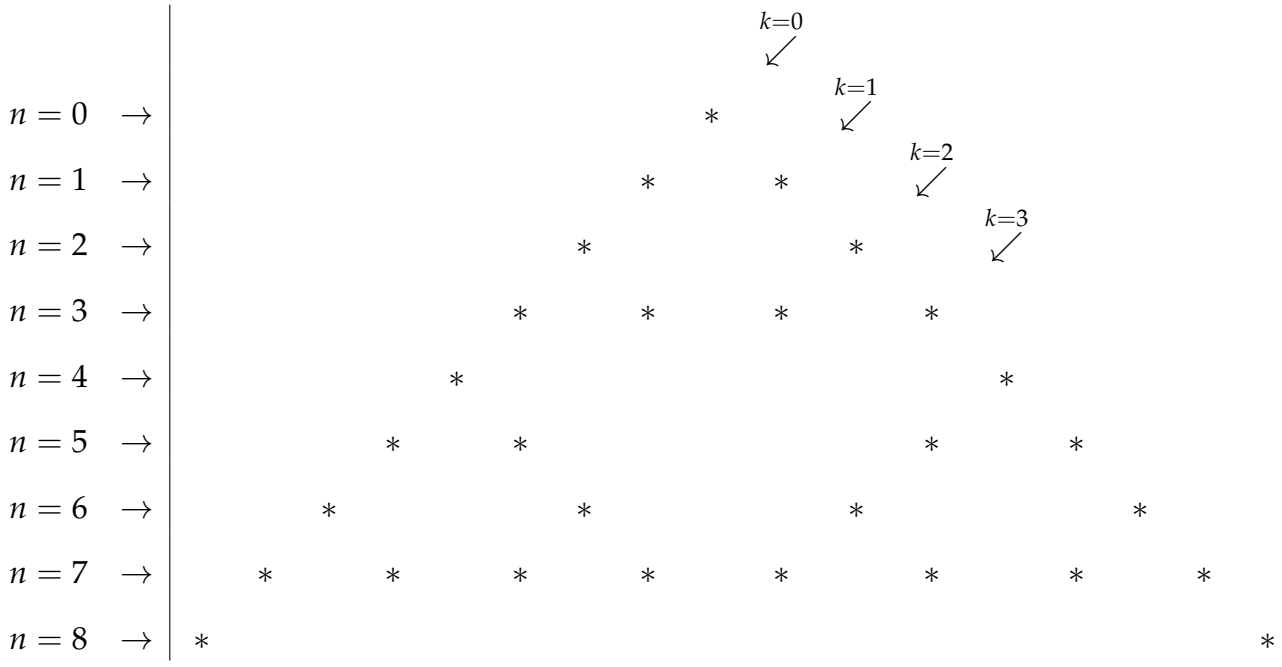
Proposition 1.3.20. Let $n \in \mathbb{N}$. Let $a, b \in \{0, 1, \ldots, 2^n - 1\}$. Then:

(a) We have $\binom{2^n + a}{b} \equiv \binom{a}{b} \bmod 2$.

(b) We have $\binom{2^n + a}{2^n + b} \equiv \binom{a}{b} \bmod 2$.

Proposition 1.3.19 appears (with proof) in [18s-hw1s, Exercise 3]; Proposition 1.3.20 appears (with proof) in [18s-hw1s, Exercise 4]. Let us briefly mention a curious consequence of these propositions, though. Consider Pascal's triangle again,

but replace every odd entry with a "$*$" and every even entry with an empty space:



If you are familiar with some fractals, you might recognize this picture as a (finite step towards) the Sierpinski triangle, with the "$*$"s corresponding to the non-removed points in the triangle. And this is indeed the case: For any $r \in \mathbb{N}$, the first 2^r rows of Pascal's triangle (i.e., the rows from $n = 0$ to $n = 2^r - 1$) form the image obtained after r steps in the construction of the Sierpinski triangle. This can be proved by induction on r, and the induction step requires understanding how the parity of the binomial coefficients $\binom{n}{k}$ with $n \in \{2^r, 2^r + 1, \ldots, 2^{r+1} - 1\}$ is connected with the parity of the binomial coefficients $\binom{n}{k}$ with $n \in \{0, 1, \ldots, 2^r - 1\}$. Proposition 1.3.20 yields an easy answer to this question.

Here are two more results we shall not prove:

Theorem 1.3.21 (Lucas's congruence)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$. Let $c, d \in \{0, 1, \ldots, p-1\}$. Then,

$$\binom{pa+c}{pb+d} \equiv \binom{a}{b}\binom{c}{d} \bmod p.$$

Theorem 1.3.22 (Babbage's congruence)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$. Then,

$$\binom{pa}{pb} \equiv \binom{a}{b} \bmod p^2.$$

Elementary proofs of Theorem 1.3.21 and Theorem 1.3.22 can be found in [Grinbe17]. Note that Theorem 1.3.21 generalizes Proposition 1.3.19.

Remark 1.3.23. Lucas's congruence has the following consequence: Let p be a prime. Let $a, b \in \mathbb{N}$. Write a and b in base p as follows:

$$a = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_0 p^0 \qquad \text{and}$$
$$b = b_k p^k + b_{k-1} p^{k-1} + \cdots + b_0 p^0$$

with $k \in \mathbb{N}$ and $a_k, a_{k-1}, \ldots, a_0, b_k, b_{k-1}, \ldots, b_0 \in \{0, 1, \ldots, p-1\}$. (Note that we allow "leading zeroes" – i.e., any of a_k and b_k can be 0.) Then,

$$\binom{a}{b} \equiv \binom{a_k}{b_k} \binom{a_{k-1}}{b_{k-1}} \cdots \binom{a_0}{b_0} \bmod p.$$

(This can be easily proven by induction on k, using Theorem 1.3.21 in the induction step.) This allows for quick computation of remainders of $\binom{a}{b}$ modulo prime numbers.

See [Mestro14] and [Granvi05] for overviews of more complicated divisibilities and congruences for binomial coefficients.

1.3.6. The binomial formula

You have likely seen the following fact:

Theorem 1.3.24 (the binomial formula)**.** Let $x, y \in \mathbb{R}$. Let $n \in \mathbb{N}$. Then,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

This is why the $\binom{n}{k}$ are called the "binomial coefficients" – they appear as coefficients in the binomial formula.

Example 1.3.25. If $n = 3$, then the claim of Theorem 1.3.24 becomes

$$\begin{aligned}(x+y)^3 &= \sum_{k=0}^{3} \binom{3}{k} x^k y^{3-k} \\ &= \underbrace{\binom{3}{0}}_{=1} \underbrace{x^0}_{=1} \underbrace{y^{3-0}}_{=y^3} + \underbrace{\binom{3}{1}}_{=3} \underbrace{x^1}_{=x} \underbrace{y^{3-1}}_{=y^2} + \underbrace{\binom{3}{2}}_{=3} x^2 \underbrace{y^{3-2}}_{=y} + \underbrace{\binom{3}{3}}_{=1} x^3 \underbrace{y^{3-3}}_{=1} \\ &= y^3 + 3xy^2 + 3x^2 y + x^3.\end{aligned}$$

Proof of Theorem 1.3.24. Let me first "simplify" the claim: I will rewrite the finite sum $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ as the **infinite** sum $\sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ (that is, a sum over **all** integers k).

In order to do so, I need to justify two things:

- I need to explain why the infinite sum $\sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ is well-defined. (We have seen why finite sums are well-defined in Subsection 1.2.2, but infinite sums are a different beast. You can easily write down nonsensical infinite sums like $\sum_{k\in\mathbb{N}} 1 = 1+1+1+\cdots$ or $\sum_{k\in\mathbb{N}} k = 0+1+2+3+\cdots$ that will quickly lead you into contradiction-land. If we want to use an infinite sum, we thus have to explain what it means.)

- I need to explain why this infinite sum equals the finite sum $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

Let me begin with the first justification: Why is the sum $\sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ well-defined?

If you think about this question very carefully, you will discover that there is another question underneath it: Why are the addends $\binom{n}{k} x^k y^{n-k}$ of this sum well-defined? This is clear when $k \in \{0,1,\ldots,n\}$, because in this case both exponents k and $n-k$ are nonnegative integers. However, if $k < 0$ or $k > n$, then one of these exponents will be negative, and this may cause trouble if x or y is 0 (because 0^j is undefined when j is negative). We fix this problem by decree: We just **decree** that an expression of the form ab is always to be understood as 0 when $a = 0$, even if b is undefined. Thus, $0 \cdot 0^{-1} = 0$, despite 0^{-1} being undefined.[56]

Having convinced ourselves that the addends of the sum $\sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ are well-defined, we can now discuss the existence of the sum itself. Let us look at the case $n = 3$. In this case, this sum has the form

$$\underbrace{\cdots+0+0+0}_{\substack{\text{addends}\\ \text{for } k<0}} + \underbrace{y^3}_{\substack{\text{addend}\\ \text{for } k=0}} + \underbrace{3xy^2}_{\substack{\text{addend}\\ \text{for } k=1}} + \underbrace{3x^2y}_{\substack{\text{addend}\\ \text{for } k=2}} + \underbrace{x^3}_{\substack{\text{addend}\\ \text{for } k=3}} + \underbrace{0+0+0+\cdots}_{\substack{\text{addends}\\ \text{for } k>3}},$$

[56] Still skeptical? Alright, there are a few more things to check. Conventions like this may lead to errors if applied improperly; for example, after having made this particular convention, we cannot also decree aa^{-1} to always equal 1 when a^{-1} is potentially undefined (since this would lead to $0 \cdot 0^{-1} = 1 \neq 0$). We need to check what exactly we are going to do with our convention. This is easy: The only situation to which we will apply our $ab = 0$ convention is when $a = 0$ and $b = x^k y^{n-k}$, and it is easy to check that the only properties we are going to use from this notation are that $x \cdot \left(ax^k y^{n-k}\right) = ax^{k+1}y^{n-k}$ and $y \cdot \left(ax^k y^{n-k}\right) = ax^k y^{n-k+1}$ and $a_1 b + a_2 b = (a_1 + a_2)\, b$; obviously, all three of these properties are true when $a = 0$ (resp. $a_1 = 0$ or $a_2 = 0$), even if the other factors are undefined.

because Lemma 1.3.10 renders all addends $\binom{n}{k} x^k y^{n-k}$ with $k \notin \{0,1,\ldots,n\}$ equal to 0. This is an infinite sum, but only finitely many of its addends are nonzero. Thus, it is clear how to give it a meaningful value: Just add the nonzero addends together and drop the zero addends. The philosophy behind this is that zero addends are not supposed to contribute to sums (no matter how many of them are present): for example, $0+0+0+0+\cdots = 0$.

The same is true for any $n \in \mathbb{N}$. Indeed, for any given $n \in \mathbb{N}$, we can easily see from Lemma 1.3.10 that the only nonzero addends in the sum $\sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}$ are the ones for which $k \in \{0,1,\ldots,n\}$ (which is not saying that all of these addends must be nonzero). Hence, this sum has only finitely many nonzero addends, and thus is well-defined.

This also explains why this sum equals the finite sum $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$: Indeed, the only difference between the infinite and the finite sum is the presence of the addends with $k \notin \{0,1,\ldots,n\}$; but these addends do not contribute anything, because they all equal 0. Hence, the two sums are equal. In other words,

$$\sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k} = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{61}$$

Thus, it remains to prove that

$$(x+y)^n = \sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k}. \tag{62}$$

We will prove (62) by induction on n:

Induction base: If $n = 0$, then both sides of the equality (62) are equal to 1 (since $(x+y)^n = (x+y)^0 = 1$ and

$$\begin{aligned}
\sum_{k\in\mathbb{Z}} \binom{n}{k} x^k y^{n-k} &= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} && \text{(by (61))} \\
&= \sum_{k=0}^{0} \binom{0}{k} x^k y^{0-k} && \text{(since } n = 0\text{)} \\
&= \underbrace{\binom{0}{0}}_{\substack{=1 \\ \text{(by (44))}}} \underbrace{x^0}_{=1} \underbrace{y^{0-0}}_{=1} = 1
\end{aligned}$$

in this case). Hence, (62) holds if $n = 0$. This completes the induction base.

Induction step: Fix $m \in \mathbb{N}$. Assume that (62) holds for $n = m$. We must prove that (62) holds for $n = m+1$.

We have assumed that (62) holds for $n = m$. In other words,

$$(x+y)^m = \sum_{k \in \mathbb{Z}} \binom{m}{k} x^k y^{m-k}. \tag{63}$$

Now, for each $k \in \mathbb{R}$, we have

$$\begin{aligned}\binom{m+1}{k} &= \binom{(m+1)-1}{k-1} + \binom{(m+1)-1}{k} \\ &\qquad \text{(by Theorem 1.3.8 (applied to } n = m+1)) \\ &= \binom{m}{k-1} + \binom{m}{k} \end{aligned} \tag{64}$$

(since $(m+1)-1=m$). But

$$(x+y)^{m+1} = (x+y) \underbrace{(x+y)^m}_{=\sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k} \text{ (by (63))}} = (x+y) \left(\sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k} \right)$$

$$= \underbrace{x \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k}}_{=\sum_{k\in\mathbb{Z}} x \binom{m}{k} x^k y^{m-k} \text{ (by (32), or rather its analogue for infinite sums)}} + \underbrace{y \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k}}_{=\sum_{k\in\mathbb{Z}} y \binom{m}{k} x^k y^{m-k} \text{ (by (32), or rather its analogue for infinite sums)}}$$

(by the distributive law)

$$= \sum_{k\in\mathbb{Z}} \underbrace{x \binom{m}{k} x^k y^{m-k}}_{=\binom{m}{k} x^{k+1} y^{m-k}} + \sum_{k\in\mathbb{Z}} \underbrace{y \binom{m}{k} x^k y^{m-k}}_{=\binom{m}{k} x^k y^{m-k+1}}$$

$$= \sum_{k\in\mathbb{Z}} \binom{m}{k} x^{k+1} y^{m-k} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m-k+1} \tag{65}$$

$$= \sum_{k\in\mathbb{Z}} \binom{m}{k-1} \underbrace{x^{(k-1)+1}}_{=x^k} \underbrace{y^{m-(k-1)}}_{=y^{m+1-k}} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k \underbrace{y^{m-k+1}}_{=y^{m+1-k}} \tag{66}$$

(here, we substituted $k-1$ for k in the first sum (since the map $\mathbb{Z}\to\mathbb{Z},\ k\mapsto k-1$ is a bijection))

$$= \sum_{k\in\mathbb{Z}} \binom{m}{k-1} x^k y^{m+1-k} + \sum_{k\in\mathbb{Z}} \binom{m}{k} x^k y^{m+1-k} \tag{67}$$

$$= \sum_{k\in\mathbb{Z}} \underbrace{\left(\binom{m}{k-1} x^k y^{m+1-k} + \binom{m}{k} x^k y^{m+1-k} \right)}_{=\left(\binom{m}{k-1} + \binom{m}{k} \right) x^k y^{m+1-k}} \tag{68}$$

(by (31), or rather its analogue for infinite sums)

$$= \sum_{k\in\mathbb{Z}} \underbrace{\left(\binom{m}{k-1} + \binom{m}{k} \right)}_{=\binom{m+1}{k} \text{ (by (64))}} x^k y^{m+1-k} = \sum_{k\in\mathbb{Z}} \binom{m+1}{k} x^k y^{m+1-k}.$$

Thus, (62) holds for $n=m+1$. This completes the induction step.

This completes the induction proof of (62). In view of (61), this equality (62) rewrites as $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$. Thus, Theorem 1.3.24 is proven. $\square$

It is instructive to try and prove Theorem 1.3.24 without taking the detour through infinite sums that we did in our above proof. Such a proof would actually be slightly shorter, but not by much: We would avoid having to explain why an infinite sum is well-defined (and what it means), but we would have to jump a few extra hurdles in our computation. Namely, instead of (65), we would get the equality

$$(x+y)^m = \sum_{k=0}^{m} \binom{m}{k} x^{k+1} y^{m-k} + \sum_{k=0}^{m} \binom{m}{k} x^k y^{m-k+1}.$$

Hence, instead of (67), we would get the equality

$$(x+y)^m = \sum_{k=1}^{m+1} \binom{m}{k-1} x^k y^{m+1-k} + \sum_{k=0}^{m} \binom{m}{k} x^k y^{m+1-k}$$

(where the first sum has bounds 1 and $m+1$ because it originates from substituting $k-1$ for k in the sum $\sum_{k=0}^{m} \binom{m}{k} x^{k+1} y^{m-k}$). At this point, we would not be able to combine the two sums on the right hand side using (31), since these two sums have (slightly) different bounds of summation. We would have to fix this by "manually" moving the bounds of summations so that both sums become $\sum_{k=0}^{m+1}$ sums:

$$\begin{aligned}
\sum_{k=1}^{m+1} \binom{m}{k-1} x^k y^{m+1-k} &= \sum_{k=0}^{m+1} \binom{m}{k-1} x^k y^{m+1-k} - \underbrace{\binom{m}{0-1}}_{\substack{=0 \\ \text{(by (43))}}} x^0 y^{0+1-k} \\
&\qquad \left(\begin{array}{c} \text{here, we extended the sum by adding an} \\ \text{extra addend for } k=0\text{, and then promptly} \\ \text{subtracted this new addend back} \end{array} \right) \\
&= \sum_{k=0}^{m+1} \binom{m}{k-1} x^k y^{m+1-k}
\end{aligned}$$

and

$$\sum_{k=0}^{m}\binom{m}{k}x^k y^{m+1-k} = \sum_{k=0}^{m+1}\binom{m}{k}x^k y^{m+1-k} - \underbrace{\binom{m}{m+1}}_{=0 \text{ (by Lemma 1.3.10)}} x^{m+1}y^{m+1-(m+1)}$$

$$\left(\begin{array}{c}\text{here, we extended the sum by adding an}\\ \text{extra addend for } k = m+1\text{, and then promptly}\\ \text{subtracted this new addend back}\end{array}\right)$$

$$= \sum_{k=0}^{m+1}\binom{m}{k}x^k y^{m+1-k}.$$

After these transformations, we could combine these two sums and proceed as in the proof above. (A slightly different but similar proof of Theorem 1.3.24 can be found in [Grinbe15, Exercise 3.6].)

So why did we take the trouble to turn our finite sum into an infinite sum, if we could have just as easily gotten away without it? Because this trick is helpful not merely in proving Theorem 1.3.24. Graham, Knuth and Patashnik ([GrKnPa94, §5.1]) frequently apply this trick, in order to avoid having "to fuss over boundary conditions" (i.e., over the bounds of the sums). Of course, this is not always possible; sometimes, when you extend a sum to a larger index set, the new addends you get will not all be 0, and the new sum will either fail to be well-defined or at least differ from the original sum. Thus, as in our proof of Theorem 1.3.24, the trick can only be applied after checking that the newly added addends are 0. (You can often do this checking in your head, but it needs to be done nevertheless.)

For the sake of future reference, let us summarize what we have learned about infinite sums in the above proof of Theorem 1.3.24:

Definition 1.3.26. Let S be a set (not necessarily infinite). For each $s \in S$, let a_s be a number.

Assume that only finitely many of these numbers are nonzero (i.e., only finitely many $s \in S$ satisfy $a_s \neq 0$). Then, the sum $\sum_{s\in S} a_s$ is well-defined (even if S is infinite): Its value is just defined to be the finite sum $\sum_{\substack{s\in S;\\ a_s\neq 0}} a_s$.

We refer to [Grinbe15, §2.14.15] for a rigorous treatment of such sums (called "finitely supported sums"). In a nutshell, all their properties can be derived from the analogous properties of finite sums simply by restricting oneself to certain finite subsets of S.

The following corollary from Theorem 1.3.24 is perhaps the most famous:

Corollary 1.3.27. Let $n \in \mathbb{N}$. Then, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Proof of Corollary 1.3.27. Theorem 1.3.24 (applied to $x = 1$ and $y = 1$) yields $(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \underbrace{1^k}_{=1} \underbrace{1^{n-k}}_{=1} = \sum_{k=0}^{n} \binom{n}{k}$. Hence, $\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$. Corollary 1.3.27 follows. □

The following fact ([Grinbe15, Proposition 3.39 **(c)**]) can be regarded as a counterpart to Corollary 1.3.27:

Proposition 1.3.28. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n = 0]. \tag{69}$$

(See Definition 1.3.15 for the meaning of $[n = 0]$ in this proposition.)

Proof of Proposition 1.3.28. If $n \neq 0$, then n is a positive integer (since $n \in \mathbb{N}$) and thus satisfies $0^n = 0$. On the other hand, if $n = 0$, then $0^n = 0^0 = 1$. Combining these two observations, we obtain

$$0^n = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases}. \tag{70}$$

On the other hand, the definition of $[n = 0]$ yields $[n = 0] = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases}$. Comparing this with (70), we find

$$0^n = [n = 0]. \tag{71}$$

Theorem 1.3.24 (applied to $x = -1$ and $y = 1$) yields

$$((-1)+1)^n = \sum_{k=0}^{n} \underbrace{\binom{n}{k} (-1)^k}_{=(-1)^k \binom{n}{k}} \underbrace{1^{n-k}}_{=1} = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

Thus,

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \left(\underbrace{(-1)+1}_{=0} \right)^n = 0^n = [n = 0] \qquad \text{(by (71))}.$$

This proves Proposition 1.3.28. □

1.3.7. Other properties of binomial coefficients

Let us see more properties of binomial coefficients, mostly without proof. We will prove some of these later (see also [Grinbe15, Chapter 3], or [GrKnPa94, Chapter 5], or essentially any other text on combinatorics). We begin with a summation identity that is known as the *hockey-stick identity*:

Theorem 1.3.29 ("Hockey-stick identity"). Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then,

$$\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}.$$

First proof of Theorem 1.3.29. Recall the notation $n^{\underline{k}}$ introduced in [19f-hw0s, Exercise 2] (and also in Remark 1.3.5). Now, [19f-hw0s, Exercise 2] says that

$$\sum_{i=0}^{n} i^{\underline{k}} = \frac{1}{k+1} (n+1)^{\underline{k+1}}.$$

Multiplying this equality by $\dfrac{1}{k!}$ yields

$$\frac{1}{k!} \sum_{i=0}^{n} i^{\underline{k}} = \frac{1}{k!} \cdot \frac{1}{k+1} (n+1)^{\underline{k+1}} = \frac{(n+1)^{\underline{k+1}}}{k! \cdot (k+1)}. \tag{72}$$

But (48) (applied to $n+1$ and $k+1$ instead of n and k) yields

$$\binom{n+1}{k+1} = \frac{(n+1)^{\underline{k+1}}}{(k+1)!} = \frac{(n+1)^{\underline{k+1}}}{k! \cdot (k+1)}$$

(since Proposition 1.3.2 (applied to $k+1$ instead of n) yields $(k+1)! = k! \cdot (k+1)$). Comparing this with (72), we obtain

$$\binom{n+1}{k+1} = \frac{1}{k!} \sum_{i=0}^{n} i^{\underline{k}} = \sum_{i=0}^{n} \frac{1}{k!} i^{\underline{k}} = \sum_{i=0}^{n} \frac{i^{\underline{k}}}{k!}.$$

Comparing this with

$$\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} = \sum_{i=0}^{n} \underbrace{\binom{i}{k}}_{\substack{= \frac{i^{\underline{k}}}{k!} \\ \text{(by (48), applied} \\ \text{to } i \text{ instead of } n)}} = \sum_{i=0}^{n} \frac{i^{\underline{k}}}{k!},$$

we obtain

$$\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}.$$

This proves Theorem 1.3.29. □

Alternatively, Theorem 1.3.29 can be proven by induction or combinatorially; we will see those proofs in Section 2.3.

Here is an alternative way to express Theorem 1.3.29:

Corollary 1.3.30 ("Hockey-stick identity", take 2)**.** Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then,

$$\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}.$$

(Here, the left-hand side means the sum $\sum_{m=k}^{n} \binom{m}{k}$. When $n < k$, this sum is empty and thus equals 0.)

Proof of Corollary 1.3.30. We have

$$\binom{m}{k} = 0 \qquad \text{for every } m \in \mathbb{N} \text{ satisfying } k > m \tag{73}$$

(by Proposition 1.3.6, applied to m instead of n).

Now, we would like to make the following argument: Splitting the sum $\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k}$ into two parts (with the first part comprising its first k addends, and the second part comprising everything else), we obtain

$$\begin{aligned}
&\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} \\
&= \underbrace{\left(\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{k-1}{k}\right)}_{\substack{=0 \\ \text{(since (73) shows that all} \\ \text{the addends in this sum are 0)}}} + \left(\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k}\right) \\
&= \binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k},
\end{aligned}$$

so that

$$\begin{aligned}
&\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k} \\
&= \binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}
\end{aligned}$$

(by Theorem 1.3.29).

Did you spot the (minor) hole in this argument? We split the sum $\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k}$ after its first k addends; but there is no guarantee that this sum

has k addends to begin with. Namely, if $n < k-1$, then it has fewer than k addends. In this case, our splitting argument does not work. This can be a source of real errors[57]. Fortunately, our proof can be easily salvaged. Namely, our argument above worked fine in the case when $n \geq k-1$; thus, we only need to deal with the case when $n < k-1$ now. So let us assume that $n < k-1$. Hence, $n+1 < k < k+1$, so that $k+1 > n+1$ and thus $\binom{n+1}{k+1} = 0$ (by Proposition 1.3.6, applied to $n+1$ and $k+1$ instead of n and k). Comparing this with

$$\begin{aligned}\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k} &= (\text{empty sum}) \qquad (\text{since } n < k-1 < k) \\ &= 0,\end{aligned}$$

we obtain $\binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}$ again. This completes our proof of Corollary 1.3.30. □

Example 1.3.31. Applying Corollary 1.3.30 to $k = 1$, we obtain

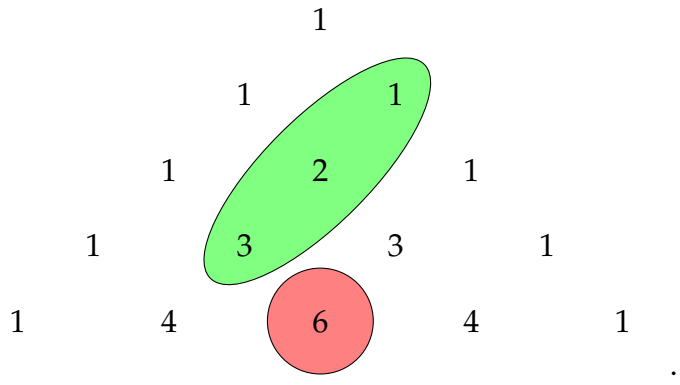
$$\binom{1}{1} + \binom{2}{1} + \binom{3}{1} + \cdots + \binom{n}{1} = \binom{n+1}{1+1} = \binom{n+1}{2}$$

for each $n \in \mathbb{N}$. In view of (45) and (46), this equality rewrites as

$$1 + 2 + 3 + \cdots + n = \frac{(n+1)\left((n+1)-1\right)}{2} = \frac{(n+1)\,n}{2} = \frac{n\,(n+1)}{2}.$$

Thus, we have obtained a new proof of Theorem 1.2.1.

Let us illustrate Corollary 1.3.30 on a picture of Pascal's triangle. On the following graphic (which shows the case $n = 3$ and $k = 1$), the addends on the left hand side of Corollary 1.3.30 are the ones surrounded by the oblong green ellipse, whereas the single binomial coefficient on the right hand side is in the red circle:



[57] For example, $1 + 2 + \cdots + k = (1+2) + (3+4+\cdots+k)$ does not hold for $k = 1$.

This picture explains where the "hockey-stick identity" got its name.

Next, we are going to express the Fibonacci numbers of Definition 1.1.10 as sums of binomial coefficients:

Proposition 1.3.32. Let $n \in \mathbb{N}$. Then, the Fibonacci number f_{n+1} is

$$f_{n+1} = \sum_{k=0}^{n} \binom{n-k}{k} = \binom{n-0}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-n}{n}.$$

We shall prove this later (in Subsection 1.4.5). For now, let us remark that roughly half the addends on the right hand side of Proposition 1.3.32 are 0 (indeed, Proposition 1.3.6 shows that $\binom{n-k}{k} = 0$ for any $k \in \{0,1,\ldots,n\}$ satisfying $k > n/2$) and thus can be discarded; nevertheless it is easier to have the sum end at $k = n$ rather than figure out where exactly its nonzero addends stop.

Here are some more examples of binomial identities (i.e., identities involving binomial coefficients):

Proposition 1.3.33. Let $n \in \mathbb{N}$. Then,

$$\binom{-1/2}{n} = \left(\frac{-1}{4}\right)^n \binom{2n}{n}.$$

Exercise 1.3.5. Prove Proposition 1.3.33.

The following fact is a neat way to restate Proposition 1.3.28:

Proposition 1.3.34. Let n be a positive integer. Then,

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}.$$

(Here, both sums are infinite, but they are well-defined, since only finitely many of their addends are nonzero.)

Proof of Proposition 1.3.34. For each $k \in \mathbb{N}$ satisfying $k \notin \{0,1,\ldots,n\}$, we have $\binom{n}{k} = 0$ (by Lemma 1.3.10). Thus, all addends of the sum $\sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k}$ with $k \notin \{0,1,\ldots,n\}$ are 0 (since they contain the $\binom{n}{k}$ factor, which is 0 when $k \notin \{0,1,\ldots,n\}$). Thus, this sum $\sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k}$ has only finitely many nonzero addends (namely, the ones for $k \in \{0,1,\ldots,n\}$), and is therefore well-defined. We

can transform this sum as follows:

$$\begin{aligned}
\sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k} &= \sum_{\substack{k\in\mathbb{N};\\ k\leq n}} (-1)^k \binom{n}{k} + \sum_{\substack{k\in\mathbb{N};\\ k>n}} (-1)^k \underbrace{\binom{n}{k}}_{=0} \\
&\qquad \text{(by Proposition 1.3.6)} \\
&\qquad \left(\begin{array}{c} \text{since each } k \in \mathbb{N} \text{ satisfies either } k \leq n \text{ or } k > n, \\ \text{but not both at the same time} \end{array} \right) \\
&= \sum_{\substack{k\in\mathbb{N};\\ k\leq n}} (-1)^k \binom{n}{k} + \underbrace{\sum_{\substack{k\in\mathbb{N};\\ k>n}} (-1)^k 0}_{=0} = \sum_{\substack{k\in\mathbb{N};\\ k\leq n}} (-1)^k \binom{n}{k} \\
&= \sum_{k\in\{0,1,\ldots,n\}} (-1)^k \binom{n}{k} \\
&\qquad \left(\begin{array}{c} \text{since the elements } k \in \mathbb{N} \text{ satisfying } k \leq n \\ \text{are precisely the elements of } \{0,1,\ldots,n\} \end{array} \right) \\
&= \sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n=0] \qquad \text{(by Proposition 1.3.28)} \\
&= 0
\end{aligned}$$

(since we don't have $n = 0$ (because n is positive)). Hence,

$$\begin{aligned}
0 = \sum_{k\in\mathbb{N}} (-1)^k \binom{n}{k} &= \sum_{\substack{k\in\mathbb{N};\\ k \text{ is even}}} \underbrace{(-1)^k}_{\substack{=1\\ \text{(since } k \text{ is even)}}} \binom{n}{k} + \sum_{\substack{k\in\mathbb{N};\\ k \text{ is odd}}} \underbrace{(-1)^k}_{\substack{=-1\\ \text{(since } k \text{ is odd)}}} \binom{n}{k} \\
&\qquad \left(\begin{array}{c} \text{since each } k \in \mathbb{N} \text{ is either even or odd,} \\ \text{but not both at the same time} \end{array} \right) \\
&= \sum_{\substack{k\in\mathbb{N};\\ k \text{ is even}}} \binom{n}{k} + \underbrace{\sum_{\substack{k\in\mathbb{N};\\ k \text{ is odd}}} (-1) \binom{n}{k}}_{= - \sum_{\substack{k\in\mathbb{N};\\ k \text{ is odd}}} \binom{n}{k}} \\
&= \underbrace{\sum_{\substack{k\in\mathbb{N};\\ k \text{ is even}}} \binom{n}{k}}_{= \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots} - \underbrace{\sum_{\substack{k\in\mathbb{N};\\ k \text{ is odd}}} \binom{n}{k}}_{= \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots} \\
&= \left(\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \right) - \left(\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots \right).
\end{aligned}$$

In other words,

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots . \tag{74}$$

Now,

$$\begin{aligned}
&2 \cdot \left(\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \right) \\
&= \left(\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \right) + \underbrace{\left(\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \right)}_{= \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots \text{ (by (74))}} \\
&= \left(\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \right) + \left(\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots \right) \\
&= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots = \sum_{k \in \mathbb{N}} \binom{n}{k} \\
&= \sum_{\substack{k \in \mathbb{N}; \\ k \leq n}} \binom{n}{k} + \sum_{\substack{k \in \mathbb{N}; \\ k > n}} \underbrace{\binom{n}{k}}_{=0 \text{ (by Proposition 1.3.6)}} \\
&\qquad \left(\begin{array}{c} \text{since each } k \in \mathbb{N} \text{ satisfies either } k \leq n \text{ or } k > n, \\ \text{but not both at the same time} \end{array} \right) \\
&= \sum_{\substack{k \in \mathbb{N}; \\ k \leq n}} \binom{n}{k} + \underbrace{\sum_{\substack{k \in \mathbb{N}; \\ k > n}} 0}_{=0} = \sum_{\substack{k \in \mathbb{N}; \\ k \leq n}} \binom{n}{k} = \sum_{k \in \{0,1,\ldots,n\}} \binom{n}{k} \\
&\qquad \left(\begin{array}{c} \text{since the elements } k \in \mathbb{N} \text{ satisfying } k \leq n \\ \text{are precisely the elements of } \{0,1,\ldots,n\} \end{array} \right) \\
&= \sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \text{(by Corollary 1.3.27)} .
\end{aligned}$$

Dividing this equality by 2, we obtain

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = 2^n / 2 = 2^{n-1}.$$

Combining this with (74), we obtain

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}.$$

This proves Proposition 1.3.34. □

The next fact is highly useful (we will see some of its uses later on):

Proposition 1.3.35 (Trinomial revision formula)**.** Let $n, a, b \in \mathbb{R}$. Then,

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}.$$

Proposition 1.3.35 is the *trinomial revision formula*, and is not hard to prove.[58] We shall prove it in the next chapter.

Proposition 1.3.36 (Absorption formula I)**.** Let $n \in \{1, 2, 3, \ldots\}$ and $m \in \mathbb{R}$. Then,

$$\binom{m}{n} = \frac{m}{n}\binom{m-1}{n-1}.$$

Proposition 1.3.36 is the *absorption formula*, and is one of the major tools for transforming binomial coefficients into more convenient forms. It is straightforward to prove. The following proof of Proposition 1.3.36 is taken from [Grinbe15, proof of Proposition 3.22][59]:

Proof of Proposition 1.3.36. We have $n \in \{1, 2, 3, \ldots\} \subseteq \mathbb{N}$. Thus, (42) (applied to m and n instead of n and k) yields

$$\begin{aligned}\binom{m}{n} &= \frac{m\,(m-1)\,(m-2)\cdots(m-n+1)}{n!} \\ &= \frac{m\,(m-1)\,(m-2)\cdots(m-n+1)}{n\cdot(n-1)!}\end{aligned} \tag{75}$$

(since Proposition 1.3.2 yields $n! = (n-1)!\cdot n = n\cdot(n-1)!$).

We have $n-1 \in \mathbb{N}$ (since $n \in \{1, 2, 3, \ldots\}$). Thus, (42) (applied to $m-1$ and $n-1$ instead of n and k) yields

$$\begin{aligned}\binom{m-1}{n-1} &= \frac{(m-1)\,((m-1)-1)\,((m-1)-2)\cdots((m-1)-(n-1)+1)}{(n-1)!} \\ &= \frac{(m-1)\,(m-2)\,(m-3)\cdots(m-n+1)}{(n-1)!}\end{aligned}$$

(since $(m-1)-1 = m-2$ and $(m-1)-2 = m-3$ and $(m-1)-(n-1)+1 = m-n+1$). Multiplying both sides of this equality by $\frac{m}{n}$, we obtain

$$\begin{aligned}\frac{m}{n}\binom{m-1}{n-1} &= \frac{m}{n}\cdot\frac{(m-1)\,(m-2)\,(m-3)\cdots(m-n+1)}{(n-1)!} \\ &= \frac{m\cdot((m-1)\,(m-2)\,(m-3)\cdots(m-n+1))}{n\cdot(n-1)!} \\ &= \frac{m\,(m-1)\,(m-2)\cdots(m-n+1)}{n\cdot(n-1)!}\end{aligned}$$

[58] See [17f-hw1s, Exercise 2 **(c)**] for the most interesting case.

[59] where it is stated only for $m \in \mathbb{Q}$, but this makes no difference to the proof

(since $m \cdot ((m-1)(m-2)(m-3)\cdots(m-n+1)) = m(m-1)(m-2)\cdots(m-n+1)$). Compared with (75), this yields $\binom{m}{n} = \frac{m}{n}\binom{m-1}{n-1}$. This proves Proposition 1.3.36. □

Theorem 1.3.37. Let $n \in \mathbb{N}$, $x \in \mathbb{R}$ and $y \in \mathbb{R}$. Then,

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}.$$

Theorem 1.3.37 is the *Chu–Vandermonde identity* (aka the *Vandermonde convolution identity*). Note its resemblance to Theorem 1.3.24; it is like a binomial formula for binomial coefficients instead of powers. We will prove it later (in Section 2.6). For now, see [Grinbe15, Theorem 3.29] for a proof (which is stated only for $x, y \in \mathbb{Q}$, but applies just as well to any numbers x and y).

The next two theorems appear in [18f-mt3s, Exercise 1]:

Theorem 1.3.38 (Cauchy's binomial formula)**.** Let $n \in \mathbb{N}$ and $x, y, z \in \mathbb{R}$. Then,

$$\sum_{k=0}^{n} \binom{n}{k} (x+kz)^k (y-kz)^{n-k} = \sum_{k=0}^{n} \frac{n!}{k!} (x+y)^k z^{n-k}.$$

Theorem 1.3.39 (Abel's binomial formula)**.** Let $n \in \mathbb{N}$ and $x, y, z \in \mathbb{R}$. Then,

$$\sum_{k=0}^{n} \binom{n}{k} \underbrace{x(x+kz)^{k-1}}_{\substack{\text{This should be read} \\ \text{as 1 if } k=0}} (y-kz)^{n-k} = (x+y)^n.$$

(More precisely, [18f-mt3s, Exercise 1] states these theorems in the particular case when $z = 1$. The general case can easily be deduced from this particular case, however.)

Note that both Theorem 1.3.38 and Theorem 1.3.39 generalize the binomial formula; indeed, Theorem 1.3.24 can be recovered from either of them by setting $z = 0$.

Exercise 1.3.6. Let $n \in \mathbb{N}$. Prove that $\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}$.

Class of 2019-10-07

1.4. Counting subsets

1.4.1. All subsets

Theorem 1.3.12 tells us how many k-element subsets a given n-element set has, where n and k are fixed. What if we don't fix k, and simply ask for the number of all subsets of an n-element set? The following theorem gives the answer:

Theorem 1.4.1. Let $n \in \mathbb{N}$. Let S be an n-element set. Then,

$$(\#\text{ of subsets of } S) = 2^n.$$

Exercise 1.4.1. Prove Theorem 1.4.1.
[**Hint:** Imitate the proof of Theorem 1.3.12.]

We will later give two other proofs of Theorem 1.4.1: an algebraic proof in Subsection 1.4.2 and a combinatorial proof in Subsection 1.5.3.[60]

1.4.2. Lacunar subsets: the basics

We have now seen the following examples of counting:

- An n-element set has 2^n subsets. (This is Theorem 1.4.1.)
- An n-element set has $\binom{n}{k}$ many k-element subsets. (This is Theorem 1.3.12.)

Let us now ask subtler questions.

Definition 1.4.2. A set S of integers is said to be *lacunar* if it contains no two consecutive integers (i.e., there is no integer i such that both $i \in S$ and $i+1 \in S$).

For example, the set $\{1,5,7\}$ is lacunar, whereas $\{1,5,6\}$ is not. Note that any 1-element subset of $\mathbb{Z}$ is lacunar, and so is the empty set.

Some people say "sparse" instead of "lacunar". I will use "lacunar", since the word "sparse" has a different meaning in computer science.

It is not hard to list the lacunar subsets of $[5]$: They are

$$\varnothing, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \{4\}, \quad \{5\}, \quad \{1,3\},$$
$$\{1,4\}, \quad \{1,5\}, \quad \{2,4\}, \quad \{2,5\}, \quad \{3,5\}, \quad \{1,3,5\}.$$

We can now ask several natural questions:

Question 1.4.3. For given $n, k \in \mathbb{N}$:
(a) How many lacunar subsets does $[n]$ have?
(b) How many k-element lacunar subsets does $[n]$ have?
(c) What is the largest size of a lacunar subset of $[n]$?

Let us start with **(c)**:

[60] The impatient reader can find the latter proof in [19f-hw0s, Exercise 1 **(a)**]. (More precisely, [19f-hw0s, Exercise 1 **(a)**] is the particular case of Theorem 1.4.1 when $S = [n]$. But it can easily be adapted to the general case.)

Definition 1.4.4. Let $x \in \mathbb{R}$. Then:

- We let $\lfloor x \rfloor$ denote the largest integer $\leq x$. This integer $\lfloor x \rfloor$ is called the *floor* of x, or "*rounding down* x".
- We let $\lceil x \rceil$ denote the smallest integer $\geq x$. This integer $\lceil x \rceil$ is called the *ceiling* of x, or "*rounding up* x".

Example 1.4.5. We have

$$\lfloor 3 \rfloor = 3; \qquad \left\lfloor \sqrt{2} \right\rfloor = 1; \qquad \lfloor \pi \rfloor = 3; \qquad \lfloor -\pi \rfloor = -4;$$
$$\lceil 3 \rceil = 3; \qquad \left\lceil \sqrt{2} \right\rceil = 2; \qquad \lceil \pi \rceil = 4; \qquad \lceil -\pi \rceil = -3.$$

Let us note that each $x \in \mathbb{R}$ satisfies $\lfloor x \rfloor \leq x \leq \lceil x \rceil$.

It is intuitively clear that there is no way to pick more than $\lceil n/2 \rceil$ distinct numbers from the set $\{1, 2, \ldots, n\}$ without picking two consecutive integers. Let us state and rigorously prove this:

Proposition 1.4.6. Let $n \in \mathbb{N}$. Then, the largest size of a lacunar subset of $[n]$ is $\lceil n/2 \rceil$.

Our proof of this will rely on the following basic fact:

Theorem 1.4.7. Let A be a finite set. Let B be a subset of A. Then:
(a) We have $|A \setminus B| = |A| - |B|$.
(b) We have $|B| \leq |A|$.
(c) If $|B| = |A|$, then $B = A$.

This theorem is fundamental. Theorem 1.4.7 **(a)** is known as the *difference rule*, and is part of the reason why $A \setminus B$ is called the "set difference" of A and B [61]. Parts **(b)** and **(c)** of Theorem 1.4.7 are (in a sense) the combinatorial manifestation of the principle "the whole is greater than its part". But before you declare them completely obvious, keep in mind that Theorem 1.4.7 **(c)** is not true for infinite sets! Indeed, if we set $B = \mathbb{N}$ and $A = \mathbb{Z}$, then $B \subseteq A$ holds, and so does $|B| = |A|$ (in the sense that the infinite sets B and A have the same cardinality), but it is not true that $B = A$. Thus, it is worth proving the theorem. Fortunately, it is a simple application of the sum rule:

Proof of Theorem 1.4.7. We know that $B \subseteq A$. Hence, the set A is the union of the two disjoint sets B and $A \setminus B$. Hence, Theorem 1.1.3 (applied to $S = A$, $k = 2$, $S_1 = B$ and

[61] although this terminology persists even in the case when B is not a subset of A, despite the fact that $|A \setminus B|$ is usually not $|A| - |B|$ in this case

$S_2 = A \setminus B$) yields $|A| = |B| + |A \setminus B|$. Thus, $|A \setminus B| = |A| - |B|$. This proves Theorem 1.4.7 **(a)**.

(b) We have $|A| = |B| + \underbrace{|A \setminus B|}_{\geq 0} \geq |B|$. In other words, $|B| \leq |A|$. This proves Theorem 1.4.7 **(b)**.

(c) Assume that $|B| = |A|$. Hence, $|B| = |A| = |B| + |A \setminus B|$. Subtracting $|B|$ from both sides of this equation, we obtain $0 = |A \setminus B|$, so that $|A \setminus B| = 0$. But this shows that $A \setminus B$ is the empty set. Hence, $A \subseteq B$, so that $A = B$ (because $B \subseteq A$). In other words, $B = A$. This proves Theorem 1.4.7 **(c)**. □

Proof of Proposition 1.4.6. The lacunar set[62]

$$\begin{aligned}\{\text{all odd elements of } [n]\} &= \{1, 3, 5, \ldots, (n \text{ or } n-1)\} \\ &= \{1 < 3 < 5 < \cdots < (n \text{ or } n-1)\}\end{aligned}$$

(where the last element is n if n is odd, and $n-1$ if n is even) is a subset of $[n]$ and has size $\lceil n/2 \rceil$. Thus, there exists a lacunar subset of $[n]$ having size $\lceil n/2 \rceil$. Hence, we only need to prove that no higher size is possible.

Let us prove this. Let L be a lacunar subset of $[n]$. We shall prove that $|L| \leq \lceil n/2 \rceil$.

Indeed, let L^+ be the set $\{s+1 \mid s \in L\}$. (In other words, L^+ is the set L "shifted by 1 to the right", in the sense that L^+ is obtained from L by adding 1 to each element. For example, if $L = \{2, 4, 7, 10\}$, then $L^+ = \{3, 5, 8, 11\}$.)

It is clear that $|L| = |L^+|$. (Formally speaking, this is a consequence of the bijection principle, because the map $L \to L^+$, $s \mapsto s+1$ is clearly a bijection.)

We have $L \subseteq [n] = \{1, 2, \ldots, n\}$ and therefore $L^+ \subseteq \{2, 3, \ldots, n+1\} \subseteq [n+1]$. Also, $L \subseteq [n] \subseteq [n+1]$. Thus, we know that both L and L^+ are subsets of $[n+1]$. Hence, their union $L \cup L^+$ is a subset of $[n+1]$ as well. Therefore, Theorem 1.4.7 **(b)** (applied to $L \cup L^+$ and $[n+1]$ instead of B and A) yields

$$\left|L \cup L^+\right| \leq |[n+1]| = n+1 \qquad (\text{since } [n+1] = \{1, 2, \ldots, n+1\}).$$

On the other hand, recall that L is lacunar. Thus, the sets L and L^+ are disjoint[63]. Hence, (4) (applied to $X = L$ and $Y = L^+$) yields

$$\left|L \cup L^+\right| = |L| + \underbrace{\left|L^+\right|}_{\substack{=|L| \\ (\text{since } |L| = \left|L^+\right|)}} = |L| + |L| = 2 \cdot |L|.$$

[62] We are using the notation $\{a_1 < a_2 < \cdots < a_k\}$ (where $a_1, a_2, \ldots, a_k$ are some integers) to mean the set $\{a_1, a_2, \ldots, a_k\}$ when we want to simultaneously assert that $a_1 < a_2 < \cdots < a_k$. For example, $\{2 < 5 < 8\}$ means the set $\{2, 5, 8\}$, whereas $\{4 < 2 < 7\}$ is not well-defined.

[63] *Proof.* Let $t \in L \cap L^+$. Thus, $t \in L \cap L^+ \subseteq L$ and $t \in L \cap L^+ \subseteq L^+ = \{s+1 \mid s \in L\}$. In other words, there exists some $s \in L$ such that $t = s+1$. Consider this s. Now, the set L contains the two consecutive integers s and $s+1$ (since $s \in L$ and $s+1 = t \in L$). But L contains no two consecutive integers (since L is lacunar). These two statements clearly contradict each other. Thus we have obtained a contradiction.

Now, forget that we fixed t. We thus have found a contradiction for each $t \in L \cap L^+$. Hence, there exists no $t \in L \cap L^+$. In other words, the sets L and L^+ are disjoint.

Hence,

$$2 \cdot |L| = \left|L \cup L^+\right| \leq n+1.$$

Thus,

$$|L| \leq (n+1)/2 = \underbrace{n/2}_{\leq \lceil n/2 \rceil} + \underbrace{1/2}_{<1} < \lceil n/2 \rceil + 1.$$

Hence,[64]

$$\begin{aligned} |L| &\leq (\lceil n/2 \rceil + 1) - 1 \qquad \text{(because } |L| \text{ and } \lceil n/2 \rceil + 1 \text{ are integers)} \\ &= \lceil n/2 \rceil . \end{aligned}$$

Now, forget that we fixed L. We thus have shown that any lacunar subset L of $[n]$ satisfies $|L| \leq \lceil n/2 \rceil$. In other words, any lacunar subset of $[n]$ has size $\leq \lceil n/2 \rceil$. Then, the largest size of a lacunar subset of $[n]$ is $\lceil n/2 \rceil$ (because we already know that there exists a lacunar subset of $[n]$ having size $\lceil n/2 \rceil$). This proves Proposition 1.4.6. □

As another application of Theorem 1.4.7, let us prove Theorem 1.4.1 again:[65]

Second proof of Theorem 1.4.1. We have $|S| = n$, since S is an n-element set. If B is any subset of S, then Theorem 1.4.7 **(b)** (applied to $A = S$) yields $|B| \leq |S| = n$ and therefore $|B| \in \{0, 1, \ldots, n\}$. Hence, the sum rule yields[66]

$$\begin{aligned} &(\text{\# of subsets of } S) \\ &= \sum_{k \in \{0,1,\ldots,n\}} \underbrace{(\text{\# of subsets } B \text{ of } S \text{ satisfying } |B| = k)}_{= (\text{\# of } k\text{-element subsets of } S) = \binom{n}{k} \text{ (by Theorem 1.3.12)}} \\ &= \sum_{k \in \{0,1,\ldots,n\}} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} \qquad \left(\text{since the symbol } \sum_{k=0}^{n} \text{ stands for } \sum_{k \in \{0,1,\ldots,n\}} \right) \\ &= 2^n \qquad \text{(by Corollary 1.3.27)} . \end{aligned}$$

This proves Theorem 1.4.1. □

1.4.3. Intermezzo: SageMath

Counting using SageMath. Our next goal is to address Question 1.4.3 **(b)**. A good way to start is by collecting some data. For example, counting the lacunar subsets of

[64] We are using the following basic fact here: If a and b are two integers satisfying $a < b$, then $a \leq b - 1$.

[65] The first proof was given in the solution to Exercise 1.4.1.

[66] The sum rule that we are using here is Theorem 1.2.5. (Namely, we are applying Theorem 1.2.5 to $\{\text{subsets of } S\}$ and $\{0, 1, \ldots, n\}$ instead of S and W, where the map $f : \{\text{subsets of } S\} \to \{0, 1, \ldots, n\}$ is defined by $f(B) = |B|$ for all $B \in \{\text{subsets of } S\}$.)

$[n]$ for the first (say) 10 positive integer values of n is a straightforward task best left to a computer. The easiest way to do so is to use the SageMath computer algebra system [sage], since it has almost all of the necessary functionality built in already. You can either install SageMath on your computer (see here for Linux binaries, here for Linux sources, and here for less up-to-date Windows installers), or run it on the CoCalc cloud, or (if your computations are quick) use the SageMathCell browser interface. The latter option is the easiest one, in my experience.

First, let us find all 3-element subsets of $[5] = \{1,2,3,4,5\}$. Typing in

```
Subsets({1, 2, 3, 4, 5}, 3)
```

returns:

```
Subsets of {1, 2, 3, 4, 5} of size 3
```

Okay, but how do we list them? For that, we use

```
list(Subsets({1, 2, 3, 4, 5}, 3))
```

and obtain

```
[{1, 2, 3},
 {1, 2, 4},
 {1, 2, 5},
 {1, 3, 4},
 {1, 3, 5},
 {1, 4, 5},
 {2, 3, 4},
 {2, 3, 5},
 {2, 4, 5},
 {3, 4, 5}]
```

These are our subsets indeed.[67] Likewise, we can get SageMath to list all subsets of $[4]$ (of all sizes):

```
list(Subsets({1, 2, 3, 4}))
```

This results in SageMath printing all 16 subsets of $[4]$.

Now, let us see which of them are lacunar – more precisely, let us make SageMath figure that out. For this, we need to define a function that checks whether a given subset is lacunar. We call it `is_lacunar`, and define it as follows:[68]

```
def is_lacunar(I):
  # Check whether a set 'I' of integers is lacunar.
  return all( e + 1 not in I for e in I )
```

[69] The `all` function here stands for the logical "for all" quantifier, so you should read "`all( e + 1 not in I for e in I )`" as "for all $e \in I$, we have $e+1 \notin I$" (which is indeed a way to say that I is lacunar).

[67] Square brackets `[...]` delimit lists in SageMath.

[68] The second line in this definition is unnecessary; it is just a comment explaining to us humans what the function is supposed to do.

[69] When pasting this code, don't forget the indentation: The second and third lines need to be indented, or else SageMath will not recognize that they are part of the definition of the function!

You can check that this function works as intended:

```
is_lacunar({1, 4, 6})
```

returns `True`, whereas

```
is_lacunar({1, 4, 5})
```

returns `False`.

If you are using the SageMathCell browser interface, you need to put **both** the definition of the function and these tests into the input box[70]. So you have to write:

```
def is_lacunar(I):
  # Check whether a set ‘I‘ of integers is lacunar.
  return all( e + 1 not in I for e in I )

is_lacunar({1, 4, 6})
```

Better yet, you can use the `print` instruction to do both of these tests at once:

```
def is_lacunar(I):
  # Check whether a set ‘I‘ of integers is lacunar.
  return all( e + 1 not in I for e in I )

print(is_lacunar({1, 4, 6}))
print(is_lacunar({1, 4, 5}))
```

(Without the `print` instruction, SageMathCell would only give you the output of the very last line.)

Now, let us make SageMath list the lacunar subsets of $[4]$. We shall ask it to do so by walking through all the subsets of $[4]$, and filtering them for lacunarity. Having defined the `is_lacunar` function, this is easy:

```
[A for A in Subsets({1, 2, 3, 4}) if is_lacunar(A)]
```

The meaning of this expression is very similar to the mathematical set-builder notation $\{A \mid A \in \mathcal{P}(\{1,2,3,4\}) \text{ and } A \text{ is lacunar}\}$; the main difference is that we are using square brackets rather than set-braces and therefore obtain a list rather than a set. The result is what we would expect:

```
[{}, {1}, {2}, {3}, {4}, {1, 3}, {1, 4}, {2, 4}]
```

This is a list of all lacunar subsets of $[4]$, each listed only once. Thus, the length of the list is the number of said subsets. We can let SageMath compute this length as follows:

```
len([A for A in Subsets({1, 2, 3, 4}) if is_lacunar(A)])
```

As expected, we get 8. In general, the SageMath function `len` can be applied both to lists and to sets, yielding the length of the former and the size of the latter.

We can now put these to use and compute the number of lacunar subsets of $[n]$ for any $n \in \mathbb{N}$ that is not too high. For example, for $n = 7$, we just need to ask SageMath the following:

[70] and, generally, you must keep the definition in the input box whenever you want to use it – as SageMathCell won't remember it for you

```
len([A for A in Subsets({1, 2, 3, 4, 5, 6, 7}) if is_lacunar(A)])
```

and we quickly obtain 34.

A bit of typing thus lets us build the following table of numbers of lacunar subsets:

n	0	1	2	3	4	5	6	7	8	9	···
#	1	2	3	5	8	13	21	34	55	89	···

(where each entry in the bottom row is the # of lacunar subsets of $[n]$ for the appropriate value of n).

At this point, you may have a good guess of what the general answer is. We will get to it, but beforehand, let me say a few words about how we could have used SageMath better than we did above, because otherwise I would feel bad for teaching you bad programming habits.

Working with general n. The way I showed above required me to type in a new command for each new value of n. Why not have the computer calculate the whole table at once? For this, we need to define a function which takes a number n as input and returns the # of lacunar subsets of n. Let me call this function `num_lacs`, and define it as follows:

```
def num_lacs(n):
  # Return the number of all lacunar subsets of `[n]`.
  N = set(range(1, n+1)) # This is the set of `1, 2, ..., n`.
  return len([A for A in Subsets(N) if is_lacunar(A)])
```

Here is what this function does: It first constructs the set $[n]$ (which it calls N). It does this by first constructing the list $(1,2,\ldots,n)$ (which is done via `range(1, n+1)` because in general, `range(a, b)` returns the list $(a,a+1,\ldots,b-1)$), and then making a set out of this list using the `set` function. Then, it returns the number of all lacunar subsets of this set $N=[n]$ (in the same way as we did above).

Having defined this function, we can make SageMath list its values for all $n \in \{0,1,\ldots,9\}$ as follows:[71]

```
for n in range(0, 10):
  print("The number of lacunar subsets of [" + str(n) + "] is " + str(
                                    num_lacs(n)))
```

This code runs through all elements n of `range(0, 10)`, which means all elements of $\{0,1,\ldots,9\}$, and prints a certain piece of text for each of them, which always has the form "The number of lacunar subsets of [", followed by the value of n, followed by the text "] is ", followed by the # of lacunar subsets of $[n]$. Here is the output:

```
The number of lacunar subsets of [0] is 1
The number of lacunar subsets of [1] is 2
```

[71] The following code fragment has only two lines. The linebreak between `str(` and `num_lacs(n))` is a consequence of lack of space on this page.

```
The number of lacunar subsets of [2] is 3
The number of lacunar subsets of [3] is 5
The number of lacunar subsets of [4] is 8
The number of lacunar subsets of [5] is 13
The number of lacunar subsets of [6] is 21
The number of lacunar subsets of [7] is 34
The number of lacunar subsets of [8] is 55
The number of lacunar subsets of [9] is 89
```

This is essentially our above table, in text form, generated all at once. (We could go further and have SageMath generate the LaTeX sourcecode of the whole table, but this would distract us here.)

Optimizing the code. Our code now looks like this:

```
def is_lacunar(I):
  # Check whether a set `I` of integers is lacunar.
  return all( e + 1 not in I for e in I )

def num_lacs(n):
  # Return the number of all lacunar subsets of `[n]`.
  N = set(range(1, n+1)) # This is the set of `1, 2, ..., n`.
  return len([A for A in Subsets(N) if is_lacunar(A)])

for n in range(0, 10):
  print("The number of lacunar subsets of [" + str(n) + "] is " + str(
                                    num_lacs(n)))
```

It is good enough for computing the required values for all $n \in \{0,1,\ldots,18\}$, but higher n's will bring SageMath to its knees. (The SageMathCell browser interface has a timeout – if your computation takes longer than 30 seconds[72], it will stop. But even on your own machine, you don't want to wait for days.)

It turns out that we can speed up our code a bit by optimizing the `num_lacs` function. In its current form, this function first computes the **list** of all lacunar subsets of $[n]$ and then returns the length of this list. Thus, it walks through all subsets of $[n]$, and whenever it encounters a lacunar one, it "writes it down" into a list (in memory). It would be faster to simply **count** these lacunar subsets, without writing them down, since we only want to know their number. The easiest way to do so is to simply start with the number 0 and then add 1 to it every time a lacunar subset is encountered. This suggests the following modified version of the `num_lacs` function:

```
def num_lacs(n):
  # Return the number of all lacunar subsets of `[n]`.
  N = set(range(1, n+1)) # This is the set of `1, 2, ..., n`.
  return sum(1 for A in Subsets(N) if is_lacunar(A))
```

[72] I believe it is 30 seconds.

The line

```
sum(1 for A in Subsets(N) if is_lacunar(A))
```

here corresponds to the mathematical expression $\sum_{\substack{A \subseteq [n]; \\ A \text{ is lacunar}}} 1$, which is exactly the # of lacunar subsets of $[n]$ (by the identity (30)).

This speeds up our code, but only by a little, because the true bulk of the time is taken by walking through all the 2^n subsets of $[n]$. Nevertheless, it is worth remembering this tactic for reducing needless busywork. There are many situations where it does make a major difference.

The manual. You have now seen a few pieces of SageMath's functionality and a few examples of how to use it. Of course, there is a lot more. Since this text is not a SageMath reference book, you will need other sources to discover what else SageMath can do for you. An overview is given in the text [SageBook]. In order to systematically explore the abilities of SageMath, you will have to consult the SageMath reference manual, which can currently be found at `https://doc.sagemath.org/html/en/reference/` . In particular, the Combinatorics page is of most relevance to us.

1.4.4. Counting lacunar subsets

Let us now return to theorems and proofs. As our SageMath computations heavily suggest, we should expect the # of lacunar subsets of $[n]$ to be a Fibonacci number, namely f_{n+2}. And this holds for all $n \in \mathbb{N}$ indeed. Moreover, it holds for $n = -1$ as well, if we extend our notation $[k]$ for $\{1, 2, \ldots, k\}$ to encompass the case when k is negative in the following way:

Definition 1.4.8. Let $k \in \mathbb{Z}$. Then, $[k]$ shall denote the set $\{1, 2, \ldots, k\}$. This is understood to be the empty set $\varnothing$ when $k \leq 0$.

Let us state our claim about the # of lacunar subsets of $[n]$ as a proposition:

Proposition 1.4.9. Let $n \in \{-1, 0, 1, \ldots\}$. Then,

$$(\#\text{ of lacunar subsets of } [n]) = f_{n+2}.$$

There are several ways to prove Proposition 1.4.9.

First proof of Proposition 1.4.9 (sketched). The following proof is similar to that of Theorem 1.3.12 above, so we will be brief and leave parts of it to the reader. A complete

version of this proof can be found in [Grinbe15, solution to Exercise 4.3][73] or in [17f-hw1s, Exercise 4 **(c)**][74].

Forget that we fixed n. For each $n \in \{-1, 0, 1, \ldots\}$, we define the integer ℓ_n by

$$\ell_n = (\text{\# of lacunar subsets of } [n]) .$$

Note that $\ell_0 = 1$ (since the only lacunar subset of the empty set $[0]$ is the empty set itself) and $\ell_{-1} = 1$ (for similar reasons).

Now, we claim that

$$\ell_n = \ell_{n-1} + \ell_{n-2} \qquad \text{for each integer } n \geq 1. \tag{76}$$

[*Proof of (76):* Let $n \geq 1$ be an integer. We shall call a subset of $[n]$

- **red** if it contains n, and
- **green** if it does not contain n.

Thus, each subset of $[n]$ is either red or green (but not both at the same time). Thus, by the sum rule, we have

$$\begin{aligned} &(\text{\# of lacunar subsets of } [n]) \\ &= (\text{\# of lacunar red subsets of } [n]) + (\text{\# of lacunar green subsets of } [n]) . \end{aligned}$$

We shall now compute the two addends on the right hand side.

First of all, we observe that the green subsets of $[n]$ are precisely the subsets of $[n-1]$. Hence,

$$\begin{aligned} &(\text{\# of lacunar green subsets of } [n]) \\ &= (\text{\# of lacunar subsets of } [n-1]) = \ell_{n-1} \end{aligned} \tag{77}$$

(since ℓ_{n-1} was defined to be the # of lacunar subsets of $[n-1]$).

What about the red subsets?

A lacunar red subset of $[n]$ must contain n (since it is red), and thus cannot contain $n-1$ (since it is lacunar, but $n-1$ and n are two consecutive integers). Hence, if R is a lacunar red subset of $[n]$, then $R \setminus \{n\}$ is not only a subset of $[n-1]$ but actually a subset of $[n-2]$. Hence, the map

$$\begin{aligned} f : \{\text{lacunar red subsets of } [n]\} &\to \{\text{lacunar subsets of } [n-2]\} , \\ R &\mapsto R \setminus \{n\} \end{aligned}$$

[73] Keep in mind that [Grinbe15, Exercise 4.3] is an equivalent restatement of our Proposition 1.4.9 (more precisely, our Proposition 1.4.9 is [Grinbe15, Exercise 4.3], applied to $n+2$ instead of n).

[74] Note that [17f-hw1s, Exercise 4 **(c)**] only covers the case when $n \in \mathbb{N}$. But the remaining case (viz., the case $n = -1$) is trivial.

is well-defined. Moreover, it is easy to see that this map is a bijection (because if P is a lacunar subset of $[n-2]$, then $P \cup \{n\}$ is a lacunar subset of $[n]$). Therefore, the bijection principle (applied to the bijection f) yields

$$|\{\text{lacunar red subsets of } [n]\}| = |\{\text{lacunar subsets of } [n-2]\}|.$$

In other words,

$$\begin{aligned} &(\#\text{ of lacunar red subsets of } [n]) \\ &= (\#\text{ of lacunar subsets of } [n-2]) = \ell_{n-2} \end{aligned} \tag{78}$$

(since ℓ_{n-2} was defined to be the # of lacunar subsets of $[n-2]$).

Now,

$$\begin{aligned} &(\#\text{ of lacunar subsets of } [n]) \\ &= \underbrace{(\#\text{ of lacunar red subsets of } [n])}_{=\ell_{n-2}} + \underbrace{(\#\text{ of lacunar green subsets of } [n])}_{=\ell_{n-1}} \\ &= \ell_{n-2} + \ell_{n-1} = \ell_{n-1} + \ell_{n-2}. \end{aligned}$$

This proves (76).]

The rest of the proof proceeds by the same argument that we used for Proposition 1.1.11: We have to show that

$$(\#\text{ of lacunar subsets of } [n]) = f_{n+2} \qquad \text{for each } n \in \{-1, 0, 1, \ldots\}.$$

In other words, we have to show that

$$\ell_n = f_{n+2} \qquad \text{for each } n \in \{-1, 0, 1, \ldots\}$$

(since $\ell_n = (\#\text{ of lacunar subsets of } [n])$). In other words, we have to show that the sequences $(\ell_{-1}, \ell_0, \ell_1, \ldots)$ and $(f_1, f_2, f_3, \ldots)$ are identical. Both of them have the property that their first entries are 1's (since $\ell_{-1} = 1$ and $f_1 = 1$), their second entries are 1's (since $\ell_0 = 1$ and $f_2 = 1$), and each of their further entries equals the sum of the preceding two entries[75]. Thus, both sequences start with the same two entries, and then are built out of these two entries according to the same rule. Hence, the two sequences must be the same. This proves Proposition 1.4.9. □

The next proof of Proposition 1.4.9 we shall give is an example of a *bijective proof*: a proof that uses the bijection principle to show that two numbers are equal. (Previous examples of such proofs are our proofs of Proposition 1.1.5 and of Proposition 1.1.9, as well as our third proof of Theorem 1.2.1.)

[75] Indeed, for the shifted Fibonacci sequence $(f_1, f_2, f_3, \ldots)$, this is clear. For the sequence $(\ell_{-1}, \ell_0, \ell_1, \ldots)$, this follows from (76).

Second proof of Proposition 1.4.9 (sketched). Let us consider domino tilings of the rectangle $R_{n+1,2}$. The # of such tilings is $d_{n+1,2}$ (because we defined $d_{n+1,2}$ to be this #). Hence,

$$\begin{aligned}
&(\#\text{ of domino tilings of } R_{n+1,2}) \\
&= d_{n+1,2} = f_{(n+1)+1} \qquad \text{(by Proposition 1.1.11, applied to } n+1 \text{ instead of } n\text{)} \\
&= f_{n+2}. \qquad (79)
\end{aligned}$$

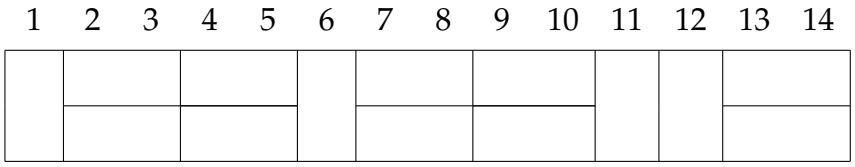
If $D = \{(i,j),(i+1,j)\}$ is a horizontal domino, then we say that D *starts* in column i. In other words, a horizontal domino starts in its western column.

We want to define a map

$$h : \{\text{domino tilings of } R_{n+1,2}\} \to \{\text{lacunar subsets of } [n]\}$$

as follows: If T is any domino tiling of $R_{n+1,2}$, then $h(T)$ shall be the set of all $i \in [n+1]$ such that at least one horizontal domino of T starts in column i.

Before we do anything with this map h, we need to check that it is well-defined. First, let us illustrate it with an example: If $n = 13$ and if T is the domino tiling



(where the numbers on the top are just the numbers of the columns), then $h(T) = \{2,4,7,9,13\}$, since the horizontal dominos of T start in columns $2,4,7,9,13$.

The proof that h is well-defined will rest on the following two observations:

> *Observation 1:* Let T be a domino tiling of $R_{n+1,2}$. Then, no horizontal domino of T starts in column $n+1$.

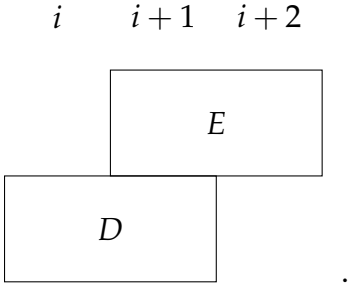
[*Proof of Observation 1:* This is clear, since any horizontal domino that starts in column $n+1$ would continue into column $n+2$ and thus fail to stay inside $R_{n+1,2}$.]

> *Observation 2:* Let T be a domino tiling of $R_{n+1,2}$. Then, no two horizontal dominos of T start in consecutive columns.

[*Proof of Observation 2:* This is easy to see by induction on n (as in the proof of Proposition 1.1.9). An alternative proof proceeds as follows: Assume the contrary. Thus, there are two horizontal dominos of T that start in consecutive columns. In other words, there are two consecutive columns of $R_{n+1,2}$, each of which has a horizontal domino of T start in it. In other words, there exists an $i \in [n]$ such that each of the two consecutive columns i and $i+1$ has a horizontal domino of T start in it. Let us pick the **smallest** such i. Therefore, the column $i-1$ has no horizontal domino of T start in it (since otherwise, $i-1$ would be a smaller candidate than i,

because each of the two consecutive columns $i-1$ and $(i-1)+1=i$ would have a horizontal domino of T start in it).

We know that column i has a horizontal domino of T start in it, and that column $i+1$ has a horizontal domino of T start in it. Let these dominos be D and E (labeled in such a way that D starts in column i, and E starts in column $i+1$). Clearly, the dominos D and E cannot lie in the same row, since otherwise they would overlap. Thus, one of D and E lies in row 1, and the other lies in row 2 (where we number rows from the bottom, so that row 1 is the bottom row of $R_{n+1,2}$). Let us WLOG assume that D lies in row 1 and E lies in row 2 (since the opposite case is analogous). Thus, $D=\{(i,1),(i+1,1)\}$ and $E=\{(i+1,2),(i+2,2)\}$. Here is how D and E look like:



.

Now, the square $(i,2)$ must belong to some domino $F \in T$. This domino F cannot be vertical (since it would otherwise overlap with D), and thus is horizontal. Moreover, this horizontal domino F cannot start in column i (since it would otherwise overlap with E), and thus must start in column $i-1$. This contradicts the fact that the column $i-1$ has no horizontal domino of T start in it. This contradiction shows that our assumption was false; hence, Observation 2 is proven.]

Now, we can confirm that the map h defined above is well-defined: If T is a domino tiling of $R_{n+1,2}$, then the set that we wanted to call $h(T)$ is actually a subset of $[n]$ (since it is a subset of $[n+1]$, but Observation 1 shows that it does not contain $n+1$), and is lacunar (by Observation 2). Thus, h is well-defined.

Next, I claim that h is a bijection. Indeed, let me construct an inverse to h: Consider the map

$$g : \{\text{lacunar subsets of } [n]\} \to \{\text{domino tilings of } R_{n+1,2}\}$$

that sends each lacunar subset S of $[n]$ to the domino tiling of $R_{n+1,2}$ that is constructed by placing two horizontal dominos into columns i and $i+1$ for each $i \in S$, and filling the rest of $R_{n+1,2}$ with vertical dominos. It is easy to see that $h \circ g = \mathrm{id}$. It is somewhat trickier to see that $g \circ h = \mathrm{id}$; this requires the following two observations:

> *Observation 3:* Let T be a domino tiling of $R_{n+1,2}$. Let $i \in [n+1]$ be such that a horizontal domino of T starts in column i. Then, **two** horizontal dominos of T start in column i, and these two dominos cover both columns i and $i+1$.

> *Observation 4:* Let T be a domino tiling of $R_{n+1,2}$. Let $i \in [n+1]$ be such that no horizontal domino of T starts in column i and no horizontal domino of T starts in column $i-1$ either. Then, column i is covered by a vertical domino of T.

It is not hard to prove these two observations. In a nutshell: Observation 3 follows from Observation 2 (because a horizontal domino only covers one square of column i, and the other square must be covered by another domino, which must also be horizontal in order to avoid overlap). Observation 4 follows by noticing that any horizontal domino that contains $(i,1)$ or $(i,2)$ must start either in column i or in column $i-1$.

Together, Observation 3 and Observation 4 show that $g \circ h = \mathrm{id}$ (make sure you understand how), and thus the maps g and h are mutually inverse (since $h \circ g = \mathrm{id}$ holds as well). Hence, the map h is invertible, i.e., a bijection. Thus, the bijection principle yields

$$|\{\text{domino tilings of } R_{n+1,2}\}| = |\{\text{lacunar subsets of } [n]\}|.$$

In other words,

$$(\#\text{ of domino tilings of } R_{n+1,2}) = (\#\text{ of lacunar subsets of } [n]).$$

Comparing this with (79), we find

$$(\#\text{ of lacunar subsets of } [n]) = f_{n+2}.$$

This proves Proposition 1.4.9 again. □

1.4.5. Counting k-element lacunar subsets

Proposition 1.4.9 has answered Question 1.4.3 **(a)**. It remains to answer Question 1.4.3 **(b)**. This is done by the following proposition:

Proposition 1.4.10. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$ be such that $k \leq n+1$. Then,

$$(\#\text{ of } k\text{-element lacunar subsets of } [n]) = \binom{n+1-k}{k}.$$

(To be pedantic, Proposition 1.4.10 only answers Question 1.4.3 **(b)** in the case when $k \leq n+1$. But the remaining case is trivial: If $k > n+1$, then $k > n+1 > n$, and thus the set $[n]$ has no k-element subsets[76], let alone k-element lacunar subsets.)

Proposition 1.4.10 appears in [17f-hw2s, Exercise 3 **(a)**], with two proofs[77]. One way to prove it is by strong induction on n, similar to the first proof of Proposition

[76] by Theorem 1.4.7 **(b)**

[77] To be **very** pedantic: [17f-hw2s, Exercise 3 **(a)**] only states Proposition 1.4.10 in the case when $n \in \mathbb{N}$. But the remaining case is trivial (since $k \leq n+1$ leads to $k = 0$ when n is negative, and thus we have to count 0-element subsets of an empty set, which is not a challenge at this point).

1.4.9. (This is the second solution of [17f-hw2s, Exercise 3 **(a)**].) There is, however, a more enlightening proof than that, which is bijective and explains the binomial coefficient on the right hand side combinatorially. This latter proof will rely on the following fact:[78]

Proposition 1.4.11. Let S be a finite set of integers. Then, there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers satisfying $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$.

Proposition 1.4.11 is just saying that any finite set of integers can be uniquely listed in increasing order (with no repetitions). This is sufficiently self-evident that I have never seen a combinatorics textbook that proves it. A detailed proof can be found in [Grinbe15, proof of Theorem 2.46][79], and a sketch at [19f-hw0s, Outline of a proof of Proposition 1.3].

Let us furthermore make the following convention (which we have already made in our proof of Proposition 1.4.6):

Definition 1.4.12. Let $a_1, a_2, \ldots, a_k$ be k numbers (integers, rational numbers or real numbers). The notation "$\{a_1 < a_2 < \cdots < a_k\}$" shall denote the set $\{a_1, a_2, \ldots, a_k\}$ and simultaneously assert that $a_1 < a_2 < \cdots < a_k$. In other words, it means the set $\{a_1, a_2, \ldots, a_k\}$ when $a_1 < a_2 < \cdots < a_k$, and otherwise is meaningless. Thus, for example, $\{2 < 5 < 8\}$ means the set $\{2, 5, 8\}$, whereas $\{5 < 2 < 8\}$ is meaningless.

Thus, Proposition 1.4.11 can be restated as follows: Each finite set of integers can be uniquely expressed in the form $\{s_1 < s_2 < \cdots < s_k\}$. Of course, the k here is the size of this set.

The following proposition is a variant of Proposition 1.4.11 for the case when $|S|$ is known:

Proposition 1.4.13. Let $m \in \mathbb{N}$. Let S be an m-element set of integers. Then, there exists a unique m-tuple $(s_1, s_2, \ldots, s_m)$ of integers satisfying $\{s_1, s_2, \ldots, s_m\} = S$ and $s_1 < s_2 < \cdots < s_m$.

The subtle difference between Proposition 1.4.11 and Proposition 1.4.13 is that the size of the tuple in Proposition 1.4.13 is specified in advance (viz., it must be $m = |S|$), whereas Proposition 1.4.13 is a statement about tuples of all possible sizes.

The overly skeptical reader may want to solve the following exercise:

[78] We use the word "tuple" as a synonym for "finite list".

[79] In [Grinbe15, §2.6], a tuple $(s_1, s_2, \ldots, s_k)$ of integers satisfying $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$ is called an *increasing list* of S. Thus, our Proposition 1.4.11 is simply saying that any finite set S of integers has a unique increasing list.

Exercise 1.4.2. Derive Proposition 1.4.13 from Proposition 1.4.11.

Now, we can give a bijective proof of Proposition 1.4.10:

Proof of Proposition 1.4.10 (sketched). We have $n+1-k \in \mathbb{N}$ (since $k \leq n+1$). Hence, the set $\{0,1,\ldots,n-k\}$ is an $(n+1-k)$-element set. Theorem 1.3.12 (applied to $n+1-k$ and $\{0,1,\ldots,n-k\}$ instead of n and S) thus shows that

$$(\#\text{ of } k\text{-element subsets of } \{0,1,\ldots,n-k\}) = \binom{n+1-k}{k}. \tag{80}$$

We shall put this equality to use by finding a bijection between
$\{k\text{-element lacunar subsets of } [n]\}$ and $\{k\text{-element subsets of } \{0,1,\ldots,n-k\}\}$.

Proposition 1.4.13 (applied to $m = k$) shows that if S is any k-element set of integers, then there exists a unique k-tuple $(s_1, s_2, \ldots, s_k)$ of integers satisfying $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$. In other words, if S is any k-element set of integers, then S can be uniquely expressed in the form $\{s_1 < s_2 < s_3 < \cdots < s_k\}$.

Hence, if S is any k-element lacunar subset of $[n]$, then S can be uniquely expressed in the form $\{s_1 < s_2 < s_3 < \cdots < s_k\}$. Moreover, the integers $s_1, s_2, \ldots, s_k$ in this expression must satisfy not only $s_i < s_{i+1}$ for each $i \in [k-1]$, but also the stronger inequality $s_i + 1 < s_{i+1}$ for each $i \in [k-1]$ (since otherwise, we would have $s_i + 1 = s_{i+1}$ for some $i \in [k-1]$, and thus the subset S would contain the two consecutive integers s_i and s_{i+1}, which would contradict its lacunarity). Hence, they must satisfy $s_1 - 1 < s_2 - 2 < s_3 - 3 < \cdots < s_k - k$ (because the inequality $s_i + 1 < s_{i+1}$ can be equivalently rewritten as $s_i - i < s_{i+1} - (i+1)$, and these inequalities can be spliced together to form the chain $s_1 - 1 < s_2 - 2 < s_3 - 3 < \cdots < s_k - k$). Furthermore, they must satisfy $s_1 - 1 \geq 0$ (since $s_1 \geq 1$) and $s_k - k \leq n - k$ (since $s_k \leq n$), and therefore the set $\{s_1 - 1 < s_2 - 2 < s_3 - 3 < \cdots < s_k - k\}$ is a well-defined k-element subset of $\{0,1,\ldots,n-k\}$.

Thus, we can define a map

$$A : \{k\text{-element lacunar subsets of } [n]\} \to \{k\text{-element subsets of } \{0,1,\ldots,n-k\}\},$$
$$\{s_1 < s_2 < s_3 < \cdots < s_k\} \mapsto \{s_1 - 1 < s_2 - 2 < s_3 - 3 < \cdots < s_k - k\}.$$

Conversely, it is easy to see that we can define a map

$$B : \{k\text{-element subsets of } \{0,1,\ldots,n-k\}\} \to \{k\text{-element lacunar subsets of } [n]\},$$
$$\{t_1 < t_2 < t_3 < \cdots < t_k\} \mapsto \{t_1 + 1 < t_2 + 2 < t_3 + 3 < \cdots < t_k + k\}.$$

It is fairly obvious that the maps A and B are mutually inverse. Hence, the map A is invertible, i.e., is a bijection. Thus, the bijection principle yields

$$|\{k\text{-element lacunar subsets of } [n]\}|$$
$$= |\{k\text{-element subsets of } \{0,1,\ldots,n-k\}\}|.$$

In other words,

$$\begin{aligned}&(\#\text{ of } k\text{-element lacunar subsets of } [n])\\&= (\#\text{ of } k\text{-element subsets of } \{0,1,\ldots,n-k\})\\&= \binom{n+1-k}{k} \qquad (\text{by (80)}).\end{aligned}$$

This proves Proposition 1.4.10. □

(The above proof of Proposition 1.4.10 can also be rewritten in terms of domino tilings instead of lacunar subsets, since we know a bijection between the former and the latter from our second proof of Proposition 1.4.9.)

By combining Proposition 1.4.9 and Proposition 1.4.10, we can now obtain a bijective proof of Proposition 1.3.32:

Proof of Proposition 1.3.32. Let $m = n-1$. Then, $m \in \{-1,0,1,\ldots\}$ (since $n \in \mathbb{N} = \{0,1,2,\ldots\}$) and $m+1 = n$. Hence, it is easy to see that $|[m]| \leq n$ [80].

If B is any subset of $[m]$, then Theorem 1.4.7 **(b)** (applied to $A = [m]$) yields $|B| \leq |[m]| \leq n$ and therefore $|B| \in \{0,1,\ldots,n\}$. Hence, the sum rule yields[81]

$$\begin{aligned}&(\#\text{ of lacunar subsets of } [m])\\&= \sum_{k\in\{0,1,\ldots,n\}} \underbrace{(\#\text{ of lacunar subsets } B \text{ of } [m] \text{ satisfying } |B| = k)}_{=(\#\text{ of } k\text{-element lacunar subsets of } [m])}\\&\qquad\qquad = \underbrace{\binom{m+1-k}{k}}_{\substack{\text{(by Proposition 1.4.10, applied to } m \text{ instead of } n)}}\\&= \sum_{k\in\{0,1,\ldots,n\}} \binom{m+1-k}{k} = \sum_{k=0}^{n} \binom{m+1-k}{k} = \sum_{k=0}^{n} \binom{n-k}{k}\end{aligned}$$

(since $m+1 = n$). Comparing this with

$$\begin{aligned}&(\#\text{ of lacunar subsets of } [m])\\&= f_{m+2} \qquad (\text{by Proposition 1.4.9, applied to } m \text{ instead of } n)\\&= f_{n+1} \qquad \left(\text{since } m+2 = \underbrace{(m+1)}_{=n}+1 = n+1\right),\end{aligned}$$

we obtain

$$f_{n+1} = \sum_{k=0}^{n} \binom{n-k}{k} = \binom{n-0}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-n}{n}.$$

This proves Proposition 1.3.32. □

[80] *Proof.* If $m \in \mathbb{N}$, then $|[m]| = m = n-1 \leq n$. Hence, if $m \in \mathbb{N}$, then we are done. Thus, we WLOG assume that $m \notin \mathbb{N}$. Combining this with $m \in \{-1,0,1,\ldots\}$, we obtain $m \in \{-1,0,1,\ldots\} \setminus \mathbb{N} = \{-1\}$, so that $m = -1$. Thus, $m+1 = 0$, so that $n = m+1 = 0$. But $m = -1$ and thus $[m] = \varnothing$ and therefore $|[m]| = |\varnothing| = 0 = n$ (since $n = 0$). Hence, $|[m]| \leq n$, qed.

[81] Again, the sum rule that we are using here is Theorem 1.2.5.

This is not the only known proof of Proposition 1.3.32. There is also a (more straightforward) proof by strong induction on n using Theorem 1.3.8. (See [Vorobi02, §1.15] for the details of this proof, or find it yourself.)

1.4.6. Counting subsets with a odd and b even elements

Question 1.4.3 is resolved. Here is another one, to illustrate a principle we shall use more often later: Given $n, a, b \in \mathbb{N}$, how many subsets of $[n]$ have exactly a even elements and exactly b odd elements? Here is the answer in the case when n is even:

Proposition 1.4.14. Let $n \in \mathbb{N}$ be even. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Then,

$$(\#\text{ of subsets of } [n] \text{ that contain } a \text{ even elements and } b \text{ odd elements}) = \binom{n/2}{a}\binom{n/2}{b}.$$

(Here, "a even elements" means "exactly a even elements", and "b odd elements" means "exactly b odd elements".)

The following proof is essentially copied from [18s-hw1s, Exercise 6 **(a)**]:

Proof of Proposition 1.4.14. Informally, our argument is as follows: Let E be the set of all even elements of $[n]$; let O be the set of all odd elements of $[n]$. We want to find the # of subsets of $[n]$ that contain a even elements and b odd elements. In order to construct such a subset, we can choose its a even elements and its b odd elements separately. The a even elements must be chosen from the set E; thus, choosing them means choosing an a-element subset of E. There are $\binom{|E|}{a}$ ways to make this choice (by Theorem 1.3.12, applied to E, $|E|$ and a instead of S, n and k). The b odd elements must be chosen from the set O; thus, choosing them means choosing a b-element subset of O. There are $\binom{|O|}{b}$ ways to make this choice (by Theorem 1.3.12, applied to O, $|O|$ and b instead of S, n and k). Hence, altogether, our choices can be made in $\binom{|E|}{a}\binom{|O|}{b}$ many ways; thus,

$$(\#\text{ of subsets of } [n] \text{ that contain } a \text{ even elements and } b \text{ odd elements}) = \binom{|E|}{a}\binom{|O|}{b}. \tag{81}$$

But n is even, and thus

$$E = \{2, 4, 6, \ldots, n\} \qquad \text{and} \qquad O = \{1, 3, 5, \ldots, n-1\}.$$

Hence, each of the two sets E and O has exactly $n/2$ elements. In other words, $|E| = n/2$ and $|O| = n/2$. Thus, the equality (81) rewrites as

$$\begin{aligned}&(\text{\# of subsets of } [n] \text{ that contain } a \text{ even elements and } b \text{ odd elements})\\ &= \binom{n/2}{a}\binom{n/2}{b}.\end{aligned}$$

This proves Proposition 1.4.14.

Here is a more rigorous way to write up the same proof (without speaking of "choices", which arguably is not a well-defined mathematical notion). Let E be the set of all even elements of $[n]$; let O be the set of all odd elements of $[n]$. Let $\mathcal{N}$ be the set of all subsets of $[n]$ that contain exactly a even elements and exactly b odd elements. Thus,

$$\begin{aligned}&(\text{\# of subsets of } [n] \text{ that contain } a \text{ even elements and } b \text{ odd elements})\\ &= |\mathcal{N}|. \end{aligned} \tag{82}$$

Hence, we need to show that $|\mathcal{N}| = \binom{n/2}{a}\binom{n/2}{b}$.

For any set X and every $k \in \mathbb{N}$, we let $\mathcal{P}_k(X)$ denote the set of all k-element subsets of X. Now, the two maps

$$\begin{aligned}\mathcal{N} &\to \mathcal{P}_a(E) \times \mathcal{P}_b(O),\\ S &\mapsto (S \cap E, S \cap O)\end{aligned}$$

and

$$\begin{aligned}\mathcal{P}_a(E) \times \mathcal{P}_b(O) &\to \mathcal{N},\\ (U, V) &\mapsto U \cup V\end{aligned}$$

are well-defined and mutually inverse[82]. Hence, these two maps are bijections.

[82]Instead of proving this in detail (which is straightforward), let me unfold the notations and explain what the two maps do:

- The first map sends any $S \in \mathcal{N}$ (that is, any subset S of $[n]$ that contains a even elements and b odd elements) to the pair $(S \cap E, S \cap O)$, which consists of
  - the set $S \cap E$ (this is the set of all even elements of S; it is an a-element set, because S contains exactly a even elements) and
  - the set $S \cap O$ (this is the set of all odd elements of S; it is a b-element set).

  In other words, the first map splits any $S \in \mathcal{N}$ into its set of even elements and its set of odd elements.
- The second map sends any pair $(U, V) \in \mathcal{P}_a(E) \times \mathcal{P}_b(O)$ to the union $U \cup V \in \mathcal{N}$. In other words, the second map takes a pair (U, V) consisting of an a-element set of even numbers and a b-element set of odd numbers, and combines them to the set $U \cup V$ (which belongs to $\mathcal{N}$, because it has a even elements and b odd elements).

From this point of view, it should be clear that the two maps are well-defined and mutually inverse.

Thus, there exists a bijection $\mathcal{N} \to \mathcal{P}_a(E) \times \mathcal{P}_b(O)$. Therefore, the bijection principle shows that

$$|\mathcal{N}| = |\mathcal{P}_a(E) \times \mathcal{P}_b(O)| = |\mathcal{P}_a(E)| \cdot |\mathcal{P}_b(O)| \tag{83}$$

(by the product rule, i.e., by (5), applied to $X = \mathcal{P}_a(E)$ and $Y = \mathcal{P}_b(O)$).

But every finite set S and every $k \in \mathbb{N}$ satisfy

$$\mathcal{P}_k(S) = \{k\text{-element subsets of } S\} \qquad \text{(by the definition of } \mathcal{P}_k(S)\text{)}$$

and thus

$$\begin{aligned} |\mathcal{P}_k(S)| &= (\#\text{ of } k\text{-element subsets of } S) \\ &= \binom{|S|}{k} \end{aligned} \tag{84}$$

(by Theorem 1.3.12, applied to $|S|$ instead of n).

Now, (83) becomes

$$|\mathcal{N}| = \underbrace{|\mathcal{P}_a(E)|}_{\substack{=\binom{|E|}{a} \\ \text{(by (84))}}} \cdot \underbrace{|\mathcal{P}_b(O)|}_{\substack{=\binom{|O|}{b} \\ \text{(by (84))}}} = \binom{|E|}{a}\binom{|O|}{b}.$$

Now, recall that n is even. Thus, there are exactly $n/2$ even numbers in the set $[n]$ (namely, $2, 4, 6, \ldots, n$). In other words, the set of all even elements of $[n]$ has size $n/2$. In other words, the set E has size $n/2$ (since E is the set of all even elements of $[n]$). In other words, $|E| = n/2$. Similarly, $|O| = n/2$. Now,

$$|\mathcal{N}| = \binom{|E|}{a}\binom{|O|}{b} = \binom{n/2}{a}\binom{n/2}{b}$$

(since $|E| = n/2$ and $|O| = n/2$). Hence, (82) becomes

$$\begin{aligned} &(\#\text{ of subsets of } [n] \text{ that contain } a \text{ even elements and } b \text{ odd elements}) \\ &= |\mathcal{N}| = \binom{n/2}{a}\binom{n/2}{b}. \end{aligned}$$

This proves Proposition 1.4.14. □

The relation between the above informal proof and its formalized version is worth pointing out explicitly: Informally, we argued that choosing a subset with a even and b odd elements is tantamount to independently choosing a elements from E and b elements from O. We formalized this argument as a bijection from $\mathcal{N}$ to $\mathcal{P}_a(E) \times \mathcal{P}_b(O)$, and then used the product rule along with the bijection principle to conclude that $|\mathcal{N}| = |\mathcal{P}_a(E)| \cdot |\mathcal{P}_b(O)|$. Thus, "independent choices" in informal arguments correspond to an application of the product rule and the bijection principle when formalized.

The analogue of Proposition 1.4.14 in the case of odd n can be proven in the same way:

Proposition 1.4.15. Let $n \in \mathbb{N}$ be odd. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Then,

$$\begin{aligned}&(\#\text{ of subsets of } [n] \text{ that contain } a \text{ even elements and } b \text{ odd elements})\\ &= \binom{(n-1)/2}{a}\binom{(n+1)/2}{b}.\end{aligned}$$

We leave the proof to the reader.

Class of 2019-10-09

1.4.7. The addition formula for Fibonacci numbers

Let us see some of these tactics being used again in proving an identity for Fibonacci numbers:

Theorem 1.4.16. Let $m, n \in \mathbb{N}$. Then, the Fibonacci sequence satisfies $f_{m+n+1} = f_m f_n + f_{m+1} f_{n+1}$.

This is not a-priori a combinatorial result; it is just an algebraic identity for the elements of a recursively defined sequence. Consequently, we should expect it to have a purely algebraic proof. And this is indeed the case: Theorem 1.4.16 can easily be proven by induction on n. For such proofs, see [18s-mt1s, solution to Exercise 3 **(e)**] or (in a slightly more general setting) [Grinbe15, proof of Theorem 2.26 **(a)**][83]. We shall, instead, derive Theorem 1.4.16 from the combinatorial interpretation of the Fibonacci numbers.

To simplify this proof, we shall front-load a little argument into a separate proposition (Proposition 1.4.18). We begin with a fairly standard piece of notation:

Definition 1.4.17. Let a and b be two integers. Then, the subset $\{a, a+1, \ldots, b\}$ of $\mathbb{Z}$ (this is the set of all integers i satisfying $a \leq i \leq b$) will be denoted by $[a, b]$. (Recall that this subset is understood to be $\varnothing$ when $b < a$.)

The subset $[a, b]$ is called the *integer interval from a to b*. (It is not an interval in the sense of real analysis, since it only contains integers; but it is the combinatorial analogue of an interval.)

For example, using this notation, we have $[2, 5] = \{2, 3, 4, 5\}$ and $[3, 3] = \{3\}$. Note that we have $[k] = [1, k]$ for each $k \in \mathbb{Z}$.

Proposition 1.4.18. Let $n \in \{-1, 0, 1, \ldots\}$ and $a \in \mathbb{Z}$. Then,

$$(\#\text{ of lacunar subsets of } [a+1, a+n]) = f_{n+2}.$$

[83] To recover Theorem 1.4.16 from [Grinbe15, Theorem 2.26 **(a)**], set $a = 1$ and $b = 1$. Then, the sequence $(x_0, x_1, x_2, \ldots)$ in [Grinbe15, Theorem 2.26 **(a)**] becomes the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$.

Proof of Proposition 1.4.18. Here is an outline: The integer interval $[a+1, a+n]$ is just the integer interval $[n]$ shifted by a. Hence, the lacunar subsets of the former interval are in 1-to-1 correspondence with the lacunar subsets of the latter interval. Hence, the number of lacunar subsets of the former interval equals the number of lacunar subsets of the latter interval. Thus,

$$(\#\text{ of lacunar subsets of } [a+1, a+n]) = (\#\text{ of lacunar subsets of } [n]) = f_{n+2}$$

(by Proposition 1.4.9). This proves Proposition 1.4.18.

Formally speaking, the argument we have just made is a bijective proof, which can be made rigorous as follows: For each subset S of $[n]$, we let $S+a$ denote the set $\{s+a \mid s \in S\}$. This set $S+a$ is clearly a subset of $[a+1, a+n]$. (Informally speaking, $S+a$ is just the set S shifted by a units on the number line.) Conversely, for each subset T of $[a+1, a+n]$, we let $T-a$ denote the set $\{t-a \mid t \in T\}$. [84] This set $T-a$ is clearly a subset of $[n]$. (Informally speaking, $T-a$ is just the set T shifted by $-a$ units on the number line.) Now, it is easy to see that the maps

$$\{\text{lacunar subsets of } [n]\} \to \{\text{lacunar subsets of } [a+1, a+n]\}, \quad S \mapsto S+a$$

and

$$\{\text{lacunar subsets of } [a+1, a+n]\} \to \{\text{lacunar subsets of } [n]\}, \quad T \mapsto T-a$$

are well-defined[85] and mutually inverse. Hence, they are bijections. Thus, the bijection principle yields

$$|\{\text{lacunar subsets of } [a+1, a+n]\}| = |\{\text{lacunar subsets of } [n]\}|.$$

In other words,

$$(\#\text{ of lacunar subsets of } [a+1, a+n]) = (\#\text{ of lacunar subsets of } [n]) = f_{n+2}$$

(by Proposition 1.4.9). This proves Proposition 1.4.18. □

We now come to our combinatorial proof of Theorem 1.4.16:

Proof of Theorem 1.4.16 (sketched). If $m = 0$, then the claim of Theorem 1.4.16 boils down to the equality $f_{n+1} = f_0 f_n + f_1 f_{n+1}$, which is obvious (since $f_0 = 0$ and $f_1 = 1$). Hence, for the rest of this proof, we WLOG assume that $m \neq 0$. For a similar reason, we WLOG assume that $n \neq 0$. From $m \neq 0$, we obtain $m \geq 1$ (since $m \in \mathbb{N}$). Hence, $m-2 \geq 1-2 = -1$, so that $m-2 \in \{-1, 0, 1, \ldots\}$.

[84] Minor annoying caveat: Some people use the minus sign $-$ for set-theoretic difference (so they write $P-Q$ for $P \setminus Q$). This is not what we mean when we write $T-a$.

[85] This means, in particular, that if a subset S of $[n]$ is lacunar, then so is $S+a$. This is all straightforward.

Similarly, $n-2 \in \{-1,0,1,\ldots\}$. Furthermore, $\underbrace{m}_{\geq 1} + \underbrace{n}_{\geq 1} - 1 \geq 1+1-1 = 1$, so that $m+n-1 \in \mathbb{N} \subseteq \{-1,0,1,\ldots\}$.

Now, let us count the lacunar subsets of $[m+n-1]$ in two different ways:

First way: Proposition 1.4.9 (applied to $m+n-1$ instead of n) yields

$$(\text{\# of lacunar subsets of } [m+n-1]) = f_{(m+n-1)+2} = f_{m+n+1}. \tag{85}$$

Second way: We shall call a subset of $[m+n-1]$

- **red** if it contains m, and
- **green** if it does not contain m.

Thus, each subset of $[m+n-1]$ is either red or green (but not both at the same time). Thus, by the sum rule, we have

$$\begin{aligned}&(\text{\# of lacunar subsets of } [m+n-1]) \\ &= (\text{\# of lacunar red subsets of } [m+n-1]) \\ &\qquad + (\text{\# of lacunar green subsets of } [m+n-1]).\end{aligned} \tag{86}$$

We shall now compute the two addends on the right hand side.

A lacunar green subset S of $[m+n-1]$ does not contain m, and thus is the union of its two subsets $\{s \in S \mid s < m\}$ and $\{s \in S \mid s > m\}$. The former of these two subsets is a lacunar subset of $[m-1]$, while the latter is a lacunar subset of $[m+1, m+n-1]$. Hence, a lacunar green subset of $[m+n-1]$ is just the union of a lacunar subset of $[m-1]$ with a lacunar subset of $[m+1, m+n-1]$. Conversely, any such union must be a lacunar green subset of $[m+n-1]$ (since an element of $[m-1]$ and an element of $[m+1, m+n-1]$ cannot be consecutive[86]). Summarizing this discussion, we conclude that the map

$$\begin{aligned}&\{\text{lacunar green subsets of } [m+n-1]\} \\ &\to \{\text{lacunar subsets of } [m-1]\} \times \{\text{lacunar subsets of } [m+1, m+n-1]\}\end{aligned}$$

that sends any lacunar green subset S of $[m+n-1]$ to the pair

$$(\{s \in S \mid s < m\}, \{s \in S \mid s > m\})$$

is well-defined and is a bijection (and the inverse of this map simply sends each pair (P, Q) to $P \cup Q$). Thus, the bijection principle yields

$$\begin{aligned}&|\{\text{lacunar green subsets of } [m+n-1]\}| \\ &= |\{\text{lacunar subsets of } [m-1]\} \times \{\text{lacunar subsets of } [m+1, m+n-1]\}| \\ &= |\{\text{lacunar subsets of } [m-1]\}| \cdot |\{\text{lacunar subsets of } [m+1, m+n-1]\}|\end{aligned}$$

[86] because m separates them

(by the product rule). In other words,

$$\begin{aligned}
&(\#\text{ of lacunar green subsets of } [m+n-1]) \\
&= \underbrace{(\#\text{ of lacunar subsets of } [m-1])}_{\substack{=f_{(m-1)+2} \\ \text{(by Proposition 1.4.9,} \\ \text{applied to } m-1 \text{ instead of } n)}} \cdot \underbrace{(\#\text{ of lacunar subsets of } [m+1, m+n-1])}_{\substack{=f_{(n-1)+2} \\ \text{(by Proposition 1.4.18,} \\ \text{applied to } m \text{ and } n-1 \text{ instead of } a \text{ and } n)}} \\
&= \underbrace{f_{(m-1)+2}}_{=f_{m+1}} \cdot \underbrace{f_{(n-1)+2}}_{=f_{n+1}} = f_{m+1} f_{n+1}. \qquad (87)
\end{aligned}$$

Now, let us take a look at lacunar red subsets.

A lacunar red subset S of $[m+n-1]$ contains m, and thus contains neither $m-1$ nor $m+1$ (since it is lacunar); hence, it is the union of its two subsets $\{s \in S \mid s < m-1\}$ and $\{s \in S \mid s > m+1\}$ and the one-element set $\{m\}$. The former of these two subsets is a lacunar subset of $[m-2]$, while the latter is a lacunar subset of $[m+2, m+n-1]$. Hence, a lacunar red subset of $[m+n-1]$ is just the union of the following three sets: a lacunar subset of $[m-2]$, a lacunar subset of $[m+2, m+n-1]$, and the one-element set $\{m\}$. Conversely, any such union must be a lacunar red subset of $[m+n-1]$ (since an element of $[m-2]$ and an element of $[m+2, m+n-1]$ cannot be consecutive, and furthermore no such element can be consecutive to m). Summarizing this discussion, we conclude that the map

$$\begin{aligned}
&\{\text{lacunar red subsets of } [m+n-1]\} \\
&\to \{\text{lacunar subsets of } [m-2]\} \times \{\text{lacunar subsets of } [m+2, m+n-1]\}
\end{aligned}$$

that sends any lacunar red subset S of $[m+n-1]$ to the pair

$$(\{s \in S \mid s < m-1\}, \{s \in S \mid s > m+1\})$$

is well-defined and is a bijection (and the inverse of this map simply sends each pair (P, Q) to $P \cup Q \cup \{m\}$). Thus, the bijection principle yields

$$\begin{aligned}
&|\{\text{lacunar red subsets of } [m+n-1]\}| \\
&= |\{\text{lacunar subsets of } [m-2]\} \times \{\text{lacunar subsets of } [m+2, m+n-1]\}| \\
&= |\{\text{lacunar subsets of } [m-2]\}| \cdot |\{\text{lacunar subsets of } [m+2, m+n-1]\}|
\end{aligned}$$

(by the product rule). In other words,

$$\begin{aligned}
&(\#\text{ of lacunar red subsets of } [m+n-1]) \\
&= \underbrace{(\#\text{ of lacunar subsets of } [m-2])}_{\substack{=f_{(m-2)+2} \\ \text{(by Proposition 1.4.9,} \\ \text{applied to } m-2 \text{ instead of } n)}} \cdot \underbrace{(\#\text{ of lacunar subsets of } [m+2, m+n-1])}_{\substack{=f_{(n-2)+2} \\ \text{(by Proposition 1.4.18,} \\ \text{applied to } m+1 \text{ and } n-2 \text{ instead of } a \text{ and } n)}} \\
&= \underbrace{f_{(m-2)+2}}_{=f_m} \cdot \underbrace{f_{(n-2)+2}}_{=f_n} = f_m f_n. \qquad (88)
\end{aligned}$$

Hence, (86) becomes

$$\begin{aligned}
&(\#\text{ of lacunar subsets of } [m+n-1]) \\
&= \underbrace{(\#\text{ of lacunar red subsets of } [m+n-1])}_{\substack{=f_m f_n \\ \text{(by (88))}}} \\
&\qquad + \underbrace{(\#\text{ of lacunar green subsets of } [m+n-1])}_{\substack{=f_{m+1} f_{n+1} \\ \text{(by (87))}}} \\
&= f_m f_n + f_{m+1} f_{n+1}. \qquad (89)
\end{aligned}$$

Comparing (85) with (89), we obtain $f_{m+n+1} = f_m f_n + f_{m+1} f_{n+1}$. Thus, Theorem 1.4.16 is proven. □

The proof we just gave is an example of a *proof by double counting*: We have counted the lacunar subsets of $[m+n-1]$ (that is, computed their number) in two different ways. In the first way, we obtained (85); in the second, we found (89). Comparing the results, we then obtained the equality $f_{m+n+1} = f_m f_n + f_{m+1} f_{n+1}$, which we had set out to prove.

Such proofs often look like magic, but they are not always hard to find: If you want to prove an identity of the form $A = B$ by double counting, all you have to do is come up with a counting problem that can be solved in two ways, one of which gives A as a result while the other gives B. The specifics of A and B often give away how the problem could look like. For example, because the identity we were proving was $f_{m+n+1} = f_m f_n + f_{m+1} f_{n+1}$, it stood to reason that the counting problem should be "how many lacunar subsets does $[m+n-1]$ have?". This way, it is immediately clear that one answer is f_{m+n+1} (by Proposition 1.4.9); it remained to find a second way to solve the counting problem and get $f_m f_n + f_{m+1} f_{n+1}$ instead. The form of this expression suggests using the sum rule, so that the lacunar subsets of $[m+n-1]$ had to somehow be subdivided into two categories (the "red" and the "green" ones in the above proof) numbering $f_m f_n$ and $f_{m+1} f_{n+1}$, respectively. Furthermore, each of these categories should have a product-like structure (i.e., a lacunar red subset should fall apart into two independent parts, and likewise for a lacunar green subset), so that the products $f_m f_n$ and $f_{m+1} f_{n+1}$ could be explained by the product rule. With these heuristics, it is not hard to come up with the exact argument given above. This kind of reverse-engineering strategy does not always work (it is an art, not a science, and it relies heavily on your preknowledge), but when it does, the result is usually worth it.

Our proof of Proposition 1.3.32 was also a proof by double counting.

Benjamin and Quinn have devoted a whole book [BenQui03] to proofs by double counting; it has many more examples. In particular, they give a proof of Theorem 1.4.16 ("Identity 3" in their book) which uses domino tilings, but essentially is the same as our proof.[87]

[87] Recall that domino tilings and lacunar subsets are more or less interchangeable, as our Second

1.4.8. More subset counting

Let us explore some more classes of subsets, each time asking ourselves have many there are. We begin with the following:

Exercise 1.4.3. A set S of integers is said to be *self-counting* if the size $|S|$ is an element of S. (For example, $\{1,3,5\}$ is self-counting, since $|\{1,3,5\}| = 3 \in \{1,3,5\}$; but $\{1,2,5\}$ is not self-counting.)

Let n be a positive integer.

(a) For each $k \in [n]$, find the # of self-counting k-element subsets of $[n]$.

(b) Find the # of all self-counting subsets of $[n]$.

This exercise is essentially [17f-hw1s, Exercise 8].

Solution to Exercise 1.4.3 (sketched). **(a)** Fix $k \in [n]$. For any k-element subset S of $[n]$, we have the following chain of logical equivalences:

$$\begin{aligned}
&(S \text{ is self-counting}) \\
&\iff (\text{the size } |S| \text{ is an element of } S) \qquad (\text{by the definition of "self-counting"}) \\
&\iff (|S| \in S) \\
&\iff (k \in S) \qquad (\text{since } |S| = k \text{ (because } S \text{ is a } k\text{-element set)}) \\
&\iff (S \text{ contains } k)\,.
\end{aligned}$$

Thus, the self-counting k-element subsets of $[n]$ are precisely the k-element subsets of $[n]$ that contain k. Hence,

$$\begin{aligned}
&(\#\text{ of self-counting } k\text{-element subsets of } [n]) \\
&= (\#\text{ of } k\text{-element subsets of } [n] \text{ that contain } k)\,.
\end{aligned} \tag{90}$$

But the maps

$$\begin{aligned}
\{k\text{-element subsets of } [n] \text{ that contain } k\} &\to \{(k-1)\text{-element subsets of } [n] \setminus \{k\}\}\,, \\
S &\mapsto S \setminus \{k\}
\end{aligned}$$

and

$$\begin{aligned}
\{(k-1)\text{-element subsets of } [n] \setminus \{k\}\} &\to \{k\text{-element subsets of } [n] \text{ that contain } k\}\,, \\
T &\mapsto T \cup \{k\}
\end{aligned}$$

are well-defined[88] and mutually inverse[89], and thus are bijections. Hence, the bijection

proof of Proposition 1.4.9 has shown.

[88] This means the following:

- If S is a k-element subset of $[n]$ that contains k, then $S \setminus \{k\}$ is a $(k-1)$-element subset of $[n] \setminus \{k\}$.
- If T is a $(k-1)$-element subset of $[n] \setminus \{k\}$, then $T \cup \{k\}$ is a k-element subset of $[n]$ that contains k.

Checking this is straightforward; you can do it in your head, but don't forget to do this!

[89] For this, you need to show that

principle yields

$$\begin{aligned}&|\{k\text{-element subsets of } [n] \text{ that contain } k\}| \\ &= |\{(k-1)\text{-element subsets of } [n] \setminus \{k\}\}| \\ &= (\#\text{ of } (k-1)\text{-element subsets of } [n] \setminus \{k\}). \end{aligned} \tag{91}$$

But $[n]$ is an n-element set; hence, $[n] \setminus \{k\}$ is an $(n-1)$-element set (since $k \in [n]$). Therefore, $n-1 \in \mathbb{N}$, and furthermore, Theorem 1.3.12 (applied to $n-1$, $k-1$ and $[n] \setminus \{k\}$ instead of n, k and S) shows that

$$\binom{n-1}{k-1} = (\#\text{ of } (k-1)\text{-element subsets of } [n] \setminus \{k\}).$$

Comparing this with (91), we obtain

$$|\{k\text{-element subsets of } [n] \text{ that contain } k\}| = \binom{n-1}{k-1}.$$

Now, (90) becomes

$$\begin{aligned}&(\#\text{ of self-counting } k\text{-element subsets of } [n]) \\ &= (\#\text{ of } k\text{-element subsets of } [n] \text{ that contain } k) \\ &= |\{k\text{-element subsets of } [n] \text{ that contain } k\}| = \binom{n-1}{k-1}. \end{aligned} \tag{92}$$

This solves Exercise 1.4.3 **(a)**.

(b) Let S be a self-counting subset of $[n]$. Then, $|S| \in S$ (since S is self-counting), and thus the set S has at least one element (namely, $|S|$). Thus, $|S| \geq 1$. But Theorem 1.4.7 **(b)** (applied to $A = [n]$ and $B = S$) yields $|S| \leq |[n]| = n$. Hence, $|S| \in [n]$ (since $|S|$ is an integer satisfying $|S| \geq 1$ and $|S| \leq n$).

Now, forget that we fixed S. We thus have shown that each self-counting subset S of $[n]$ satisfies $|S| \in [n]$. Hence, by the sum rule, we have

$$\begin{aligned}&(\#\text{ of self-counting subsets of } [n]) \\ &= \sum_{k \in [n]} \underbrace{(\#\text{ of self-counting subsets } S \text{ of } [n] \text{ such that } |S| = k)}_{= (\#\text{ of self-counting } k\text{-element subsets of } [n])} = \sum_{k \in [n]} \underbrace{\binom{n-1}{k-1}}_{\substack{= \binom{n-1}{k-1} \\ \text{(by (92))}}} \\ &= \sum_{k=1}^{n} \binom{n-1}{k-1} \qquad \left(\text{since the summation sign } \sum_{k \in [n]} \text{ means the same as } \sum_{k=1}^{n}\right) \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} \qquad (\text{here, we have substituted } k \text{ for } k-1 \text{ in the sum}). \end{aligned}$$

- If S is a k-element subset of $[n]$ that contains k, then $(S \setminus \{k\}) \cup \{k\} = S$.
- If T is a $(k-1)$-element subset of $[n] \setminus \{k\}$, then $(T \cup \{k\}) \setminus \{k\} = T$.

This is again entirely straightforward.

But $n-1 \in \mathbb{N}$ (since n is a positive integer). Thus, Corollary 1.3.27 (applied to $n-1$ instead of n) yields $\sum_{k=0}^{n-1} \binom{n-1}{k} = 2^{n-1}$. Hence,

$$(\#\text{ of self-counting subsets of } [n]) = \sum_{k=0}^{n-1} \binom{n-1}{k} = 2^{n-1}.$$

This solves Exercise 1.4.3 **(b)**. □

Our next exercise is a slight variation on this one, in which we count subsets of $[n]$ whose size is not just some element but in fact the smallest one:

Exercise 1.4.4. A set S of integers is said to be *self-starting* if the size $|S|$ is the smallest element of S. (For example, the set $\{3,4,6\}$ is self-starting, since $|\{3,4,6\}| = 3$ is its smallest element; but $\{1,3,6\}$ and $\{1,2,6\}$ are not self-starting.)

Let n be a positive integer.

(a) For each $k \in [n]$, find the # of self-starting k-element subsets of $[n]$.

(b) Find the # of all self-starting subsets of $[n]$.

This exercise is essentially [18s-hw1s, Exercise 7]. Note that self-starting sets are called "maximal sets" in [Chu19].

Solution to Exercise 1.4.4 (sketched). Recall the notation from Definition 1.4.17; in particular, if $k \in \mathbb{Z}$, then $[k+1, n]$ will mean the integer interval $\{k+1, k+2, \ldots, n\}$.

(a) Fix $k \in [n]$. For any k-element subset S of $[n]$, we have the following chain of logical equivalences:

$$\begin{aligned}
&(S \text{ is self-starting}) \\
\iff\ &(|S| \text{ is the smallest element of } S) \qquad \text{(by the definition of "self-starting")} \\
\iff\ &(k \text{ is the smallest element of } S) \\
&\qquad \text{(since } |S| = k \text{ (because } S \text{ is a } k\text{-element set))} \\
\iff\ &(k \in S, \text{ but all elements of } S \text{ other than } k \text{ are larger than } k) \\
\iff\ &(k \in S, \text{ but all elements of } S \text{ other than } k \text{ belong to } [k+1, n]) \\
&\qquad \left(\begin{array}{c} \text{because an element of } S \text{ is larger than } k \text{ if and only if} \\ \text{it belongs to } [k+1, n] \text{ (since it belongs to } [n]\text{)} \end{array} \right) \\
\iff\ &(k \in S, \text{ but all elements of } S \setminus \{k\} \text{ belong to } [k+1, n]) \\
&\qquad \left(\begin{array}{c} \text{since the elements of } S \text{ other than } k \\ \text{are precisely the elements of } S \setminus \{k\} \end{array} \right) \\
\iff\ &(k \in S \text{ and } S \setminus \{k\} \subseteq [k+1, n])
\end{aligned}$$

(since the statement "all elements of $S \setminus \{k\}$ belong to $[k+1, n]$" means the same as "$S \setminus \{k\} \subseteq [k+1, n]$"). Thus, the self-starting k-element subsets of $[n]$ are precisely the k-element subsets of $[n]$ that contain k and satisfy $S \setminus \{k\} \subseteq [k+1, n]$. Hence, the maps

$$\begin{aligned}
\{\text{self-starting } k\text{-element subsets of } [n]\} &\to \{(k-1)\text{-element subsets of } [k+1, n]\}, \\
S &\mapsto S \setminus \{k\}
\end{aligned}$$

and

$$\{(k-1)\text{-element subsets of } [k+1,n]\} \to \{\text{self-starting } k\text{-element subsets of } [n]\},$$
$$T \mapsto T \cup \{k\}$$

are well-defined[90] and mutually inverse, and thus are bijections. Hence, the bijection principle yields

$$\begin{aligned} &|\{\text{self-starting } k\text{-element subsets of } [n]\}| \\ &= |\{(k-1)\text{-element subsets of } [k+1,n]\}| \\ &= (\#\text{ of } (k-1)\text{-element subsets of } [k+1,n]). \end{aligned} \tag{93}$$

But $[k+1,n] = \{k+1, k+2, \ldots, n\}$ is an $(n-k)$-element set (since $k \in [n]$ yields $k \leq n$). Therefore, $n-k \in \mathbb{N}$, and furthermore, Theorem 1.3.12 (applied to $n-k$, $k-1$ and $[k+1,n]$ instead of n, k and S) shows that

$$\binom{n-k}{k-1} = (\#\text{ of } (k-1)\text{-element subsets of } [k+1,n]).$$

Comparing this with (93), we obtain

$$|\{\text{self-starting } k\text{-element subsets of } [n]\}| = \binom{n-k}{k-1}.$$

In other words,

$$(\#\text{ of self-starting } k\text{-element subsets of } [n]) = \binom{n-k}{k-1}. \tag{94}$$

This solves Exercise 1.4.4 **(a)**.

(b) Let S be a self-starting subset of $[n]$. Then, $|S|$ is the smallest element of S (since S is self-starting), and thus the set S has at least one element (namely, $|S|$). Thus, $|S| \geq 1$. But Theorem 1.4.7 **(b)** (applied to $A = [n]$ and $B = S$) yields $|S| \leq |[n]| = n$. Hence, $|S| \in [n]$ (since $|S|$ is an integer satisfying $|S| \geq 1$ and $|S| \leq n$).

Now, forget that we fixed S. We thus have shown that each self-starting subset S of $[n]$

[90] As in the solution to Exercise 1.4.3, all these claims need to be thoroughly checked, but this can be quickly done in your head.

satisfies $|S| \in [n]$. Hence, by the sum rule, we have

$$\begin{aligned}
&(\text{\# of self-starting subsets of } [n]) \\
&= \sum_{k \in [n]} \underbrace{(\text{\# of self-starting subsets } S \text{ of } [n] \text{ such that } |S| = k)}_{= (\text{\# of self-starting } k\text{-element subsets of } [n])} \\
&\qquad\qquad = \underbrace{\binom{n-k}{k-1}}_{\text{(by (94))}} \\
&= \sum_{k \in [n]} \underbrace{\binom{n-k}{k-1}}_{= \binom{(n-1)-(k-1)}{k-1}} = \sum_{k \in [n]} \binom{(n-1)-(k-1)}{k-1} = \sum_{k=1}^{n} \binom{(n-1)-(k-1)}{k-1} \\
&\qquad\qquad \text{(since } n-k=(n-1)-(k-1)\text{)} \\
&\qquad \left(\text{since the summation sign } \sum_{k \in [n]} \text{ means the same as } \sum_{k=1}^{n} \right) \\
&= \sum_{k=0}^{n-1} \binom{(n-1)-k}{k} \qquad (95)
\end{aligned}$$

(here, we have substituted k for $k-1$ in the sum).

We now assume (for the time being) that $n \neq 0$. Hence, n is a positive integer. Thus, $n-1 \in \mathbb{N}$. Therefore, the first equality sign of Proposition 1.3.32 (applied to $n-1$ instead of n) yields

$$f_{(n-1)+1} = \sum_{k=0}^{n-1} \binom{(n-1)-k}{k}.$$

Comparing this with (95), we obtain

$$(\text{\# of self-starting subsets of } [n]) = f_{(n-1)+1} = f_n.$$

We have proved this formula in the case when $n \neq 0$. But it is easy to check directly that it holds for $n = 0$ as well (because there are no self-starting subsets of $[0]$, but the Fibonacci number f_0 is also 0). Thus, this formula holds for all $n \in \mathbb{N}$. So our answer is

$$(\text{\# of self-starting subsets of } [n]) = f_n. \qquad (96)$$

This solves Exercise 1.4.4 **(b)**. □

The answers we obtained for this exercise might make you wonder whether there is a direct connection between self-starting subsets and lacunar subsets – after all, their numbers are both given by Fibonacci numbers! More precisely, a comparison of (96) with Proposition 1.4.9 may suggest that there might be a bijection

$$\{\text{self-starting subsets of } [n]\} \to \{\text{lacunar subsets of } [n-2]\}$$

whenever n is positive (since both of these sets have size f_n); furthermore, a comparison of (94) with Proposition 1.4.10 may suggest that there might be a bijection

$$\{k\text{-element self-starting subsets of } [n]\} \to \{(k-1)\text{-element lacunar subsets of } [n-2]\}$$

for each $k \in [n]$. And indeed, such bijections exist, and both of them are given by the same formula:

$$\{k < i_1 < i_2 < \cdots < i_{k-1}\} \mapsto \underbrace{\{i_1 - k < i_2 - (k-1) < i_3 - (k-2) < \cdots < i_{k-1} - 2\}}_{=\left\{i_j - (k-j+1) \ \mid \ j \in [k-1]\right\}}.$$

(We leave it to the reader to verify that this defines a valid bijection.)

We can mutate Exercise 1.4.4 into yet another similar-looking counting problem by replacing "smallest element" by "largest element":

Exercise 1.4.5. A set S of integers is said to be *self-ending* if the size $|S|$ is the largest element of S. (For example, the set $\{1,2,3\}$ is self-ending, since $|\{1,2,3\}| = 3$ is its largest element; but $\{1,3,6\}$ and $\{1,2,6\}$ are not self-ending.)

Let n be a positive integer.

(a) For each $k \in [n]$, find the # of self-ending k-element subsets of $[n]$.

(b) Find the # of all self-ending subsets of $[n]$.

This exercise is essentially [18f-hw1s, Exercise 6 **(a)**]. It looks analogous to Exercise 1.4.4, but is its answer also analogous to the answer of the latter exercise?

Solution to Exercise 1.4.5 (sketched). **(a)** Let $k \in [n]$. We claim the following:

Claim 1: The only self-ending k-element subset of $[n]$ is $[k]$.

[*Proof of Claim 1:* The set $[k] = \{1,2,\ldots,k\}$ has size k, but its largest element is also k. Thus, $[k]$ is self-ending. Consequently, $[k]$ is a self-ending k-element subset of $[n]$. It remains to show that $[k]$ is the **only** self-ending k-element subset of $[n]$.

Let S be a self-ending k-element subset of $[n]$. Thus, $|S| = k$ (since S is a k-element set). But $|S|$ is the largest element of S (since S is self-ending). In other words, k is the largest element of S (since $|S| = k$). Hence, all elements of S are $\leq k$ and thus belong to the set $[k]$. In other words, S is a subset of $[k]$. Therefore, Theorem 1.4.7 **(c)** (applied to $A = [k]$ and $B = S$) shows that $S = [k]$ (since $|S| = k = |[k]|$).

Now, forget that we fixed S. We thus have shown that each self-ending k-element subset S of $[n]$ satisfies $S = [k]$. In other words, each self-ending k-element subset S of $[n]$ must equal $[k]$. Hence, $[k]$ is the **only** self-ending k-element subset of $[n]$ (since we already know that $[k]$ is such a subset). This proves Claim 1.]

Claim 1 obviously yields that

$$(\#\text{ of self-ending } k\text{-element subsets of } [n]) = 1. \tag{97}$$

This solves Exercise 1.4.5 **(a)**.

(b) It is easy to see that each self-ending subset S of $[n]$ satisfies $|S| \in [n]$ [91]. Hence, by

[91] Indeed, you can prove this in the same way as we showed the analogous claim about self-starting subsets in our solution to Exercise 1.4.4 **(b)**.

the sum rule, we have

$$\begin{aligned}
&(\#\text{ of self-ending subsets of } [n]) \\
&= \sum_{k \in [n]} \underbrace{(\#\text{ of self-ending subsets } S \text{ of } [n] \text{ such that } |S| = k)}_{\substack{=(\#\text{ of self-ending } k\text{-element subsets of } [n]) \\ =1 \\ (\text{by (97)})}} \\
&= \sum_{k \in [n]} 1 = |[n]| \cdot 1 = |[n]| = n.
\end{aligned}$$

This solves Exercise 1.4.5 **(b)**. □

The moral of this story is: similar-looking counting problems don't always have similar answers. Counting problems can vary wildly in difficulty and method of solution. Eventually, we will see some where no good formula for the answer is known!

Have you been experimenting in SageMath along with the above? In that case, you have probably defined functions to check whether a set of integers is self-counting, resp. self-starting, resp. self-ending. Here is one way to do so:

```
def is_self_counting(S):
  # Check whether a set `S` of integers is self-counting.
  return S.cardinality() in S
  # Note: "S.cardinality()" is the size of `S`.

def is_self_starting(S):
  # Check whether a set `S` of integers is self-starting.
  c = S.cardinality()
  return c in S and all(c <= i for i in S)
  # This is checking that the size `c` of `S` is in `S`
  # and is smaller or equal to all elements of `S`.

def is_self_ending(S):
  # Check whether a set `S` of integers is self-ending.
  c = S.cardinality()
  return c in S and all(c >= i for i in S)
```

With these functions, you can ask SageMath to compute (for example) the # of self-starting 3-element subsets of $[8]$ as follows:

```
sum(1 for S in Subsets(8, 3) if is_self_starting(S))
```

(Note that `Subsets(8, 3)` is a shorthand for `Subsets({1, 2, 3, 4, 5, 6, 7, 8}, 3)` that SageMath understands.)

Exercise 1.4.6. A set S of integers is said to be $O<E<O<E<...$ (this is an adjective) if it can be written in the form $S = \{s_1, s_2, \ldots, s_k\}$ where

- $s_1 < s_2 < \cdots < s_k$;
- the integer s_i is even whenever i is even;

- the integer s_i is odd whenever i is odd.

(For example, $\{1,4,5,8,11\}$ is an O<E<O<E<... set, while $\{2,3\}$ and $\{1,4,6\}$ are not. Note that k is allowed to be 0, whence $\varnothing$ is an O<E<O<E<... set.)

For each $n \in \mathbb{N}$, we let $a(n)$ denote the number of all O<E<O<E<... subsets of $[n]$, and let $b(n)$ denote the number of all O<E<O<E<... subsets of $[n]$ that contain n.

(a) Show that $a(n) = a(n-1) + b(n)$ for each $n > 0$.

(b) Show that $a(n) = 1 + \sum_{k=0}^{n} b(k)$ for each $n \in \mathbb{N}$.

(c) Show that $b(n) = \sum_{\substack{k \in \{0,1,\ldots,n-1\}; \\ k \equiv n-1 \bmod 2}} b(k) + [n \text{ is odd}]$ for each $n \in \mathbb{N}$. (Here, we are using the Iverson bracket notation, defined in Definition 1.3.15.)

(d) Show that $b(n) + b(n-1) = 1 + \sum_{k=0}^{n-1} b(k)$ for each $n > 0$.

(e) Show that $b(n) = 1 + \sum_{k=0}^{n-2} b(k)$ for each $n > 0$.

(f) Show that $b(n) = a(n-2)$ for each $n \geq 2$.

(g) Show that $a(n) = f_{n+2}$ for each $n \in \mathbb{N}$.

Exercise 1.4.7. For each $n \in \mathbb{N}$, we let $c(n)$ denote the number of all subsets of $[n]$ that are simultaneously lacunar and O<E<O<E<....

Prove that $c(n) = c(n-2) + c(n-3)$ for all $n \geq 3$.

Remark 1.4.19. The sequence $(c(0), c(1), c(2), c(3), \ldots)$ from Exercise 1.4.7 is the *Padovan sequence* (starting with $1,2,2,3,4,5,7,9,12,16,21,28,37,49$).

Exercise 1.4.8. A set S of integers is said to be 2-*lacunar* if every $i \in S$ satisfies $i+1 \notin S$ and $i+2 \notin S$. (That is, any two distinct elements of S are at least a distance of 3 apart on the real axis.) For example, $\{1,5,8\}$ is 2-lacunar, but $\{1,5,7\}$ and $\{1,5,6\}$ are not.

For any $n \in \mathbb{N}$, we let $h(n)$ denote the number of all 2-lacunar subsets of $[n]$.

(a) Prove that $h(n) = h(n-1) + h(n-3)$ for each $n \geq 3$.

(b) Prove that $h(n) = \sum_{\substack{k \in \mathbb{N}; \\ 2k \leq n+2}} \binom{n+2-2k}{k}$ for each $n \in \mathbb{N}$.

1.4.9. Counting subsets containing a given subset

For a given $k \in \mathbb{N}$, how many k-element subsets of a given set N contain a given subset D as a subset? The following proposition gives an answer to this question:

Proposition 1.4.20. Let $n \in \mathbb{N}$, $d \in \mathbb{N}$ and $k \in \mathbb{R}$. Let N be an n-element set. Let D be a d-element subset of N. Then,

$$(\#\text{ of } k\text{-element subsets } A \text{ of } N \text{ satisfying } D \subseteq A) = \binom{n-d}{k-d}.$$

Example 1.4.21. Let $N = \{1,2,3,4\}$ and $D = \{1,2\}$. Then, the subsets A of N satisfying $D \subseteq A$ are $\{1,2\}$, $\{1,2,3\}$, $\{1,2,4\}$ and $\{1,2,3,4\}$. Thus, 1 of them has 2 elements; 2 have 3 elements; and 1 has 4 elements. This agrees with Proposition 1.4.20 (for $n = 4$ and $d = 2$).

Proof of Proposition 1.4.20 (informal version). As usual, let me first show the informal idea, and then its formalization.

Informally, how can we construct a k-element subset A of N satisfying $D \subseteq A$? We need to choose k elements of N to go into A; but we cannot choose them freely, because we must ensure that $D \subseteq A$. Thus, the d elements of D must necessarily go into A; the only freedom that we have is to decide which of the remaining $n-d$ elements of N will go into A. More precisely, we need to choose $k-d$ many of these $n-d$ elements, because the total size of A has to be k (and d of its elements have already been decided). Thus, our decision boils down to choosing a $(k-d)$-element subset of the $(n-d)$-element set $N \setminus D$. According to Theorem 1.3.12 (applied to $n-d$, $k-d$ and $N \setminus D$ instead of n, k and S), there are $\binom{n-d}{k-d}$ many such subsets. Thus, the total # of k-element subsets A of N satisfying $D \subseteq A$ is $\binom{n-d}{k-d}$. □

To formalize this argument, we have to replace our "boils down" handwaving with a bijection. Here is how the result looks like:

Proof of Proposition 1.4.20 (formal version). We have $|D| = d$ (since D is a d-element set) and $|N| = n$ (since N is an n-element set). Also, D is a subset of N. Thus, Theorem 1.4.7 **(a)** (applied to $A = N$ and $B = D$) yields $|N \setminus D| = \underbrace{|N|}_{=n} - \underbrace{|D|}_{=d} = n-d$. Hence, $N \setminus D$ is an $(n-d)$-element set. Thus, Theorem 1.3.12 (applied to $n-d$, $k-d$ and $N \setminus D$ instead of n, k and S) yields

$$\binom{n-d}{k-d} = (\#\text{ of } (k-d)\text{-element subsets of } N \setminus D). \tag{98}$$

If A is a k-element subset of N satisfying $D \subseteq A$, then $A \setminus D$ is a $(k-d)$-element subset of $N \setminus D$ [92]. Hence, the map

$$\{k\text{-element subsets } A \text{ of } N \text{ satisfying } D \subseteq A\} \to \{(k-d)\text{-element subsets of } N \setminus D\},$$
$$A \mapsto A \setminus D$$

[92] *Proof.* Let A be a k-element subset of N satisfying $D \subseteq A$. Then, $|A| = k$ (since A is a k-element set). But D is a subset of A (since $D \subseteq A$). Hence, Theorem 1.4.7 **(a)** (applied to $B = D$) yields

is well-defined.

On the other hand, if B is a $(k-d)$-element subset of $N \setminus D$, then $B \cup D$ is a k-element subset A of N that satisfies $D \subseteq A$ [93]. Hence, the map

$$\{(k-d)\text{-element subsets of } N \setminus D\} \to \{k\text{-element subsets } A \text{ of } N \text{ satisfying } D \subseteq A\},$$
$$B \mapsto B \cup D$$

is well-defined.

It is easy to see that these two maps are mutually inverse[94]. Thus, they are bijections. Hence, the bijection principle yields

$$\begin{aligned}&(\#\text{ of } k\text{-element subsets } A \text{ of } N \text{ satisfying } D \subseteq A)\\ &= (\#\text{ of } (k-d)\text{-element subsets of } N \setminus D) = \binom{n-d}{k-d}\end{aligned}$$

(by (98)). This proves Proposition 1.4.20. □

1.5. Counting tuples and maps

1.5.1. Tuples

Before we continue with counting problems, let us recall the notion of the Cartesian product of several sets:

Definition 1.5.1. Let $A_1, A_2, \ldots, A_n$ be any n sets. Then, the *Cartesian product* $A_1 \times A_2 \times \cdots \times A_n$ of these n sets is defined to be the set of all n-tuples $(a_1, a_2, \ldots, a_n)$ for which $a_i \in A_i$ for all $i \in [n]$. In other words,

$$\begin{aligned}&A_1 \times A_2 \times \cdots \times A_n\\ &= \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for all } i \in [n]\}\\ &= \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1 \text{ and } a_2 \in A_2 \text{ and } \cdots \text{ and } a_n \in A_n\}.\end{aligned}$$

$|A \setminus D| = \underbrace{|A|}_{=k} - \underbrace{|D|}_{=d} = k-d$. In other words, $A \setminus D$ is a $(k-d)$-element set. Hence, $A \setminus D$ is a $(k-d)$-element subset of $N \setminus D$ (because $\underbrace{A}_{\subseteq N} \setminus D \subseteq N \setminus D$).

[93] *Proof.* Let B be a $(k-d)$-element subset of $N \setminus D$. Thus, $B \subseteq N \setminus D$ and $|B| = k-d$ (since B is a $(k-d)$-element set). From $B \subseteq N \setminus D$, we conclude that the sets B and D are disjoint. Thus, (4) (applied to $X = B$ and $Y = D$) yields $|B \cup D| = \underbrace{|B|}_{=k-d} + \underbrace{|D|}_{=d} = (k-d) + d = k$. Hence, $B \cup D$ is a k-element set. Moreover, combining $B \subseteq N \setminus D \subseteq N$ with $D \subseteq N$, we obtain $B \cup D \subseteq N$. Hence, $B \cup D$ is a k-element subset of N (since $B \cup D$ is a k-element set). Thus, $B \cup D$ is a k-element subset A of N that satisfies $D \subseteq A$ (since $D \subseteq B \cup D$).

[94] Indeed, this relies on the following two observations:

- If A is any k-element subset of N satisfying $D \subseteq A$, then $(A \setminus D) \cup D = A$. (This follows from $D \subseteq A$.)
- If B is any $(k-d)$-element subset of $N \setminus D$, then $(B \cup D) \setminus D = B$. (This follows from $B \subseteq N \setminus D$.)

Applying Definition 1.5.1 to $n = 2$, we obtain the Cartesian product $A_1 \times A_2$ of two sets A_1 and A_2; it consists of pairs of an element of A_1 and an element of A_2. For instance, the Cartesian product $\{1,2\} \times \{5,6,7\}$ consists of the six pairs $(1,5)$, $(1,6)$, $(1,7)$, $(2,5)$, $(2,6)$ and $(2,7)$.

Applying Definition 1.5.1 to $n = 1$, we obtain the Cartesian product A_1 of a single set A_1; this is the set of all 1-tuples (a_1) of a single element $a_1 \in A_1$. The notation hides a minor discrepancy: Strictly speaking, a 1-tuple (a_1) is not the same as its underlying element a_1, and thus the Cartesian product of the single set A_1 is not the same as the set A_1 itself, despite looking precisely the same in our notation. Fortunately, the sets are "as good as equal": The map

$$\begin{aligned}(\text{the original set } A_1) &\to (\text{the Cartesian product of the single set } A_1)\,, \\ a_1 &\mapsto (a_1)\end{aligned}$$

(sending each element a_1 of A_1 to the 1-tuple (a_1)) is a bijection. Thus, the two sets denoted A_1 have the same size, at least, and it is rare that anything bad comes out of equating them.

Applying Definition 1.5.1 to $n = 0$, we obtain the Cartesian product of 0 sets; this is called the *empty Cartesian product*, and consists of all 0-tuples. There is only one 0-tuple, namely the empty list $()$; thus, this Cartesian product is the 1-element set $\{()\}$.

The Cartesian product of sets is not quite associative! For example, if A, B and C are three sets, then the three Cartesian products $A \times B \times C$, $(A \times B) \times C$ and $A \times (B \times C)$ are not literally the same. The first of them consists of triples[95] (a,b,c); the second consists of nested pairs $((a,b),c)$; the third consists of nested pairs $(a,(b,c))$. These are different things, and should not be equated[96]. Again, however, there are bijections between these products: The maps

$$\begin{aligned}A \times B \times C &\to (A \times B) \times C, \\ (a,b,c) &\mapsto ((a,b),c)\end{aligned}$$

and

$$\begin{aligned}A \times B \times C &\to A \times (B \times C)\,, \\ (a,b,c) &\mapsto (a,(b,c))\end{aligned}$$

are bijections. More generally:

Proposition 1.5.2. Let $A_1, A_2, \ldots, A_n$ be any n sets.
(a) If $n > 0$, then the map

$$\begin{aligned}A_1 \times A_2 \times \cdots \times A_n &\to (A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n, \\ (a_1, a_2, \ldots, a_n) &\mapsto ((a_1, a_2, \ldots, a_{n-1}), a_n)\end{aligned}$$

[95] Recall that the word "*triple*" means a 3-tuple. Tuples are always ordered by definition.

[96] For example, the first entry of the triple (a,b,c) is a, while the first entry of the pair $((a,b),c)$ is the pair (a,b).

is a bijection.

(b) If $k \in \{0, 1, \ldots, n\}$ is arbitrary, then the map

$$A_1 \times A_2 \times \cdots \times A_n \to (A_1 \times A_2 \times \cdots \times A_k) \times (A_{k+1} \times A_{k+2} \times \cdots \times A_n),$$
$$(a_1, a_2, \ldots, a_n) \mapsto ((a_1, a_2, \ldots, a_k), (a_{k+1}, a_{k+2}, \ldots, a_n))$$

is a bijection.

I consider Proposition 1.5.2 obvious (or, more precisely, to be part of an introductory course in axiomatic set theory that I am not giving here). From an algorithmic viewpoint, the bijection in Proposition 1.5.2 **(b)** splits a list into two sublists (the one formed by its first k entries, and the one formed by its remaining entries).

Using Proposition 1.5.2, we can generalize our product rule for two sets (Theorem 1.1.4) to n sets:

Theorem 1.5.3 (The product rule for n sets)**.** Let $A_1, A_2, \ldots, A_n$ be any n finite sets. Then, $A_1 \times A_2 \times \cdots \times A_n$ is a finite set with size

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|.$$

The intuition behind Theorem 1.5.3 is the following: In order to choose an n-tuple $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, it suffices to choose an element a_1 of A_1, an element a_2 of A_2, and so on (a total of n choices). These n choices are mutually independent (e.g., the value of a_1 we choose does not constrain us in our choice of a_2), and thus the total number of options should be the product of the total numbers of options for each of the n choices (which numbers are $|A_1|, |A_2|, \ldots, |A_n|$). In this form, Theorem 1.5.3 is usually considered obvious and called the "rule of product" or "multiplication principle". We nevertheless give a rigorous proof in order to get some feeling for Cartesian products:

Proof of Theorem 1.5.3. We will prove Theorem 1.5.3 by induction on n:

Induction base: We have

$$A_1 \times A_2 \times \cdots \times A_0 = (\text{empty Cartesian product}) = \{()\}$$

(this is a one-element set) and therefore

$$|A_1 \times A_2 \times \cdots \times A_0| = |\{()\}| = 1.$$

Comparing this with

$$|A_1| \cdot |A_2| \cdot \cdots \cdot |A_0| = (\text{empty product}) = 1,$$

we obtain $|A_1 \times A_2 \times \cdots \times A_0| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_0|$. In other words, Theorem 1.5.3 is true for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that Theorem 1.5.3 holds for $n = m$. We must prove that Theorem 1.5.3 holds for $n = m + 1$.

Let $A_1, A_2, \ldots, A_{m+1}$ be any $m+1$ finite sets. Recall that we assumed that Theorem 1.5.3 holds for $n = m$. Hence,

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_m| .$$

But Proposition 1.5.2 **(a)** (applied to $n = m+1$) yields that the map

$$\begin{aligned} A_1 \times A_2 \times \cdots \times A_{m+1} &\to \left(A_1 \times A_2 \times \cdots \times A_{(m+1)-1}\right) \times A_{m+1}, \\ (a_1, a_2, \ldots, a_{m+1}) &\mapsto \left(\left(a_1, a_2, \ldots, a_{(m+1)-1}\right), a_{m+1}\right) \end{aligned}$$

is a bijection. Hence, the bijection principle shows that

$$\begin{aligned} &|A_1 \times A_2 \times \cdots \times A_{m+1}| \\ &= \left|\left(A_1 \times A_2 \times \cdots \times A_{(m+1)-1}\right) \times A_{m+1}\right| \\ &= \underbrace{\left|A_1 \times A_2 \times \cdots \times A_{(m+1)-1}\right|}_{\substack{=|A_1 \times A_2 \times \cdots \times A_m| \\ =|A_1| \cdot |A_2| \cdot \cdots \cdot |A_m|}} \cdot |A_{m+1}| \\ &\qquad \left(\text{by (5), applied to } X = A_1 \times A_2 \times \cdots \times A_{(m+1)-1} \text{ and } Y = A_{m+1}\right) \\ &= \left(|A_1| \cdot |A_2| \cdot \cdots \cdot |A_m|\right) \cdot |A_{m+1}| \\ &= |A_1| \cdot |A_2| \cdot \cdots \cdot |A_{m+1}| . \end{aligned}$$

In particular, this shows that the set $A_1 \times A_2 \times \cdots \times A_{m+1}$ is finite.

Forget that we fixed $A_1, A_2, \ldots, A_{m+1}$. We thus have proven that if $A_1, A_2, \ldots, A_{m+1}$ are any $m+1$ finite sets, then $A_1 \times A_2 \times \cdots \times A_{m+1}$ is a finite set with size

$$|A_1 \times A_2 \times \cdots \times A_{m+1}| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_{m+1}| .$$

In other words, Theorem 1.5.3 holds for $n = m+1$. This completes the induction step, and with it the proof of Theorem 1.5.3. □

A particular case of a Cartesian product is obtained when all the "factors" are equal:

Definition 1.5.4. Let A be a set, and let $n \in \mathbb{N}$. Then, the n-th *(Cartesian) power* A^n of A is defined to be the Cartesian product $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$.

This Cartesian power A^n is often denoted by $A^{\times n}$ as well.

For example, if A is any set, then $A^0 = \{()\}$, whereas A^1 is "more or less the same as" A (as explained before, not exactly the same, but there is an obvious bijection).

Corollary 1.5.5. Let A be a finite set. Let $n \in \mathbb{N}$. Then, A^n is a finite set with size $|A^n| = |A|^n$.

Proof of Corollary 1.5.5. Definition 1.5.4 yields $A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$. But Theorem 1.5.3 (applied to $A_i = A$) shows that $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$ is a finite set with size $\left|\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}\right| = \underbrace{|A| \cdot |A| \cdot \cdots \cdot |A|}_{n \text{ times}}$. In view of $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}} = A^n$ and $\underbrace{|A| \cdot |A| \cdot \cdots \cdot |A|}_{n \text{ times}} = |A|^n$, we can rewrite this as follows: The set A^n is a finite set with size $|A^n| = |A|^n$. This proves Corollary 1.5.5. □

1.5.2. Counting maps

Let us now use these results to count maps between two sets. First, we introduce a notation for them:

Definition 1.5.6. Let A and B be two sets. Then, B^A shall mean the set of all maps from A to B.

This notation B^A is somewhat counterintuitive (who in their right mind would put the target B first?), but it is explained by the following property:

Theorem 1.5.7. Let A and B be two finite sets. Then, the set B^A is finite, and its size is

$$\left|B^A\right| = |B|^{|A|}.$$

Example 1.5.8. Theorem 1.5.7 (applied to $A = [2]$ and $B = [3]$) says that the set $[3]^{[2]}$ is finite, and that its size is $\left|[3]^{[2]}\right| = |[3]|^{|[2]|} = 3^2 = 9$. In other words, there are exactly 9 maps from $[2]$ to $[3]$. Here are these 9 maps (written in two-line notation, as explained in Definition 1.2.11):

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix}.$$

Proof of Theorem 1.5.7. Let $(a_1, a_2, \ldots, a_k)$ be a list of all elements of A in some order (with no repetitions). Thus, $a_1, a_2, \ldots, a_k$ are distinct and satisfy $A = \{a_1, a_2, \ldots, a_k\}$. Hence, $|A| = k$.

Recall that B^A is the set of all maps from A to B. In other words, B^A is the set of all functions from A to B. (The nouns "map" and "function" are synonyms

in mathematics. I usually prefer "map" for its shortness, but here, I am using "function" in order to separate the maps from A to B (which I call "functions") from maps between B^A and B^k (which I shall consider soon, and will call "maps").)

Consider the map

$$\begin{aligned}\Phi : B^A &\to B^k, \\ f &\mapsto (f(a_1), f(a_2), \ldots, f(a_k)).\end{aligned}$$

This map Φ sends each function $f : A \to B$ to its list of values at the points[97] $a_1, a_2, \ldots, a_k$. This list of values clearly determines f uniquely (since $A = \{a_1, a_2, \ldots, a_k\}$, so that each value of f appears somewhere in the list[98]); thus, the map Φ is injective. Furthermore, for each k-tuple $(b_1, b_2, \ldots, b_k) \in B^k$, there exists a function $f : A \to B$ such that $(f(a_1), f(a_2), \ldots, f(a_k)) = (b_1, b_2, \ldots, b_k)$ (indeed, this latter function f is given by

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \\ b_1 & b_2 & \cdots & b_k \end{pmatrix}$$

in two-line notation). Hence, the map Φ is surjective. Thus, we know that the map Φ is both injective and surjective. Therefore, Φ is bijective, i.e., is a bijection. Hence, the bijection principle yields $\left|B^A\right| = \left|B^k\right|$.

Corollary 1.5.5 (applied to B and k instead of A and n) shows that B^k is a finite set with size $\left|B^k\right| = |B|^k$. Hence, $\left|B^A\right| = \left|B^k\right| = |B|^k = |B|^{|A|}$ (since $k = |A|$). Thus, in particular, B^A is a finite set. This proves Theorem 1.5.7. □

In one of the next chapters, we will count certain restricted types of maps (injective maps, surjective maps, etc.).

1.5.3. Applications

Theorem 1.5.7 and Theorem 1.5.3 can be used not only in the kind of problems that are visibly concerned with subsets or tuples. In fact, often one can discover a bijection between the objects one wants to count and some kind of maps or tuples. The most famous example is a combinatorial proof of Theorem 1.4.1:

Third proof of Theorem 1.4.1. The set S is an n-element set. Let us denote its n elements by $s_1, s_2, \ldots, s_n$ (in an arbitrary order, with no repetitions). Thus, $s_1, s_2, \ldots, s_n$ are n distinct elements of S and satisfy $S = \{s_1, s_2, \ldots, s_n\}$.

We will construct a bijection from the set $\{\text{subsets of } S\}$ to $\{0,1\}^n$. This will then let us apply Corollary 1.5.5 (and the bijection principle) and obtain $|\{\text{subsets of } S\}| = 2^n$. So let us construct such a bijection:

We define the map $A : \{\text{subsets of } S\} \to \{0,1\}^n$ by setting[99]

$$A(T) = ([s_1 \in T], [s_2 \in T], \ldots, [s_n \in T]) \qquad \text{for each subset } T \text{ of } S.$$

[97] I am just using "point" as just a suggestive way of saying "element of A" here.

[98] And we know where exactly it appears in the list, because $a_1, a_2, \ldots, a_k$ are fixed.

[99] We are using the Iverson bracket notation (defined in Definition 1.3.15).

(This is well-defined, since each of the truth values $[s_1 \in T], [s_2 \in T], \ldots, [s_n \in T]$ belongs to $\{0,1\}$.) For example, if $n = 5$ and $T = \{s_2, s_4, s_5\}$, then $A(T) = (0,1,0,1,1)$. (Some call $A(T)$ the *indicator vector* of T, since its i-th entry indicates whether s_i belongs to T or not.)

In order to prove that A is a bijection, we shall next construct a map B in the other direction, and then show that it is inverse to A.

We define the map $B : \{0,1\}^n \to \{\text{subsets of } S\}$ by setting

$$B((i_1, i_2, \ldots, i_n)) = \{s_k \mid k \in [n] \text{ and } i_k = 1\} \quad \text{for each } (i_1, i_2, \ldots, i_n) \in \{0,1\}^n.$$

(Note that $\{s_k \mid k \in [n] \text{ and } i_k = 1\}$ is always a subset of S, since $s_1, s_2, \ldots, s_n$ are elements of S.)

We want to show that the maps A and B are mutually inverse. In order to do this, we must show that $A \circ B = \mathrm{id}$ and that $B \circ A = \mathrm{id}$.

Intuitively, this is fairly obvious: The map A encodes a subset of S as an n-tuple, each of whose entries equals either 0 or 1 depending on whether the corresponding element of S belongs to the subset or not.[100] The map B, in turn, decodes such an n-tuple back into a subset of S, by gathering the elements of S corresponding to those positions at which the n-tuple has a 1. It is thus clear that the maps A and B undo one another, i.e., they satisfy the two equalities $A \circ B = \mathrm{id}$ and $B \circ A = \mathrm{id}$.

Here is a more formal way to prove these equalities:

- In order to show that $A \circ B = \mathrm{id}$, we fix some $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$. We shall show that $(A \circ B)((i_1, i_2, \ldots, i_n)) = (i_1, i_2, \ldots, i_n)$.

  Set $T = B((i_1, i_2, \ldots, i_n))$. Thus, $T = B((i_1, i_2, \ldots, i_n)) = \{s_k \mid k \in [n] \text{ and } i_k = 1\}$ (by the definition of B). Now,

$$(A \circ B)((i_1, i_2, \ldots, i_n)) = A\left(\underbrace{B((i_1, i_2, \ldots, i_n))}_{=T}\right) = A(T) = ([s_1 \in T], [s_2 \in T], \ldots, [s_n \in T]) \tag{99}$$

  (by the definition of A). Now, we shall show that each $j \in [n]$ satisfies $[s_j \in T] = i_j$.

  Indeed, let $j \in [n]$. Thus, $i_j \in \{0,1\}$ (since $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$). Recall that $T = \{s_k \mid k \in [n] \text{ and } i_k = 1\}$. Hence, if $i_j = 1$, then $s_j \in T$ and therefore $[s_j \in T] = 1 = i_j$. Therefore, we have proved $[s_j \in T] = i_j$ in the case when $i_j = 1$. On the other hand, if $i_j \neq 1$, then $i_j = 0$ (since $i_j \in \{0,1\}$) and $s_j \notin T$ [101] and therefore

[100] The "corresponding element of S" to the k-th entry is understood to be s_k. This correspondence between the n positions in the n-tuple and the elements of S is fixed (since we have fixed $s_1, s_2, \ldots, s_n$).

[101] *Proof.* Assume that $i_j \neq 1$. We must prove that $s_j \notin T$.

Assume the contrary. Thus, $s_j \in T = \{s_k \mid k \in [n] \text{ and } i_k = 1\}$. In other words, there exists some $k \in [n]$ such that $i_k = 1$ and $s_j = s_k$. Consider this k. From $s_j = s_k$, we obtain $j = k$ (since $s_1, s_2, \ldots, s_n$ are distinct). Thus, $i_j = i_k = 1$. This contradicts $i_j \neq 1$. This contradiction shows that our assumption was false, qed.

$\left[s_j \in T\right] = 0 = i_j$. Thus, we have proved $\left[s_j \in T\right] = i_j$ in the case when $i_j \neq 1$. We have now proved $\left[s_j \in T\right] = i_j$ both in the case when $i_j = 1$ and in the case when $i_j \neq 1$. These two cases cover all possibilities; thus, we always have $\left[s_j \in T\right] = i_j$.

Forget that we fixed j. We thus have shown that $\left[s_j \in T\right] = i_j$ for each $j \in [n]$. Hence,

$$\left(\left[s_1 \in T\right], \left[s_2 \in T\right], \ldots, \left[s_n \in T\right]\right) = \left(i_1, i_2, \ldots, i_n\right).$$

Hence, (99) becomes

$$\begin{aligned}(A \circ B)\left(\left(i_1, i_2, \ldots, i_n\right)\right) &= \left(\left[s_1 \in T\right], \left[s_2 \in T\right], \ldots, \left[s_n \in T\right]\right) = \left(i_1, i_2, \ldots, i_n\right) \\ &= \mathrm{id}\left(\left(i_1, i_2, \ldots, i_n\right)\right). \end{aligned} \tag{100}$$

Now, forget that we fixed $(i_1, i_2, \ldots, i_n)$. We thus have proven (100) for each $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$. Hence, $A \circ B = \mathrm{id}$.

- In order to prove that $B \circ A = \mathrm{id}$, we fix $T \in \{\text{subsets of } S\}$. We are going to show that $(B \circ A)(T) = T$.

  We know that T is a subset of S (since $T \in \{\text{subsets of } S\}$). In other words, $T \subseteq S$.

  We have $A(T) = \left(\left[s_1 \in T\right], \left[s_2 \in T\right], \ldots, \left[s_n \in T\right]\right)$ by the definition of A. Now,

$$\begin{aligned}(B \circ A)(T) &= B\left(\underbrace{A(T)}_{=\left(\left[s_1 \in T\right], \left[s_2 \in T\right], \ldots, \left[s_n \in T\right]\right)}\right) \\ &= B\left(\left(\left[s_1 \in T\right], \left[s_2 \in T\right], \ldots, \left[s_n \in T\right]\right)\right) \\ &= \left\{s_k \mid k \in [n] \text{ and } \left[s_k \in T\right] = 1\right\} \end{aligned} \tag{101}$$

  (by the definition of B).

  From this, we can easily conclude that $(B \circ A)(T) \subseteq T$ [102] and $T \subseteq (B \circ A)(T)$ [103]. Combining these two relations, we obtain $(B \circ A)(T) = T$. In other words, $(B \circ A)(T) = \mathrm{id}(T)$ (since $\mathrm{id}(T) = T$).

  Now, forget that we fixed T. We thus have shown that $(B \circ A)(T) = \mathrm{id}(T)$ for each $T \in \{\text{subsets of } S\}$. In other words, $B \circ A = \mathrm{id}$.

[102] *Proof.* Let $s \in (B \circ A)(T)$. Thus, $s \in (B \circ A)(T) = \{s_k \mid k \in [n] \text{ and } [s_k \in T] = 1\}$. In other words, $s = s_k$ for some $k \in [n]$ satisfying $[s_k \in T] = 1$. Consider this k. From $[s_k \in T] = 1$, we conclude that $s_k \in T$ must be true (by the definition of the Iverson bracket notation). Hence, $s = s_k \in T$.

Forget that we fixed s. We thus have proved that $s \in T$ for each $s \in (B \circ A)(T)$. In other words, $(B \circ A)(T) \subseteq T$.

[103] *Proof.* Let $s \in T$. Then, $s \in T \subseteq S = \{s_1, s_2, \ldots, s_n\}$. In other words, $s = s_j$ for some $j \in [n]$. Consider this j. Then, $s_j = s \in T$. Hence, $\left[s_j \in T\right] = 1$. Thus, j is a $k \in [n]$ satisfying $[s_k \in T] = 1$ (because $j \in [n]$ and $\left[s_j \in T\right] = 1$). Hence, $s_j \in \{s_k \mid k \in [n] \text{ and } [s_k \in T] = 1\}$. In view of (101), this rewrites as $s_j \in (B \circ A)(T)$. Thus, $s = s_j \in (B \circ A)(T)$.

Forget that we fixed s. We thus have proved that $s \in (B \circ A)(T)$ for each $s \in T$. In other words, $T \subseteq (B \circ A)(T)$.

We now know that $A \circ B = \mathrm{id}$ and $B \circ A = \mathrm{id}$. Combining these equalities, we conclude that the maps A and B are mutually inverse. Hence, the map A is invertible, i.e., bijective. In other words, $A : \{\text{subsets of } S\} \to \{0,1\}^n$ is a bijection. Thus, Theorem 1.1.6 (applied to $X = \{\text{subsets of } S\}$, $Y = \{0,1\}^n$ and $f = A$) yields

$$\begin{aligned} |\{\text{subsets of } S\}| &= \left|\{0,1\}^n\right| = |\{0,1\}|^n \\ &\qquad \text{(by Corollary 1.5.5, applied to } \{0,1\} \text{ instead of } A\text{)} \\ &= 2^n \qquad (\text{since } |\{0,1\}| = 2)\,. \end{aligned}$$

Hence, $2^n = |\{\text{subsets of } S\}| = (\#\text{ of subsets of } S)$. This proves Theorem 1.4.1 once again.[104] □

The key idea in the above proof of Theorem 1.4.1 was to encode any subset of the n-element set S as an n-tuple $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$. Instead of using an n-tuple, we could have just as well used a map from $[n]$ to $\{0,1\}$, since we learned to translate between tuples and maps in the above proof of Theorem 1.5.7. The reader can easily restate our above proof of Theorem 1.4.1 using maps instead of tuples.

Here are some other counting exercises that can easily be reduced to counting tuples or maps:

Exercise 1.5.1. Let $n \in \mathbb{N}$.

(a) Find the number of all triples (A, B, C) of subsets of $[n]$ satisfying $A \cup B \cup C = [n]$ and $A \cap B \cap C = \varnothing$.

(b) Find the number of all triples (A, B, C) of subsets of $[n]$ satisfying $B \cap C = C \cap A = A \cap B$.

(c) Find the number of all triples (A, B, C) of subsets of $[n]$ satisfying $A \cap B = A \cap C$.

(d) Find the number of 4-tuples (A, B, C, D) of subsets of $[n]$ satisfying $A \cap B = C \cap D$.

(e) Find the number of 4-tuples (A, B, C, D) of subsets of $[n]$ satisfying $A \cap B = C \cup D$.

Exercise 1.5.2. A set S of integers is said to be *shadowed* if it has the following property: Whenever an **odd** integer i belongs to S, the next integer $i + 1$ must also belong to S. (For example, $\varnothing$, $\{2,4\}$ and $\{1,2,5,6,8\}$ are shadowed, but $\{1,5,6\}$ is not, since 1 belongs to $\{1,5,6\}$ but 2 does not.)

(a) Let $n \in \mathbb{N}$ be even. How many shadowed subsets of $[n]$ exist?

(b) Let $n \in \mathbb{N}$ be odd. How many shadowed subsets of $[n]$ exist?

Class of 2019-10-11

[104] This proof has been taken from [19f-hw0s, solution to Exercise 1 **(a)**] (but slightly adapted for the fact that we are using the set S rather than $[n]$ here).

1.6. Interchange of summations

1.6.1. The finite Fubini principle

In Subsection 1.2.3, we have seen a few rules for manipulating finite sums. Let me now show another: the *(finite) Fubini principle*. Let us first state it; we will see it in action soon:

Theorem 1.6.1 ((Finite) Fubini principle)**.** Let X and Y be two finite sets. Let $a_{(x,y)}$ be a number for each pair $(x,y) \in X \times Y$. Then,

$$\sum_{x \in X} \sum_{y \in Y} a_{(x,y)} = \sum_{(x,y) \in X \times Y} a_{(x,y)} = \sum_{y \in Y} \sum_{x \in X} a_{(x,y)}. \tag{102}$$

Theorem 1.6.1 is called the *finite Fubini principle* or *Fubini's theorem for finite sums*, since it is a discrete analogue of Fubini's principle for double integrals. A proof of Theorem 1.6.1 is outlined in [Grinbe15, §1.4.2] (and an alternative proof can easily be obtained by induction on $|X|$); here I shall restrict myself to illustrating it on an example:

Example 1.6.2. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $a_{(x,y)}$ be a number for each pair $(x,y) \in [n] \times [m]$. Then, (102) (applied to $X = [n]$ and $Y = [m]$) yields

$$\sum_{x=1}^{n} \sum_{y=1}^{m} a_{(x,y)} = \sum_{(x,y) \in [n] \times [m]} a_{(x,y)} = \sum_{y=1}^{m} \sum_{x=1}^{n} a_{(x,y)}. \tag{103}$$

This equality, when rewritten to avoid the use of summation signs, looks as follows:

$$\begin{aligned}
&\left(a_{(1,1)} + a_{(1,2)} + \cdots + a_{(1,m)}\right) \\
&\qquad + \left(a_{(2,1)} + a_{(2,2)} + \cdots + a_{(2,m)}\right) \\
&\qquad + \cdots \\
&\qquad + \left(a_{(n,1)} + a_{(n,2)} + \cdots + a_{(n,m)}\right) \\
&= a_{(1,1)} + a_{(1,2)} + \cdots + a_{(n,m)} \qquad \left(\text{this is the sum of all } nm \text{ numbers } a_{(x,y)}\right) \\
&= \left(a_{(1,1)} + a_{(2,1)} + \cdots + a_{(n,1)}\right) \\
&\qquad + \left(a_{(1,2)} + a_{(2,2)} + \cdots + a_{(n,2)}\right) \\
&\qquad + \cdots \\
&\qquad + \left(a_{(1,m)} + a_{(2,m)} + \cdots + a_{(n,m)}\right).
\end{aligned}$$

So this equality says that if we have a rectangular $n \times m$-table of numbers:

$$\begin{array}{|cccc|}\hline a_{(1,1)} & a_{(1,2)} & \cdots & a_{(1,m)} \\ a_{(2,1)} & a_{(2,2)} & \cdots & a_{(2,m)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(n,1)} & a_{(n,2)} & \cdots & a_{(n,m)} \\ \hline \end{array} ,$$

then the following three procedures all produce the same result:

(a) summing up the m numbers in each row of the table separately, and then summing up these n "row tallies";

(b) summing up all the nm numbers in the table;

(c) summing up the n numbers in each column of the table separately, and then summing up these m "column tallies".

This is, of course, exactly how you would expect sums to behave.

I like to abbreviate the equality (102) as follows:

$$\sum_{x \in X} \sum_{y \in Y} = \sum_{(x,y) \in X \times Y} = \sum_{y \in Y} \sum_{x \in X} .$$

This is an "equality between summation signs"; it should be understood as follows: Every time you see an "$\sum_{x \in X} \sum_{y \in Y}$" in an expression, you can replace it by a "$\sum_{(x,y) \in X \times Y}$" or by a "$\sum_{y \in Y} \sum_{x \in X}$", and similarly the other ways round. Thus, in particular, you can replace the sequence "$\sum_{x \in X} \sum_{y \in Y}$" of two summation signs by the reverse sequence "$\sum_{y \in Y} \sum_{x \in X}$" and vice versa.[105] This is called *interchange of summations* or *interchanging the order of summation*.

As a first example of how (102) can be applied, let us solve a simple exercise:

Exercise 1.6.1. Let $n \in \mathbb{N}$. Let S be an n-element set. Find the sum of the sizes of all subsets of S; in other words, find the sum

$$\sum_{T \subseteq S} |T| .$$

[105] Of course, you can do this only if X and Y are finite sets that have a well-defined meaning independent of x and y. Thus, you cannot replace the sequence "$\sum_{x \in [n]} \sum_{y \in [x]}$" by "$\sum_{y \in [x]} \sum_{x \in [n]}$": The latter sequence would be meaningless, since the "x" under the first summation sign now refers to nothing. We will soon see how such double summations can be transformed.

We shall solve this using the following simple fact:[106]

Proposition 1.6.3 ("Counting by roll call")**.** Let S be a finite set.

(a) If T is a subset of S, then

$$|T| = \sum_{s \in S} [s \in T] .$$

(b) For each $s \in S$, let $\mathcal{A}(s)$ be a logical statement (which can be either true or false depending on s; for example, $\mathcal{A}(s)$ could be "s is even" if S is a set of integers, or "s is empty" if S is a set of sets). Then,

$$(\#\text{ of } s \in S \text{ that satisfy } \mathcal{A}(s)) = \sum_{s \in S} [\mathcal{A}(s)] .$$

Example 1.6.4. (a) Applying Proposition 1.6.3 **(a)** to $S = [5]$ and $T = \{1,3,5\}$, we obtain

$$|\{1,3,5\}| = \sum_{s \in [5]} [s \in \{1,3,5\}] = 1+0+1+0+1.$$

(b) Applying Proposition 1.6.3 **(b)** to $S = [5]$ and $\mathcal{A}(s) = (\text{"}s \text{ is odd"})$, we obtain

$$(\#\text{ of } s \in [5] \text{ that are odd}) = \sum_{s \in [5]} [s \text{ is odd}] = 1+0+1+0+1.$$

Why am I calling this "counting by roll call"? Because Proposition 1.6.3 **(a)** formalizes a way to count the elements of the subset T by "calling the roll" of all elements of S and adding a 1 every time an element of T is encountered. Proposition 1.6.3 **(b)** does the same thing, except we are no longer counting the elements of T, but instead are counting the elements s of S that satisfy $\mathcal{A}(s)$. The two parts of Proposition 1.6.3 are easily seen to be equivalent to each other, since any subset T of S gives rise to a logical statement $\mathcal{A}(s) = (\text{"}s \in T\text{"})$ for each $s \in S$, and conversely, any logical statement $\mathcal{A}(s)$ defined for each $s \in S$ can be used to carve out a subset $\{s \in S \mid \mathcal{A}(s) \text{ holds}\}$ of S.

The formal proof is not much more complicated:

Proof of Proposition 1.6.3. **(b)** Let Q be the set of all $s \in S$ that satisfy $\mathcal{A}(s)$. Then,

$$|Q| = (\#\text{ of } s \in S \text{ that satisfy } \mathcal{A}(s)) .$$

Furthermore, the elements $s \in S$ for which $\mathcal{A}(s)$ is true are precisely the elements of Q (because this is how Q is defined).

[106] For the meaning of the square brackets on the right hand side, see Definition 1.3.15.

Now, apply the formula (28) to $a_s = [\mathcal{A}(s)]$. Thus, we obtain

$$\begin{aligned}
\sum_{s\in S} [\mathcal{A}(s)] &= \sum_{\substack{s\in S;\\ \mathcal{A}(s) \text{ is true}}} \underbrace{[\mathcal{A}(s)]}_{\substack{=1\\ (\text{since } \mathcal{A}(s) \text{ is true})}} + \sum_{\substack{s\in S;\\ \mathcal{A}(s) \text{ is false}}} \underbrace{[\mathcal{A}(s)]}_{\substack{=0\\ (\text{since } \mathcal{A}(s) \text{ is false})}} \\
&= \sum_{\substack{s\in S;\\ \mathcal{A}(s) \text{ is true}}} 1 + \sum_{\substack{s\in S;\\ \underbrace{\mathcal{A}(s) \text{ is false}}_{=0}}} 0 = \sum_{\substack{s\in S;\\ \mathcal{A}(s) \text{ is true}}} 1 = \sum_{s\in Q} 1 \\
&\qquad \left(\begin{array}{c} \text{since the elements } s \in S \text{ for which } \mathcal{A}(s) \text{ is true} \\ \text{are precisely the elements of } Q \end{array} \right) \\
&= |Q| \qquad (\text{by (30), applied to } Q \text{ instead of } S) \\
&= (\#\text{ of } s \in S \text{ that satisfy } \mathcal{A}(s)) .
\end{aligned}$$

This proves Proposition 1.6.3 **(b)**.

(a) Let T be a subset of S. Thus, $S \cap T = T$. Applying Proposition 1.6.3 **(b)** to the statements $\mathcal{A}(s) = (\text{“}s \in T\text{”})$, we obtain

$$(\#\text{ of } s \in S \text{ that satisfy } s \in T) = \sum_{s\in S} [s \in T] .$$

Comparing this with

$$(\#\text{ of } s \in S \text{ that satisfy } s \in T) = \left| \underbrace{\{s \in S \mid s \in T\}}_{=S\cap T=T} \right| = |T| ,$$

we obtain $|T| = \sum_{s\in S} [s \in T]$. This proves Proposition 1.6.3 **(a)**. □

First solution to Exercise 1.6.1. Let $\mathcal{P}(S)$ denote the powerset of S. This is a finite set, since S is finite.

We have $|S| = n$ (since S is an n-element set). But

$$\sum_{T\subseteq S} \underbrace{|T|}_{\substack{=\sum_{s\in S}[s\in T]\\ (\text{by Proposition 1.6.3 } \textbf{(a)})}} = \sum_{T\subseteq S} \sum_{s\in S} [s \in T] = \sum_{s\in S} \sum_{T\subseteq S} [s \in T] , \tag{104}$$

where the last equality has been obtained by interchanging the two summation signs (using the Fubini principle)[107]. Hence,

$$\sum_{T\subseteq S} |T| = \sum_{s\in S} \sum_{T\subseteq S} [s \in T] = \sum_{x\in S} \sum_{T\subseteq S} [x \in T] \tag{105}$$

[107] In more detail: Theorem 1.6.1 (applied to $X = \mathcal{P}(S)$, $Y = S$ and $a_{(x,y)} = [y \in x]$) yields

$$\sum_{x\in\mathcal{P}(S)} \sum_{y\in S} [y \in x] = \sum_{(x,y)\in\mathcal{P}(S)\times S} [y \in x] = \sum_{y\in S} \sum_{x\in\mathcal{P}(S)} [y \in x] .$$

Renaming the summation indices x and y as T and s (in order to match the notations in (104)),

(here, we have renamed the summation index s as x in the outer sum).

Now, fix $x \in S$. We shall simplify the sum $\sum_{T \subseteq S} [x \in T]$. Indeed, an application of Proposition 1.6.3 **(b)** yields

$$\sum_{T \subseteq S} [x \in T] = (\#\text{ of subsets } T \text{ of } S \text{ that satisfy } x \in T) \tag{106}$$

[108]. But there is a bijection

$$\{\text{subsets } T \text{ of } S \text{ that satisfy } x \in T\} \to \{\text{subsets of } S \setminus \{x\}\}, \\ R \mapsto R \setminus \{x\}$$

[109]. By the bijection principle, this entails that

$$|\{\text{subsets } T \text{ of } S \text{ that satisfy } x \in T\}| = |\{\text{subsets of } S \setminus \{x\}\}|.$$

---

we rewrite this as

$$\sum_{T \in \mathcal{P}(S)} \sum_{s \in S} [s \in T] = \sum_{(T,s) \in \mathcal{P}(S) \times S} [s \in T] = \sum_{s \in S} \sum_{T \in \mathcal{P}(S)} [s \in T].$$

Since the summation sign $\sum_{T \in \mathcal{P}(S)}$ is synonymous to $\sum_{T \subseteq S}$, we can further rewrite this as follows:

$$\sum_{T \subseteq S} \sum_{s \in S} [s \in T] = \sum_{(T,s) \in \mathcal{P}(S) \times S} [s \in T] = \sum_{s \in S} \sum_{T \subseteq S} [s \in T].$$

This justifies the last equality sign in (104).

[108] In more detail: We can apply Proposition 1.6.3 **(b)** to $\mathcal{P}(S)$ and ("$x \in s$") instead of S and $\mathcal{A}(s)$. This results in the equality

$$(\#\text{ of } s \in \mathcal{P}(S) \text{ that satisfy } x \in s) = \sum_{s \in \mathcal{P}(S)} [x \in s].$$

Renaming the "s" here as T, we can rewrite this as

$$(\#\text{ of } T \in \mathcal{P}(S) \text{ that satisfy } x \in T) = \sum_{T \in \mathcal{P}(S)} [x \in T].$$

Since the summation sign $\sum_{T \in \mathcal{P}(S)}$ is a synonym for $\sum_{T \subseteq S}$, this further rewrites as

$$(\#\text{ of } T \in \mathcal{P}(S) \text{ that satisfy } x \in T) = \sum_{T \subseteq S} [x \in T].$$

Hence,

$$\sum_{T \subseteq S} [x \in T] = (\#\text{ of } T \in \mathcal{P}(S) \text{ that satisfy } x \in T) \\ = (\#\text{ of subsets } T \text{ of } S \text{ that satisfy } x \in T),$$

because the $T \in \mathcal{P}(S)$ are precisely the subsets of S.

[109] Indeed, this map is easily seen to be well-defined, and it has an inverse map which sends each $Q \in \{\text{subsets of } S \setminus \{x\}\}$ to $Q \cup \{x\} \in \{\text{subsets } T \text{ of } S \text{ that satisfy } x \in T\}$. This is essentially the same construction that we used to count red subsets in the proof of Theorem 1.3.12, except that this time we are not fixing the size of our subsets but considering all subsets together.

In other words,

$$(\#\text{ of subsets } T \text{ of } S \text{ that satisfy } x \in T) = (\#\text{ of subsets of } S \setminus \{x\}).$$

Furthermore, $S \setminus \{x\}$ is an $(n-1)$-element set (since S is an n-element set, and $x \in S$), and thus $n-1 = |S \setminus \{x\}| \in \mathbb{N}$; hence, Theorem 1.4.1 (applied to $n-1$ and $S \setminus \{x\}$ instead of n and S) yields

$$(\#\text{ of subsets of } S \setminus \{x\}) = 2^{n-1}.$$

Thus, (106) becomes

$$\begin{aligned}\sum_{T \subseteq S} [x \in T] &= (\#\text{ of subsets } T \text{ of } S \text{ that satisfy } x \in T) \\ &= (\#\text{ of subsets of } S \setminus \{x\}) = 2^{n-1}. \end{aligned} \tag{107}$$

Now, forget that we fixed x. We thus have proved that (107) holds for each $x \in S$. Hence, (105) becomes

$$\sum_{T \subseteq S} |T| = \sum_{x \in S} \underbrace{\sum_{T \subseteq S} [x \in T]}_{\substack{=2^{n-1} \\ \text{(by (107))}}} = \sum_{s \in S} 2^{n-1} = \underbrace{|S|}_{=n} \cdot 2^{n-1} = n \cdot 2^{n-1}.$$

This solves Exercise 1.6.1. □

In the future, we will no longer explicitly cite the Fubini principle whenever we interchange summation signs, let alone rename our summation indices to match those in Theorem 1.6.1 and rewrite signs like $\sum_{T \subseteq S}$ in the standard form $\sum_{T \in \mathcal{P}(S)}$. We will also cut down on the details when invoking Proposition 1.6.3. Thus, the solution we just gave will take the following short form:

First solution to Exercise 1.6.1 (short version). We have $|S| = n$ (since S is an n-element set). But

$$\begin{aligned}\sum_{T \subseteq S} \underbrace{|T|}_{\substack{=\sum_{s \in S}[s \in T] \\ \text{(by Proposition 1.6.3 \textbf{(a)})}}} &= \underbrace{\sum_{T \subseteq S} \sum_{s \in S}}_{=\sum_{s \in S} \sum_{T \subseteq S}} [s \in T] = \sum_{s \in S} \sum_{T \subseteq S} [s \in T] \\ &= \sum_{x \in S} \sum_{T \subseteq S} [x \in T] \end{aligned} \tag{108}$$

(here, we have renamed the summation index s as x in the outer sum).

Now, for each $x \in S$, we have

$$\begin{aligned}\sum_{T \subseteq S} [x \in T] &= (\text{\# of subsets } T \text{ of } S \text{ that satisfy } x \in T) \\ &\qquad (\text{by an application of Proposition 1.6.3 } \textbf{(b)}) \\ &= (\text{\# of subsets of } S \setminus \{x\}) \\ &\qquad \left(\begin{array}{c}\text{by the bijection principle,} \\ \text{since there is a bijection} \\ \text{from } \{\text{subsets } T \text{ of } S \text{ that satisfy } x \in T\} \\ \text{to } \{\text{subsets of } S \setminus \{x\}\} \\ \text{that sends each } R \text{ to } R \setminus \{x\}\end{array}\right) \\ &= 2^{n-1} \qquad \left(\begin{array}{c}\text{by Theorem 1.4.1, applied to } n-1 \\ \text{and } S \setminus \{x\} \text{ instead of } n \text{ and } S\end{array}\right). \qquad (109)\end{aligned}$$

Hence, (108) becomes

$$\sum_{T \subseteq S} |T| = \sum_{x \in S} \underbrace{\sum_{T \subseteq S} [x \in T]}_{\substack{=2^{n-1} \\ (\text{by (109)})}} = \sum_{s \in S} 2^{n-1} = \underbrace{|S|}_{=n} \cdot 2^{n-1} = n \cdot 2^{n-1}.$$

This solves Exercise 1.6.1. □

Thus, interchanging summations (even if it requires strategically introducing extra summation signs) can lead to short and slick proofs.

Our solution to Exercise 1.6.1 resulted in the expression $n \cdot 2^{n-1}$, which is rather obviously the simplest possible answer (it cannot be simplified any further). Nevertheless, it is worth seeing a different solution to Exercise 1.6.1, which results in a different (more complicated) expression for the answer. This is not a bad thing, because as a consequence we will immediately conclude the equality between the two expressions (once again, a proof by double counting!).

Second solution to Exercise 1.6.1. Let $\mathcal{P}(S)$ denote the powerset of S. This is a finite set, since S is finite. For each $T \in \mathcal{P}(S)$, we have $|T| \in \{0, 1, \ldots, n\}$ [110]. Hence, we can define a map

$$\begin{aligned} f : \mathcal{P}(S) &\to \{0, 1, \ldots, n\}, \\ T &\mapsto |T|. \end{aligned}$$

Consider this map f. Now, (37) (applied to $\mathcal{P}(S)$, $\{0, 1, \ldots, n\}$ and $|s|$ instead of S, W and a_s) yields

$$\sum_{s \in \mathcal{P}(S)} |s| = \sum_{w \in \{0,1,\ldots,n\}} \sum_{\substack{s \in \mathcal{P}(S); \\ f(s) = w}} |s|.$$

[110] *Proof.* Let $T \in \mathcal{P}(S)$. Thus, T is a subset of S (by the definition of $\mathcal{P}(S)$). Hence, Theorem 1.4.7 **(b)** (applied to $A = S$ and $B = T$) yields $|T| \leq |S| = n$ (since S is an n-element set). Hence, $|T| \in \{0, 1, \ldots, n\}$ (since $|T|$ is clearly a nonnegative integer).

Renaming the summation index s as T everywhere in this equality, we can rewrite this as

$$\sum_{T \in \mathcal{P}(S)} |T| = \sum_{w \in \{0,1,\ldots,n\}} \sum_{\substack{T \in \mathcal{P}(S); \\ f(T)=w}} |T| .$$

In other words,

$$\sum_{T \subseteq S} |T| = \sum_{w \in \{0,1,\ldots,n\}} \sum_{\substack{T \subseteq S; \\ f(T)=w}} |T|$$

(since "$T \in \mathcal{P}(S)$" under a summation sign can always be abbreviated as "$T \subseteq S$"). Renaming the summation index w as k on the right hand side, we can further rewrite this as

$$\sum_{T \subseteq S} |T| = \sum_{k \in \{0,1,\ldots,n\}} \sum_{\substack{T \subseteq S; \\ f(T)=k}} |T| . \tag{110}$$

The left hand side of this equality is the sum we want to find; let us get a better understanding of the right hand side.

Let $k \in \{0, 1, \ldots, n\}$. The definition of f shows that $f(T) = |T|$ for each subset T of S. Hence,

$$\begin{aligned}
\sum_{\substack{T \subseteq S; \\ f(T)=k}} |T| &= \sum_{\substack{T \subseteq S; \\ |T|=k}} \underbrace{|T|}_{=k} = \sum_{\substack{T \subseteq S; \\ |T|=k}} k = \sum_{T \in \{k\text{-element subsets of } S\}} k \\
&\qquad \left(\begin{array}{c} \text{since the subsets } T \text{ of } S \text{ satisfying } |T| = k \\ \text{are precisely the } k\text{-element subsets of } S \end{array} \right) \\
&= \underbrace{\left| \{k\text{-element subsets of } S\} \right|}_{=(\#\text{ of } k\text{-element subsets of } S)} \cdot k \qquad \text{(by an application of (29))} \\
&\qquad = \binom{n}{k} \\
&\qquad \text{(by Theorem 1.3.12)} \\
&= \binom{n}{k} \cdot k = k \binom{n}{k}.
\end{aligned} \tag{111}$$

Forget that we fixed k. We thus have proven (111) for each $k \in \{0, 1, \ldots, n\}$. Hence, (110) becomes

$$\sum_{T \subseteq S} |T| = \sum_{k \in \{0,1,\ldots,n\}} \underbrace{\sum_{\substack{T \subseteq S; \\ f(T)=k}} |T|}_{\substack{=k\binom{n}{k} \\ \text{(by (111))}}} = \sum_{k \in \{0,1,\ldots,n\}} k \binom{n}{k} = \sum_{k=0}^{n} k \binom{n}{k}.$$

Thus we have solved Exercise 1.6.1 again. □

The solution we just gave illustrates another method of dealing with sums: namely, by splitting them into batches using (37). (We chose the batches in such a way that all addends in any given batch are equal, which means that the sum of the batch simplifies to a product: $\sum\limits_{\substack{T\subseteq S;\\ |T|=k}} k = |\{k\text{-element subsets of } S\}| \cdot k$. This is not the only strategy to split a sum, but it is one of the simplest strategies.) In the future, we will not explicitly mention the formula (37) (let alone explain how exactly it is being applied) when we perform such a splitting; we will simply say that we are "splitting the sum $\sum\limits_{T\subseteq S} |T|$ according to the value of $|T|$". Thus, our Second solution to Exercise 1.6.1 takes the following short form:

Second solution to Exercise 1.6.1 (short version). If T is any subset of S, then $|T| \in \{0,1,\ldots,n\}$ [111]. Hence, we can split the sum $\sum\limits_{T\subseteq S} |T|$ according to the value of $|T|$ as follows:

$$\sum_{T\subseteq S} |T| = \sum_{k\in\{0,1,\ldots,n\}} \sum_{\substack{T\subseteq S;\\ |T|=k}} |T| . \tag{112}$$

However, for each $k \in \{0,1,\ldots,n\}$, we have

$$\sum_{\substack{T\subseteq S;\\ |T|=k}} \underbrace{|T|}_{=k} = \sum_{\substack{T\subseteq S;\\ |T|=k}} k = \underbrace{(\#\text{ of all } T\subseteq S \text{ satisfying } |T|=k)}_{=(\#\text{ of } k\text{-element subsets of } S)} \cdot k = \underbrace{\binom{n}{k}}_{\substack{=\binom{n}{k}\\ \text{(by Theorem 1.3.12)}}} \cdot k = k\binom{n}{k}.$$

Hence, (112) becomes

$$\sum_{T\subseteq S} |T| = \sum_{k\in\{0,1,\ldots,n\}} \underbrace{\sum_{\substack{T\subseteq S;\\ |T|=k}} |T|}_{=k\binom{n}{k}} = \sum_{k\in\{0,1,\ldots,n\}} k\binom{n}{k} = \sum_{k=0}^{n} k\binom{n}{k}.$$

Thus we have solved Exercise 1.6.1 again. □

Now, by comparing the results of the two solutions of Exercise 1.6.1, we get the following identity for free:

Corollary 1.6.5. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}.$$

[111] because Theorem 1.4.7 **(b)** (applied to $A = S$ and $B = T$) yields $|T| \leq |S| = n$ (since S is an n-element set)

Proof of Corollary 1.6.5. Let $S = [n]$. Then, S is an n-element set.

In the first solution to Exercise 1.6.1, we have shown that

$$\sum_{T \subseteq S} |T| = n \cdot 2^{n-1}.$$

In the second solution to Exercise 1.6.1, we have shown that

$$\sum_{T \subseteq S} |T| = \sum_{k=0}^{n} k \binom{n}{k}.$$

Comparing these two equalities, we obtain $\sum_{k=0}^{n} k \binom{n}{k} = n \cdot 2^{n-1}$. This proves Corollary 1.6.5. □

There are easier ways to prove Corollary 1.6.5 as well; in particularly, it can be proven purely algebraically using Proposition 1.3.36 and Corollary 1.3.27 (exercise!).

1.6.2. The Fubini principle with a predicate

Theorem 1.6.1 is a useful tool for interchanging summation signs that are independent of one another – i.e., the indexing set of the inner summation sign must not depend on the summation index of the other. Thus, for example, we can use Theorem 1.6.1 to interchange the two summation signs in $\sum_{x=1}^{5} \sum_{y=1}^{6}$, but not in $\sum_{x=1}^{5} \sum_{y=1}^{x}$. Nevertheless, in the latter situation, we would still like to bring the y "out", i.e., to transform $\sum_{x=1}^{5} \sum_{y=1}^{x}$ into $\sum_{x=?}^{?} \sum_{y=?}^{?}$ for some values of the question marks. There is a Fubini-like rule for this, which we will see soon (Corollary 1.6.9). (The answer is: $\sum_{x=1}^{5} \sum_{y=1}^{x}$ transforms into $\sum_{y=1}^{5} \sum_{x=y}^{5}$.)

First, let us state the most general version of this rule, which is a generalization of Fubini's principle to tables that have "gaps":

Theorem 1.6.6 (Finite Fubini's principle with a predicate)**.** Let X and Y be two finite sets. For each pair $(x, y) \in X \times Y$, let $\mathcal{A}(x, y)$ be some statement (for example, "$x + y$ is even" or "$x < y$", if X and Y are sets of numbers). For each pair $(x, y) \in X \times Y$ satisfying $\mathcal{A}(x, y)$, let $a_{(x,y)}$ be a number. Then,

$$\sum_{x \in X} \sum_{\substack{y \in Y; \\ \mathcal{A}(x,y)}} a_{(x,y)} = \sum_{\substack{(x,y) \in X \times Y; \\ \mathcal{A}(x,y)}} a_{(x,y)} = \sum_{y \in Y} \sum_{\substack{x \in X; \\ \mathcal{A}(x,y)}} a_{(x,y)}. \tag{113}$$

(Here, the "$\mathcal{A}(x, y)$" under the summation signs means "$\mathcal{A}(x, y)$ is true".)

For example, if $n, m \in \mathbb{N}$, and if $a_{(x,y)}$ is a number for each pair $(x,y) \in [n] \times [m]$, then Theorem 1.6.6 (applied to $X = [n]$ and $Y = [m]$ and $\mathcal{A}(x,y) =$ ("$x+y$ is even")) shows that

$$\sum_{x \in [n]} \sum_{\substack{y \in [m]; \\ x+y \text{ is even}}} a_{(x,y)} = \sum_{\substack{(x,y) \in [n] \times [m]; \\ x+y \text{ is even}}} a_{(x,y)} = \sum_{y \in [m]} \sum_{\substack{x \in [n]; \\ x+y \text{ is even}}} a_{(x,y)}.$$

The idea behind Theorem 1.6.6 is the same as the one behind Theorem 1.6.1: We have a table of numbers, and we can add up the numbers in this table in three different ways (row by row, in a random order, or column by column). The difference is that this time, the table can have empty cells (more precisely, only the cells (x,y) for which $\mathcal{A}(x,y)$ is true have a number in them); of course, these empty cells don't contribute to the sums.[112]

The formula (113) allows us to replace a sequence "$\sum\limits_{x \in X} \sum\limits_{\substack{y \in Y; \\ \mathcal{A}(x,y)}}$" of summation signs by "$\sum\limits_{y \in Y} \sum\limits_{\substack{x \in X; \\ \mathcal{A}(x,y)}}$". This is still considered to be an interchange of summations – with the only caveat that the statement $\mathcal{A}(x,y)$ has to stay put under the inner sum, whatever this inner sum is.

By choosing appropriate statements $\mathcal{A}(x,y)$ in Theorem 1.6.6, we can obtain various templates for interchange of non-independent summation signs. Here is one such template:

Corollary 1.6.7 (Triangular Fubini's principle I)**.** Let $n \in \mathbb{N}$. For each pair $(x,y) \in [n] \times [n]$ with $x + y \leq n$, let $a_{(x,y)}$ be a number. Then,

$$\sum_{x=1}^{n} \sum_{y=1}^{n-x} a_{(x,y)} = \sum_{\substack{(x,y) \in [n] \times [n]; \\ x+y \leq n}} a_{(x,y)} = \sum_{y=1}^{n} \sum_{x=1}^{n-y} a_{(x,y)}.$$

Example 1.6.8. If we set $n = 4$ in Corollary 1.6.7 and rewrite the result without using summation signs, then we obtain

$$\begin{aligned}
&\left(a_{(1,1)} + a_{(1,2)} + a_{(1,3)}\right) + \left(a_{(2,1)} + a_{(2,2)}\right) + a_{(3,1)} + (\text{empty sum}) \\
&= a_{(1,1)} + a_{(1,2)} + \cdots + a_{(3,1)} \qquad \left(\text{this is the sum of all the numbers } a_{(x,y)}\right) \\
&= \left(a_{(1,1)} + a_{(2,1)} + a_{(3,1)}\right) + \left(a_{(1,2)} + a_{(2,2)}\right) + a_{(1,3)} + (\text{empty sum}).
\end{aligned}$$

[112] We remark that Theorem 1.6.6 can easily be derived from Theorem 1.6.1. Indeed, if we define the (hitherto undefined) number $a_{(x,y)}$ to be 0 whenever $(x,y) \in X \times Y$ does **not** satisfy $\mathcal{A}(x,y)$, then we can apply Theorem 1.6.1, and the equality (102) we obtain quickly rewrites as (113).

In other words, if we are given a triangular table of numbers:

$$\begin{array}{|ccc} \hline a_{(1,1)} & a_{(1,2)} & a_{(1,3)} \\ \hline a_{(2,1)} & a_{(2,2)} & \multicolumn{1}{c}{} \\ \cline{1-2} a_{(3,1)} & \multicolumn{2}{c}{} \\ \cline{1-1} \end{array},$$

then the following three procedures all produce the same result:

(a) summing up the numbers in each row of the table separately, and then summing up these "row tallies";

(b) summing up all the 6 numbers in the table;

(c) summing up the numbers in each column of the table separately, and then summing up these "column tallies".

Proof of Corollary 1.6.7. Theorem 1.6.6 (applied to $X = [n]$, $Y = [n]$ and $\mathcal{A}(x,y) = (\text{"}x+y \leq n\text{"})$) yields

$$\sum_{x\in[n]} \sum_{\substack{y\in[n]; \\ x+y\leq n}} a_{(x,y)} = \sum_{\substack{(x,y)\in[n]\times[n]; \\ x+y\leq n}} a_{(x,y)} = \sum_{y\in[n]} \sum_{\substack{x\in[n]; \\ x+y\leq n}} a_{(x,y)}. \tag{114}$$

We shall now rewrite the two inner sums in this chain of equalities.

Let $x \in [n]$. Then, $x \geq 1 \geq 0$, so that $n - x \leq n$. Thus, $[n-x] \subseteq [n]$, so that $[n-x] \cap [n] = [n-x]$. Hence, the elements $y \in [n]$ that satisfy $y \leq n - x$ are precisely the elements of $[n-x]$ (indeed, they are clearly the elements of $[n-x] \cap [n]$; but we just showed that $[n-x] \cap [n] = [n-x]$).

However, the statement "$x + y \leq n$" for an integer y is equivalent to "$y \leq n - x$", and thus can be replaced by the latter statement whenever it appears under a summation sign. Thus,

$$\begin{aligned} \sum_{\substack{y\in[n]; \\ x+y\leq n}} a_{(x,y)} &= \sum_{\substack{y\in[n]; \\ y\leq n-x}} a_{(x,y)} \\ &= \sum_{y\in[n-x]} a_{(x,y)} \qquad \left(\begin{array}{c} \text{since the elements } y \in [n] \text{ that satisfy } y \leq n-x \\ \text{are precisely the elements of } [n-x] \end{array} \right) \\ &= \sum_{y=1}^{n-x} a_{(x,y)}. \end{aligned} \tag{115}$$

Forget that we fixed x. We thus have proved (115) for each $x \in [n]$. Likewise, we can prove that

$$\sum_{\substack{x\in[n]; \\ x+y\leq n}} a_{(x,y)} = \sum_{x=1}^{n-y} a_{(x,y)} \tag{116}$$

for each $y \in [n]$. In light of the two equalities (115) and (116), we can rewrite the chain of equalities (114) as follows:

$$\sum_{x\in[n]} \sum_{y=1}^{n-x} a_{(x,y)} = \sum_{\substack{(x,y)\in[n]\times[n]; \\ x+y\leq n}} a_{(x,y)} = \sum_{y\in[n]} \sum_{x=1}^{n-y} a_{(x,y)}.$$

In other words,

$$\sum_{x=1}^{n} \sum_{y=1}^{n-x} a_{(x,y)} = \sum_{\substack{(x,y)\in[n]\times[n]; \\ x+y\leq n}} a_{(x,y)} = \sum_{y=1}^{n} \sum_{x=1}^{n-y} a_{(x,y)}$$

(since the summation sign $\sum\limits_{x\in[n]}$ is synonymous to $\sum\limits_{x=1}^{n}$, whereas the summation sign $\sum\limits_{y\in[n]}$ is synonymous to $\sum\limits_{y=1}^{n}$). This proves Corollary 1.6.7. □

Let us apply Corollary 1.6.7 to solving an exercise (arguably, one that could be more easily solved by other means, but this does not preclude it from being a useful illustration):

Exercise 1.6.2. Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=1}^{n} k\,(n-k) = \binom{n+1}{3}.$$

Solution to Exercise 1.6.2. For each $x \in [n]$, we have $n - x \in \mathbb{N}$ (since $x \in [n]$ entails $x \leq n$ and thus $n - x \geq 0$), so that

$$\sum_{y=1}^{n-x} 1 = (n-x)\cdot 1 = n - x. \tag{117}$$

Renaming the index k as x in the sum $\sum\limits_{k=1}^{n} k\,(n-k)$, we obtain

$$\begin{aligned}\sum_{k=1}^{n} k\,(n-k) &= \sum_{x=1}^{n} x \underbrace{(n-x)}_{\substack{=\sum_{y=1}^{n-x} 1 \\ \text{(by (117))}}} = \sum_{x=1}^{n} \underbrace{x \sum_{y=1}^{n-x} 1}_{\substack{=\sum_{y=1}^{n-x} x\cdot 1 \\ \text{(by (32))}}} \\ &= \sum_{x=1}^{n} \sum_{y=1}^{n-x} \underbrace{x\cdot 1}_{=x} = \sum_{x=1}^{n} \sum_{y=1}^{n-x} x. \end{aligned} \tag{118}$$

But Corollary 1.6.7 (applied to $a_{(x,y)} = x$) yields

$$\sum_{x=1}^{n} \sum_{y=1}^{n-x} x = \sum_{\substack{(x,y) \in [n] \times [n]; \\ x+y \leq n}} x = \sum_{y=1}^{n} \sum_{x=1}^{n-y} x. \tag{119}$$

Furthermore, each $y \in [n]$ satisfies $n - y \in \mathbb{N}$ (since $y \in [n]$ entails $y \leq n$ and thus $n - y \geq 0$), so that

$$\begin{aligned} \sum_{x=1}^{n-y} x &= 1 + 2 + \cdots + (n-y) = \frac{(n-y)\left((n-y)+1\right)}{2} \\ &\qquad \text{(by Theorem 1.2.1, applied to } n-y \text{ instead of } n\text{)} \\ &= \frac{(n+1-y)(n-y)}{2} = \binom{n+1-y}{2} \end{aligned} \tag{120}$$

(since (46) (applied to $n+1-y$ instead of n) yields

$$\binom{n+1-y}{2} = \frac{(n+1-y)\left((n+1-y)-1\right)}{2} = \frac{(n+1-y)(n-y)}{2}$$

). Hence, (118) becomes

$$\begin{aligned} \sum_{k=1}^{n} k(n-k) &= \sum_{x=1}^{n} \sum_{y=1}^{n-x} x = \sum_{y=1}^{n} \underbrace{\sum_{x=1}^{n-y} x}_{\substack{= \binom{n+1-y}{2} \\ \text{(by (120))}}} \qquad \text{(by (119))} \\ &= \sum_{y=1}^{n} \binom{n+1-y}{2} = \sum_{i=1}^{n} \binom{i}{2} \\ &\qquad \left(\begin{array}{c} \text{here, we have substituted } i \text{ for } n+1-y \text{ in the sum} \\ \text{(since the map } [n] \to [n],\ y \mapsto n+1-y \text{ is a bijection)} \end{array} \right) \\ &= \binom{1}{2} + \binom{2}{2} + \cdots + \binom{n}{2} \\ &= \underbrace{\left(\binom{0}{2} + \binom{1}{2} + \binom{2}{2} + \cdots + \binom{n}{2} \right)}_{\substack{= \binom{n+1}{2+1} \\ \text{(by Theorem 1.3.29, applied to } k=2\text{)}}} - \underbrace{\binom{0}{2}}_{\substack{= \frac{0(0-1)}{2} \\ \text{(by (46))}}} \\ &= \binom{n+1}{2+1} - \underbrace{\frac{0(0-1)}{2}}_{=0} = \binom{n+1}{2+1} = \binom{n+1}{3}. \end{aligned}$$

This solves Exercise 1.6.2. □

In the future, of course, we won't be as detailed as in the solution we just gave; instead of explicitly invoking Corollary 1.6.7, we will simply write the following:

$$\underbrace{\sum_{x=1}^{n}\sum_{y=1}^{n-x}}_{=\sum_{y=1}^{n}\sum_{x=1}^{n-y}} x = \sum_{y=1}^{n}\sum_{x=1}^{n-y} x.$$

Here is another template for interchanging summation signs:

Corollary 1.6.9 (Triangular Fubini's principle II)**.** Let $n \in \mathbb{N}$. For each pair $(x,y) \in [n] \times [n]$ with $x \leq y$, let $a_{(x,y)}$ be a number. Then,

$$\sum_{x=1}^{n}\sum_{y=x}^{n} a_{(x,y)} = \sum_{\substack{(x,y)\in[n]\times[n]; \\ x\leq y}} a_{(x,y)} = \sum_{y=1}^{n}\sum_{x=1}^{y} a_{(x,y)}.$$

Example 1.6.10. If we set $n = 4$ in Corollary 1.6.9 and rewrite the result without using summation signs, then we obtain

$$\begin{aligned}
&\left(a_{(1,1)} + a_{(1,2)} + a_{(1,3)} + a_{(1,4)}\right) \\
&\qquad + \left(a_{(2,2)} + a_{(2,3)} + a_{(2,4)}\right) \\
&\qquad + \left(a_{(3,3)} + a_{(3,4)}\right) \\
&\qquad + a_{(4,4)} \\
&= a_{(1,1)} + a_{(1,2)} + \cdots + a_{(4,4)} \qquad \left(\text{this is the sum of all the numbers } a_{(x,y)}\right) \\
&= a_{(1,1)} \\
&\qquad + \left(a_{(1,2)} + a_{(2,2)}\right) \\
&\qquad + \left(a_{(1,3)} + a_{(2,3)} + a_{(3,3)}\right) \\
&\qquad + \left(a_{(1,4)} + a_{(2,4)} + a_{(3,4)} + a_{(4,4)}\right).
\end{aligned}$$

In other words, if we are given a triangular table of numbers:

$$\begin{array}{|cccc|}
\hline
a_{(1,1)} & a_{(1,2)} & a_{(1,3)} & a_{(1,4)} \\
\cline{2-4}
 & a_{(2,2)} & a_{(2,3)} & a_{(2,4)} \\
\cline{3-4}
 & & a_{(3,3)} & a_{(3,4)} \\
\cline{4-4}
 & & & a_{(4,4)} \\
\hline
\end{array},$$

then the following three procedures all produce the same result:

(a) summing up the numbers in each row of the table separately, and then summing up these "row tallies";

(b) summing up all the 10 numbers in the table;

(c) summing up the numbers in each column of the table separately, and then summing up these "column tallies".

Proof of Corollary 1.6.9. This is similar to the proof of Corollary 1.6.7; we just need to define the statements $\mathcal{A}(x,y)$ differently. Theorem 1.6.6 (applied to $X = [n]$, $Y = [n]$ and $\mathcal{A}(x,y) = (\text{"}x \leq y\text{"})$) yields

$$\sum_{x\in[n]} \sum_{\substack{y\in[n];\\ x\leq y}} a_{(x,y)} = \sum_{\substack{(x,y)\in[n]\times[n];\\ x\leq y}} a_{(x,y)} = \sum_{y\in[n]} \sum_{\substack{x\in[n];\\ x\leq y}} a_{(x,y)}. \tag{121}$$

We shall now rewrite the two inner sums in this chain of equalities.

Let $x \in [n]$. Then, $1 \leq x \leq n$. Hence, the elements $y \in [n]$ that satisfy $x \leq y$ are precisely the elements of $\{x, x+1, \ldots, n\}$. Thus,

$$\sum_{\substack{y\in[n];\\ x\leq y}} a_{(x,y)} = \sum_{y\in\{x,x+1,\ldots,n\}} a_{(x,y)} = \sum_{y=x}^{n} a_{(x,y)}. \tag{122}$$

Forget that we fixed x. We thus have proved (122) for each $x \in [n]$.

Next, let $y \in [n]$. Then, $1 \leq y \leq n$. Hence, the elements $x \in [n]$ that satisfy $x \leq y$ are precisely the elements of $\{1, 2, \ldots, y\}$. Thus,

$$\sum_{\substack{x\in[n];\\ x\leq y}} a_{(x,y)} = \sum_{x\in\{1,2,\ldots,y\}} a_{(x,y)} = \sum_{x=1}^{y} a_{(x,y)}. \tag{123}$$

Forget that we fixed y. We thus have proved (123) for each $y \in [n]$.

In light of the two equalities (122) and (123), we can rewrite the chain of equalities (121) as follows:

$$\sum_{x\in[n]} \sum_{y=x}^{n} a_{(x,y)} = \sum_{\substack{(x,y)\in[n]\times[n];\\ x\leq y}} a_{(x,y)} = \sum_{y\in[n]} \sum_{x=1}^{y} a_{(x,y)}.$$

In other words,

$$\sum_{x=1}^{n} \sum_{y=x}^{n} a_{(x,y)} = \sum_{\substack{(x,y)\in[n]\times[n];\\ x\leq y}} a_{(x,y)} = \sum_{y=1}^{n} \sum_{x=1}^{y} a_{(x,y)}$$

(since the summation sign $\sum_{x\in[n]}$ is synonymous to $\sum_{x=1}^{n}$, whereas the summation sign $\sum_{y\in[n]}$ is synonymous to $\sum_{y=1}^{n}$). This proves Corollary 1.6.9. □

Let us illustrate Corollary 1.6.9 on two examples of its use. The first is an exercise ([19f-hw2s, Exercise 1]) about harmonic numbers:

Exercise 1.6.3. For each $n \in \mathbb{N}$, we define the *n-th harmonic number* H_n by

$$H_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}.$$

Prove that

$$H_1 + H_2 + \cdots + H_n = (n+1)\left(H_{n+1} - 1\right)$$

for each $n \in \mathbb{N}$.

It is not hard to solve this exercise by induction on n (see [19f-hw2s, First solution to Exercise 1]); but here is a different solution, using Corollary 1.6.9:

Solution to Exercise 1.6.3. Each $n \in \mathbb{N}$ satisfies

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

(by the definition of H_n). Renaming n as m in this statement, we obtain the following: Each $m \in \mathbb{N}$ satisfies

$$H_m = \sum_{k=1}^{m} \frac{1}{k}. \tag{124}$$

Now, let $n \in \mathbb{N}$. Then,

$$H_1 + H_2 + \cdots + H_n = \sum_{m=1}^{n} \underbrace{H_m}_{\substack{= \sum_{k=1}^{m} \frac{1}{k} \\ \text{(by (124))}}} = \sum_{m=1}^{n} \sum_{k=1}^{m} \frac{1}{k}. \tag{125}$$

Now, Corollary 1.6.9 (applied to $a_{(x,y)} = \dfrac{1}{x}$) yields

$$\sum_{x=1}^{n} \sum_{y=x}^{n} \frac{1}{x} = \sum_{\substack{(x,y) \in [n] \times [n]; \\ x \leq y}} \frac{1}{x} = \sum_{y=1}^{n} \sum_{x=1}^{y} \frac{1}{x}.$$

Renaming the summation indices x and y as k and m in this equality, we obtain

$$\sum_{k=1}^{n} \sum_{m=k}^{n} \frac{1}{k} = \sum_{\substack{(k,m) \in [n] \times [n]; \\ k \leq m}} \frac{1}{k} = \sum_{m=1}^{n} \sum_{k=1}^{m} \frac{1}{k}.$$

Comparing this with (125), we obtain

$$H_1 + H_2 + \cdots + H_n = \sum_{k=1}^{n} \underbrace{\sum_{m=k}^{n} \frac{1}{k}}_{\substack{=(n-k+1)\cdot\frac{1}{k} \\ \text{(since this is a sum of } n-k+1 \\ \text{many equal addends)}}} = \sum_{k=1}^{n} (n-k+1) \cdot \frac{1}{k}.$$

Comparing this with

$$\begin{aligned}
&(n+1)\,(H_{n+1}-1) \\
&= (n+1) \underbrace{H_{n+1}}_{\substack{=\sum_{k=1}^{n+1}\frac{1}{k} \\ \text{(by (124), applied to } m=n+1)}} - \underbrace{(n+1)}_{\substack{=\sum_{k=1}^{n+1} 1 \\ \text{(since } \sum_{k=1}^{n+1} 1 = (n+1)\cdot 1 = n+1)}} \\
&= (n+1) \sum_{k=1}^{n+1} \frac{1}{k} - \sum_{k=1}^{n+1} 1 = \sum_{k=1}^{n+1} \underbrace{\left((n+1) \cdot \frac{1}{k} - 1 \right)}_{=(n-k+1)\cdot\frac{1}{k}} = \sum_{k=1}^{n+1} (n-k+1) \cdot \frac{1}{k} \\
&= \underbrace{(n-(n+1)+1)}_{=0} \cdot \frac{1}{n+1} + \sum_{k=1}^{n} (n-k+1) \cdot \frac{1}{k} \\
&\qquad \text{(here, we have split off the addend for } k = n+1 \text{ from the sum)} \\
&= \sum_{k=1}^{n} (n-k+1) \cdot \frac{1}{k},
\end{aligned}$$

we obtain $H_1 + H_2 + \cdots + H_n = (n+1)\,(H_{n+1} - 1)$. This solves Exercise 1.6.3. □

A more intricate application of Corollary 1.6.9 is the following identity for binomial coefficients:

Exercise 1.6.4. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k} \binom{n}{k} = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Exercise 1.6.4 is not too hard to solve by induction (see [Grinbe15, Exercise 3.19] for such a solution); but for illustrative purposes, let me solve it using Corollary 1.6.9 here:

Solution to Exercise 1.6.4. Let $k \in [n]$. Then, $1 \leq k \leq n$, so that $k \geq 1$ and thus $k-1 \in \mathbb{N}$. Note that $k \geq 1$ also entails $k \in \{1,2,3,\ldots\}$. Furthermore, $n \geq 1$ (since $1 \leq n$) and thus $n-1 \in \mathbb{N}$. Hence, Corollary 1.3.30 (applied to $n-1$ and $k-1$ instead of n and k) yields

$$\begin{aligned}&\binom{k-1}{k-1} + \binom{(k-1)+1}{k-1} + \binom{(k-1)+2}{k-1} + \cdots + \binom{n-1}{k-1} \\ &= \binom{(n-1)+1}{(k-1)+1} = \binom{n}{k} \qquad (\text{since } (n-1)+1 = n \text{ and } (k-1)+1 = k).\end{aligned}$$

Hence,

$$\begin{aligned}\binom{n}{k} &= \binom{k-1}{k-1} + \binom{(k-1)+1}{k-1} + \binom{(k-1)+2}{k-1} + \cdots + \binom{n-1}{k-1} \\ &= \binom{k-1}{k-1} + \binom{k}{k-1} + \binom{k+1}{k-1} + \cdots + \binom{n-1}{k-1} = \sum_{i=k}^{n} \binom{i-1}{k-1}.\end{aligned}$$

Multiplying both sides of this equality by $\dfrac{(-1)^{k-1}}{k}$, we obtain

$$\begin{aligned}\frac{(-1)^{k-1}}{k}\binom{n}{k} &= \frac{(-1)^{k-1}}{k} \sum_{i=k}^{n} \binom{i-1}{k-1} \\ &= \sum_{i=k}^{n} \underbrace{\frac{(-1)^{k-1}}{k}}_{\substack{= \frac{(-1)^{k-1}}{i} \cdot \frac{i}{k} \\ (\text{since } i \neq 0 \text{ (because } i \geq k \geq 1 > 0))}} \binom{i-1}{k-1} \qquad (\text{by (32)}) \\ &= \sum_{i=k}^{n} \frac{(-1)^{k-1}}{i} \cdot \underbrace{\frac{i}{k}\binom{i-1}{k-1}}_{\substack{= \binom{i}{k} \\ (\text{since Proposition 1.3.36 (applied to } i \text{ and } k \text{ instead of } m \text{ and } n) \\ \text{yields } \binom{i}{k} = \frac{i}{k}\binom{i-1}{k-1})}} \\ &= \sum_{i=k}^{n} \frac{(-1)^{k-1}}{i}\binom{i}{k}. \qquad (126)\end{aligned}$$

Now forget that we fixed k. We thus have proved (126) for each $k \in [n]$. Hence,

$$\sum_{k=1}^{n} \underbrace{\frac{(-1)^{k-1}}{k}\binom{n}{k}}_{\substack{=\sum_{i=k}^{n}\frac{(-1)^{k-1}}{i}\binom{i}{k} \\ \text{(by (126))}}} = \sum_{k=1}^{n}\sum_{i=k}^{n}\frac{(-1)^{k-1}}{i}\binom{i}{k}$$

$$= \sum_{i=1}^{n}\sum_{k=1}^{i}\frac{(-1)^{k-1}}{i}\binom{i}{k}. \tag{127}$$

Here, the last equality sign has been obtained by applying Corollary 1.6.9 to $a_{(x,y)} = \frac{(-1)^{x-1}}{y}\binom{y}{x}$ (and then renaming the summation indices x and y as k and i).

Now, fix $i \in [n]$. Thus, $1 \leq i \leq n$, so that $i \geq 1 > 0$ and therefore $i \neq 0$. Hence, $[i = 0] = 0$. But (69) (applied to i instead of n) yields

$$\sum_{k=0}^{i}(-1)^k\binom{i}{k} = [i = 0] = 0.$$

Hence,

$$0 = \sum_{k=0}^{i}(-1)^k\binom{i}{k} = \underbrace{(-1)^0}_{=1}\underbrace{\binom{i}{0}}_{\substack{=1 \\ \text{(by (44))}}} + \sum_{k=1}^{i}(-1)^k\binom{i}{k}$$

(here, we have split off the addend for $k = 0$ from the sum)

$$= 1 + \sum_{k=1}^{i}\underbrace{(-1)^k}_{=-(-1)^{k-1}}\binom{i}{k} = 1 + \underbrace{\sum_{k=1}^{i}\left(-(-1)^{k-1}\right)\binom{i}{k}}_{=-\sum_{k=1}^{i}(-1)^{k-1}\binom{i}{k}}$$

$$= 1 - \sum_{k=1}^{i}(-1)^{k-1}\binom{i}{k}.$$

In other words,

$$\sum_{k=1}^{i}(-1)^{k-1}\binom{i}{k} = 1. \tag{128}$$

Now, forget that we fixed i. We thus have proven (128) for each $i \in [n]$. Thus,

(127) becomes

$$\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k}\binom{n}{k} = \sum_{i=1}^{n} \sum_{k=1}^{i} \underbrace{\frac{(-1)^{k-1}}{i}}_{=\frac{1}{i}\cdot(-1)^{k-1}} \binom{i}{k} = \sum_{i=1}^{n} \underbrace{\sum_{k=1}^{i} \frac{1}{i}\cdot(-1)^{k-1}\binom{i}{k}}_{=\frac{1}{i}\sum_{k=1}^{i}(-1)^{k-1}\binom{i}{k} \text{ (by (32))}}$$

$$= \sum_{i=1}^{n} \frac{1}{i} \underbrace{\sum_{k=1}^{i} (-1)^{k-1}\binom{i}{k}}_{=1 \text{ (by (128))}} = \sum_{i=1}^{n} \frac{1}{i}\cdot 1 = \sum_{i=1}^{n} \frac{1}{i} = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}.$$

This solves Exercise 1.6.4. □

1.6.3. A cautionary tale about infinite sums

In Definition 1.3.26, I claimed that infinite sums (i.e., sums of the form $\sum_{x\in X} a_x$ where the indexing set X is infinite) are still well-defined as long as they only have finitely many nonzero addends; moreover, I claimed that they satisfy the same rules as finite sums. This is true for all the rules listed above (including the Fubini principle in all its forms) **as long as** we assume that **each** of the sums appearing in the rule has only finitely many nonzero addends. Usually, it suffices to assume that **some** of the sums have only finitely many nonzero addends, and then it follows that so do the others.

Let us illustrate this on the example of (31). If S is an arbitrary set (not necessarily finite), and if a_s and b_s are two numbers for each $s \in S$, then the equality (31) holds as long as we assume that the two sums $\sum_{s\in S} a_s$ and $\sum_{s\in S} b_s$ have only finitely many nonzero addends (i.e., there are only finitely many $s \in S$ satisfying $a_s \neq 0$, and there are only finitely many $s \in S$ satisfying $b_s \neq 0$). We don't need to assume that the sum $\sum_{s\in S} (a_s + b_s)$ has only finitely many nonzero addends, because this follows "for free" from the analogous assumptions on the sums $\sum_{s\in S} a_s$ and $\sum_{s\in S} b_s$. However, it does not suffice to assume that the sum $\sum_{s\in S} (a_s + b_s)$ has only finitely many nonzero addends, if we don't also make the analogous assumptions on $\sum_{s\in S} a_s$ and $\sum_{s\in S} b_s$. For example, if S is an infinite set, then the following transformation makes no sense:

$$\sum_{s\in S} \underbrace{0}_{=1+(-1)} = \sum_{s\in S} (1 + (-1)) = \sum_{s\in S} 1 + \sum_{s\in S} (-1) \qquad \text{(by (31))}.$$

The formula (31) is being misapplied here, since the sums $\sum_{s\in S} 1$ and $\sum_{s\in S} (-1)$ have infinitely many nonzero addends.

Something similar needs to be taken into account when extending Theorem 1.6.1 to infinite sums. It suffices to assume that the sum $\sum_{(x,y)\in X\times Y} a_{(x,y)}$ has only finitely many nonzero addends (i.e., that only finitely many pairs $(x,y) \in X \times Y$ satisfy $a_{(x,y)} \neq 0$). In other words, the following analogue of Theorem 1.6.1 holds for infinite sums:

Theorem 1.6.11. Let X and Y be two sets. Let $a_{(x,y)}$ be a number for each pair $(x,y) \in X \times Y$. Assume that only finitely many pairs $(x,y) \in X \times Y$ satisfy $a_{(x,y)} \neq 0$. Then, we have

$$\sum_{x\in X} \sum_{y\in Y} a_{(x,y)} = \sum_{(x,y)\in X\times Y} a_{(x,y)} = \sum_{y\in Y} \sum_{x\in X} a_{(x,y)},$$

and in particular, each of the five sums in this equality has only finitely many nonzero addends.

See [19s, proof of Proposition 7.2.11 (specifically, the proof of (227))] for a rigorous proof of this theorem (but the idea is obvious: reduce it to the case of finite X and Y by restricting the sums appropriately).

Thus, in order to make Theorem 1.6.1 work for infinite sums, it suffices to assume the middle sum $\sum_{(x,y)\in X\times Y} a_{(x,y)}$ to have only finitely many nonzero addends. However, it is tempting to think that even if this middle sum has infinitely many nonzero addends, we may still get the equality $\sum_{x\in X} \sum_{y\in Y} a_{(x,y)} = \sum_{y\in Y} \sum_{x\in X} a_{(x,y)}$ as long as all the four sums appearing in this equality have only finitely many nonzero addends. In other words, it is tempting to use the following "fact":

Incorrect Fubini rule. Let X and Y be two sets. Let $a_{(x,y)}$ be a number for each pair $(x,y) \in X \times Y$. Then,

$$\sum_{x\in X} \sum_{y\in Y} a_{(x,y)} = \sum_{y\in Y} \sum_{x\in X} a_{(x,y)}, \tag{129}$$

as long as all four sums appearing in this equality have only finitely many nonzero addends.

This, however, is false. Here is a counterexample:

Example 1.6.12 ("the serial debtor"). Let $X = \{1,2,3,\ldots\}$ and $Y = \{1,2,3,\ldots\}$. Define a number $a_{(x,y)}$ for each pair $(x,y) \in X \times Y$ by setting

$$a_{(x,y)} = [y = x] - [y = x+1].$$

Here is a table showing these numbers:

$a_{(x,y)}$	$y=1$	$y=2$	$y=3$	$y=4$	$y=5$	$\cdots$
$x=1$	1	-1				$\cdots$
$x=2$		1	-1			$\cdots$
$x=3$			1	-1		$\cdots$
$x=4$				1	-1	$\cdots$
$x=5$					1	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

, (130)

where empty slots are understood to contain the number 0. It is easy to see that all four sums in (129) have only finitely many nonzero addends. Indeed, for each $x \in X$, we have

$$\sum_{y \in Y} a_{(x,y)} = 0 \tag{131}$$

(since the only nonzero addends of this sum are 1 and -1, which clearly sum up to 0). Hence,

$$\sum_{x \in X} \underbrace{\sum_{y \in Y} a_{(x,y)}}_{=0} = \sum_{x \in X} 0 = 0. \tag{132}$$

On the other hand, for each $y \in Y$, we have

$$\sum_{x \in X} a_{(x,y)} = \begin{cases} 1, & \text{if } y = 1; \\ 0, & \text{if } y \neq 1 \end{cases}$$

(since the only nonzero addends of this sum are 1 and -1, except that there is no -1 when $y = 1$). Hence,

$$\sum_{y \in Y} \underbrace{\sum_{x \in X} a_{(x,y)}}_{= \begin{cases} 1, & \text{if } y = 1; \\ 0, & \text{if } y \neq 1 \end{cases}} = \sum_{y \in Y} \begin{cases} 1, & \text{if } y = 1; \\ 0, & \text{if } y \neq 1 \end{cases} = 1. \tag{133}$$

Comparing this with (132), we see that (129) becomes $0 = 1$, which is clearly false. Hence, the Incorrect Fubini rule is false. But Theorem 1.6.11 does not apply here, since infinitely many pairs $(x,y) \in X \times Y$ satisfy $a_{(x,y)} \neq 0$.

(Example 1.6.12 can be thought of as a mathematical model of check kiting, or more generally of paying back a debt by opening a new line of credit. In this metaphor, each row of the table (130) represents a line of credit, while each column represents a day, with the entry 1 standing for incurring debt and the entry -1 standing for paying it back. The equality (131) says that each single debt gets eventually paid back, but the equality (133) shows that the debtor has an extra ("undeserved") unit of money at his disposal. This paradox would not work if there were only finitely many lines of credit; one day the debtor would have to pay back his last debt.)

Note that we are only considering the simplest kind of infinite sums here: the ones that have only finitely many nonzero addends. In analysis, more general situations are studied in which an infinite sum can have a well-defined (finite) value. In those situations, there are much subtler criteria for when summation signs can be interchanged (such as absolute summability). But this is a combinatorics course, so we will not need them.

1.7. Counting permutations: an introduction

We now come back to take another look at counting maps. Namely, we restrict ourselves to a special class of maps: the *permutations*.

1.7.1. Permutations and derangements

There are two different things called "permutations" in mathematics. One is a kind of maps ("active permutations"); the other is a kind of lists ("passive permutations"). We are always going to use the word "permutation" for the former, at least when we are speaking of permutations of a set. Here is how it is defined:

Definition 1.7.1. A *permutation* of a set X means a bijection from X to X.

We shall use the two-line notation for maps (see Definition 1.2.11). Thus, for example,

$$\begin{pmatrix} 0 & 1 & 5 & 7 & 9 \\ 1 & 7 & 5 & 0 & 9 \end{pmatrix}$$

denotes the map from $\{0,1,5,7,9\}$ to $\{0,1,5,7,9\}$ that sends $0,1,5,7,9$ to $1,7,5,0,9$, respectively. This map is a permutation of the set $\{0,1,5,7,9\}$. On the other hand, the map

$$\begin{pmatrix} 0 & 1 & 5 & 7 & 9 \\ 1 & 7 & 0 & 0 & 9 \end{pmatrix}$$

is not a permutation, since it fails to be injective (indeed, it sends both 5 and 7 to 0) and therefore also fails to be bijective. Also, the map

$$\begin{pmatrix} 0 & 1 & 5 & 7 & 9 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

is not a permutation, since it is a map between two different sets (while a permutation must be a map from a set to itself).

The most obvious counting question you can now ask has a simple answer:

Theorem 1.7.2. Let $n \in \mathbb{N}$. Let X be an n-element set. Then,

$$(\#\text{ of permutations of } X) = n!.$$

We shall prove this theorem later (in Subsection 2.4.4). (The idea of the proof is simple, but formalizing it is tricky at this point.)

Example 1.7.3. The set $[3] = \{1,2,3\}$ has $3! = 6$ many permutations; they are (written in two-line notation)

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Let us next focus on a specific kind of permutations.

Definition 1.7.4. Let X be a set.

(a) If $f : X \to X$ is a map, then a *fixed point* of f means an element $x \in X$ such that $f(x) = x$.

(b) A *derangement* of X means a permutation of X that has no fixed points.

Example 1.7.5. (a) The fixed points of the map

$$\begin{pmatrix} 0 & 1 & 5 & 7 & 9 \\ 1 & 7 & 5 & 0 & 9 \end{pmatrix}$$

are 5 and 9. Thus, this map is not a derangement of $\{0,1,5,7,9\}$ (even though it is a permutation of $\{0,1,5,7,9\}$).

(b) The map

$$\begin{pmatrix} 0 & 1 & 5 & 7 & 9 \\ 1 & 7 & 9 & 0 & 5 \end{pmatrix}$$

has no fixed points, and thus is a derangement of $\{0,1,5,7,9\}$ (since it is a permutation of $\{0,1,5,7,9\}$).

We can restate Definition 1.7.4 as follows: A *derangement* of a set X means a permutation f of X such that

$$f(x) \neq x \qquad \text{for all } x \in X.$$

1.7.2. Only the size counts

How many derangements does an n-element set have?

A first simplification is to restrict our focus to a specific n-element set, namely $[n]$, because all n-element sets should be interchangeable as far as this question is concerned. This relies on the following lemma:

Lemma 1.7.6. Let $n \in \mathbb{N}$. Let X be any n-element set. Then,

$$(\#\text{ of derangements of } X) = (\#\text{ of derangements of } [n])\,.$$

This lemma might be so obvious to you that you would wonder what there is to be proven about it; shouldn't it be clear that the # of derangements of a set only depends on the size of that set? The following proof, which we shall first give in an informal version, just spells out this idea:

Proof of Lemma 1.7.6 (informal version). We have $|X| = n$ (since X is an n-element set) and $|[n]| = n$, so that $|X| = n = |[n]|$. Thus, the sets X and $[n]$ have the same size. Hence, Theorem 1.1.7 (applied to $Y = [n]$) shows that there is a bijection $\phi : X \to [n]$. Fix such a ϕ.

We can regard this bijection ϕ as a way to label the elements of X by the numbers $1, 2, \ldots, n$ (with each element $a \in X$ getting the label $\phi(a) \in [n]$). For example, if X is a 3-element set $\{x, y, z\}$, and $\phi : X \to [3]$ is the bijection[113] $\begin{pmatrix} x & y & z \\ 1 & 2 & 3 \end{pmatrix}$, then we can think of ϕ as labeling the elements x, y, z as $1, 2, 3$, respectively.

Now, we claim that any derangement of X can be transformed into a derangement of $[n]$. Indeed, if a derangement of X is written in two-line notation, then we can simply replace each $a \in X$ appearing in this two-line notation by its "label" $\phi(a) \in [n]$, and thus obtain a derangement of $[n]$ written in two-line notation. For example, if X is a 3-element set $\{x, y, z\}$, and ϕ is the bijection $\begin{pmatrix} x & y & z \\ 1 & 2 & 3 \end{pmatrix} : X \to [3]$, then the derangement

$$\begin{pmatrix} x & y & z \\ y & z & x \end{pmatrix} \qquad \text{of } X$$

becomes the derangement

$$\begin{pmatrix} \phi(x) & \phi(y) & \phi(z) \\ \phi(y) & \phi(z) & \phi(x) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \text{of } [3]\,.$$

This way, we have assigned a derangement of $[n]$ to each derangement of X. This assignment is "obviously"[114] a bijection from the set $\{\text{derangements of } X\}$ to the

[113] In this version of this proof, all maps will be written in two-line notation.

[114] See below for a rigorous point of view.

set $\{\text{derangements of } [n]\}$. The bijection principle thus yields that

$$|\{\text{derangements of } X\}| = |\{\text{derangements of } [n]\}|,$$

and this quickly yields Lemma 1.7.6. □

This proof was somewhat informal: We have not shown that our assignment is a well-defined map from $\{\text{derangements of } X\}$ to $\{\text{derangements of } [n]\}$ (and this is not obvious, because a map usually can be written in two-line notation in several ways); nor have we shown that it is a bijection. I shall thus rewrite this proof in a more rigorous and formal way below.

First of all, let me recall some basic notations regarding maps. Recall that if $g : A \to B$ and $f : B \to C$ are two maps (between some sets A, B and C), then the *composition* $f \circ g$ of these two maps is defined to be the map

$$\begin{aligned} A &\to C, \\ a &\mapsto f(g(a)). \end{aligned}$$

(I pronounce "$f \circ g$" as "f after g", because this composition $f \circ g$ acts on an element $a \in A$ by first applying g and afterwards applying f to the result.)

The composition of maps is associative: i.e., if f, g and h are three maps for which the compositions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ make sense[115], then these two compositions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ are equal, and thus both of them can be called $f \circ g \circ h$. (See [Grinbe15, Proposition 2.82] for a proof of this fact, and [Grinbe15, Theorem 2.86] for its analogue for more than three maps.)

It is easy to see that any composition of bijections is again a bijection. In particular, if f, g and h are three bijections for which the composition $f \circ g \circ h$ makes sense, then this composition $f \circ g \circ h$ is a bijection.

Now, the bijection from $\{\text{derangements of } X\}$ to $\{\text{derangements of } [n]\}$ that we have constructed in our above proof of Lemma 1.7.6 can be viewed in a new light: This bijection sends any derangement ω of X to the composition

$$\phi \circ \omega \circ \phi^{-1} : [n] \to [n]$$

(where $\phi^{-1} : [n] \to X$ is the inverse of the bijection $\phi : X \to [n]$). Indeed, if a derangement ω of X is given by

$$\omega = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \qquad \text{in two-line notation,}$$

then

$$\phi \circ \omega \circ \phi^{-1} = \begin{pmatrix} \phi(a_1) & \phi(a_2) & \cdots & \phi(a_n) \\ \phi(b_1) & \phi(b_2) & \cdots & \phi(b_n) \end{pmatrix} \qquad \text{in two-line notation}$$

[115] This means that the target of h is the domain of g, and that the target of g is the domain of f.

[116], which is precisely what we obtain when we replace each $a \in X$ appearing in the two-line notation of ω by its "label" $\phi(a) \in [n]$. Thus, we don't need to speak about two-line notations at all when defining our bijection; we can simply define it as the map that sends each derangement ω of X to the derangement $\phi \circ \omega \circ \phi^{-1}$ of $[n]$. Thus, our above proof of Lemma 1.7.6 takes the following rigorous shape:

Proof of Lemma 1.7.6 (formal version). We have $|X| = n$ (since X is an n-element set) and $|[n]| = n$, so that $|X| = n = |[n]|$. Thus, the sets X and $[n]$ have the same size. Hence, Theorem 1.1.7 (applied to $Y = [n]$) shows that there is a bijection $\phi : X \to [n]$. Fix such a ϕ.

Now, the map $\phi : X \to [n]$ is a bijection; thus, it has an inverse map $\phi^{-1} : [n] \to X$. Hence, for any map $\omega : X \to X$, we can form the composition

$$\phi \circ \omega \circ \phi^{-1} : [n] \to [n].$$

Moreover, if ω is a derangement of X, then $\phi \circ \omega \circ \phi^{-1}$ is a derangement of $[n]$ [117]. Hence, we can define a map

$$A : \{\text{derangements of } X\} \to \{\text{derangements of } [n]\},$$
$$\omega \mapsto \phi \circ \omega \circ \phi^{-1}.$$

A similar argument shows that we can define a map

$$B : \{\text{derangements of } [n]\} \to \{\text{derangements of } X\},$$
$$\eta \mapsto \phi^{-1} \circ \eta \circ \phi.$$

[116] because each $i \in [n]$ satisfies

$$\left(\phi \circ \omega \circ \phi^{-1}\right)(\phi(a_i)) = \phi\left(\omega\left(\underbrace{\phi^{-1}(\phi(a_i))}_{=a_i}\right)\right) = \phi(\omega(a_i)) = \phi(b_i)$$
$$\left(\text{since } \omega = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \text{ shows that } \omega(a_i) = b_i\right)$$

[117] *Proof.* Let ω be a derangement of X. Thus, ω is a permutation of X that has no fixed points (by the definition of a derangement). If the map $\phi \circ \omega \circ \phi^{-1}$ had a fixed point $y \in [n]$, then $\phi^{-1}(y) \in X$ would be a fixed point of ω (since it would satisfy

$$\phi\left(\omega\left(\phi^{-1}(y)\right)\right) = \left(\phi \circ \omega \circ \phi^{-1}\right)(y) = y \qquad \left(\text{since } y \text{ is a fixed point of } \phi \circ \omega \circ \phi^{-1}\right)$$

and therefore $\omega\left(\phi^{-1}(y)\right) = \phi^{-1}(y)$); but this would contradict the fact that ω has no fixed points. Hence, the map $\phi \circ \omega \circ \phi^{-1}$ has no fixed points either. Furthermore, the map ω is a permutation of X, that is, a bijection from X to X. Moreover, the maps ϕ and ϕ^{-1} are bijections. Hence, the composition $\phi \circ \omega \circ \phi^{-1} : [n] \to [n]$ is also a bijection (because it is a composition of the three bijections ϕ, ω and ϕ^{-1}). Thus, $\phi \circ \omega \circ \phi^{-1}$ is a bijection from $[n]$ to $[n]$. In other words, $\phi \circ \omega \circ \phi^{-1}$ is a permutation of $[n]$. Thus, $\phi \circ \omega \circ \phi^{-1}$ is a permutation of $[n]$ that has no fixed points (since we have previously shown that $\phi \circ \omega \circ \phi^{-1}$ has no fixed points). In other words, $\phi \circ \omega \circ \phi^{-1}$ is a derangement of $[n]$ (by the definition of a derangement). Qed.

It is easy to see that these two maps A and B are mutually inverse[118]. Hence, the map A is invertible, and thus a bijection. Therefore, the bijection principle yields

$$|\{\text{derangements of } X\}| = |\{\text{derangements of } [n]\}|.$$

In other words,

$$(\#\text{ of derangements of } X) = (\#\text{ of derangements of } [n]).$$

This proves Lemma 1.7.6. □

Lemma 1.7.6 is not specific to derangements; it is merely an instance of a far-ranging principle, which I will not state in its general form because that would require a detour into category theory. Roughly speaking, the principle says the following:

> **"Isomorphism principle" (informal):** Assume that we are given a way to assign a number $f(S)$ to any finite set S, and this way does not depend on what the elements of S are (i.e., it has a definition that works the same no matter whether the elements of S are numbers or tuples or maps or anything else). Let $n \in \mathbb{N}$. Let X be any n-element set. Then, $f(X) = f([n])$.

Of course, this is not rigorous until we formalize what "does not depend on what the elements of S are" means. This I am not going to do; but let me delineate it through a few examples:

We can apply the "isomorphism principle" to $f(S) = (\#\text{ of derangements of } S)$, because the # of derangements of S is defined in a way that does not depend on what the elements of S are. Thus, we obtain Lemma 1.7.6.

Likewise, we can apply the "isomorphism principle" to $f(S) = (\#\text{ of permutations of } S)$. Thus, we obtain the fact that if $n \in \mathbb{N}$, and if X is an n-element set, then

$$(\#\text{ of permutations of } X) = (\#\text{ of permutations of } [n]). \tag{134}$$

[118] *Proof.* We need to check that $A \circ B = \mathrm{id}$ and $B \circ A = \mathrm{id}$. We shall only prove that $A \circ B = \mathrm{id}$, and leave the analogous proof of $B \circ A = \mathrm{id}$ to the reader.

Let η be a derangement of $[n]$. Then, $B(\eta) = \phi^{-1} \circ \eta \circ \phi$ (by the definition of B). Applying the map A to both sides of this equality, we find

$$\begin{aligned} A(B(\eta)) &= A\left(\phi^{-1} \circ \eta \circ \phi\right) = \phi \circ \left(\phi^{-1} \circ \eta \circ \phi\right) \circ \phi^{-1} \qquad \text{(by the definition of } A\text{)} \\ &= \underbrace{\phi \circ \phi^{-1}}_{=\mathrm{id}} \circ \eta \circ \underbrace{\phi \circ \phi^{-1}}_{=\mathrm{id}} = \mathrm{id} \circ \eta \circ \mathrm{id} = \eta. \end{aligned}$$

Thus, $(A \circ B)(\eta) = A(B(\eta)) = \eta = \mathrm{id}(\eta)$.

Forget that we fixed η. We thus have proved that $(A \circ B)(\eta) = \mathrm{id}(\eta)$ for each derangement η of $[n]$. In other words, $A \circ B = \mathrm{id}$. As we said, the proof of $B \circ A = \mathrm{id}$ is analogous. Thus, it follows that the maps A and B are mutually inverse.

Likewise, we can apply the "isomorphism principle" to $f(S) = (\#\text{ of subsets of } S)$. Thus, we obtain the fact that if $n \in \mathbb{N}$, and if X is an n-element set, then

$$(\#\text{ of subsets of } X) = (\#\text{ of subsets of } [n]). \tag{135}$$

Likewise, we can apply the "isomorphism principle" to $f(S) = (\#\text{ of subsets of } S \text{ having even size})$. Thus, we obtain the fact that if $n \in \mathbb{N}$, and if X is an n-element set, then

$$(\#\text{ of subsets of } X \text{ having even size}) = (\#\text{ of subsets of } [n] \text{ having even size}).$$

The number $f(S)$ in the "isomorphism principle" doesn't have to be the # of some objects. We can just as well apply the "isomorphism principle" to $f(S) = \sum_{T \subseteq S} |T|$ (that is, the sum of the sizes of all subsets of S). Thus, we obtain the fact that if $n \in \mathbb{N}$, and if X is an n-element set, then

$$\sum_{T \subseteq X} |T| = \sum_{T \subseteq [n]} |T|.$$

What we **cannot** do is apply the "isomorphism principle" to $f(S) = (\#\text{ of lacunar subsets of } S)$. Indeed, the word "lacunar" is only defined for sets of integers, and whether a subset of S is lacunar depends on what its elements are. And unsurprisingly, it is **not** true that if $n \in \mathbb{N}$, and if X is an n-element set of integers, then

$$(\#\text{ of lacunar subsets of } X) = (\#\text{ of lacunar subsets of } [n]).$$

For example, if $n = 3$ and $X = \{1,3,5\}$, then all 8 subsets of X are lacunar, but only 5 subsets of $[n] = [3]$ are lacunar.

Likewise, we **cannot** apply the "isomorphism principle" to $f(S) = (\#\text{ of self-counting subsets of } S)$. Indeed, for example, if we relabel the elements 1 and 2 of the set $[2]$ as 8 and 9, then the self-counting subset $[1]$ will no longer be self-counting.

Since I am not proving the "isomorphism principle" in its general form, let me say a few words on how to prove its specific instances. Essentially, every instance of the "isomorphism principle" can be proven by the same strategy that we used in our proof of Lemma 1.7.6: Namely, we fix a bijection $\phi : X \to [n]$, and we use it to construct a bijection from $\{\text{the objects counted by } f(X)\}$ to $\{\text{the objects counted by } f([n])\}$, which proceeds by replacing each element $a \in X$ by its "label" $\phi(a) \in [n]$. When formalized, these proofs may look rather different, but the underlying idea is always this one. In particular, the formal proof of (134) resembles our formal proof of Lemma 1.7.6 very closely (but is shorter, because we don't have to show that $\phi \circ \omega \circ \phi^{-1}$ and $\phi^{-1} \circ \eta \circ \phi$ are derangements), whereas the formal proof of (135) requires a different formula for the maps A and B [119] (but

[119] namely,

$$A : \{\text{subsets of } X\} \to \{\text{subsets of } [n]\},$$
$$U \mapsto \phi(U) = \{\phi(u) \mid u \in U\}$$

otherwise, again, proceeds in the same way). I hope it is clear enough how these formal proofs can be constructed more or less mechanically whenever the need arises.

1.7.3. Intermezzo: OEIS

Lemma 1.7.6 shows that, in order to count the derangements of any finite set X, it suffices to count the derangements of $[n]$ for any $n \in \mathbb{N}$. Let us do this now.

Definition 1.7.7. For each $n \in \mathbb{N}$, let

$$D_n = (\#\text{ of derangements of } [n]).$$

Example 1.7.8. Let us compute D_3. Indeed, we know from Example 1.7.3 that the set $[3]$ has 6 permutations (which are all listed in Example 1.7.3). Among these 6 permutations, only 2 are derangements, namely

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

(written in two-line notation). Thus, the # of derangements of $[3]$ is 2. In other words, $D_3 = 2$.

In a similar manner, we can count the derangements of any other given finite set. In particular, we thus obtain

$D_0 = 1$ (since $\mathrm{id} : \varnothing \to \varnothing$ is a derangement);
$D_1 = 0$ (since $\mathrm{id} : [1] \to [1]$ is **not** a derangement);
$D_2 = 1$ $\left(\text{since the only derangement of } [2] \text{ is } \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right)$;
$D_3 = 2$ (as we have just seen);
$D_4 = 9$.

These days, when you have a sequence of integers you want to learn more about, and you know a few of its values, you can look it up at the OEIS (the Online Encyclopedia of Integer Sequences, available at `https://oeis.org`). Let us try this on the sequence $(D_0, D_1, D_2, D_3, \ldots)$. We know its first five values $D_0 = 1$, $D_1 = 0$, $D_2 = 1$, $D_3 = 2$, $D_4 = 9$, so let us enter "`1,0,1,2,9`" into the input field

---

and

$$B : \{\text{subsets of } [n]\} \to \{\text{subsets of } X\},$$
$$V \mapsto \phi^{-1}(V) = \left\{\phi^{-1}(v) \mid v \in V\right\}$$

of the OEIS. We press "Search" and are greeted with a list of several[120] known sequences that contain these five values somewhere in them (in five consecutive positions). The first hit is a sequence labeled A000166, and named "Subfactorial or rencontres numbers, or derangements: number of permutations of n elements with no fixed points". This is, of course, precisely our sequence (no wonder that such a simple concept as derangements is well-known). The OEIS has collected a lot of information on this sequence, including a long list of entries, combinatorial interpretations, formulas (including many we don't yet understand), references and links. Here is only a small selection of the formulas that are claimed in the OEIS for this sequence:

Theorem 1.7.9. **(a)** We have $D_n = (n-1)\left(D_{n-1} + D_{n-2}\right)$ for all $n \geq 2$.
(b) We have $D_n = nD_{n-1} + (-1)^n$ for all integers $n \geq 1$.
(c) We have

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k} \qquad \text{for all } n \in \mathbb{N}.$$

(d) We have

$$D_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \qquad \text{for all } n \in \mathbb{N}.$$

(e) Set $\operatorname{round}(x) = \left\lfloor x + \frac{1}{2} \right\rfloor$ for each $x \in \mathbb{R}$. Then,

$$D_n = \operatorname{round}\left(\frac{n!}{e}\right) \qquad \text{for all } n \geq 1,$$

where $e = \sum_{k=0}^{\infty} \frac{1}{k!} \approx 2.718\ldots$ is the base of the natural logarithm.

Some of these formulas will be proven in Subsection 2.9.5. (Theorem 1.7.9 **(b)** follows from Theorem 1.7.9 **(a)** via [19f-hw1s, Exercise 5].) Note that parts **(a)** and **(b)** of Theorem 1.7.9 are two recurrences for the sequence $(D_0, D_1, D_2, \ldots)$ that make its computation rather easy; both are due to Euler.

The OEIS can be used in many ways. It knows thousands of sequences that have appeared in mathematics (not only combinatorics). You can search for them both by entries (as we did above) and by keywords (such as "permutations" or "derangements"). It even acts as a bare-bones social network: If two mathematicians encounter the same sequence in their work, and the first one records it in the OEIS, the second can then find it and contact the first. This has led to a number of collaborations between mathematicians working in rather different disciplines; often, the appearance of the same integer sequence in different places hints at a deeper connection between the theories.

It is known from basic set theory that there exists a bijection between $\mathbb{N}$ and $\mathbb{N}^2$. Thus, a "2-dimensional sequence" (i.e., a family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ of numbers whose entries are indexed

[120] currently 45, but quite possibly more by the time you are reading this

by two rather than one nonnegative integers) can be re-parametrized as a (regular, i.e., 1-dimensional) sequence. Thus, such "2-dimensional sequences" and similar families of numbers can also be found in the OEIS. For example, Pascal's triangle (i.e., the family $\left(\binom{n}{k}\right)_{(n,k)\in\mathbb{N}^2;\ k\leq n}$) appears as sequence A007318.

1.7.4. The one-line notation

If σ is a permutation of the set $[n]$ (for some $n \in \mathbb{N}$), then we can write σ in two-line notation as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

But you'll quickly tire of this notation, since its whole top row is useless: It just contains the numbers $1, 2, \ldots, n$ in increasing order. Thus, we can omit this top row and only write the bottom row down[121]. The bottom row is usually written as an n-tuple (so the elements $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are separated by commas). This is the so-called *one-line notation* of σ:

Definition 1.7.10. Let $n \in \mathbb{N}$. Let σ be a permutation of $[n]$. Then, the *one-line notation* of σ is defined to be the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$.

Warning: This notation clashes with a different notation (the *cycle notation*), which is used in many textbooks. We shall avoid this conflict by using a different notation for cycles, but you should keep this in mind when consulting other texts. Other authors often avoid this conflict by using square brackets instead of parentheses in the one-line notation[122]; but we prefer not to do so, since we are already using square brackets for myriad other things.

Example 1.7.11. The 6 permutations of the set $[3]$ have been listed in Example 1.7.3. In one-line notation, they look as follows:

$$(1,2,3), \quad (1,3,2), \quad (2,1,3), \quad (2,3,1), \quad (3,1,2), \quad (3,2,1).$$

Let us observe that the one-line notation (as defined in Definition 1.7.10) can be used not only for permutations of $[n]$, but for any maps from $[n]$ to an arbitrary set X.

Perhaps the most useful thing about one-line notations is that they turn permutations (a somewhat abstract object) into n-tuples of numbers (a much more tangible object). Usually, it is easier to manipulate tuples (e.g., by inserting or removing elements) than to manipulate permutations. Using the one-line notation, we can substitute the former for the latter. This relies on the following simple fact:

[121] Of course, we can only do this if we agree that the top row is $1, 2, \ldots, n$ rather than some other ordering of the elements of $[n]$.

[122] i.e., they write the one-line notation of σ as $[\sigma(1), \sigma(2), \ldots, \sigma(n)]$

Proposition 1.7.12. Let $n \in \mathbb{N}$. Then:

(a) If σ is any permutation of $[n]$, then the one-line notation of σ is an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$.

(b) If $(i_1, i_2, \ldots, i_n)$ is an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$, then there exists a unique permutation σ of $[n]$ such that the one-line notation of σ is $(i_1, i_2, \ldots, i_n)$.

(c) Let

$$T_n = \{n\text{-tuples of distinct elements of } [n] \text{ that contain all elements of } [n]\}.$$

The map

$$\{\text{permutations of } [n]\} \to T_n,$$
$$\sigma \mapsto (\text{one-line notation of } \sigma) = (\sigma(1), \sigma(2), \ldots, \sigma(n))$$

is well-defined and is a bijection.

Proof of Proposition 1.7.12. This is a simple exercise in understanding what bijectivity means:

(a) Let σ be a permutation of $[n]$. Thus, σ is a bijection from $[n]$ to $[n]$ (by the definition of a permutation). Hence, the map σ is bijective, i.e., both injective and surjective.

The one-line notation of σ is defined to be the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. This n-tuple consists of n distinct entries[123], all of which are elements of $[n]$. Furthermore, this n-tuple contains all elements of $[n]$ [124]. Hence, the one-line notation of σ is an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$. This proves Proposition 1.7.12 **(a)**.

(b) Let $(i_1, i_2, \ldots, i_n)$ be an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$. Then, $i_1, i_2, \ldots, i_n$ are elements of $[n]$. Hence, we can define a map

$$f : [n] \to [n],$$
$$j \mapsto i_j.$$

This map f is injective[125] and surjective[126]. Hence, f is bijective. In other words, f is a bijection from $[n]$ to $[n]$. In other words, f is a permutation of $[n]$ (by the definition of a

[123] *Proof.* If i and j are two distinct elements of $[n]$, then $i \neq j$ and thus $\sigma(i) \neq \sigma(j)$ (since σ is injective). In other words, the n entries of the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ are distinct. Qed.

[124] *Proof.* Let $x \in [n]$. We must prove that this n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ contains x. In other words, we must prove that there exists a $y \in [n]$ such that $\sigma(y) = x$. But this follows from the fact that σ is surjective. Qed.

[125] *Proof.* The elements of the n-tuple $(i_1, i_2, \ldots, i_n)$ are distinct (by the definition of this n-tuple). Now, let a and b be two distinct elements of $[n]$. Thus, $a \neq b$, so that $i_a \neq i_b$ (since the elements of the n-tuple $(i_1, i_2, \ldots, i_n)$ are distinct). The definition of f yields $f(a) = i_a$ and $f(b) = i_b$. Hence, $f(a) = i_a \neq i_b = f(b)$.

Forget that we fixed a and b. We thus have shown that if a and b are two distinct elements of $[n]$, then $f(a) \neq f(b)$. In other words, the map f is injective.

[126] *Proof.* Let $x \in [n]$. The n-tuple $(i_1, i_2, \ldots, i_n)$ contains all elements of $[n]$. Thus, in particular, it contains x. In other words, there exists some $j \in [n]$ such that $i_j = x$. Consider this j. The definition of f now yields $f(j) = i_j = x$, so that $x = f(j)$. In other words, x is an image under f.

Forget that we fixed x. We thus have shown that each $x \in [n]$ is an image under f. In other words, the map f is surjective.

permutation). Moreover, the one-line notation of f is

$$\begin{aligned}&(f(1), f(2), \ldots, f(n)) \qquad \text{(by the definition of the one-line notation)}\\ &= (i_1, i_2, \ldots, i_n) \qquad \big(\text{since } f(j) = i_j \text{ for each } j \in [n] \text{ (by the definition of } f)\big).\end{aligned}$$

Hence, there is **at least one** permutation σ of $[n]$ such that the one-line notation of σ is $(i_1, i_2, \ldots, i_n)$ (namely, $\sigma = f$). Moreover, it is easy to see that there is **at most one** such permutation[127]. Combining these two observations, we conclude that there is a **unique** permutation σ of $[n]$ such that the one-line notation of σ is $(i_1, i_2, \ldots, i_n)$. This proves Proposition 1.7.12 **(b)**.

(c) If σ is a permutation of $[n]$, then the one-line notation of σ is an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$ (by Proposition 1.7.12 **(a)**). In other words, if σ is a permutation of $[n]$, then the one-line notation of σ belongs to T_n (because of how T_n was defined). Thus, the map

$$\begin{aligned}&\{\text{permutations of } [n]\} \to T_n,\\ &\qquad \sigma \mapsto (\text{one-line notation of } \sigma) = (\sigma(1), \sigma(2), \ldots, \sigma(n))\end{aligned}$$

is well-defined. It remains to prove that this map is a bijection.

Let us denote this map by OLN (which is short for "one-line notation"). We thus must prove that OLN is a bijection.

The map OLN is injective[128] and surjective[129]. Hence, OLN is bijective. In other words, OLN is a bijection. This completes the proof of Proposition 1.7.12 **(c)**. □

[127] *Proof.* Let α be any such permutation. We shall prove that $\alpha = f$.

Indeed, α is a permutation σ of $[n]$ such that the one-line notation of σ is $(i_1, i_2, \ldots, i_n)$. In other words, α is a permutation of $[n]$, and its one-line notation is $(i_1, i_2, \ldots, i_n)$. Hence,

$$(i_1, i_2, \ldots, i_n) = (\text{the one-line notation of } \alpha) = (\alpha(1), \alpha(2), \ldots, \alpha(n)),$$

so that

$$(\alpha(1), \alpha(2), \ldots, \alpha(n)) = (i_1, i_2, \ldots, i_n) = (f(1), f(2), \ldots, f(n))$$

(since $(f(1), f(2), \ldots, f(n)) = (i_1, i_2, \ldots, i_n)$). In other words, $\alpha(x) = f(x)$ for each $x \in [n]$. Since both α and f are maps from $[n]$ to $[n]$ (being permutations of $[n]$), we thus conclude that $\alpha = f$.

Now, forget that we fixed α. We thus have shown that if α is any permutation σ of $[n]$ such that the one-line notation of σ is $(i_1, i_2, \ldots, i_n)$, then $\alpha = f$. Hence, there is **at most one** permutation σ of $[n]$ such that the one-line notation of σ is $(i_1, i_2, \ldots, i_n)$.

[128] *Proof.* Let σ and τ be two permutations of $[n]$ such that $\mathrm{OLN}(\sigma) = \mathrm{OLN}(\tau)$. Thus, the definition of OLN yields $\mathrm{OLN}(\sigma) = (\text{one-line notation of } \sigma) = (\sigma(1), \sigma(2), \ldots, \sigma(n))$ and similarly $\mathrm{OLN}(\tau) = (\tau(1), \tau(2), \ldots, \tau(n))$. Hence,

$$(\sigma(1), \sigma(2), \ldots, \sigma(n)) = \mathrm{OLN}(\sigma) = \mathrm{OLN}(\tau) = (\tau(1), \tau(2), \ldots, \tau(n)).$$

In other words, $\sigma(x) = \tau(x)$ for each $x \in [n]$. Hence, $\sigma = \tau$ (since both σ and τ are maps from $[n]$ to $[n]$).

Forget that we fixed σ and τ. We thus have shown that if σ and τ are two permutations of $[n]$ such that $\mathrm{OLN}(\sigma) = \mathrm{OLN}(\tau)$, then $\sigma = \tau$. In other words, the map OLN is injective.

[129] *Proof.* Let $\mathbf{x} \in T_n$. Thus, $\mathbf{x} \in T_n = \{n\text{-tuples of distinct elements of } [n] \text{ that contain all elements of } [n]\}$; in other words, $\mathbf{x}$ is an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$. Hence, we can write $\mathbf{x}$ in the form $\mathbf{x} = (i_1, i_2, \ldots, i_n)$. Thus, $(i_1, i_2, \ldots, i_n) = \mathbf{x}$ is an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$. Therefore, Proposition 1.7.12 **(b)** shows that

Class of 2019-10-16

1.7.5. Short-legged permutations

Derangements are just one special type of permutations. Many others can be defined. For example, let me define what I call the *short-legged permutations*:

Definition 1.7.13. Let $n \in \mathbb{N}$. A permutation σ of $[n]$ is said to be *short-legged* if each $i \in [n]$ satisfies $|\sigma(i) - i| \leq 1$.

The word "short-legged" is my own creation (and refers to the idea that a short-legged permutation of $[n]$ "carries no $i \in [n]$ any further than 1 step", a way of visualizing the inequality $|\sigma(i) - i| \leq 1$). But this type of permutations has a long history, and appears naturally in the study of determinants (specifically, of determinants of tridiagonal matrices – see, e.g., [Grinbe15, Second solution to Exercise 6.27]).

Example 1.7.14. **(a)** Among the 6 permutations of $[3]$, exactly 3 are short-legged, namely

$$(1,2,3), \qquad (1,3,2), \qquad (2,1,3)$$

(in one-line notation). Indeed, for example, the permutation $\sigma = (1,3,2)$ is short-legged (since it has $|\sigma(1) - 1| = |1-1| = 0 \leq 1$ and $|\sigma(2) - 2| = |3-2| = 1 \leq 1$ and $|\sigma(3) - 3| = |2-3| = 1 \leq 1$), whereas the permutation $\sigma = (2,3,1)$ is not short-legged (since it has $|\sigma(3) - 3| = |1-3| = 2 > 1$).

(b) Among the 24 permutations of $[4]$, exactly 5 are short-legged, namely

$$(1,2,3,4), \qquad (1,2,4,3), \qquad (1,3,2,4), \qquad (2,1,3,4), \qquad (2,1,4,3).$$

We can now wonder: How many permutations of $[n]$ are short-legged?

Proposition 1.7.15. Let $n \in \mathbb{N}$. Then,

$$(\#\text{ of short-legged permutations of } [n]) = f_{n+1}.$$

(Here, $(f_0, f_1, f_2, \ldots)$ again denotes the Fibonacci sequence, as defined in Definition 1.1.10.)

there exists a unique permutation σ of $[n]$ such that the one-line notation of σ is $(i_1, i_2, \ldots, i_n)$. Consider this σ. The definition of OLN yields

$$\begin{aligned} \operatorname{OLN}(\sigma) &= (\text{one-line notation of } \sigma) \\ &= (i_1, i_2, \ldots, i_n) \qquad (\text{since the one-line notation of } \sigma \text{ is } (i_1, i_2, \ldots, i_n)) \\ &= \mathbf{x}. \end{aligned}$$

Hence, $\mathbf{x}$ is an image under the map OLN.

Now, forget that we fixed $\mathbf{x}$. We thus have shown that every $\mathbf{x} \in T_n$ is an image under the map OLN. In other words, the map OLN is surjective.

That makes yet another question answered by the Fibonacci numbers! I will not prove this proposition in full detail, but let me sketch the main ideas of two proofs:

First proof of Proposition 1.7.15 (sketched). Let w_n denote the # of short-legged permutations of $[n]$. Then, it suffices to show that $w_n = w_{n-1} + w_{n-2}$ for each $n \geq 2$ (because we can then argue as in the proof of Proposition 1.1.11).

So let $n \geq 2$. How do we prove $w_n = w_{n-1} + w_{n-2}$?

If σ is any short-legged permutation of $[n]$, then $|\sigma(n) - n| \leq 1$ (by the definition of "short-legged"), so that $\sigma(n) \in \{n-1, n, n+1\}$ and therefore either $\sigma(n) = n-1$ or $\sigma(n) = n$ (since $\sigma(n)$ has to belong to $[n]$). We shall call σ **red** if $\sigma(n) = n$, and **green** if $\sigma(n) = n-1$. Thus, each short-legged permutation of $[n]$ is either red or green (but never both at the same time).

Our goal will be to show that

$$(\text{\# of red short-legged permutations of } [n]) = w_{n-1}$$

and

$$(\text{\# of green short-legged permutations of } [n]) = w_{n-2}.$$

Proposition 1.7.12 **(c)** allows us to identify each permutation σ of $[n]$ with its one-line notation $(\sigma(1), \sigma(2), \ldots, \sigma(n))$, which is an n-tuple of distinct elements of $[n]$. Let us do so.[130] Thus:

- A permutation of $[n]$ is the same as an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$.
- A short-legged permutation of $[n]$ is the same as an n-tuple of distinct elements of $[n]$ that contains all elements of $[n]$ and whose i-th entry is either $i-1$ or i or $i+1$ for each $i \in [n]$.
- A red short-legged permutation of $[n]$ is the same as a short-legged permutation whose last entry is n.
- A green short-legged permutation of $[n]$ is the same as a short-legged permutation whose last entry is $n-1$.

We similarly identify permutations of $[n-1]$ with certain $(n-1)$-tuples, and permutations of $[n-2]$ with certain $(n-2)$-tuples. However, the words "red" and "green" will be used for permutations of $[n]$ only (so "green short-legged permutation" will mean "green short-legged permutation of $[n]$", and likewise for red).

So we know that a red short-legged permutation of $[n]$ is the same as a short-legged permutation of $[n]$ whose last entry is n. If we remove said last entry, then

[130] Actually, if you **define** an n-tuple of elements of a set X to be a map from $[n]$ to X, then there is nothing to identify here: In this case, a permutation of $[n]$ is already identical to its one-line notation. But I don't want to make assumptions about your definition of tuples.

we obtain an $(n-1)$-tuple of elements of $[n-1]$, which is easily seen to be a short-legged permutation of $[n-1]$. In other words, if $\sigma = (\sigma(1), \sigma(2), \ldots, \sigma(n))$ is a red short-legged permutation of $[n]$, then $(\sigma(1), \sigma(2), \ldots, \sigma(n-1))$ is a short-legged permutation of $[n-1]$. Thus, the map

$$\{\text{red short-legged permutations}\} \to \{\text{short-legged permutations of } [n-1]\}, \\ \sigma \mapsto (\sigma(1), \sigma(2), \ldots, \sigma(n-1))$$

is well-defined. It is easy to see that this map is a bijection[131]. Thus, the bijection principle yields

$$\begin{aligned} &(\#\text{ of red short-legged permutations}) \\ &= (\#\text{ of short-legged permutations of } [n-1]) \\ &= w_{n-1} \end{aligned}$$

(since w_{n-1} was defined as the # of short-legged permutations of $[n-1]$).

Next, we analyze the green short-legged permutations of $[n]$. Each green short-legged permutation σ is an n-tuple whose last entry is $n-1$. This entails that its second-to-last entry must be n. Indeed, σ must contain n somewhere (since it is a permutation of $[n]$), but the only positions in which a short-legged permutation can contain n are its $(n-1)$-st and n-th entries (because any other position of n would violate the "short-legged" condition), and the n-th entry is already taken by $n-1$. Thus, each green short-legged permutation σ is an n-tuple that ends with the two entries n and $n-1$ (in this order). If we remove these two entries, then we obtain an $(n-2)$-tuple of elements of $[n-2]$, which is easily seen to be a short-legged permutation of $[n-2]$. In other words, if $\sigma = (\sigma(1), \sigma(2), \ldots, \sigma(n))$ is a green short-legged permutation of $[n]$, then $(\sigma(1), \sigma(2), \ldots, \sigma(n-2))$ is a short-legged permutation of $[n-2]$. Thus, the map

$$\{\text{green short-legged permutations}\} \to \{\text{short-legged permutations of } [n-2]\}, \\ \sigma \mapsto (\sigma(1), \sigma(2), \ldots, \sigma(n-2))$$

is well-defined. It is easy to see that this map is a bijection[132]. Thus, the bijection principle yields

$$\begin{aligned} &(\#\text{ of green short-legged permutations}) \\ &= (\#\text{ of short-legged permutations of } [n-2]) \\ &= w_{n-2} \end{aligned}$$

(since w_{n-2} was defined as the # of short-legged permutations of $[n-2]$).

[131] Indeed, its inverse simply appends an n to the end of a short-legged permutation of $[n-1]$ (where the latter is regarded as an $(n-1)$-tuple).

[132] Indeed, its inverse simply appends an n and then an $n-1$ to the end of a short-legged permutation of $[n-2]$ (where the latter is regarded as an $(n-2)$-tuple).

Now, recall that each short-legged permutation of $[n]$ is either red or green (but never both at the same time). Hence, the sum rule shows that

$$\begin{aligned}
&(\#\text{ of short-legged permutations of } [n]) \\
&= \underbrace{(\#\text{ of red short-legged permutations})}_{=w_{n-1}} + \underbrace{(\#\text{ of green short-legged permutations})}_{=w_{n-2}} \\
&= w_{n-1} + w_{n-2}.
\end{aligned}$$

Thus, the definition of w_n yields

$$w_n = (\#\text{ of short-legged permutations of } [n]) = w_{n-1} + w_{n-2}.$$

As we already know, this quickly completes the proof of Proposition 1.7.15. □

Second proof of Proposition 1.7.15 (sketched). Here is the outline of a different proof.

Recall Definition 1.4.2. I claim that the map

$$\begin{aligned}
F : \{\text{short-legged permutations of } [n]\} &\to \{\text{lacunar subsets of } [n-1]\}, \\
\sigma &\mapsto \{i \in [n-1] \mid \sigma(i) = i+1\}
\end{aligned}$$

is well-defined and is a bijection. Once we have proven this, the bijection principle will yield

$$\begin{aligned}
&(\#\text{ of short-legged permutations of } [n]) \\
&= (\#\text{ of lacunar subsets of } [n-1]) \\
&= f_{(n-1)+2} \qquad (\text{by Proposition 1.4.9, applied to } n-1 \text{ instead of } n) \\
&= f_{n+1},
\end{aligned}$$

and thus Proposition 1.7.15 will be proven.

Why is the map F well-defined and a bijection? In order to prove that F is well-defined, we only need to check the following statement:

Statement 1: If σ is a short-legged permutation of $[n]$, then $\{i \in [n-1] \mid \sigma(i) = i+1\}$ is a lacunar subset of $[n-1]$.

I leave this to you, dear reader, with the following hint: If σ is a short-legged permutation, and some $a \in [n-2]$ satisfies $\sigma(a) = a+1$ and $\sigma(a+1) = a+2$, then prove that $\sigma(a+2) = a+3$ (because the values $a+1$ and $a+2$ are already taken) and $\sigma(a+3) = a+4$ (because the values $a+2$ and $a+3$ are already taken) and $\sigma(a+4) = a+5$ (likewise) and so on... but this eventually leads to $\sigma(n) = n+1$, which is absurd.

Statement 1 shows that F is well-defined. In order to show that F is bijective, we need to prove the following two facts:

Statement 2: If σ and τ are two short-legged permutations of $[n]$ satisfying $F(\sigma) = F(\tau)$, then $\sigma = \tau$.

Statement 3: If J is a lacunar subset of $[n-1]$, then there exists a short-legged permutation σ of $[n]$ satisfying $F(\sigma) = J$.

To prove Statement 2, you need to find a way to reconstruct a short-legged permutation σ from the lacunar subset $F(\sigma)$. Here is such a way: The permutation σ will send each $j \in [n]$ to $\begin{cases} j+1, & \text{if } j \in F(\sigma); \\ j-1, & \text{if } j-1 \in F(\sigma); \\ j, & \text{otherwise} \end{cases}$. Of course, this needs to be proven – again, LTTR. Same applies for Statement 3.

Alternatively, this proof can be restated in terms of domino tilings of $R_{n,2}$. Indeed, we already know from the Second proof of Proposition 1.4.9 that there is a bijection

$$h : \{\text{domino tilings of } R_{n+1,2}\} \to \{\text{lacunar subsets of } [n]\}.$$

Applying this to $n-1$ instead of n, we obtain a bijection

$$h' : \{\text{domino tilings of } R_{n,2}\} \to \{\text{lacunar subsets of } [n-1]\}.$$

Composing the inverse of this bijection h' with the bijection F above, we obtain a bijection

$$\{\text{short-legged permutations of } [n]\} \to \{\text{domino tilings of } R_{n,2}\}.$$

We leave it to the reader to describe this bijection more directly and prove its bijectivity without the detour through lacunar subsets. □

1.7.6. Long-legged permutations

If short-legged permutations were so easy to count, what about the "opposite" notion?

Definition 1.7.16. Let $n \in \mathbb{N}$. A permutation σ of $[n]$ is said to be *long-legged* if each $i \in [n]$ satisfies $|\sigma(i) - i| > 1$.

How many long-legged permutations does $[n]$ have?

As in Subsection 1.4.3, we can compute these #s using SageMath for small n. As in Subsection 1.7.3, we can then enter the results into the OEIS and hope that the sequence will be recognized. Here is the SageMath code:[133]

```
def is_longlegged(s):
  # Check whether a permutation ‘s‘ is long-legged.
  n = len(s)
  # This finds the ‘n‘ such that
  # ‘s‘ is a permutation of ‘[n]‘.
  return all( abs(s(i) - i) > 1 for i in range(1, n+1) )
```

[133] This computes the #s for $n \in \{0, 1, \ldots, 9\}$. You can try to go further, but keep in mind that the # of permutations of $[n]$ is $n!$, which grows a lot faster than 2^n (the # of subsets of $[n]$).

```
def num_of_longlegged(n):
  # Return the number of long-legged permutations
  # of `[n]`.
  return sum(1 for s in Permutations(n) if is_longlegged(s))

for n in range(10):
  print("The number of long-legged permutations of [" + str(n) + "] is
                                    " + str(num_of_longlegged(n)))
```

Its output is:

```
The number of long-legged permutations of [0] is 1
The number of long-legged permutations of [1] is 0
The number of long-legged permutations of [2] is 0
The number of long-legged permutations of [3] is 0
The number of long-legged permutations of [4] is 1
The number of long-legged permutations of [5] is 4
The number of long-legged permutations of [6] is 29
The number of long-legged permutations of [7] is 206
The number of long-legged permutations of [8] is 1708
The number of long-legged permutations of [9] is 15702
```

So we enter these values $1, 0, 0, 0, 1, 4, 29, 206, 1708, 15702$ into OEIS and instantly obtain the result: OEIS sequence A001883, described as "Number of permutations s of {1,2,...,n} such that |s(i)-i|>1 for each i=1,2,...,n", which clears any doubts as to whether it is the right sequence.

In the "Formula" section of the OEIS page, we spot the following recursion:

```
a(n) = n*a(n-1) + 4*a(n-2) - 3*(n-3)*a(n-3) + (n-4)*a(n-4)
 + 2*(n-5)*a(n-5) - (n-7)*a(n-6) - a(n-7).
```

In other words:

Proposition 1.7.17. For each $n \in \mathbb{N}$, let

$$a_n = (\#\text{ of long-legged permutations of } [n]).$$

Then, for each integer $n \geq 7$, we have

$$a_n = na_{n-1} + 4a_{n-2} - 3(n-3)a_{n-3} + (n-4)a_{n-4} + 2(n-5)a_{n-5} - (n-7)a_{n-6} - a_{n-7}.$$

This recurrence is credited to Vaclav Kotesovec (2017), and probably has been proved by reducing it to another recurrence (by J. Riordan, in an unpublished Bell Labs memorandum from 1963), which involves the Lucas sequence (a variant of the Fibonacci sequence: same recursion, but different starting values). The latter recurrence has been proved (in said memorandum, which can be downloaded from the OEIS page) using *generating functions* and an enumerative technique known as

rook theory (see [BCHR11] for an introduction). The argument would be both too advanced and too intricate to present at this point.

There is probably no hope of finding a "closed-form" expression for the a_n in Proposition 1.7.17. Not every counting problem has a closed-form solution; even a recurrent formula such as Proposition 1.7.17 is sometimes too much to ask for![134]

Thus ends our introductory tour of enumerative combinatorics. We shall next focus on one of the most basic topics: the binomial coefficients.

2. Binomial coefficients

We have already started exploring the binomial coefficients in Section 1.3. In this chapter, we shall explore them further, with a focus on proving identities involving them. We will build up a toolbox of techniques for this, some combinatorial and some algebraic.

2.1. The alternating sum of a row of Pascal's triangle

Recall Proposition 1.3.28, which says that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n = 0] \qquad \text{for each } n \in \mathbb{N}.$$

We have previously proved this proposition using the binomial formula. Let us now give two more proofs for it, as they involve techniques worth seeing.

2.1.1. Telescoping sums

For the second proof, we will use the *telescope principle* – or, more precisely, the *telescoping sum principle* (as there is an analogous version for products):

Theorem 2.1.1 (Telescoping sum principle)**.** Let u and v be two integers with $u \leq v+1$. Let $a_u, a_{u+1}, \ldots, a_{v+1}$ be any numbers. Then,

$$\sum_{j=u}^{v} \left(a_{j+1} - a_j\right) = a_{v+1} - a_u.$$

[134] A famous counting problem that has neither a known closed-form solution nor a known recurrence is counting Latin squares. The corresponding number sequence is A002860 in the OEIS.

First proof of Theorem 2.1.1 (informal version). If $u = v+1$, then

$$\sum_{j=u}^{v} \left(a_{j+1} - a_j\right) = \sum_{j=v+1}^{v} \left(a_{j+1} - a_j\right) = (\text{empty sum}) = 0$$
$$= \underbrace{a_u}_{\substack{=a_{v+1} \\ (\text{since } u=v+1)}} - a_u = a_{v+1} - a_u.$$

Hence, Theorem 2.1.1 is proved in the case when $u = v+1$. Thus, for the rest of this proof, we WLOG assume that $u \neq v+1$. Hence, $u < v+1$ (since $u \leq v+1$), so that $u+1 \leq v+1$ (since u and $v+1$ are integers). In other words, $u \leq v$.

Now, here is an informal version of how the proof proceeds from here: We have

$$\sum_{j=u}^{v} \underbrace{\left(a_{j+1} - a_j\right)}_{=-a_j+a_{j+1}}$$
$$= \sum_{j=u}^{v} \left(-a_j + a_{j+1}\right)$$
$$= \left(-a_u + a_{u+1}\right) + \left(-a_{u+1} + a_{u+2}\right) + \left(-a_{u+2} + a_{u+3}\right) + \cdots + \left(-a_v + a_{v+1}\right).$$

The right hand side of this equality is a sum of $2 \cdot (v-u+1)$ addends (once expanded out), but all but 2 of them cancel out (indeed, the second addend in each parenthesis cancels the first addend in the next parenthesis). The 2 addends left over are $-a_u$ and a_{v+1}. Thus, the sum "contracts" like a telescope (thus the name "telescoping sum principle"):

$$\left(-a_u + a_{u+1}\right) + \left(-a_{u+1} + a_{u+2}\right) + \left(-a_{u+2} + a_{u+3}\right) + \cdots + \left(-a_v + a_{v+1}\right)$$
$$= -a_u + a_{v+1} = a_{v+1} - a_u.$$

Combining, we obtain

$$\sum_{j=u}^{v} \left(a_{j+1} - a_j\right)$$
$$= \left(-a_u + a_{u+1}\right) + \left(-a_{u+1} + a_{u+2}\right) + \left(-a_{u+2} + a_{u+3}\right) + \cdots + \left(-a_v + a_{v+1}\right)$$
$$= a_{v+1} - a_u.$$

This proves Theorem 2.1.1. □

You might not like how we waved our hands talking of cancelling addends in the proof above. But formalizing the proof is a simple matter of reframing it as an induction argument:

First proof of Theorem 2.1.1 (formal version). From $u \leq v+1$, we obtain $v+1-u \geq 0$ and thus $v+1-u \in \mathbb{N}$. Hence, we can prove Theorem 2.1.1 by induction on $v+1-u$:

Induction base: It is easy to see that Theorem 2.1.1 holds if $v+1-u=0$ [135]. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume (as the induction hypothesis) that Theorem 2.1.1 holds if $v+1-u=m$. We must prove that Theorem 2.1.1 holds if $v+1-u=m+1$.

We have assumed that Theorem 2.1.1 holds if $v+1-u=m$. In other words, the following claim holds:

> *Claim 1:* Let u and v be two integers with $u \leq v+1$ and $v+1-u=m$. Let $a_u, a_{u+1}, \ldots, a_{v+1}$ be any numbers. Then,
>
> $$\sum_{j=u}^{v} \left(a_{j+1}-a_j\right) = a_{v+1}-a_u.$$

We must prove that Theorem 2.1.1 holds if $v+1-u=m+1$. In other words, we must prove the following claim:

> *Claim 2:* Let u and v be two integers with $u \leq v+1$ and $v+1-u=m+1$. Let $a_u, a_{u+1}, \ldots, a_{v+1}$ be any numbers. Then,
>
> $$\sum_{j=u}^{v} \left(a_{j+1}-a_j\right) = a_{v+1}-a_u.$$

[*Proof of Claim 2:* We have $v-u = \underbrace{(v+1-u)}_{=m+1} - 1 = (m+1)-1 = m \geq 0$ (since $m \in \mathbb{N}$) and thus $v \geq u$. Hence, we can split off the addend for $j=v$ from the sum $\sum_{j=u}^{v} \left(a_{j+1}-a_j\right)$. We thus obtain

$$\sum_{j=u}^{v} \left(a_{j+1}-a_j\right) = \left(a_{v+1}-a_v\right) + \sum_{j=u}^{v-1} \left(a_{j+1}-a_j\right). \tag{136}$$

But $u \leq (v-1)+1$ (since $(v-1)+1 = v \geq u$) and $(v-1)+1-u = v-u = m$. Hence, we can apply Claim 1 to $v-1$ instead of v. We thus obtain

$$\sum_{j=u}^{v-1} \left(a_{j+1}-a_j\right) = \underbrace{a_{(v-1)+1}}_{=a_v} - a_u = a_v - a_u.$$

Thus, (136) becomes

$$\sum_{j=u}^{v} \left(a_{j+1}-a_j\right) = \left(a_{v+1}-a_v\right) + \underbrace{\sum_{j=u}^{v-1} \left(a_{j+1}-a_j\right)}_{=a_v-a_u} = \left(a_{v+1}-a_v\right) + \left(a_v-a_u\right) = a_{v+1}-a_u.$$

[135] *Proof.* Let u, v and $a_u, a_{u+1}, \ldots, a_{v+1}$ be as in Theorem 2.1.1, and assume that $v+1-u=0$. Thus, $u=v+1$ (since $v+1-u=0$). Therefore,

$$\sum_{j=u}^{v} \left(a_{j+1}-a_j\right) = \sum_{j=v+1}^{v} \left(a_{j+1}-a_j\right) = (\text{empty sum}) = 0 = \underbrace{a_u}_{\substack{=a_{v+1} \\ (\text{since } u=v+1)}} - a_u = a_{v+1}-a_u.$$

This is precisely the claim of Theorem 2.1.1. Hence, we have showed that Theorem 2.1.1 holds if $v+1-u=0$.

This proves Claim 2.]

Now, we have proved Claim 2. In other words, we have proved that Theorem 2.1.1 holds if $v+1-u = m+1$. This completes the induction step. Thus, Theorem 2.1.1 is proved by induction. □

There is also a different proof of Theorem 2.1.1, relying on basic manipulations of sums:

Second proof of Theorem 2.1.1. We have

$$\sum_{j=u}^{v} \left(a_{j+1} - a_j\right) = \sum_{j=u}^{v} a_{j+1} - \sum_{j=u}^{v} a_j = \sum_{j=u+1}^{v+1} a_j - \sum_{j=u}^{v} a_j \tag{137}$$

(here, we have substituted j for $j+1$ in the first sum).

Now, it is tempting to argue that

$$\sum_{j=u+1}^{v+1} a_j = a_{v+1} + \sum_{j=u+1}^{v} a_j \qquad \text{and} \qquad \sum_{j=u}^{v} a_j = a_u + \sum_{j=u+1}^{v} a_j$$

(and then subtract these two equalities). Unfortunately, these two equalities are false in the border case $u = v+1$, because you cannot split off a (non-existing) addend from an empty sum. Of course, we could get around this issue by treating this border case separately (it is trivial). But it is a bit easier to make a similar argument that avoids this nuisance altogether: Instead of making the sums $\sum_{j=u+1}^{v+1} a_j$ and $\sum_{j=u}^{v} a_j$ equal by splitting off an addend from each, we make them equal by adding an extra addend to each. This can be done as follows:

We have $u \leq v+1$. Thus, we can split off the addend for $j = v+1$ from the sum $\sum_{j=u}^{v+1} a_j$, and obtain

$$\sum_{j=u}^{v+1} a_j = a_{v+1} + \sum_{j=u}^{v} a_j.$$

Thus,

$$\sum_{j=u}^{v} a_j = \sum_{j=u}^{v+1} a_j - a_{v+1}.$$

But we can also split off the addend for $j = u$ from the sum $\sum_{j=u}^{v+1} a_j$, and obtain

$$\sum_{j=u}^{v+1} a_j = a_u + \sum_{j=u+1}^{v+1} a_j.$$

Thus,

$$\sum_{j=u+1}^{v+1} a_j = \sum_{j=u}^{v+1} a_j - a_u.$$

Hence, (137) becomes

$$\sum_{j=u}^{v}\left(a_{j+1}-a_j\right) = \underbrace{\sum_{j=u+1}^{v+1} a_j}_{=\sum_{j=u}^{v+1} a_j - a_u} - \underbrace{\sum_{j=u}^{v} a_j}_{=\sum_{j=u}^{v+1} a_j - a_{v+1}}$$
$$= \left(\sum_{j=u}^{v+1} a_j - a_u\right) - \left(\sum_{j=u}^{v+1} a_j - a_{v+1}\right) = a_{v+1} - a_u.$$

This proves Theorem 2.1.1 again. □

Remark 2.1.2. Equivalent versions of Theorem 2.1.1 abound all across the literature. For example, [19f-hw0s, Proposition 2.2] says that if $m \in \mathbb{N}$ and if $a_0, a_1, \ldots, a_m$ are any $m+1$ numbers, then

$$\sum_{i=1}^{m}\left(a_i - a_{i-1}\right) = a_m - a_0.$$

This follows from Theorem 2.1.1, because substituting $j+1$ for i in the sum $\sum_{i=1}^{m}\left(a_i - a_{i-1}\right)$ yields

$$\sum_{i=1}^{m}\left(a_i - a_{i-1}\right) = \sum_{j=0}^{m-1}\left(a_{j+1} - a_j\right) = \underbrace{a_{(m-1)+1}}_{=a_m} - a_0$$
$$\text{(by Theorem 2.1.1, applied to } u=0 \text{ and } v=m-1)$$
$$= a_m - a_0.$$

Also, [Grinbe15, (16)] says that if u and v are two integers such that $u-1 \leq v$, and a_s is a number for each $s \in \{u-1, u, \ldots, v\}$, then

$$\sum_{s=u}^{v}\left(a_s - a_{s-1}\right) = a_v - a_{u-1}.$$

This is precisely Theorem 2.1.1, applied to a_{j-1} instead of a_j.

Let us note that Theorem 2.1.1 is a discrete version of the famous "Second Fundamental Theorem of Calculus", which says that any two real numbers u and v with $u \leq v$ and any differentiable function $F : [u,v]_{\mathbb{R}} \to \mathbb{R}$ satisfy[136]

$$\int_u^v F'(x)\,dx = F(v) - F(u).$$

Indeed, the summation sign $\sum$ is a discrete analogue of the integral sign $\int$, whereas the differences $a_{j+1} - a_j$ of consecutive entries of the sequence $a_u, a_{u+1}, \ldots, a_{v+1}$ are a discrete analogue of (the values of) the derivative of a function.

We can now re-prove Proposition 1.3.28:

[136] Here, $[u,v]_{\mathbb{R}}$ denotes the **real** interval from u to v.

Second proof of Proposition 1.3.28. If $n = 0$, then Proposition 1.3.28 boils down to the identity $1 = 1$, which is true. Thus, for the rest of this proof, we WLOG assume that $n \neq 0$. Hence, $[n = 0] = 0$ and $n \geq 1$ (since $n \in \mathbb{N}$). From $n \geq 1$, we obtain $n - 1 \in \mathbb{N}$. Hence, Proposition 1.3.6 (applied to $n-1$ and n instead of n and k) yields $\binom{n-1}{n} = 0$ (since $n - 1 < n$). Now, for each $k \in \mathbb{N}$, we have

$$\begin{aligned}
&(-1)^k \underbrace{\binom{n}{k}}_{=\binom{n-1}{k-1}+\binom{n-1}{k} \text{ (by Theorem 1.3.8)}} \\
&= (-1)^k \left(\binom{n-1}{k-1} + \binom{n-1}{k} \right) = \underbrace{(-1)^k}_{=-(-1)^{k-1}} \binom{n-1}{k-1} + (-1)^k \binom{n-1}{k} \\
&= -(-1)^{k-1} \binom{n-1}{k-1} + (-1)^k \binom{n-1}{k} = (-1)^k \binom{n-1}{k} - (-1)^{k-1} \binom{n-1}{k-1}.
\end{aligned}$$

Hence,

$$\begin{aligned}
&\sum_{k=0}^{n} \underbrace{(-1)^k \binom{n}{k}}_{=(-1)^k \binom{n-1}{k} - (-1)^{k-1} \binom{n-1}{k-1}} \\
&= \sum_{k=0}^{n} \left((-1)^k \binom{n-1}{k} - (-1)^{k-1} \binom{n-1}{k-1} \right) \\
&= \sum_{j=-1}^{n-1} \left((-1)^{j+1} \binom{n-1}{j+1} - (-1)^j \binom{n-1}{j} \right) \\
&\qquad \text{(here, we have substituted } j+1 \text{ for } k \text{ in the sum)} \\
&= (-1)^{(n-1)+1} \underbrace{\binom{n-1}{(n-1)+1}}_{=\binom{n-1}{n}=0} - (-1)^{-1} \underbrace{\binom{n-1}{-1}}_{\substack{=0 \\ \text{(by (43), applied to } n-1 \text{ and } -1 \\ \text{instead of } n \text{ and } k)}} \\
&\qquad \left(\text{by Theorem 2.1.1, applied to } u = -1, v = n-1 \text{ and } a_j = (-1)^j \binom{n-1}{j} \right) \\
&= 0 - 0 = 0 = [n = 0] \qquad (\text{since } [n = 0] = 0).
\end{aligned}$$

This proves Proposition 1.3.28 again. □

When applying Theorem 2.1.1, one usually does not directly mention Theorem 2.1.1; instead, one says that the sum $\sum_{j=u}^{v} \left(a_{j+1} - a_j \right)$ "*telescopes to*" $a_{v+1} - a_u$. Thus,

for example, in the proof of Proposition 1.3.28 we just gave, the sum $\sum_{j=-1}^{n-1}\left((-1)^{j+1}\binom{n-1}{j+1}-(-1)^{j}\binom{n-1}{j}\right)$ telescoped to $(-1)^{(n-1)+1}\binom{n-1}{(n-1)+1}-(-1)^{-1}\binom{n-1}{-1}$.

Exercise 2.1.1. **(a)** Let $n \in \mathbb{R}$. Let $m \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{m}(-1)^{k}\binom{n}{k}=(-1)^{m}\binom{n-1}{m}.$$

(b) Explain why Proposition 1.3.28 is a particular case of Exercise 2.1.1 **(a)**.

Let us illustrate the telescoping sum principle on another application: a new proof of the hockey-stick identity (Theorem 1.3.29):

Second proof of Theorem 1.3.29. For each $j \in \mathbb{Z}$, we have

$$\begin{aligned}\binom{j+1}{k+1} &= \binom{(j+1)-1}{(k+1)-1}+\binom{(j+1)-1}{k+1} \\ &\qquad \left(\begin{array}{c}\text{by Theorem 1.3.8, applied to } j+1 \text{ and } k+1 \\ \text{instead of } n \text{ and } k\end{array}\right) \\ &= \binom{j}{k}+\binom{j}{k+1} \qquad (\text{since } (j+1)-1=j \text{ and } (k+1)-1=k)\end{aligned}$$

and therefore

$$\binom{j}{k}=\binom{j+1}{k+1}-\binom{j}{k+1}. \tag{138}$$

But $n \in \mathbb{N}$, thus $0 \leq n \leq n+1$. Also, $k \in \mathbb{N}$, thus $k+1>0$ and therefore $k+1 \neq 0$. Hence, $[k+1=0]=0$. Now, Lemma 1.3.14 (applied to $k+1$ instead of k) yields $\binom{0}{k+1}=[k+1=0]=0$.

But

$$\begin{aligned}&\binom{0}{k}+\binom{1}{k}+\binom{2}{k}+\cdots+\binom{n}{k} \\ &= \sum_{j=0}^{n}\underbrace{\binom{j}{k}}_{=\binom{j+1}{k+1}-\binom{j}{k+1}\ (\text{by (138)})} = \sum_{j=0}^{n}\left(\binom{j+1}{k+1}-\binom{j}{k+1}\right) \\ &\qquad \left(\text{by Theorem 2.1.1, applied to } u=0 \text{ and } v=n \text{ and } a_j=\binom{j}{k+1}\right) \\ &= \binom{n+1}{k+1}-\underbrace{\binom{0}{k+1}}_{=0} \\ &= \binom{n+1}{k+1}.\end{aligned}$$

This proves Theorem 1.3.29 again. □

2.1.2. A war between the odd and the even

Proposition 1.3.28 does not seem vulnerable to bijective proof strategies: The sum $\sum_{k=0}^{n} (-1)^k \binom{n}{k}$ contains both positive and negative numbers, and of course negative numbers cannot be interpreted as sizes of sets. Nevertheless, it turns out that there is a bijective proof of Proposition 1.3.28, and a rather slick and simple one:

Third proof of Proposition 1.3.28 (sketched). As in the Second proof of Proposition 1.3.28 above, we see that Proposition 1.3.28 holds for $n = 0$. Thus, we WLOG assume that $n \neq 0$. Hence, $[n = 0] = 0$. We thus need to show that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

But the left hand side of this equality is

$$\begin{aligned}
\sum_{k=0}^{n} (-1)^k \binom{n}{k} &= \sum_{k \in \{0,1,\ldots,n\}} (-1)^k \binom{n}{k} \\
&= \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is even}}} \underbrace{(-1)^k}_{\substack{=1 \\ (\text{since } k \text{ is even})}} \binom{n}{k} + \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is odd}}} \underbrace{(-1)^k}_{\substack{=-1 \\ (\text{since } k \text{ is odd})}} \binom{n}{k} \\
&\qquad \left(\begin{array}{c} \text{since each } k \in \{0,1,\ldots,n\} \text{ is either even or odd,} \\ \text{but not both at the same time} \end{array} \right) \\
&= \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is even}}} \binom{n}{k} + \underbrace{\sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is odd}}} (-1) \binom{n}{k}}_{= - \sum\limits_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is odd}}} \binom{n}{k}} \\
&= \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is even}}} \binom{n}{k} - \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is odd}}} \binom{n}{k}.
\end{aligned}$$

Thus, we only need to prove that

$$\sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ even}}} \binom{n}{k} = \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ odd}}} \binom{n}{k}. \tag{139}$$

We can prove this bijectively:

The left-hand side of (139) is the # of subsets of $[n]$ of even size[137]. The right-hand side of (139) is the # of subsets of $[n]$ of odd size[138]. Hence, the equality (139) is equivalent to

$$(\#\text{ of subsets of } [n] \text{ of even size}) = (\#\text{ of subsets of } [n] \text{ of odd size}).$$

This will follow immediately from the bijection principle, once we can find a bijection

$$\{\text{subsets of } [n] \text{ of even size}\} \to \{\text{subsets of } [n] \text{ of odd size}\}.$$

Here is such a bijection:

$$\{\text{subsets of } [n] \text{ of even size}\} \to \{\text{subsets of } [n] \text{ of odd size}\},$$
$$A \mapsto \begin{cases} A \cup \{1\}, & \text{if } 1 \notin A; \\ A \setminus \{1\}, & \text{if } 1 \in A \end{cases}.$$

We need to actually convince ourselves that this map is well-defined[139] and actually a bijection[140]. Thus, (139) is proved. As we have said, this entails Proposition 1.3.28. □

The bijection we have used in this proof can be rewritten in an even simpler way using a basic set-theoretical operation (almost as basic as union and intersection of sets), called the *symmetric difference*:

[137] *Proof.* We have $|[n]| = n$. If B is any subset of $[n]$, then Theorem 1.4.7 **(b)** (applied to $A = [n]$) yields $|B| \leq |[n]| = n$ and therefore $|B| \in \{0, 1, \ldots, n\}$. Furthermore, if B is any subset of $[n]$ of even size, then $|B|$ is an even element of $\{0, 1, \ldots, n\}$ (because we just saw that $|B| \in \{0, 1, \ldots, n\}$, but we also know now that $|B|$ is even). Hence, the sum rule yields

$$\begin{aligned} &(\#\text{ of subsets of } [n] \text{ of even size}) \\ &= \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is even}}} \underbrace{(\#\text{ of subsets } B \text{ of } [n] \text{ satisfying } |B| = k)}_{\substack{= (\#\text{ of } k\text{-element subsets of } [n]) \\ = \binom{n}{k} \\ \text{(by Theorem 1.3.12,} \\ \text{applied to } S = [n])}} \\ &= \sum_{\substack{k \in \{0,1,\ldots,n\}; \\ k \text{ is even}}} \binom{n}{k} = (\text{the left-hand side of (139)}). \end{aligned}$$

[138] for an analogous reason

[139] This means proving that if A is any subset of $[n]$ of even size, then $\begin{cases} A \cup \{1\}, & \text{if } 1 \notin A; \\ A \setminus \{1\}, & \text{if } 1 \in A \end{cases}$ is a subset of $[n]$ of odd size. This relies on the following facts:

- We have $1 \in [n]$ (since $n \neq 0$).
- If $1 \notin A$, then $|A \cup \{1\}| = |A| + 1$ is odd (since $|A|$ is even).
- If $1 \in A$, then $|A \setminus \{1\}| = |A| - 1$ is odd (since $|A|$ is even).

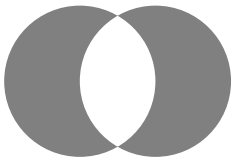
[140] To prove this, we need to find an inverse to it. This is easy: The inverse is given by the exact same

Definition 2.1.3. Let X and Y be two sets. Then, the *symmetric difference* of X and Y is the set

$$\begin{aligned}&\{\text{all elements that lie in exactly one of the two sets } X \text{ and } Y\}\\&= (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y)\,.\end{aligned}$$

This set is denoted by $X \triangle Y$.

The Venn diagram for $X \triangle Y$ is



(where the two circles represent X and Y).

Example 2.1.4. We have $\{1,2,3,4\} \triangle \{3,4,5,6\} = \{1,2,5,6\}$.

The notion of symmetric difference has the following properties (which are all straightforward to check using Venn diagrams or elementwise verification):

Proposition 2.1.5. **(a)** We have $X \triangle X = \varnothing$ for any set X.
(b) We have $X \triangle \varnothing = X$ for any set X.
(c) We have $X \triangle Y = Y \triangle X$ for any two sets X and Y.
(d) We have $(X \triangle Y) \triangle Z = X \triangle (Y \triangle Z)$ for any three sets X, Y and Z.
(e) We have $X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z)$ for any three sets X, Y and Z.
(f) If X and Y are two finite sets, then $|X \triangle Y| = |X| + |Y| - 2\,|X \cap Y| \equiv |X| + |Y| \bmod 2$.

Using symmetric differences, we can now rewrite the bijection that we used in the above Third proof of Proposition 1.3.28 as

$$\begin{aligned}\{\text{subsets of } [n] \text{ of even size}\} &\to \{\text{subsets of } [n] \text{ of odd size}\}\,,\\ A &\mapsto A \triangle \{1\}\,.\end{aligned}$$

This makes it even easier to check that this map is well-defined and a bijection.

formula! That is, the inverse is the map

$$\begin{aligned}\{\text{subsets of } [n] \text{ of odd size}\} &\to \{\text{subsets of } [n] \text{ of even size}\}\,,\\ A &\mapsto \begin{cases} A \cup \{1\}\,, & \text{if } 1 \notin A;\\ A \setminus \{1\}\,, & \text{if } 1 \in A \end{cases}.\end{aligned}$$

In order to see that this is really an inverse to our map, we need to show the following:

- If $1 \notin A$, then $1 \in A \cup \{1\}$ and $(A \cup \{1\}) \setminus \{1\} = A$.
- If $1 \in A$, then $1 \notin A \setminus \{1\}$ and $(A \setminus \{1\}) \cup \{1\} = A$.

Of course, both of these claims are completely obvious.

2.2. The trinomial revision formula

2.2.1. An algebraic proof

Recall the trinomial revision formula (Proposition 1.3.35), which states that

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b} \qquad \text{for all } n, a, b \in \mathbb{R}.$$

We have previously stated this without proof; let us prove it now:

Proof of Proposition 1.3.35. We must be in one of the following four cases:
Case 1: We have $b \notin \mathbb{N}$.
Case 2: We have $b \in \mathbb{N}$ and $a \notin \mathbb{N}$.
Case 3: We have $b \in \mathbb{N}$ and $a \in \mathbb{N}$ but $a < b$.
Case 4: We have $b \in \mathbb{N}$ and $a \in \mathbb{N}$ and $a \geq b$.

Let us first consider Case 1. In this case, we have $b \notin \mathbb{N}$. Hence, (43) (applied to a and b instead of n and k) yields $\binom{a}{b} = 0$. Also, (43) (applied to $k = b$) yields $\binom{n}{b} = 0$. Now, comparing

$$\binom{n}{a}\underbrace{\binom{a}{b}}_{=0} = 0 \qquad \text{with} \qquad \underbrace{\binom{n}{b}}_{=0}\binom{n-b}{a-b} = 0,$$

we obtain $\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}$. Thus, Proposition 1.3.35 is proven in Case 1.

Let us now consider Case 2. In this case, we have $b \in \mathbb{N}$ and $a \notin \mathbb{N}$. Hence, (43) (applied to $k = a$) yields $\binom{n}{a} = 0$. Also, $a - b \notin \mathbb{N}$ [141]. Hence, (43) (applied to $n - b$ and $a - b$ instead of n and k) yields $\binom{n-b}{a-b} = 0$. Now, comparing

$$\underbrace{\binom{n}{a}}_{=0}\binom{a}{b} = 0 \qquad \text{with} \qquad \binom{n}{b}\underbrace{\binom{n-b}{a-b}}_{=0} = 0,$$

we obtain $\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}$. Thus, Proposition 1.3.35 is proven in Case 2.

Let us now consider Case 3. In this case, we have $b \in \mathbb{N}$ and $a \in \mathbb{N}$ but $a < b$. From $a < b$, we obtain $a - b < 0$, so that $a - b \notin \mathbb{N}$. Hence, (43) (applied to $n - b$

[141] *Proof.* Assume the contrary. Thus, $a - b \in \mathbb{N}$. Hence, $a = \underbrace{a-b}_{\in\mathbb{N}} + \underbrace{b}_{\in\mathbb{N}} \in \mathbb{N}$ (since the sum of two elements of $\mathbb{N}$ is always an element of $\mathbb{N}$), which contradicts $a \notin \mathbb{N}$. Hence, we have obtained a contradiction. This shows that our assumption was false, qed.

and $a-b$ instead of n and k) yields $\binom{n-b}{a-b} = 0$. Also, $b > a$ (since $a < b$). Hence, Proposition 1.3.6 (applied to a and b instead of n and k) yields $\binom{a}{b} = 0$. Now, comparing

$$\binom{n}{a}\underbrace{\binom{a}{b}}_{=0} = 0 \qquad \text{with} \qquad \binom{n}{b}\underbrace{\binom{n-b}{a-b}}_{=0} = 0,$$

we obtain $\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}$. Thus, Proposition 1.3.35 is proven in Case 3.

Let us finally consider Case 4. In this case, we have $b \in \mathbb{N}$ and $a \in \mathbb{N}$ and $a \geq b$. From this, we conclude that $a-b \in \mathbb{N}$ and $b \leq a$. Hence, Theorem 1.3.9 (applied to a and b instead of n and k) yields

$$\binom{a}{b} = \frac{a!}{b! \cdot (a-b)!}. \tag{140}$$

Also, (42) (applied to $k = a$) yields

$$\binom{n}{a} = \frac{n\,(n-1)\,(n-2)\cdots(n-a+1)}{a!}.$$

Multiplying this equality by (140), we obtain

$$\begin{aligned}\binom{n}{a}\binom{a}{b} &= \frac{n\,(n-1)\,(n-2)\cdots(n-a+1)}{a!} \cdot \frac{a!}{b!\,(a-b)!} \\ &= \frac{n\,(n-1)\,(n-2)\cdots(n-a+1)}{b! \cdot (a-b)!}.\end{aligned} \tag{141}$$

On the other hand, (42) (applied to $k = b$) yields

$$\binom{n}{b} = \frac{n\,(n-1)\,(n-2)\cdots(n-b+1)}{b!}.$$

Furthermore, (42) (applied to $n-b$ and $a-b$ instead of n and k) yields

$$\begin{aligned}\binom{n-b}{a-b} &= \frac{(n-b)\,(n-b-1)\,(n-b-2)\cdots((n-b)-(a-b)+1)}{(a-b)!} \\ &= \frac{(n-b)\,(n-b-1)\,(n-b-2)\cdots(n-a+1)}{(a-b)!}.\end{aligned}$$

Multiplying these two equalities, we find

$$\begin{aligned}
&\binom{n}{b}\binom{n-b}{a-b} \\
&= \frac{n\,(n-1)\,(n-2)\cdots(n-b+1)}{b!} \cdot \frac{(n-b)\,(n-b-1)\,(n-b-2)\cdots(n-a+1)}{(a-b)!} \\
&= \frac{(n\,(n-1)\,(n-2)\cdots(n-b+1)) \cdot ((n-b)\,(n-b-1)\,(n-b-2)\cdots(n-a+1))}{b!\cdot(a-b)!} \\
&= \frac{n\,(n-1)\,(n-2)\cdots(n-a+1)}{b!\cdot(a-b)!}
\end{aligned}$$

(because

$$\begin{aligned}
&(n\,(n-1)\,(n-2)\cdots(n-b+1)) \cdot ((n-b)\,(n-b-1)\,(n-b-2)\cdots(n-a+1)) \\
&= n\,(n-1)\,(n-2)\cdots(n-a+1) \\
&\qquad \left(\begin{array}{c} \text{since } 0 \leq b \leq a\text{, and thus the} \\ \text{product } n\,(n-1)\,(n-2)\cdots(n-a+1) \text{ can be split into} \\ (n\,(n-1)\,(n-2)\cdots(n-b+1)) \\ \cdot ((n-b)\,(n-b-1)\,(n-b-2)\cdots(n-a+1)) \end{array} \right)
\end{aligned}$$

). Comparing this with (141), we obtain

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}.$$

Thus, Proposition 1.3.35 is proven in Case 4.

We have now proved Proposition 1.3.35 in each of the four Cases 1, 2, 3 and 4. Hence, Proposition 1.3.35 always holds. □

It is worth taking a second look at the structure of our above proof of Proposition 1.3.35: This proof was subdivided into four cases. In the first three of these cases, the proposition boiled down to $0 = 0$ (but for different reasons in each case). Only in the fourth case did we end up proving anything interesting. This suggests that the generality in which we stated Proposition 1.3.35 (allowing all of n, a, b to be arbitrary reals) was perhaps more of a handicap than a helpful feature. Nevertheless, this generality pays off: We only need to prove the proposition once, and then we get to use it as often as we want, so a few extra cases are worth the trouble.

As an application of Proposition 1.3.35, let us prove a slight generalization of the absorption formula (Proposition 1.3.36):

Corollary 2.2.1 (Absorption formula II)**.** Let $n \in \mathbb{R} \setminus \{0\}$ and $m \in \mathbb{R}$. Then,

$$\binom{m}{n} = \frac{m}{n}\binom{m-1}{n-1}.$$

Proof of Corollary 2.2.1. Proposition 1.3.35 (applied to m, n and 1 instead of n, a and b) yields

$$\binom{m}{n}\binom{n}{1} = \binom{m}{1}\binom{m-1}{n-1}. \tag{142}$$

But we have $\binom{n}{1} = n$ (by (45)) and $\binom{m}{1} = m$ (likewise). Hence, the formula (142) rewrites as

$$\binom{m}{n} n = m\binom{m-1}{n-1}.$$

Dividing both sides of this equality by n, we find

$$\binom{m}{n} = \frac{m\binom{m-1}{n-1}}{n} = \frac{m}{n}\binom{m-1}{n-1}.$$

This proves Corollary 2.2.1. □

Exercise 2.2.1. Let $n \in \mathbb{Q}$, $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

(a) Prove that every integer $j \geq a$ satisfies

$$\binom{n}{j}\binom{j}{a}\binom{n-j}{b} = \binom{n}{a}\binom{n-a}{b}\binom{n-a-b}{j-a}.$$

(b) Compute the sum $\sum_{j=a}^{n} \binom{n}{j}\binom{j}{a}\binom{n-j}{b}$ for every integer $n \geq a$. (The result should contain no summation signs.)

Class of 2019-10-18

2.2.2. A double counting proof

Let us give a different proof of Proposition 1.3.35 – or, more precisely, a partial proof, since it will only work in the case when $n \in \mathbb{N}$. (In Subsection 2.6.4, we will learn a trick that will allow us to extend this proof to a complete proof of Proposition 1.3.35; essentially, we will learn a way to (rigorously) argue that if an identity such as $\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}$ holds for all $n \in \mathbb{N}$, then it must also hold for all $n \in \mathbb{R}$, and therefore it suffices to prove it for $n \in \mathbb{N}$ only. This is called the "polynomial identity trick", and, in a nutshell, the thing that makes it work is that both $\binom{n}{a}\binom{a}{b}$ and $\binom{n}{b}\binom{n-b}{a-b}$ are polynomials in n. But for now, let us just prove Proposition 1.3.35 in the case when $n \in \mathbb{N}$.)

Let us first present our partial proof in an informal way:

Second proof of Proposition 1.3.35 for $n \in \mathbb{N}$ (informal version). Assume that $n \in \mathbb{N}$.

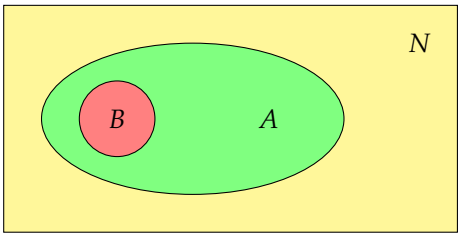
Fix a set N of n people.

We consider pairs (A, B), where A is a committee consisting of a people from N (that is, an a-element subset of N) and where B is a subcommittee consisting of b people from this committee A (that is, a b-element subset of A). [142] Formally speaking, these are simply pairs (A, B) of sets satisfying $B \subseteq A \subseteq N$ and $|A| = a$ and $|B| = b$. How many such pairs (A, B) are there? We shall refer to such pairs as *CS pairs*[143], and we shall count their # in two ways[144]:

First way: In order to construct a CS pair (A, B), we first choose the committee A and then choose its subcommittee B. We have $\binom{n}{a}$ many options for A (because A has to be an a-element subset of the n-element set N), and after choosing A, we have $\binom{a}{b}$ many options for B (because B has to be a b-element subset of A). Thus, the total # of CS pairs is a sum of $\binom{n}{a}$ many copies of $\binom{a}{b}$. In other words, this # is $\binom{n}{a}\binom{a}{b}$.

Second way: In order to construct a CS pair (A, B), we first choose the subcommittee B and then choose the committee A. We have $\binom{n}{b}$ many options for B (because B has to be a b-element subset of the n-element set N). After choosing B, how many options do we have for A ? The committee A has to be an a-element subset of N, but it is also required to contain the (already chosen) subcommittee B as a subset, so that b of its a elements are already decided. We only need to choose the remaining $a - b$ elements of A. These elements have to come from the $(n - b)$-element set $N \setminus B$ (because the elements of B have already been chosen to lie in A). Thus, we are choosing an $(a - b)$-element subset of the $(n - b)$-element set $N \setminus B$. Thus, we have $\binom{n-b}{a-b}$ many options for choosing A. Hence, the total # of CS pairs is a sum of $\binom{n}{b}$ many copies of $\binom{n-b}{a-b}$. In other words, this # is

[142] Here is a symbolic picture of this situation:



.

[143] short for "committee-subcommittee pairs"

[144] We will be using Theorem 1.3.12 in both of these ways.

$\binom{n}{b}\binom{n-b}{a-b}$.

Now, we have computed the # of CS pairs in two different ways. The first way gave us the result $\binom{n}{a}\binom{a}{b}$, while the second way gave us the result $\binom{n}{b}\binom{n-b}{a-b}$. Comparing these results, we find $\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}$. Thus, Proposition 1.3.35 is proven (in the case when $n \in \mathbb{N}$). □

How can we formalize this argument? It is clear how to formalize the notion of a CS pair (just replace "n people" by n mathematical objects, such as the numbers $1, 2, \ldots, n$). But how do we formalize our two ways of counting the # of CS pairs?

Let us look at the first way. On its surface, it may seem like we have applied the product rule (Theorem 1.1.4) in order to obtain $\binom{n}{a}\binom{a}{b}$ (similarly to how we applied it back in the proof of Proposition 1.4.14). But this appearance is misleading. If we wanted to apply Theorem 1.1.4, we would have to interpret $\binom{n}{a}\binom{a}{b}$ as $|X| \cdot |Y|$ for two sets X and Y. Thus, we would need two sets X and Y such that the CS pairs are elements of $X \times Y$ (or at least are in obvious bijection to the latter[145]). The obvious choice would be $X = \{a\text{-element subsets of } N\}$ and $Y = \{b\text{-element subsets of } A\}$, but this does not work: The set Y needs to be defined independently of A; but here it clearly is not. This is no surprise: If we choose a CS pair (A, B) by first choosing A, then the options available for B will depend on which A we have chosen (because we must have $B \subseteq A$). We are in luck because the **number** of these options does not depend on A (but always is $\binom{a}{b}$); but the **set** of these options does depend on A. Theorem 1.1.4 is not general enough to accommodate this situation.

There are two ways to resolve this problem. One is to generalize Theorem 1.1.4 to cover dependent choices. This results in a "dependent product rule", which (informally) says the following:

> **"Dependent product rule" for two sets:** Consider a situation in which you have to make two choices (sequentially). Assume that you have a_1 options available in choice 1, and then (after making choice 1) you have a_2 options available in choice 2 (no matter which option you chose in choice 1). Then, the total # of ways to make both choices[146] is $a_1 a_2$.

To formalize this, we can let X be the set of all available options in choice 1, and let Y be the set of all options that may be available in choice 2 (including the ones

[145] We are using some basic combinatorial slang here: We say that objects of some type are *in bijection with* objects of another type if there exists a bijection from {objects of the first type} to {objects of the second type}.

[146] i.e., of pairs (x, y), where x is an option you can choose in choice 1, and y is an option you can choose in choice 2 after choosing x in choice 1

whose availability depends on what you chose in choice 1), and let S be the set of all ways to make both choices. Then, our "dependent product rule" turns into the following rigorous fact:

Theorem 2.2.2. Let a_1 and a_2 be two numbers. Let X and Y be finite sets. Let S be a subset of $X \times Y$. Assume that $|X| = a_1$. Assume further that for each $x \in X$, there are precisely a_2 many elements $y \in Y$ such that $(x, y) \in S$ (even though the set of these y may depend on x). Then, $|S| = a_1 a_2$.

We leave the proof of this theorem to the reader, as we will not use it:

Exercise 2.2.2. Prove Theorem 2.2.2.

More generally, Theorem 1.5.3 can be generalized to cover several dependent choices:

> **"Dependent product rule" for n sets:** Consider a situation in which you have to make n choices (sequentially). Assume that you have a_1 options available in choice 1, and then (after making choice 1) you have a_2 options available in choice 2 (no matter which option you chose in choice 1), and then (after both choices 1 and 2) you have a_3 options available in choice 3 (no matter which options you chose in choices 1 and 2), and so on. Then, the total # of ways to make all n choices is $a_1 a_2 \cdots a_n$.

Formal versions of this rule can be found in [Loehr11, §1.8] and in [Newste19, Theorem 7.2.19].

However, all of this is entirely optional, because there is a simpler way to formalize our proof of Proposition 1.3.35. Instead of adapting the product rule, we can simply apply the sum rule (more precisely, Theorem 1.2.5) and observe that all addends of the resulting sum are equal (which means that the sum simplifies to a product). This leads to the following proof:

Second proof of Proposition 1.3.35 for $n \in \mathbb{N}$ (formal version). Let $N = [n]$. Thus, N is an n-element set.

A *CS pair* shall mean a pair (A, B) of sets satisfying $B \subseteq A \subseteq N$ and $|A| = a$ and $|B| = b$. Hence, if (A, B) is a CS pair, then A is an a-element subset of N (since $A \subseteq N$ and $|A| = a$), and B is a b-element subset of N (since $B \subseteq N$ and $|B| = b$).

We shall compute the number $|\{\text{CS pairs}\}|$ in two ways.

First way: Let $f : \{\text{CS pairs}\} \to \{a\text{-element subsets of } N\}$ be the map that sends each CS pair (A, B) to its first entry A. (This is well-defined, because if (A, B) is a CS pair, then A is an a-element subset of N.)

Theorem 1.2.5 (applied to $S = \{\text{CS pairs}\}$ and $W = \{a\text{-element subsets of } N\}$) yields

$$\begin{aligned}
&|\{\text{CS pairs}\}| \\
&= \sum_{w \in \{a\text{-element subsets of } N\}} (\#\text{ of } s \in \{\text{CS pairs}\} \text{ satisfying } f(s) = w) \\
&= \sum_{C \in \{a\text{-element subsets of } N\}} \underbrace{(\#\text{ of } s \in \{\text{CS pairs}\} \text{ satisfying } f(s) = C)}_{\substack{=(\#\text{ of CS pairs } s \text{ satisfying } f(s)=C) \\ =(\#\text{ of CS pairs whose first entry is } C) \\ (\text{because if } s \text{ is a CS pair, then } f(s) \text{ is the first entry of } s \\ (\text{by the definition of } f))}} \\
&\qquad (\text{here, we have renamed the index } w \text{ as } C) \\
&= \sum_{C \in \{a\text{-element subsets of } N\}} (\#\text{ of CS pairs whose first entry is } C)\,. \qquad (143)
\end{aligned}$$

Now, fix $C \in \{a\text{-element subsets of } N\}$. Thus, C is an a-element subset of N. Thus, $|C| = a$, so that $a = |C| \in \mathbb{N}$. Now, what are the CS pairs whose first entry is C ? They are precisely the CS pairs of the form (C, B) for some b-element subset B of C. Thus, the map

$$\begin{aligned}
\{\text{CS pairs whose first entry is } C\} &\to \{b\text{-element subsets of } C\}\,, \\
(C, B) &\mapsto B
\end{aligned}$$

is well-defined. In the other direction, there is a map

$$\begin{aligned}
\{b\text{-element subsets of } C\} &\to \{\text{CS pairs whose first entry is } C\}\,, \\
B &\mapsto (C, B)\,.
\end{aligned}$$

Clearly, these two maps are mutually inverse. Thus, they are bijections. Hence, the bijection principle yields

$$\begin{aligned}
&(\#\text{ of CS pairs whose first entry is } C) \\
&= (\#\text{ of } b\text{-element subsets of } C) = \binom{a}{b} \qquad (144)
\end{aligned}$$

(by Theorem 1.3.12, applied to a, C and b instead of n, S and k).

Now, forget that we fixed C. We thus have shown that (144) holds for every

$C \in \{a\text{-element subsets of } N\}$. Thus, (143) becomes

$$\begin{aligned}
&|\{\text{CS pairs}\}| \\
&= \sum_{C \in \{a\text{-element subsets of } N\}} \underbrace{(\#\text{ of CS pairs whose first entry is } C)}_{= \binom{a}{b} \text{ (by (144))}} \qquad (145) \\
&= \sum_{C \in \{a\text{-element subsets of } N\}} \binom{a}{b} = \underbrace{|\{a\text{-element subsets of } N\}|}_{=(\#\text{ of } a\text{-element subsets of } N) = \binom{n}{a} \text{ (by Theorem 1.3.12, applied to } S=N \text{ and } k=a)} \cdot \binom{a}{b} \\
&= \binom{n}{a}\binom{a}{b}. \qquad (146)
\end{aligned}$$

Second way: Forget about the map f defined previously.

Instead, let $f : \{\text{CS pairs}\} \to \{b\text{-element subsets of } N\}$ be the map that sends each CS pair (A, B) to its second entry B. (This is well-defined, because if (A, B) is a CS pair, then B is a b-element subset of N.)

Theorem 1.2.5 (applied to $S = \{\text{CS pairs}\}$ and $W = \{b\text{-element subsets of } N\}$) yields

$$\begin{aligned}
&|\{\text{CS pairs}\}| \\
&= \sum_{w \in \{b\text{-element subsets of } N\}} (\#\text{ of } s \in \{\text{CS pairs}\} \text{ satisfying } f(s) = w) \\
&= \sum_{D \in \{b\text{-element subsets of } N\}} \underbrace{(\#\text{ of } s \in \{\text{CS pairs}\} \text{ satisfying } f(s) = D)}_{\substack{=(\#\text{ of CS pairs } s \text{ satisfying } f(s)=D) \\ =(\#\text{ of CS pairs whose second entry is } D) \\ \text{(because if } s \text{ is a CS pair, then } f(s) \text{ is the second entry of } s \\ \text{(by the definition of } f))}} \\
&\qquad (\text{here, we have renamed the index } w \text{ as } D) \\
&= \sum_{D \in \{b\text{-element subsets of } N\}} (\#\text{ of CS pairs whose second entry is } D). \qquad (147)
\end{aligned}$$

Now, fix $D \in \{b\text{-element subsets of } N\}$. Thus, D is a b-element subset of N. Hence, $|D| = b$, so that $b = |D| \in \mathbb{N}$. Now, what are the CS pairs whose second entry is D ? They are precisely the CS pairs of the form (A, D) for some a-element subset A of N satisfying $D \subseteq A$. Thus, the map

$$\begin{aligned}
\{\text{CS pairs whose second entry is } D\} &\to \{a\text{-element subsets } A \text{ of } N \text{ satisfying } D \subseteq A\}, \\
(A, D) &\mapsto A
\end{aligned}$$

is well-defined. In the other direction, there is a map

$$\begin{aligned}
\{a\text{-element subsets } A \text{ of } N \text{ satisfying } D \subseteq A\} &\to \{\text{CS pairs whose second entry is } D\}, \\
A &\mapsto (A, D).
\end{aligned}$$

Clearly, these two maps are mutually inverse. Thus, they are bijections. Hence, the bijection principle yields

$$\begin{aligned}&(\#\text{ of CS pairs whose second entry is } D)\\&= (\#\text{ of } a\text{-element subsets } A \text{ of } N \text{ satisfying } D \subseteq A)\\&= \binom{n-b}{a-b}\end{aligned} \tag{148}$$

(by Proposition 1.4.20, applied to $d = b$ and $k = a$).

Now, forget that we fixed D. We thus have shown that (148) holds for every $D \in \{b\text{-element subsets of } N\}$. Thus, (147) becomes

$$\begin{aligned}&|\{\text{CS pairs}\}|\\&= \sum_{D \in \{b\text{-element subsets of } N\}} \underbrace{(\#\text{ of CS pairs whose second entry is } D)}_{= \binom{n-b}{a-b} \text{ (by (148))}}\\&= \sum_{D \in \{b\text{-element subsets of } N\}} \binom{n-b}{a-b} = \underbrace{|\{b\text{-element subsets of } N\}|}_{=(\#\text{ of } b\text{-element subsets of } N)} \cdot \binom{n-b}{a-b}\\&\qquad\qquad = \binom{n}{b} \text{ (by Theorem 1.3.12, applied to } S{=}N \text{ and } k{=}b)\\&= \binom{n}{b}\binom{n-b}{a-b}.\end{aligned} \tag{149}$$

Now, comparing (146) with (149), we obtain

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b}.$$

This proves Proposition 1.3.35 in the case when $n \in \mathbb{N}$. □

Remark 2.2.3. Something looks fishy. In the second proof of Proposition 1.3.35 we gave above, we have assumed that $n \in \mathbb{N}$, but we have not assumed that $a \in \mathbb{N}$. But then, how did we manage to obtain a combinatorial interpretation for $\binom{a}{b}$ such as (144), which shows that $\binom{a}{b}$ is an integer? Doesn't this contradict the fact that $\binom{a}{b}$ is usually not an integer when $a \notin \mathbb{N}$? Where is our mistake?

It turns out that there is nothing wrong with our proof. The crux of the matter is the little sentence "Now, fix $C \in \{a\text{-element subsets of } N\}$". This sentence provides the context in which the equality (144) was stated. In other words, we have only claimed that the equality (144) holds **for each**

$C \in \{a\text{-element subsets of } N\}$. Thus, $\binom{a}{b}$ will be an integer **for each** $C \in \{a\text{-element subsets of } N\}$. Even though $\binom{a}{b}$ does not depend on C, we cannot just throw the "for each $C \in \{a\text{-element subsets of } N\}$" part of this statement away, because there is no a-priori guarantee that there exists a $C \in \{a\text{-element subsets of } N\}$. And indeed, such a C can exist only when $a \in \mathbb{N}$ (and, even stronger, $a \in \{0, 1, \ldots, n\}$); and $\binom{a}{b}$ is indeed an integer in this case. When such a C does not exist, $\binom{a}{b}$ will **not** always be an integer. So the equality (144) leads to a contradiction if we take it out of its context, but inside its context it is perfectly correct.

The sentence "Now, forget that we fixed C" that appeared later on in the proof marks the end of this context. After this sentence, C is no longer a fixed a-element subset of N, and the equality (146) can be applied to any a-element subset of N in the role of C. (Thus, in particular, (146) can be applied to manipulate the addends in the sum appearing in (145), because this sum ranges over all a-element subsets of N. Of course, when $a \notin \mathbb{N}$, then this sum is an empty sum.)

Exercise 2.2.3. Let k be a positive integer.

(a) How many k-digit numbers are there? (A "k-digit number" means a nonnegative integer that has k digits without leading zeroes. For example, 3902 is a 4-digit number, not a 5-digit number. Note that 0 counts as a 0-digit number, not as a 1-digit number.)

(b) How many k-digit numbers are there that have no two equal digits?

(c) How many k-digit numbers have an even sum of digits?

(d) How many k-digit numbers are palindromes? (A "*palindrome*" is a number such that reading its digits from right to left yields the same number. For example, 5 and 1331 and 49094 are palindromes. Your answer may well depend on the parity of k.)

2.2.3. A variant

For later convenience, let us state an easy variant of the trinomial revision formula that is better suited for certain applications:

Proposition 2.2.4 (Alternative trinomial revision formula)**.** Let $n, a, b \in \mathbb{R}$. Then,

$$\binom{n}{a}\binom{a}{b} = \binom{n}{a-b}\binom{n-a+b}{b}.$$

Exercise 2.2.4. Prove Proposition 2.2.4.

2.3. The hockey-stick identity revisited

Next, we return to the hockey-stick identity (Theorem 1.3.29), which we have already proven in two ways (once in Subsection 1.3.7, and once in Subsection 2.1.1). Let us give two more proofs for it:

Third proof of Theorem 1.3.29 (sketched). Let us try to rewrite $\binom{n+1}{k+1}$ as a sum of binomial coefficients with a k at the bottom (that is, of binomial coefficients of the form $\binom{?}{k}$ for some values of ?). The first step towards this goal is to rewrite $\binom{n+1}{k+1}$ as follows:

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1} \qquad \left(\text{by Theorem 1.3.8}\right).$$

This is a good start, since it gives us a $\binom{n}{k}$ addend, which is of the desired form. But the other addend, $\binom{n}{k+1}$, is not. So let us rewrite it in the same way, viz., as follows:

$$\binom{n+1}{k+1} = \binom{n}{k} + \underbrace{\binom{n}{k+1}}_{= \binom{n-1}{k} + \binom{n-1}{k+1} \text{ (by Theorem 1.3.8)}} = \binom{n-1}{k} + \binom{n-1}{k} + \binom{n-1}{k+1}.$$

This looks even better, since we now have two addends of the desired form; but we still have an addend, $\binom{n-1}{k+1}$, which is not of this form. So let us rewrite it in the

same way, and keep doing this over and over:

$$\begin{aligned}
\binom{n+1}{k+1} &= \binom{n}{k} + \underbrace{\binom{n}{k+1}}_{=\binom{n-1}{k}+\binom{n-1}{k+1} \text{ (by Theorem 1.3.8)}} && \text{(by Theorem 1.3.8)} \\
&= \binom{n}{k} + \binom{n-1}{k} + \underbrace{\binom{n-1}{k+1}}_{=\binom{n-2}{k}+\binom{n-2}{k+1} \text{ (by Theorem 1.3.8)}} \\
&= \binom{n}{k} + \binom{n-1}{k} + \binom{n-2}{k} + \underbrace{\binom{n-2}{k+1}}_{=\binom{n-3}{k}+\binom{n-3}{k+1} \text{ (by Theorem 1.3.8)}} \\
&= \binom{n}{k} + \binom{n-1}{k} + \binom{n-2}{k} + \binom{n-3}{k} + \binom{n-3}{k+1} \\
&= \cdots\cdots\cdots && \text{(keep doing the same transformation)}.
\end{aligned}$$

We could go on like this forever, but let us stop at the point when the single "bad" addend (i.e., the binomial coefficient that has a $k+1$ at the bottom) is $\binom{0}{k+1}$. We thus have found

$$\begin{aligned}
&\binom{n+1}{k+1} \\
&= \binom{n}{k} + \binom{n-1}{k} + \binom{n-2}{k} + \cdots + \binom{0}{k} + \underbrace{\binom{0}{k+1}}_{\substack{=0 \\ \text{(by Lemma 1.3.14,} \\ \text{since } k+1>0)}} \qquad (150) \\
&= \binom{n}{k} + \binom{n-1}{k} + \binom{n-2}{k} + \cdots + \binom{0}{k} \\
&= \binom{0}{k} + \binom{1}{k} + \cdots + \binom{n}{k}.
\end{aligned}$$

Thus, Theorem 1.3.29 holds.

This is not yet a formal proof, because "keep doing the same transformation" is not a well-defined term in rigorous mathematics. (A computation cannot have an indefinite length!) But it is easy to formalize this argument: We are really proving

the equality

$$\binom{n+1}{k+1} = \underbrace{\binom{n}{k} + \binom{n-1}{k} + \cdots + \binom{n-i+1}{k}}_{\substack{\text{a sum of } i \text{ binomial coefficients} \\ \text{with } n, n-1, \ldots, n-i+1 \text{ at the top and (always) } k \text{ at the bottom}}} + \binom{n-i+1}{k+1}$$

for each $i \in \mathbb{N}$. (This equality is our expression for $\binom{n+1}{k+1}$ after i transformations of the form described above.) Of course, this equality is proved by induction on i. Once it is proved, we can apply it to $i = n+1$, and obtain (150), after which we proceed as before. The details are LTTR. □

Fourth proof of Theorem 1.3.29 (sketched). Let us count the $(k+1)$-element subsets of $[n+1]$ according to their largest element.

First of all, why are their largest elements well-defined? Each $(k+1)$-element subset of $[n+1]$ is nonempty (since its size is $k+1 > k \geq 0$), and thus has a unique largest element. This largest element obviously belongs to $[n+1]$. (Even better, this largest element belongs to $\{k+1, k+2, \ldots, n+1\}$, but we don't need this.)

Theorem 1.3.12 (applied to $n+1$, $k+1$ and $[n+1]$ instead of n, k and S) yields

$$\begin{aligned}\binom{n+1}{k+1} &= (\#\text{ of } (k+1)\text{-element subsets of } [n+1]) \\ &= \sum_{j \in [n+1]} (\#\text{ of } (k+1)\text{-element subsets of } [n+1] \text{ whose largest element is } j)\end{aligned} \tag{151}$$

as a consequence of the sum rule[147] (since each $(k+1)$-element subset of $[n+1]$ has a unique largest element, which belongs to $[n+1]$).

Now, fix $j \in [n+1]$. How many $(k+1)$-element subsets of $[n+1]$ are there whose largest element is j ?

The answer is:

$$\begin{aligned}&(\#\text{ of } (k+1)\text{-element subsets of } [n+1] \text{ whose largest element is } j) \\ &= \binom{j-1}{k}.\end{aligned} \tag{152}$$

[*Proof of (152):* Informally, this can be justified as follows: If we want to choose a $(k+1)$-element subset of $[n+1]$ whose largest element is j, then we already know that j has to be an element of this subset, and we only need to choose its remaining k elements. These remaining k elements have to belong to $\{1, 2, \ldots, j-1\}$ (in order to ensure that j is the largest element of the resulting subset). Thus, we are really just

[147] To be more precise: of Theorem 1.2.5, applied to $S = \{(k+1)\text{-element subsets of } [n+1]\}$, $W = [n+1]$ and f being the map that sends each $(k+1)$-element subset of $[n+1]$ to its largest element

choosing a k-element subset of $\{1,2,\ldots,j-1\}$. Since $\{1,2,\ldots,j-1\}$ is a $(j-1)$-element set, we thus have $\dbinom{j-1}{k}$ many choices (by Theorem 1.3.12). This proves (152).

Here is a rigorous version of this argument: If S is a $(k+1)$-element subset of $[n+1]$ whose largest element is j, then $S \setminus \{j\}$ is a k-element subset of $\{1,2,\ldots,j-1\}$. Hence, there is a map

$$\begin{aligned}&\{(k+1)\text{-element subsets of } [n+1] \text{ whose largest element is } j\}\\&\to \{k\text{-element subsets of } \{1,2,\ldots,j-1\}\}\end{aligned}$$

which sends each S to $S \setminus \{j\}$. This map is furthermore a bijection[148]. Thus, the bijection principle yields

$$\begin{aligned}&(\#\text{ of } (k+1)\text{-element subsets of } [n+1] \text{ whose largest element is } j)\\&= (\#\text{ of } k\text{-element subsets of } \{1,2,\ldots,j-1\})\\&= \binom{j-1}{k}\end{aligned}$$

(by Theorem 1.3.12, applied to $j-1$ and $\{1,2,\ldots,j-1\}$ instead of n and S). This proves (152) formally.]

Either way, we have thus shown that (152) holds. Hence, (151) becomes

$$\begin{aligned}&\binom{n+1}{k+1}\\&= \underbrace{\sum_{j\in[n+1]}}_{=\sum_{j=1}^{n+1}} \underbrace{(\#\text{ of } (k+1)\text{-element subsets of } [n+1] \text{ whose largest element is } j)}_{=\binom{j-1}{k} \text{ (by (152))}}\\&= \sum_{j=1}^{n+1} \binom{j-1}{k} = \sum_{i=0}^{n} \binom{i}{k} \qquad \text{(here, we have substituted } i \text{ for } j-1 \text{ in the sum)}\\&= \binom{0}{k} + \binom{1}{k} + \cdots + \binom{n}{k}.\end{aligned}$$

This proves Theorem 1.3.29 again. □

Remark 2.3.1. In the above fourth proof of Theorem 1.3.29, we have observed that the largest element of a $(k+1)$-element subset of $[n+1]$ not only belongs to $[n+1]$, but actually belongs to the smaller set $\{k+1,k+2,\ldots,n+1\}$ as well. But we have not used this observation. What if we had used it, thus obtaining a sum over all $j \in \{k+1,k+2,\ldots,n+1\}$ instead of a sum over all $j \in [n+1]$?

We would have obtained Corollary 1.3.30 instead of Theorem 1.3.29.

[148] Its inverse map sends each T to $T \cup \{j\}$. (We leave all the necessary verifications to the reader, who by now should find them completely routine.)

2.4. Counting maps

2.4.1. All maps

How many maps are there from an m-element set to an n-element set? We already know the answer (Theorem 1.5.7); let us just restate it a bit:

Theorem 2.4.1. Let $m, n \in \mathbb{N}$. Let A be an m-element set. Let B be an n-element set. Then,

$$(\#\text{ of maps from } A \text{ to } B) = n^m.$$

Proof of Theorem 2.4.1. We have $B^A = \{\text{maps } A \to B\}$ (by the definition of B^A). Also, $|A| = m$ (since A is an m-element set) and $|B| = n$ (likewise). Now,

$$\begin{aligned}
(\#\text{ of maps from } A \text{ to } B) &= |\{\text{maps } A \to B\}| \\
&= \left|B^A\right| \qquad \left(\text{since } \{\text{maps } A \to B\} = B^A\right) \\
&= |B|^{|A|} \qquad (\text{by Theorem 1.5.7}) \\
&= n^m \qquad (\text{since } |B| = n \text{ and } |A| = m).
\end{aligned}$$

This proves Theorem 2.4.1. □

Now, what if we want to count not all maps, but only some maps?

Recall that if $f : A \to B$ is a map between any two sets, then $f(A)$ denotes the image of this map (i.e., the subset $\{f(a) \mid a \in A\}$ of B). More generally, if $f : A \to B$ is a map and S is any subset of A, then $f(S)$ denotes the subset $\{f(a) \mid a \in S\}$ of B.

Exercise 2.4.1. Let A and B be two sets. Let C be a finite subset of B. Assume that A is finite, too.

(a) Prove that

$$(\#\text{ of maps } f : A \to B \text{ satisfying } f(A) \subseteq C) = |C|^{|A|}.$$

(b) Prove that

$$(\#\text{ of maps } f : A \to B \text{ satisfying } f(A) = C) = (\#\text{ of surjective maps from } A \text{ to } C).$$

2.4.2. Injective maps

In Remark 1.3.5 (and in [19f-hw0s, Exercise 2]), we have introduced the notation $n^{\underline{k}}$ (called a "falling factorial"). Since we are now going to use this notation more substantially, let us state its definition in detail:

Definition 2.4.2. Let $n \in \mathbb{R}$ and $k \in \mathbb{N}$. Then, the *falling factorial* $n^{\underline{k}}$ is the number defined by

$$n^{\underline{k}} = n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right) \tag{153}$$

$$= \prod_{i=0}^{k-1}\left(n-i\right). \tag{154}$$

Falling factorials are also called *lower factorials* or *descending factorials*. Let us state a few of their basic properties:

Proposition 2.4.3. Let $n \in \mathbb{R}$.
(a) We have $n^{\underline{0}} = 1$.
(b) We have $n^{\underline{1}} = n$.
(c) We have $n^{\underline{k}} = k! \cdot \dbinom{n}{k}$ for each $k \in \mathbb{N}$.
(d) If $n \in \mathbb{N}$, then $n^{\underline{n}} = n!$.
(e) If $n \in \mathbb{N}$, and if $k \in \mathbb{N}$ satisfies $k > n$, then $n^{\underline{k}} = 0$.
(f) We have $n^{\underline{k}} \cdot \left(n-k\right) = n^{\underline{k+1}}$ for each $k \in \mathbb{N}$.

By now, the proof of this is a near-trivial exercise:

Proof of Proposition 2.4.3. **(a)** Applying (153) to $k = 0$, we obtain

$$n^{\underline{0}} = \underbrace{n\left(n-1\right)\left(n-2\right)\cdots\left(n-0+1\right)}_{\text{a product with 0 factors}} = (\text{empty product}) = 1.$$

This proves Proposition 2.4.3 **(a)**.
(b) Applying (153) to $k = 1$, we obtain

$$n^{\underline{1}} = \underbrace{n\left(n-1\right)\left(n-2\right)\cdots\left(n-1+1\right)}_{\text{a product with 1 factor}} = n. \tag{155}$$

This proves Proposition 2.4.3 **(b)**.
(c) Let $k \in \mathbb{N}$. Then, multiplying both sides of the equality (42) by $k!$, we obtain

$$k! \cdot \binom{n}{k} = k! \cdot \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!} = n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right).$$

Comparing this with (153), we obtain $n^{\underline{k}} = k! \cdot \dbinom{n}{k}$. This proves Proposition 2.4.3 **(c)**.
(d) Let $n \in \mathbb{N}$. Then, (153) (applied to $k = n$) yields

$$n^{\underline{n}} = n\left(n-1\right)\left(n-2\right)\cdots\left(n-n+1\right) = n\left(n-1\right)\left(n-2\right)\cdots 1 = 1 \cdot 2 \cdot \cdots \cdot n = n!$$

(since $n!$ is defined to be $1 \cdot 2 \cdot \cdots \cdot n$). This proves Proposition 2.4.3 **(d)**.

(e) Let $n \in \mathbb{N}$, and let $k \in \mathbb{N}$ satisfy $k > n$. Then, Proposition 2.4.3 **(c)** yields

$$n^{\underline{k}} = k! \cdot \underbrace{\binom{n}{k}}_{=0 \text{ (by Proposition 1.3.6)}} = 0.$$

This proves Proposition 2.4.3 **(e)**.

(f) Let $k \in \mathbb{N}$. Multiplying both sides of the equality (153) by $n-k$, we obtain

$$n^{\underline{k}} \cdot (n-k) = (n(n-1)(n-2)\cdots(n-k+1)) \cdot (n-k) = n(n-1)(n-2)\cdots(n-k).$$

On the other hand, (153) (applied to $k+1$ instead of k) yields

$$n^{\underline{k+1}} = n(n-1)(n-2)\cdots(n-(k+1)+1) = n(n-1)(n-2)\cdots(n-k).$$

Comparing these two equalities, we obtain $n^{\underline{k}} \cdot (n-k) = n^{\underline{k+1}}$. This proves Proposition 2.4.3 **(f)**. □

We are now ready to count the injective maps between two finite sets:

Theorem 2.4.4. Let $m, n \in \mathbb{N}$. Let A be an m-element set. Let B be an n-element set. Then,

$$(\#\text{ of injective maps from } A \text{ to } B) = n^{\underline{m}}. \tag{156}$$

Remark 2.4.5. (a) If $m = 0$, then the right-hand side of (156) is $n^{\underline{0}} = 1$ (by Proposition 2.4.3 **(a)**). And indeed, there is exactly one injective map from $A = \varnothing$ to B (namely, the "empty map", which sends nothing anywhere).

(b) If $m > n$, then the right-hand side of (156) is $n^{\underline{m}} = 0$ (by Proposition 2.4.3 **(e)**). Thus, Theorem 2.4.4 yields that there are no injective maps from A to B in this case. This is intuitively clear (as B has "not enough elements" to find a distinct image for each $a \in A$); we are later going to state this as a theorem, which we shall call the "Pigeonhole Principle for Injections".

Let us first prove Theorem 2.4.4 in an informal way, using the "dependent product rule" for n sets that we have stated in Subsection 2.2.2:

Proof of Theorem 2.4.4 (informal version). Let $a_1, a_2, \ldots, a_m$ be the m elements of A (listed without repetitions). Then, in order to construct a map f from A to B, we only have to choose the m values $f(a_1), f(a_2), \ldots, f(a_m)$. Moreover, to ensure that this map f is injective, we need to choose these m values to be distinct. In other words, we need to choose these m values to satisfy

$$\begin{aligned}
&f(a_1) \in B; \\
&f(a_2) \in B \setminus \{f(a_1)\}; \\
&f(a_3) \in B \setminus \{f(a_1), f(a_2)\}; \\
&f(a_4) \in B \setminus \{f(a_1), f(a_2), f(a_3)\}; \\
&\quad \vdots \\
&f(a_m) \in B \setminus \{f(a_1), f(a_2), \ldots, f(a_{m-1})\}.
\end{aligned}$$

We can construct such an injective map f by the following m-step procedure:

- first choose the value $f(a_1)$ to be any element of B (there are n options for it, since B is an n-element set);
- then choose the value $f(a_2)$ to be any element of $B \setminus \{f(a_1)\}$ (there are $n-1$ options for it[149]);
- then choose the value $f(a_3)$ to be any element of $B \setminus \{f(a_1), f(a_2)\}$ (there are $n-2$ options for it[150]);
- then choose the value $f(a_4)$ to be any element of $B \setminus \{f(a_1), f(a_2), f(a_3)\}$ (there are $n-3$ options for it[151]);
- and so on;
- at last, choose the value $f(a_m)$ to be any element of $B \setminus \{f(a_1), f(a_2), \ldots, f(a_{m-1})\}$ (there are $n-(m-1)$ options for it).

Thus, by the dependent product rule, the total # of ways to make all m choices is

$$n(n-1)(n-2)\cdots(n-(m-1)) = n(n-1)(n-2)\cdots(n-m+1) = n^{\underline{m}}$$

(since $n^{\underline{m}}$ is defined to be $n(n-1)(n-2)\cdots(n-m+1)$). Thus, the # of injective maps from A to B is $n^{\underline{m}}$. This proves Theorem 2.4.4. □

How can we formalize this argument? The words "and so on" suggest that we should frame it as an induction over m, and the use of the dependent product rule hints at using Theorem 1.2.5 (which, as we recall from our Second proof of Proposition 1.3.35, can be used as a stand-in replacement for the dependent product rule, at least for its two-set version; but as we will see, it works for the general case just as well). This leads us to the following proof:

Proof of Theorem 2.4.4 (formal version). Forget that we fixed n, m, A and B. If A and B are any two sets, then we let $\operatorname{Inj}(A, B)$ denote the set of all injective maps from A to B.

Now, we shall prove Theorem 2.4.4 by induction on m:

---

[149] since $\underbrace{B}_{\text{an } n\text{-element set}} \setminus \underbrace{\{f(a_1)\}}_{\text{a 1-element subset of } B}$ is an $(n-1)$-element set

[150] since $\underbrace{B}_{\text{an } n\text{-element set}} \setminus \underbrace{\{f(a_1), f(a_2)\}}_{\substack{\text{a 2-element subset of } B \\ \text{(since } f(a_1) \text{ and } f(a_2) \text{ are distinct} \\ \text{(because we chose } f(a_2) \text{ out of } B \setminus \{f(a_1)\}\text{))}}}$ is an $(n-2)$-element set

[151] since $\underbrace{B}_{\text{an } n\text{-element set}} \setminus \underbrace{\{f(a_1), f(a_2), f(a_3)\}}_{\substack{\text{a 3-element subset of } B \\ \text{(since } f(a_1), f(a_2) \text{ and } f(a_3) \text{ are distinct} \\ \text{(since we chose } f(a_2) \text{ out of } B \setminus \{f(a_1)\}, \\ \text{and since we chose } f(a_3) \text{ out of } B \setminus \{f(a_1), f(a_2)\}\text{))}}}$ is an $(n-3)$-element set

Induction base: Theorem 2.4.4 holds when $m = 0$ [152]. This completes the induction base.

Induction step: Let $k \in \mathbb{N}$. Assume (as the induction hypothesis) that Theorem 2.4.4 holds for $m = k$. We must now prove that Theorem 2.4.4 holds for $m = k+1$.

Let $n \in \mathbb{N}$. Let A be a $(k+1)$-element set, and let B be an n-element set. We must show that

$$(\#\text{ of injective maps from } A \text{ to } B) = n^{\underline{k+1}}. \tag{157}$$

The set A is a $(k+1)$-element set; thus, $|A| = k+1 > k \geq 0$. Hence, A is nonempty. Choose any $a \in A$. (Such an a exists, since A is nonempty.)

The set $A \setminus \{a\}$ has size

$$\begin{aligned} |A \setminus \{a\}| &= \underbrace{|A|}_{=k+1} - 1 \qquad (\text{since } a \in A) \\ &= (k+1) - 1 = k. \end{aligned}$$

Hence, $A \setminus \{a\}$ is a k-element set. Thus, we can apply Theorem 2.4.4 to $A \setminus \{a\}$ and k instead of A and m (since our induction hypothesis says that Theorem 2.4.4 holds for $m = k$). As a result, we obtain

$$(\#\text{ of injective maps from } A \setminus \{a\} \text{ to } B) = n^{\underline{k}}.$$

But $\operatorname{Inj}(A \setminus \{a\}, B)$ is the set of all injective maps from $A \setminus \{a\}$ to B (since this is how $\operatorname{Inj}(A \setminus \{a\}, B)$ is defined). Thus,

$$\begin{aligned} |\operatorname{Inj}(A \setminus \{a\}, B)| &= (\#\text{ of injective maps from } A \setminus \{a\} \text{ to } B) \\ &= n^{\underline{k}}. \end{aligned} \tag{158}$$

Now, if $h \in \operatorname{Inj}(A, B)$, then h is an injective map from A to B, and therefore the restriction $h\,|_{A \setminus \{a\}}$ of h to $A \setminus \{a\}$ is an injective map from $A \setminus \{a\}$ to B (since a restriction of an injective map to a subset is still injective). Thus, the map

$$\begin{aligned} R : \operatorname{Inj}(A, B) &\to \operatorname{Inj}(A \setminus \{a\}, B), \\ h &\mapsto h\,|_{A \setminus \{a\}} \end{aligned}$$

[152] *Proof.* Let m, n, A, B be as in Theorem 2.4.4, and assume that $m = 0$. We must prove the equality (156).

The set A is an m-element set; thus, $|A| = m = 0$. Hence, $A = \varnothing$. Thus, there is exactly one map from A to B (namely, the "empty map"); this map is clearly injective. Hence, there is exactly one injective map from A to B. In other words, $(\#\text{ of injective maps from } A \text{ to } B) = 1$. Comparing this with

$$\begin{aligned} n^{\underline{m}} &= n^{\underline{0}} \qquad (\text{since } m = 0) \\ &= 1 \qquad (\text{by Proposition 2.4.3 } \textbf{(a)}), \end{aligned}$$

we obtain $(\#\text{ of injective maps from } A \text{ to } B) = n^{\underline{m}}$. This proves the equality (156) under the assumption that $m = 0$. Hence, Theorem 2.4.4 holds when $m = 0$.

is well-defined. (All this map does is to restrict an injective map $h \in \operatorname{Inj}(A, B)$ to the subset $A \setminus \{a\}$. In other words, it "throws away" the value of the map at a.)

[*Example:* If $A = \{1,2,3\}$ and B is any set and $h = \begin{pmatrix} 1 & 2 & 3 \\ x & y & z \end{pmatrix}$ (a map from A to B in two-line notation) and $a = 2$, then $R(h) = h|_{\{1,3\}} = \begin{pmatrix} 1 & 3 \\ x & z \end{pmatrix}$.]

We now ask ourselves: For a given injective map $g \in \operatorname{Inj}(A \setminus \{a\}, B)$, how many injective maps $h \in \operatorname{Inj}(A, B)$ are there that satisfy $R(h) = g$? In other words, how many ways are there to extend a given injective map $g \in \operatorname{Inj}(A \setminus \{a\}, B)$ to an injective map $h \in \operatorname{Inj}(A, B)$? (The word "extends" here means that $h|_{A \setminus \{a\}}$ should be g, that is, $R(h) = g$.)

The answer to this question turns out to be nice – in particular, it does not depend on g:

Observation 1: Let $g \in \operatorname{Inj}(A \setminus \{a\}, B)$. Then,

$$(\#\text{ of maps } h \in \operatorname{Inj}(A, B) \text{ satisfying } R(h) = g) = n - k.$$

[*Proof of Observation 1:* Let us first argue informally: The map $g : A \setminus \{a\} \to B$ is injective (since $g \in \operatorname{Inj}(A \setminus \{a\}, B)$); thus, it has k different values (since $|A \setminus \{a\}| = k$). In other words, $|g(A \setminus \{a\})| = k$. Hence, $|B \setminus g(A \setminus \{a\})| = n - k$ (since $g(A \setminus \{a\})$ is a subset of the n-element set B).

To construct an $h \in \operatorname{Inj}(A, B)$ satisfying $R(h) = g$, we only need to choose a value $h(a)$ (since the condition $R(h) = g$ already forces all the other values of h to equal the corresponding values of g). This value $h(a)$ must be distinct from all values of g (in order for h to be injective); in other words, it has to belong to $B \setminus g(A \setminus \{a\})$. Thus, there are $n - k$ many options for $h(a)$ (since $|B \setminus g(A \setminus \{a\})| = n - k$). Hence, there are $n - k$ many maps $h \in \operatorname{Inj}(A, B)$ satisfying $R(h) = g$. This proves Observation 1.

Here is a formal version of this argument:

The map $g : A \setminus \{a\} \to B$ is injective (since $g \in \operatorname{Inj}(A \setminus \{a\}, B)$). However, if X and Y are two finite sets, and if $z : X \to Y$ is an injective map, then $|z(X)| = |X|$ [153]. Applying this to $X = A \setminus \{a\}$, $Y = B$ and $z = g$, we obtain $|g(A \setminus \{a\})| = |A \setminus \{a\}| = k$. But recall that $|B| = n$ (since B is an n-element set). Also, $g(A \setminus \{a\})$ is clearly a subset of B. Hence,

[153] *Proof.* This is a classical fact, with a simple proof: Let X and Y be two finite sets, and let $z : X \to Y$ be an injective map. Let $x_1, x_2, \ldots, x_p$ be all elements of X (listed without repetitions); then, the elements $x_1, x_2, \ldots, x_p$ are distinct, and $|X| = p$. But the map z is injective, and thus sends distinct elements to distinct elements. Hence, $z(x_1), z(x_2), \ldots, z(x_p)$ are distinct (since $x_1, x_2, \ldots, x_p$ are distinct). Therefore, the set $\{z(x_1), z(x_2), \ldots, z(x_p)\}$ has p distinct elements; in other words, $|\{z(x_1), z(x_2), \ldots, z(x_p)\}| = p$. But $X = \{x_1, x_2, \ldots, x_p\}$ (since $x_1, x_2, \ldots, x_p$ are all elements of X) and thus

$$z(X) = z(\{x_1, x_2, \ldots, x_p\}) = \{z(x_1), z(x_2), \ldots, z(x_p)\},$$

so that $|z(X)| = |\{z(x_1), z(x_2), \ldots, z(x_p)\}| = p = |X|$, qed.

Theorem 1.4.7 **(a)** (applied to B and $g(A \setminus \{a\})$ instead of A and B) yields

$$|B \setminus g(A \setminus \{a\})| = \underbrace{|B|}_{=n} - \underbrace{|g(A \setminus \{a\})|}_{=k} = n - k.$$

If $h \in \operatorname{Inj}(A, B)$ satisfies $R(h) = g$, then $h(a) \in B \setminus g(A \setminus \{a\})$ [154]. Hence, the map

$$\begin{aligned} \{h \in \operatorname{Inj}(A, B) \mid R(h) = g\} &\to B \setminus g(A \setminus \{a\}), \\ h &\mapsto h(a) \end{aligned} \tag{159}$$

is well-defined. It is easy to see that this map is a bijection[155]. Thus, the bijection principle yields

$$|\{h \in \operatorname{Inj}(A, B) \mid R(h) = g\}| = |B \setminus g(A \setminus \{a\})| = n - k.$$

Thus,

$$\begin{aligned} &(\#\text{ of maps } h \in \operatorname{Inj}(A, B) \text{ satisfying } R(h) = g) \\ &= |\{h \in \operatorname{Inj}(A, B) \mid R(h) = g\}| = n - k. \end{aligned}$$

Thus, Observation 1 is rigorously proven.]

Now, Theorem 1.2.5 (applied to $S = \operatorname{Inj}(A, B)$, $W = \operatorname{Inj}(A \setminus \{a\}, B)$ and $f = R$)

[154] *Proof.* Let $h \in \operatorname{Inj}(A, B)$ satisfy $R(h) = g$. Thus, $g = R(h) = h|_{A \setminus \{a\}}$ (by the definition of R), and furthermore, the map $h : A \to B$ is injective (since $h \in \operatorname{Inj}(A, B)$). Now, if we had $h(a) \in g(A \setminus \{a\})$, then there would exist some $u \in A \setminus \{a\}$ such that $h(a) = g(u)$. This u would then satisfy $h(a) = \underbrace{g}_{=h|_{A \setminus \{a\}}}(u) = \left(h|_{A \setminus \{a\}}\right)(u) = h(u)$ and thus $h(u) = h(a)$, which would lead to $u = a$ (since h is injective); but this would contradict $u \in A \setminus \{a\}$. Thus, we cannot have $h(a) \in g(A \setminus \{a\})$. Hence, $h(a) \notin g(A \setminus \{a\})$. Combining this with $h(a) \in B$, we obtain $h(a) \in B \setminus g(A \setminus \{a\})$, qed.

[155] Indeed, we can construct an inverse to it: For each $b \in B \setminus g(A \setminus \{a\})$, we let h_b be the map from A to B that sends each $c \in A$ to $\begin{cases} b, & \text{if } c = a; \\ g(c), & \text{if } c \neq a \end{cases}$. It is easy to see that this map h_b is injective. (In fact, its values at the elements of $A \setminus \{a\}$ are precisely the values of g, and thus are distinct because g is injective; but its value at a is b, which is distinct from its values at the elements of $A \setminus \{a\}$ because $b \notin g(A \setminus \{a\})$.) Hence, for each $b \in B \setminus g(A \setminus \{a\})$, we have defined an injective map h_b from A to B which furthermore satisfies $R(h_b) = g$ (since $h_b(c) = g(c)$ for all $c \in A \setminus \{a\}$). Thus, we obtain a map

$$\begin{aligned} B \setminus g(A \setminus \{a\}) &\to \{h \in \operatorname{Inj}(A, B) \mid R(h) = g\}, \\ b &\mapsto h_b. \end{aligned}$$

It is now completely straightforward to check that this map is inverse to the map (159).

yields

$$\begin{aligned}
|\mathrm{Inj}\,(A,B)| &= \sum_{w \in \mathrm{Inj}(A\setminus\{a\},B)} (\#\text{ of } s \in \mathrm{Inj}\,(A,B) \text{ satisfying } R(s) = w) \\
&= \sum_{g \in \mathrm{Inj}(A\setminus\{a\},B)} \underbrace{(\#\text{ of } h \in \mathrm{Inj}\,(A,B) \text{ satisfying } R(h) = g)}_{\substack{=(\#\text{ of maps } h \in \mathrm{Inj}(A,B) \text{ satisfying } R(h)=g) \\ =n-k \\ \text{(by Observation 1)}}} \\
&\qquad \text{(here, we have renamed the indices } w \text{ and } s \text{ as } g \text{ and } h) \\
&= \sum_{g \in \mathrm{Inj}(A\setminus\{a\},B)} (n-k) = \underbrace{|\mathrm{Inj}\,(A\setminus\{a\},B)|}_{\substack{=n^{\underline{k}} \\ \text{(by (158))}}} \cdot (n-k) \\
&= n^{\underline{k}} \cdot (n-k) = n^{\underline{k+1}} \qquad \text{(by Proposition 2.4.3 } \textbf{(f)}\text{)}.
\end{aligned}$$

But recall that $\mathrm{Inj}\,(A,B)$ is the set of all injective maps from A to B (since this is how $\mathrm{Inj}\,(A,B)$ is defined). Thus,

$$|\mathrm{Inj}\,(A,B)| = (\#\text{ of injective maps from } A \text{ to } B),$$

so that

$$(\#\text{ of injective maps from } A \text{ to } B) = |\mathrm{Inj}\,(A,B)| = n^{\underline{k+1}}.$$

Now, forget that we fixed n, A and B. We thus have shown that if $n \in \mathbb{N}$, if A is a $(k+1)$-element set, and if B is an n-element set, then

$$(\#\text{ of injective maps from } A \text{ to } B) = n^{\underline{k+1}}.$$

In other words, Theorem 2.4.4 holds for $m = k+1$. This completes the induction step. Thus, Theorem 2.4.4 is proven by induction. □

2.4.3. The pigeonhole principles

We shall now state two fundamental facts about maps between finite sets – the so-called *Pigeonhole Principles*. These facts are intuitively fairly self-evident, but we will nevertheless give rigorous proofs due to their importance.

The first of these facts is the *Pigeonhole Principle for Injections*:

Theorem 2.4.6 (Pigeonhole Principle for Injections)**.** Let A and B be two finite sets. Let $f : A \to B$ be an injective map. Then:
(a) We have $|A| \leq |B|$.
(b) If $|A| = |B|$, then f is bijective.

Proof of Theorem 2.4.6. Let $a_1, a_2, \ldots, a_k$ be the elements of A (listed without repetitions). Thus, the elements $a_1, a_2, \ldots, a_k$ are distinct and we have $|A| = k$. But the map f is injective, and thus sends distinct elements to distinct elements. Hence,

$f(a_1), f(a_2), \ldots, f(a_k)$ are distinct (since $a_1, a_2, \ldots, a_k$ are distinct). Hence, the set $\{f(a_1), f(a_2), \ldots, f(a_k)\}$ has k distinct elements. In other words,

$$|\{f(a_1), f(a_2), \ldots, f(a_k)\}| = k = |A|. \tag{160}$$

But $\{f(a_1), f(a_2), \ldots, f(a_k)\}$ is clearly a subset of B. Therefore, Theorem 1.4.7 **(b)** (applied to B and $\{f(a_1), f(a_2), \ldots, f(a_k)\}$ instead of A and B) yields

$$|\{f(a_1), f(a_2), \ldots, f(a_k)\}| \leq |B|.$$

Now, (160) shows that $|A| = |\{f(a_1), f(a_2), \ldots, f(a_k)\}| \leq |B|$. This proves Theorem 2.4.6 **(a)**.

(b) Assume that $|A| = |B|$. Then, (160) becomes $|\{f(a_1), f(a_2), \ldots, f(a_k)\}| = |A| = |B|$. Hence, Theorem 1.4.7 **(c)** (applied to B and $\{f(a_1), f(a_2), \ldots, f(a_k)\}$ instead of A and B) yields $\{f(a_1), f(a_2), \ldots, f(a_k)\} = B$. But this means that f is surjective[156]. Thus, f is bijective (since f is both injective and surjective). This proves Theorem 2.4.6 **(b)**. □

The following similar-looking theorem is known as the *Pigeonhole Principle for Surjections*:

Theorem 2.4.7 (Pigeonhole Principle for Surjections)**.** Let A and B be two finite sets. Let $f : A \to B$ be a surjective map. Then:
(a) We have $|A| \geq |B|$.
(b) If $|A| = |B|$, then f is bijective.

Proof of Theorem 2.4.7. Let $a_1, a_2, \ldots, a_k$ be the elements of A (listed without repetitions). Thus, $|A| = k$ and $A = \{a_1, a_2, \ldots, a_k\}$. The k elements $f(a_1), f(a_2), \ldots, f(a_k)$ may or may not be distinct; thus, the set $\{f(a_1), f(a_2), \ldots, f(a_k)\}$ has at most k elements[157]. In other words,

$$|\{f(a_1), f(a_2), \ldots, f(a_k)\}| \leq k = |A|. \tag{161}$$

But f is surjective; hence, $\{f(a_1), f(a_2), \ldots, f(a_k)\} = B$ [158]. Thus, (161) rewrites as $|B| \leq |A|$. In other words, $|A| \geq |B|$. This proves Theorem 2.4.7 **(a)**.

[156] *Proof.* Let $b \in B$. Then, $b \in B = \{f(a_1), f(a_2), \ldots, f(a_k)\}$. In other words, $b = f(a_i)$ for some $i \in [k]$. Consider this i. Thus, b is a value of f (namely, the value at a_i).

Forget that we fixed b. We thus have showed that each $b \in B$ is a value of f. In other words, f is surjective.

[157] Here, we are tacitly using the following fact: If $u_1, u_2, \ldots, u_k$ are any k objects (distinct or not), then the set $\{u_1, u_2, \ldots, u_k\}$ has at most k elements. Shouldn't this, too, be proved?

(Yes, but I am leaving this to the texts on foundations. That said, you can easily construct a proof by induction on k, using the even more fundamental fact that every finite set A and every object s satisfy $|A \cup \{s\}| = \begin{cases} |A|, & \text{if } s \in A; \\ |A| + 1, & \text{if } s \notin A \end{cases}$.)

[158] *Proof.* Let $b \in B$. Then, there exists some $a \in A$ such that $b = f(a)$ (since f is surjective). Consider this a. We have $a \in A = \{a_1, a_2, \ldots, a_k\}$. In other words, $a = a_i$ for some $i \in [k]$. Consider this i.

(b) Assume that $|A| = |B|$. We must prove that f is bijective. First, we shall show that f is injective.

Indeed, let x and y be two distinct elements of A. We shall show that $f(x) \neq f(y)$.

Indeed, assume the contrary. Thus, $f(x) = f(y)$. But $x \in A = \{a_1, a_2, \ldots, a_k\}$; thus, x can be written in the form $x = a_i$ for some $i \in [k]$. Likewise, y can be written in the form $y = a_j$ for some $j \in [k]$. Consider these i and j. If we had $i = j$, then we would have $a_i = a_j$ and thus $x = a_i = a_j = y$, which would contradict the fact that x and y are distinct. Hence, we must have $i \neq j$.

But recall that $f(x) = f(y)$. This rewrites as $f(a_i) = f(a_j)$ (since $x = a_i$ and $y = a_j$). Since $i \neq j$, this equality reveals that at least two of the k elements $f(a_1), f(a_2), \ldots, f(a_k)$ are equal (namely, $f(a_i)$ and $f(a_j)$). Therefore, there are at most $k-1$ distinct elements among these k elements $f(a_1), f(a_2), \ldots, f(a_k)$. In other words,

$$|\{f(a_1), f(a_2), \ldots, f(a_k)\}| \leq k-1.$$

[159] In view of $\{f(a_1), f(a_2), \ldots, f(a_k)\} = B$, this rewrites as $|B| \leq k-1$. Hence, $|B| \leq k-1 < k = |A| = |B|$. This is, of course, absurd. This contradiction shows that our assumption was false.

Hence, we have shown that $f(x) \neq f(y)$.

Now, $b = f\left(\underbrace{a}_{=a_i}\right) = f(a_i) \in \{f(a_1), f(a_2), \ldots, f(a_k)\}$.

Forget that we fixed b. We thus have shown that $b \in \{f(a_1), f(a_2), \ldots, f(a_k)\}$ for each $b \in B$. In other words, $B \subseteq \{f(a_1), f(a_2), \ldots, f(a_k)\}$. Combining this with $\{f(a_1), f(a_2), \ldots, f(a_k)\} \subseteq B$ (which is obvious), we obtain $\{f(a_1), f(a_2), \ldots, f(a_k)\} = B$.

[159] If you insist on proving this more formally than this, here is the argument that we tacitly used here: Let G be the set

$$\{f(a_1), f(a_2), \ldots, f(a_{j-1}), f(a_{j+1}), f(a_{j+2}), \ldots, f(a_k)\} = \{f(a_p) \mid p \in [k] \setminus \{j\}\},$$

which collects all of the k elements $f(a_1), f(a_2), \ldots, f(a_k)$ except for the j-th one. This set G clearly has size $|G| \leq k-1$ (because $f(a_1), f(a_2), \ldots, f(a_{j-1}), f(a_{j+1}), f(a_{j+2}), \ldots, f(a_k)$ are $k-1$ elements). Since $i \neq j$, the element $f(a_i)$ is one of the $k-1$ elements $f(a_1), f(a_2), \ldots, f(a_{j-1}), f(a_{j+1}), f(a_{j+2}), \ldots, f(a_k)$ that constitute the set G (because $i \neq j$ entails $i \in [k] \setminus \{j\}$), and thus belongs to G. Therefore, $\{f(a_i)\} \subseteq G$, so that $G \cup \{f(a_i)\} = G$. Hence,

$$\begin{aligned}
G &= G \cup \{f(a_i)\} = G \cup \{f(a_j)\} \qquad (\text{since } f(a_i) = f(a_j)) \\
&= \{f(a_1), f(a_2), \ldots, f(a_{j-1}), f(a_{j+1}), f(a_{j+2}), \ldots, f(a_k)\} \cup \{f(a_j)\} \\
&\qquad (\text{since } G = \{f(a_1), f(a_2), \ldots, f(a_{j-1}), f(a_{j+1}), f(a_{j+2}), \ldots, f(a_k)\}) \\
&= \{f(a_1), f(a_2), \ldots, f(a_{j-1}), f(a_{j+1}), f(a_{j+2}), \ldots, f(a_k), f(a_j)\} \\
&= \{f(a_1), f(a_2), \ldots, f(a_k)\}
\end{aligned}$$

(because the k elements $f(a_1), f(a_2), \ldots, f(a_{j-1}), f(a_{j+1}), f(a_{j+2}), \ldots, f(a_k), f(a_j)$ are exactly the k elements $f(a_1), f(a_2), \ldots, f(a_k)$, up to order). Thus, the inequality $|G| \leq k-1$, which we have previously proved, rewrites as $|\{f(a_1), f(a_2), \ldots, f(a_k)\}| \leq k-1$.

Now, forget that we fixed x and y. We thus have proved that if x and y are two distinct elements of A, then $f(x) \neq f(y)$. In other words, the map f sends distinct elements to distinct elements. In other words, f is injective.

Hence, f is bijective (since f is both injective and surjective). This proves Theorem 2.4.7 **(b)**. □

Remark 2.4.8. The parts **(b)** of both Pigeonhole Principles become false if the sets A and B are not finite. For example:

- The map $\mathbb{N} \to \mathbb{N}$, $i \mapsto i+1$ is injective, but not bijective. Thus, Theorem 2.4.6 **(b)** fails if A and B are infinite.
- The map $\mathbb{N} \to \mathbb{N}$, $i \mapsto \begin{cases} 0, & \text{if } i = 0; \\ i-1, & \text{if } i > 0 \end{cases}$ is surjective, but not bijective. Thus, Theorem 2.4.7 **(b)** fails if A and B are infinite.

2.4.4. Permutations

We can now prove Theorem 1.7.2:

Proof of Theorem 1.7.2. The set X is finite (since it is an n-element set) and satisfies $|X| = |X|$. Hence, Theorem 2.4.6 **(b)** shows that if $f : X \to X$ is an injective map, then f is bijective. In other words, every injective map from X to X is bijective. The converse also holds (by definition). Thus, the injective maps from X to X are precisely the bijective maps from X to X. Hence,

$$\begin{aligned} &\{\text{injective maps from } X \text{ to } X\} = \{\text{bijective maps from } X \text{ to } X\} \\ &\qquad = \{\text{bijections from } X \text{ to } X\} = \{\text{permutations of } X\} \end{aligned}$$

(because the permutations of X are defined to be the bijections from X to X). Hence,

$$(\#\text{ of injective maps from } X \text{ to } X) = (\#\text{ of permutations of } X).$$

But Theorem 2.4.4 (applied to $m = n$, $A = X$ and $B = X$) shows that

$$(\#\text{ of injective maps from } X \text{ to } X) = n^{\underline{n}} = n!$$

(by Proposition 2.4.3 **(d)**). Comparing these two equalities, we obtain

$$(\#\text{ of permutations of } X) = n!.$$

This proves Theorem 1.7.2. □

2.4.5. Surjective maps

After having counted injective maps, let us count surjective maps. The answer will not be as simple as the one we obtained for injective maps in Theorem 2.4.4. First, we introduce a notation (which we already have used in Theorem 1.2.10):

Definition 2.4.9. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Then, $\operatorname{sur}(m,n)$ shall mean the # of surjective maps from $[m]$ to $[n]$.

Example 2.4.10. We have $\operatorname{sur}(3,2) = 6$, because there are exactly 6 surjective maps from $[3]$ to $[2]$; namely, these maps are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix}$$

(written in two-line notation).

A priori, these numbers $\operatorname{sur}(m,n)$ only count surjective maps between the specific finite sets $[m]$ and $[n]$; but it is easy to see that they also count surjective maps between any two finite sets:

Proposition 2.4.11. Let $m, n \in \mathbb{N}$. Let A be an m-element set. Let B be an n-element set. Then,

$$(\#\text{ of surjective maps from } A \text{ to } B) = \operatorname{sur}(m,n).$$

Proof of Proposition 2.4.11 (sketched). This is a relabeling argument, similar to our proof of Lemma 1.7.6: Relabel the m elements of A as $1, 2, \ldots, m$, and relabel the n elements of B as $1, 2, \ldots, n$. The details are LTTR.[160] □

[160] For the formal proof, you have to construct a bijection from the set $\{\text{surjective maps from } A \text{ to } B\}$ to the set $\{\text{surjective maps from } [m] \text{ to } [n]\}$. Here is how to do this:

We have $|A| = m$ (since A is an m-element set) and $|[m]| = m$, so that $|A| = m = |[m]|$. Thus, the sets A and $[m]$ have the same size. Hence, Theorem 1.1.7 (applied to $X = A$ and $Y = [m]$) shows that there is a bijection $\alpha : A \to [m]$. Likewise, there is a bijection $\beta : B \to [n]$. Consider these α and β. Now, it is easy to see that the maps

$$\{\text{surjective maps from } A \text{ to } B\} \to \{\text{surjective maps from } [m] \text{ to } [n]\},$$
$$f \mapsto \beta \circ f \circ \alpha^{-1}$$

and

$$\{\text{surjective maps from } [m] \text{ to } [n]\} \to \{\text{surjective maps from } A \text{ to } B\},$$
$$f \mapsto \beta^{-1} \circ f \circ \alpha$$

are well-defined and mutually inverse; thus, they are bijections. Hence, the bijection principle

Recall that "surjection" is a shorthand for "surjective map". Thus, for any $m, n \in \mathbb{N}$, we have

$$\begin{aligned}&(\text{\# of surjections from } [m] \text{ to } [n])\\ &= (\text{\# of surjective maps from } [m] \text{ to } [n]) = \operatorname{sur}(m,n)\end{aligned} \tag{162}$$

(since $\operatorname{sur}(m,n)$ is defined as the # of surjective maps from $[m]$ to $[n]$).

Let us next determine some values of $\operatorname{sur}(m,n)$ (with heavy use of Iverson brackets):

Proposition 2.4.12. **(a)** We have $\operatorname{sur}(m,0) = [m=0]$ for all $m \in \mathbb{N}$.
(b) We have $\operatorname{sur}(m,1) = [m \neq 0] = 1 - [m=0]$ for all $m \in \mathbb{N}$.
(c) We have $\operatorname{sur}(m,2) = 2^m - 2 + [m=0]$ for all $m \in \mathbb{N}$.
(d) We have $\operatorname{sur}(0,k) = [k=0]$ for all $k \in \mathbb{N}$.
(e) We have $\operatorname{sur}(1,k) = [k=1]$ for all $k \in \mathbb{N}$.
(f) We have $\operatorname{sur}(m,n) = 0$ for all $m, n \in \mathbb{N}$ satisfying $m < n$.

Proving this proposition is an easy exercise in understanding what surjectivity of maps means (as well as applying Theorem 2.4.1 and Theorem 2.4.7 **(a)**):

Proof of Proposition 2.4.12. The set $[0]$ is empty. Thus, there is exactly one map from $[0]$ to $[0]$ (namely, the "empty map", which sends nothing anywhere). This map is surjective[161]. Hence, there is exactly one surjective map from $[0]$ to $[0]$. In other words, $\operatorname{sur}(0,0) = 1$ (since $\operatorname{sur}(0,0)$ is defined as the # of surjective maps from $[0]$ to $[0]$). Comparing $\operatorname{sur}(0,0) = 1$ with $[0=0] = 1$, we obtain $\operatorname{sur}(0,0) = [0=0]$.

(a) Let $m \in \mathbb{N}$. Recall that $\operatorname{sur}(0,0) = [0=0]$. In other words, Proposition 2.4.12 **(a)** holds for $m = 0$. Thus, for the rest of this proof, we WLOG assume that $m \neq 0$. Hence, $m > 0$ (since $m \in \mathbb{N}$). Thus, $1 \in [m]$. Hence, there exists no map from $[m]$ to $[0]$ (because such a map would have to send 1 to some element of $[0]$, but there is no element of $[0]$ to send it to). Thus, a fortiori, there exists no surjective map from $[m]$ to $[0]$. In other words, $\operatorname{sur}(m,0) = 0$ (since $\operatorname{sur}(m,0)$ is defined as the # of surjective maps from $[m]$ to $[0]$). Comparing this with $[m=0] = 0$ (which follows from $m \neq 0$), we obtain $\operatorname{sur}(m,0) = [m=0]$. Thus, Proposition 2.4.12 **(a)** is proved.

(f) Let $m, n \in \mathbb{N}$ be such that $m < n$. Theorem 2.4.7 **(a)** (applied to $A = [m]$ and $B = [n]$) shows that if $f : [m] \to [n]$ is a surjective map, then $|[m]| \geq |[n]|$; but this contradicts $|[m]| = m < n = |[n]|$. Thus, we obtain a contradiction for each surjective map $f : [m] \to [n]$. Hence, there exists no such map. In other words, there is no surjective map from $[m]$ to $[n]$. In other words, $\operatorname{sur}(m,n) = 0$ (since $\operatorname{sur}(m,n)$ is defined as the # of surjective maps from $[m]$ to $[n]$). This proves Proposition 2.4.12 **(f)**.

---

yields

$$\begin{aligned}&(\text{\# of surjective maps from } A \text{ to } B)\\ &= (\text{\# of surjective maps from } [m] \text{ to } [n]) = \operatorname{sur}(m,n)\end{aligned}$$

(since $\operatorname{sur}(m,n)$ was defined to be the # of surjective maps from $[m]$ to $[n]$).

[161] Indeed, a map $f : A \to B$ (where A and B are two sets) is surjective if and only if each element of B lies in its image. If the set B is empty, then this is vacuously true.

(d) Let $k \in \mathbb{N}$. Recall that $\operatorname{sur}(0,0) = [0=0]$. In other words, Proposition 2.4.12 **(d)** holds for $k = 0$. Hence, for the rest of this proof, we WLOG assume that $k \neq 0$. Hence, $k > 0$ (since $k \in \mathbb{N}$), so that $0 < k$. Thus, Proposition 2.4.12 **(f)** (applied to $m = 0$ and $n = k$) yields $\operatorname{sur}(0,k) = 0$. Comparing this with $[k=0] = 0$ (which follows from $k \neq 0$), we obtain $\operatorname{sur}(0,k) = [k=0]$. This proves Proposition 2.4.12 **(d)**.

(b) Let $m \in \mathbb{N}$. We need to prove the chain of equalities $\operatorname{sur}(m,1) = [m \neq 0] = 1 - [m=0]$. The second of these equalities is easily checked[162]. Thus, it remains to prove the first equality, i.e., the equality $\operatorname{sur}(m,1) = [m \neq 0]$.

Proposition 2.4.12 **(d)** (applied to $k = 1$) yields $\operatorname{sur}(0,1) = [1=0] = 0$ (since $1 \neq 0$). Comparing this with $[0 \neq 0] = 0$ (since $0 = 0$), we obtain $\operatorname{sur}(0,1) = [0 \neq 0]$. In other words, the equality $\operatorname{sur}(m,1) = [m \neq 0]$ (which we intend to prove) holds for $m = 0$. Thus, for the rest of this proof, we WLOG assume that $m \neq 0$. Hence, $m > 0$ (since $m \in \mathbb{N}$), so that $1 \in [m]$. Now, the set $[1]$ has only one element, namely 1. Thus, there is exactly one map from $[m]$ to $[1]$: namely, the map f that sends each element of $[m]$ to 1 (because the only possible value for this map is 1). This map is surjective, because the only element of $[1]$ (namely, 1) is a value of this map (indeed, it is the value of this map at $1 \in [m]$). Thus, there is exactly one surjective map from $[m]$ to $[1]$. In other words, $\operatorname{sur}(m,1) = 1$ (since $\operatorname{sur}(m,1)$ is defined as the # of surjective maps from $[m]$ to $[1]$). Comparing this with $[m \neq 0] = 1$ (which follows from $m \neq 0$), we obtain $\operatorname{sur}(m,1) = [m \neq 0]$. This completes our proof of Proposition 2.4.12 **(b)**.

(e) Let $k \in \mathbb{N}$. Proposition 2.4.12 **(b)** (applied to $m = 1$) yields $\operatorname{sur}(1,1) = [1 \neq 0] = 1 - [1=0]$. Hence, $\operatorname{sur}(1,1) = [1 \neq 0] = 1$ (since $1 \neq 0$). Compared with $[1=1] = 1$, this yields $\operatorname{sur}(1,1) = [1=1]$. In other words, Proposition 2.4.12 **(e)** holds for $k = 1$. Hence, for the rest of this proof, we WLOG assume that $k \neq 1$.

Proposition 2.4.12 **(a)** (applied to $m = 1$) yields $\operatorname{sur}(1,0) = [1=0] = 0$ (since $1 \neq 0$). Compared with $[0=1] = 0$, this yields $\operatorname{sur}(1,0) = [0=1]$. In other words, Proposition 2.4.12 **(e)** holds for $k = 0$. Hence, for the rest of this proof, we WLOG assume that $k \neq 0$.

We now have $k \neq 0$ and $k \neq 1$. Hence, $k \geq 2$ (since $k \in \mathbb{N}$). Thus, $k \geq 2 > 1$, so that $1 < k$. Hence, Proposition 2.4.12 **(f)** (applied to $m = 1$ and $n = k$) yields $\operatorname{sur}(1,k) = 0$. Comparing this with $[k=1] = 0$ (which is because $k \neq 1$), we obtain $\operatorname{sur}(1,k) = [k=1]$. This proves Proposition 2.4.12 **(e)**.

(c) Let $m \in \mathbb{N}$. Proposition 2.4.12 **(d)** (applied to $k = 2$) yields $\operatorname{sur}(0,2) = [2=0] = 0$. Comparing this with $\underbrace{2^0}_{=1} - 2 + \underbrace{[0=0]}_{=1} = 1 - 2 + 1 = 0$, we obtain $\operatorname{sur}(0,2) = 2^0 - 2 + [0=0]$. Thus, Proposition 2.4.12 **(c)** holds for $m = 0$. Hence, for the rest of this proof, we WLOG assume that $m \neq 0$. Hence, $1 \in [m]$. Now, Theorem 2.4.1 (applied to $n = 2$, $A = [m]$ and $B = [2]$) yields

$$(\#\text{ of maps from } [m] \text{ to } [2]) = 2^m.$$

In other words, there are exactly 2^m maps from $[m]$ to $[2]$. Which of these 2^m maps are surjective? Obviously, in order for a map $f : [m] \to [2]$ to be surjective, it suffices that both 1 and 2 appear as its values; in other words, it must avoid sending all elements of $[m]$ to 1, and it must avoid sending all elements of $[m]$ to 2. Thus, among the 2^m maps from $[m]$ to $[2]$, only two fail to be surjective: namely, the map α that sends all elements of $[m]$ to 1,

[162] Indeed, it is a particular case of the equality $[\text{not } \mathcal{A}] = 1 - [\mathcal{A}]$, which holds for any logical statement $\mathcal{A}$. Applying the latter equality to $\mathcal{A} =$ ("$m = 0$"), we obtain $[\text{not } (m=0)] = 1 - [m=0]$. In other words, $[m \neq 0] = 1 - [m=0]$.

and the map β that sends all elements of $[m]$ to 2. Moreover, these two maps α and β are distinct (because $\alpha(1) = 1 \neq 2 = \beta(1)$). Hence, exactly 2 out of the 2^m maps from $[m]$ to $[2]$ fail to be surjective. Thus,

$$(\#\text{ of surjective maps from } [m] \text{ to } [2]) = 2^m - 2.$$

This rewrites as $\operatorname{sur}(m,2) = 2^m - 2$ (since $\operatorname{sur}(m,2)$ is defined as the # of surjective maps from $[m]$ to $[2]$). Compared with $2^m - 2 + \underbrace{[m=0]}_{\substack{=0 \\ (\text{since } m \neq 0)}} = 2^m - 2$, this yields $\operatorname{sur}(m,2) = 2^m - 2 + [m=0]$. Thus, Proposition 2.4.12 **(c)** is proved. □

Proposition 2.4.12 gives us many values of $\operatorname{sur}(m,n)$, but far from all of them – and certainly not the most interesting ones. For example, what is $\operatorname{sur}(30,20)$?

It thus is reasonable to look for a recursive formula for $\operatorname{sur}(m,n)$. We shall show two different approaches to this question, giving two different recursive formulas.

1st approach: Fix $m \in \mathbb{N}$ and a positive integer $n > 0$. Thus, $n \in [n]$.

Given a surjective map $f : [m] \to [n]$, we let J_f be the set of all $i \in [m]$ such that $f(i) = n$. [163] Clearly, this set J_f is a subset of $[m]$ and satisfies $J_f \neq \varnothing$ (since f is surjective, so there exists at least one $i \in [m]$ such that $f(i) = n$). Thus, the sum rule yields

$$\begin{aligned}&(\#\text{ of all surjective maps } f : [m] \to [n]) \\ &= \sum_{\substack{J \subseteq [m]; \\ J \neq \varnothing}} \left(\#\text{ of all surjective maps } f : [m] \to [n] \text{ satisfying } J_f = J\right). \end{aligned} \tag{163}$$

Now, fix a subset J of $[m]$ that satisfies $J \neq \varnothing$. What is the # of all surjective maps $f : [m] \to [n]$ satisfying $J_f = J$? Such a map f must satisfy

$$J = J_f = \{i \in [m] \mid f(i) = n\} \qquad \left(\text{by the definition of } J_f\right).$$

In other words, such a map f must send all elements of J, but no other elements, to n. In other words, it must send all elements of J to n, and send all other elements of $[m]$ to numbers different from n. The latter numbers are, of course, the elements of $[n] \setminus \{n\} = [n-1]$. Thus, a surjective map $f : [m] \to [n]$ satisfying $J_f = J$ must send all elements of J to n, and send all elements of $[m] \setminus J$ to elements of $[n-1]$. Hence, if f is such a map, then f is uniquely determined by its values at the elements of $[m] \setminus J$, and said values must belong to $[n-1]$. In other words, if f is such a map, then f is uniquely determined by its restriction $f\mid_{[m]\setminus J}$, and furthermore this restriction must "actually" be a map from $[m] \setminus J$ to $[n-1]$, in the sense that all its values belong to $[n-1]$. Moreover, in order for the map f to

[163] For example, if $m = 4$ and $n = 3$, and if $f : [m] \to [n]$ is the surjective map written in two-line notation as $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 3 & 2 \end{pmatrix}$, then $J_f = \{1,3\}$, because 1 and 3 are precisely the $i \in [4]$ such that $f(i) = 3$.

be surjective, all of the numbers $1, 2, \ldots, n$ must be values of f. Since $J \neq \varnothing$, we know that n will always be a value of f (indeed, f sends any element of J to n, and there is at least one element of J, since $J \neq \varnothing$); we thus only need to ensure that $1, 2, \ldots, n-1$ are values of f as well. Obviously, these values must be taken at elements of $[m] \setminus J$ (because f sends all elements of J to n). In other words, if we restrict f to the set $[m] \setminus J$, then the resulting map $f\mid_{[m]\setminus J}\colon [m] \setminus J \to [n]$ needs to take all the numbers $1, 2, \ldots, n-1$ as values; i.e., if we consider $f\mid_{[m]\setminus J}$ as a map from $[m] \setminus J$ to $[n-1]$, then $f\mid_{[m]\setminus J}$ should be surjective. Thus, in order to construct a surjective map $f : [m] \to [n]$ satisfying $J_f = J$, we need to construct a surjective map from $[m] \setminus J$ to $[n-1]$. Hence,

$$\begin{aligned}&\left(\text{\# of all surjective maps } f : [m] \to [n] \text{ satisfying } J_f = J\right)\\ &= \left(\text{\# of all surjective maps from } [m] \setminus J \text{ to } [n-1]\right). \end{aligned} \tag{164}$$

(Formally speaking, this can be proved using the bijection principle[164].)

On the other hand, $J \subseteq [m]$, and thus an application of Theorem 1.4.7 **(a)** yields $|[m] \setminus J| = \underbrace{|[m]|}_{=m} - |J| = m - |J|$. Thus, $[m] \setminus J$ is an $(m-|J|)$-element set. Also, $[n-1]$ is an $(n-1)$-element set (since n is a positive integer, so that $n-1 \in \mathbb{N}$). Hence, Proposition 2.4.11 (applied to $[m] \setminus J$, $[n-1]$, $|[m] \setminus J|$, and $|[n-1]|$ instead of A, B, m and n) yields

$$\left(\text{\# of all surjective maps } [m] \setminus J \to [n-1]\right) = \operatorname{sur}\left(m - |J|, n-1\right).$$

Thus, (164) becomes

$$\begin{aligned}&\left(\text{\# of all surjective maps } f : [m] \to [n] \text{ satisfying } J_f = J\right)\\ &= \left(\text{\# of all surjective maps from } [m] \setminus J \text{ to } [n-1]\right)\\ &= \operatorname{sur}\left(m - |J|, n-1\right). \end{aligned} \tag{165}$$

Now, forget that we fixed J. We thus have proved (165) for each subset J of $[m]$

[164] More precisely, we need to apply the bijection principle to the bijection

$$\left\{\text{surjective maps } f : [m] \to [n] \text{ satisfying } J_f = J\right\} \to \left\{\text{surjective maps from } [m] \setminus J \text{ to } [n-1]\right\}$$

that sends each f to its restriction $f\mid_{[m]\setminus J}$ (considered as a map from $[m] \setminus J$ to $[n-1]$).

Here, of course, we are using the fact that if $f : [m] \to [n]$ satisfies $J_f = J$, then the restriction $f\mid_{[m]\setminus J}$ can be considered as a map from $[m] \setminus J$ to $[n-1]$, since it does not take the value n.

satisfying $J \neq \varnothing$. Hence, (163) becomes

$$\begin{aligned}
&(\#\text{ of all surjective maps } f : [m] \to [n]) \\
&= \sum_{\substack{J \subseteq [m]; \\ J \neq \varnothing}} \underbrace{\left(\#\text{ of all surjective maps } f : [m] \to [n] \text{ satisfying } J_f = J\right)}_{\substack{= \operatorname{sur}(m-|J|, n-1) \\ \text{(by (165))}}} \\
&= \sum_{\substack{J \subseteq [m]; \\ J \neq \varnothing}} \operatorname{sur}\left(m - |J|, n-1\right) = \underbrace{\sum_{j \in \{1,2,\ldots,m\}}}_{= \sum_{j=1}^{m}} \sum_{\substack{J \subseteq [m]; \\ J \neq \varnothing; \\ |J| = j}} \operatorname{sur}\left(m - \underbrace{|J|}_{=j}, n-1\right) \\
&\qquad \left(\begin{array}{c} \text{here, we have split the sum according to the value of } |J|, \\ \text{because each subset } J \text{ of } [m] \text{ satisfying } J \neq \varnothing \text{ (that is,} \\ \text{each nonempty subset } J \text{ of } [m]) \text{ satisfies } |J| \in \{1, 2, \ldots, m\} \\ \text{(since } J \subseteq [m] \text{ entails } |J| \leq m, \text{ whereas } J \neq \varnothing \text{ entails } |J| \geq 1) \end{array} \right) \\
&= \sum_{j=1}^{m} \underbrace{\sum_{\substack{J \subseteq [m]; \\ J \neq \varnothing; \\ |J| = j}} \operatorname{sur}\left(m-j, n-1\right)}_{= (\#\text{ of } J \subseteq [m] \text{ such that } J \neq \varnothing \text{ and } |J| = j) \cdot \operatorname{sur}(m-j, n-1)} \\
&= \sum_{j=1}^{m} (\#\text{ of } J \subseteq [m] \text{ such that } J \neq \varnothing \text{ and } |J| = j) \cdot \operatorname{sur}\left(m-j, n-1\right). \qquad (166)
\end{aligned}$$

We shall next simplify the # on the right hand side of this equation. Indeed, let $j \in [m]$. Thus, $j \geq 1 > 0$. Hence, each subset J of $[m]$ satisfying $|J| = j$ must automatically be nonempty (since $|J| = j > 0$); in other words, it must satisfy $J \neq \varnothing$. Thus, the requirement $J \neq \varnothing$ in "# of $J \subseteq [m]$ such that $J \neq \varnothing$ and $|J| = j$" is redundant. Hence,

$$\begin{aligned}
&(\#\text{ of } J \subseteq [m] \text{ such that } J \neq \varnothing \text{ and } |J| = j) \\
&= (\#\text{ of } J \subseteq [m] \text{ such that } |J| = j) \\
&= (\#\text{ of } j\text{-element subsets of } [m]) = \binom{m}{j} \qquad (167)
\end{aligned}$$

(by Theorem 1.3.12, applied to m, j and $[m]$ instead of n, k and S).

Forget that we fixed j. We thus have proved (167) for each $j \in [m]$. Hence, (166)

becomes

$$\begin{aligned}
&(\#\text{ of all surjective maps } f : [m] \to [n]) \\
&= \sum_{j=1}^{m} \underbrace{(\#\text{ of } J \subseteq [m] \text{ such that } J \neq \varnothing \text{ and } |J| = j)}_{= \binom{m}{j} \text{ (by (167))}} \cdot \operatorname{sur}(m-j, n-1) \\
&= \sum_{j=1}^{m} \underbrace{\binom{m}{j}}_{= \binom{m}{m-j} \text{ (by Theorem 1.3.11, applied to } m \text{ and } j \text{ instead of } n \text{ and } k)} \cdot \operatorname{sur}(m-j, n-1) = \sum_{j=1}^{m} \binom{m}{m-j} \cdot \operatorname{sur}(m-j, n-1) \\
&= \sum_{j=0}^{m-1} \binom{m}{j} \cdot \operatorname{sur}(j, n-1)
\end{aligned}$$

(here, we have substituted $m-j$ for j in the sum). Hence,

$$\begin{aligned}
\operatorname{sur}(m,n) &= (\#\text{ of all surjective maps } f : [m] \to [n]) \\
&= \sum_{j=1}^{m} \binom{m}{j} \cdot \operatorname{sur}(m-j, n-1) = \sum_{j=0}^{m-1} \binom{m}{j} \cdot \operatorname{sur}(j, n-1).
\end{aligned}$$

Forget that we fixed m and n. Thus, we have proved the following recursive formula for the numbers $\operatorname{sur}(m,n)$:

Proposition 2.4.13. Let $m \in \mathbb{N}$, and let n be a positive integer. Then,

$$\operatorname{sur}(m,n) = \sum_{j=1}^{m} \binom{m}{j} \cdot \operatorname{sur}(m-j, n-1) = \sum_{j=0}^{m-1} \binom{m}{j} \cdot \operatorname{sur}(j, n-1).$$

Using this proposition and Proposition 2.4.12 **(a)**, it is easy to compute $\operatorname{sur}(m,n)$ recursively.

Class of 2019-10-23

2nd approach: Here is another way to get a recursive formula for $\operatorname{sur}(m,n)$.

Fix two positive integers m and n. Let us classify the surjections $[m] \to [n]$ according to the image of m.

A surjection $f : [m] \to [n]$ will be called

- **red** if $f(m) = f(i)$ for some $i \in [m-1]$;
- **green** if it is not red (i.e., if $f(m) \neq f(i)$ for all $i \in [m-1]$).

[*Examples:* If $m = 4$ and $n = 3$, then the surjection $f_1 : [m] \to [n]$ written in two-line notation as $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 2 \end{pmatrix}$ is red (since $f_1(m) = f_1(1)$ with $1 \in [m-1]$), while the surjection $f_2 : [m] \to [n]$ written in two-line notation as $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 2 & 3 \end{pmatrix}$ is green (since $f_2(m) = 3 \neq f_2(i)$ for all $i \in [m-1]$).]

If $f : [m] \to [n]$ is a red surjection, then its restriction $f|_{[m-1]} : [m-1] \to [n]$ is "still" a surjection[165]. Conversely, if $f : [m] \to [n]$ is any map whose restriction $f|_{[m-1]} : [m-1] \to [n]$ is a surjection, then f must be a red surjection[166].

Thus, we get the following algorithm for constructing a red surjection $f : [m] \to [n]$:

- first, we choose $f(m)$ (there are n choices for this, since we want $f(m) \in [n]$);
- then, we choose $f(1), f(2), \ldots, f(m-1)$; in other words, we choose the restriction $f|_{[m-1]}$ (there are $\operatorname{sur}(m-1, n)$ choices for this, since $f|_{[m-1]}$ has to be a surjection from $[m-1]$ to $[n]$).

Hence, the dependent product rule yields

$$(\#\text{ of red surjections } f : [m] \to [n]) = n \cdot \operatorname{sur}(m-1, n). \tag{168}$$

[165] *Formal proof.* Let $f : [m] \to [n]$ be a red surjection. Then, f is surjective; thus, $f([m]) = [n]$. Also, $f(m) = f(i)$ for some $i \in [m-1]$ (since f is red). Consider this i. From $i \in [m-1] = \{1, 2, \ldots, m-1\}$, we obtain $f(i) \in \{f(1), f(2), \ldots, f(m-1)\}$. Hence, $f(m) = f(i) \in \{f(1), f(2), \ldots, f(m-1)\}$, so that $\{f(m)\} \subseteq \{f(1), f(2), \ldots, f(m-1)\}$.

Now, the image of the restriction $f|_{[m-1]}$ is the set

$$\left(f|_{[m-1]}\right)([m-1]) = \left\{ \underbrace{\left(f|_{[m-1]}\right)(j)}_{\substack{=f(j) \\ (\text{since } f|_{[m-1]} \text{ is a restriction of } f)}} \mid j \in [m-1] \right\} = \{f(j) \mid j \in [m-1]\}$$

$$= \{f(1), f(2), \ldots, f(m-1)\} = \{f(1), f(2), \ldots, f(m-1)\} \cup \{f(m)\}$$

$$\left(\text{since } \{f(m)\} \subseteq \{f(1), f(2), \ldots, f(m-1)\}\right)$$

$$= \{f(1), f(2), \ldots, f(m-1), f(m)\} = \{f(1), f(2), \ldots, f(m)\} = f([m]) = [n]$$

(since f is surjective). Thus, the map $f|_{[m-1]} : [m-1] \to [n]$ is surjective. In other words, $f|_{[m-1]} : [m-1] \to [n]$ is a surjection.

[166] Check this! (The idea is: Since $f|_{[m-1]} : [m-1] \to [n]$ is surjective, we know that each element of $[n]$ is a value of f at one of the numbers $1, 2, \ldots, m-1$. Hence, f is surjective. Moreover, $f(m) \in [n]$ must also be a value of $f|_{[m-1]}$ (since $f|_{[m-1]}$ is surjective); but this is saying that $f(m) = f(i)$ for some $i \in [m-1]$. This shows that the surjection f is red.)

(You might want to see how this argument can be formalized without speaking of "choices". See Exercise 2.4.2 further below for the answer.)

On the other hand, if $f : [m] \to [n]$ is a green surjection, then the restriction $f\mid_{[m-1]}$ has image $[n] \setminus \{f(m)\}$ [167], and thus can be viewed as a surjection $[m-1] \to [n] \setminus \{f(m)\}$. Conversely, if $f : [m] \to [n]$ is any map whose restriction $f\mid_{[m-1]}$ is a surjection from $[m-1]$ to $[n] \setminus \{f(m)\}$, then f must be a green surjection[168]. Hence, we get the following algorithm for constructing a green surjection $f : [m] \to [n]$:

- first, we choose $f(m)$ (there are n choices);
- then, we choose $f(1), f(2), \ldots, f(m-1)$; in other words, we choose the restriction $f\mid_{[m-1]}$ (there are $\operatorname{sur}(m-1, n-1)$ choices for this, because $f\mid_{[m-1]}$ needs to be a surjection $[m-1] \to [n] \setminus \{f(m)\}$, and Proposition 2.4.11 shows that the # of such surjections is $\operatorname{sur}\left(\underbrace{|[m-1]|}_{=m-1}, \underbrace{|[n] \setminus \{f(m)\}|}_{=n-1}\right) = \operatorname{sur}(m-1, n-1)$).

Hence,

$$(\#\text{ of green surjections } f : [m] \to [n]) = n \cdot \operatorname{sur}(m-1, n-1). \tag{169}$$

(Again, see Exercise 2.4.2 further below for a rigorous proof of this equality.)
Hence, (162) becomes

$$\begin{aligned}
&\operatorname{sur}(m, n) \\
&= (\#\text{ of surjections } f : [m] \to [n]) \\
&= \underbrace{(\#\text{ of red surjections } f : [m] \to [n])}_{\substack{=n\cdot\operatorname{sur}(m-1,n) \\ \text{(by (168))}}} + \underbrace{(\#\text{ of green surjections } f : [m] \to [n])}_{\substack{=n\cdot\operatorname{sur}(m-1,n-1) \\ \text{(by (169))}}} \\
&\qquad \left(\begin{array}{c}\text{since each surjection } f : [m] \to [n] \text{ is either red or green} \\ \text{(but not both at the same time)}\end{array}\right) \\
&= n \cdot \operatorname{sur}(m-1, n) + n \cdot \operatorname{sur}(m-1, n-1) \\
&= n \cdot (\operatorname{sur}(m-1, n) + \operatorname{sur}(m-1, n-1)).
\end{aligned}$$

Forget that we fixed m and n. Thus, we have proved the following fact:

[167] The proof proceeds roughly as follows: Let $f : [m] \to [n]$ be a green surjection. Then, the image of f contains all elements of $[n]$ (since f is a surjective), but the value n is taken by f only once, namely at m (because f is green). Thus, if we remove m from the domain of f, then f will no longer take the value n. In other words, the restriction $f\mid_{[m-1]}$ no longer takes the value n. Other than that, of course, this restriction takes all the values that f takes; thus, it takes all the elements of $[n]$ as values except for $f(m)$. In other words, it has image $[n] \setminus \{f(m)\}$.

[168] Check this!

Proposition 2.4.14. Let m and n be positive integers. Then,

$$\operatorname{sur}(m,n) = n \cdot (\operatorname{sur}(m-1,n) + \operatorname{sur}(m-1,n-1)).$$

Exercise 2.4.2. Give rigorous proofs of the equalities (168) and (169) above.

Proposition 2.4.14 is an even better recursion than Proposition 2.4.13; it is almost as simple as Theorem 1.3.8. Let us draw a conclusion from it:

Corollary 2.4.15. **(a)** We have $\operatorname{sur}(n,n) = n!$ for all $n \in \mathbb{N}$.
(b) The integer $\operatorname{sur}(m,n)$ is a multiple of $n!$ for all $n \in \mathbb{N}$ and $m \in \mathbb{N}$.

First proof of Corollary 2.4.15 (rough idea). Both parts can easily be shown by induction using Proposition 2.4.14. (Use induction on n for part **(a)**, and induction on m for part **(b)**.) □

Exercise 2.4.3. Complete this proof of Corollary 2.4.15.

Second proof of Corollary 2.4.15 (rough idea). **(a)** Let $n \in \mathbb{N}$. The surjections $[n] \to [n]$ are bijections (by Theorem 2.4.7 **(b)**). Thus, they are precisely the bijections $[n] \to [n]$. In other words, they are precisely the permutations of $[n]$. Hence, their number is $n!$ (according to Theorem 1.7.2). Thus, $\operatorname{sur}(n,n) = n!$. This proves Corollary 2.4.15 **(a)**.

(b) Here is just the idea behind the proof (as we are, so far, missing the language for formalizing it): Each surjection $f : [m] \to [n]$ provides a way of "grouping" the elements of $[m]$ into n nonempty (disjoint) subsets – namely, the subsets

$$\underbrace{\{i \in [m] \mid f(i) = 1\}}_{\substack{\text{the elements} \\ \text{sent to 1 by } f}}, \quad \underbrace{\{i \in [m] \mid f(i) = 2\}}_{\substack{\text{the elements} \\ \text{sent to 2 by } f}}, \quad \ldots, \quad \underbrace{\{i \in [m] \mid f(i) = n\}}_{\substack{\text{the elements} \\ \text{sent to } n \text{ by } f}}.$$

(These n subsets are nonempty, since f is surjective.) For example, the surjection $f : [6] \to [3]$ that is given in two-line notation as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 2 & 3 & 3 & 2 \end{pmatrix}$$

groups the elements of $[6]$ into the 3 subsets

$$\underbrace{\{2\}}_{\substack{\text{the elements} \\ \text{sent to 1 by } f}}, \quad \underbrace{\{1,3,6\}}_{\substack{\text{the elements} \\ \text{sent to 2 by } f}}, \quad \underbrace{\{4,5\}}_{\substack{\text{the elements} \\ \text{sent to 3 by } f}}.$$

Conversely, each such "grouping" comes from a unique surjection $f : [m] \to [n]$ (namely, the surjection which sends the elements of the 1-st subset to 1, the elements of the 2-nd subset to 2, and so on). Hence, the # of such "groupings" is

$\operatorname{sur}(m,n)$. However, if we forget the order of the subsets in each grouping (i.e., we forget which subset is the 1-st subset, which subset is the 2-nd subset, and so on, and only remember the **set** of these subsets), then the # of all such "groupings" becomes $\operatorname{sur}(m,n)/n!$, because each unordered "grouping" can be ordered in precisely $n!$ many different ways. Thus, $\operatorname{sur}(m,n)/n! \in \mathbb{N}$. This proves Corollary 2.4.15 **(b)**.

For the details of this argument, see [18s-hw3s, §0.3 (on "set partitions")] (specifically, [18s-hw3s, Definition 0.13]). □

Remark 2.4.16. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. The number $\operatorname{sur}(m,n)/n!$ is often denoted $\left\{ {m \atop n} \right\}$, and is called a *Stirling number of the second kind*. This number is an integer, because of Corollary 2.4.15 **(b)**.

(Of course, the expression "$\operatorname{sur}(m,n)/n!$" is to be interpreted as $(\operatorname{sur}(m,n))/n!$.)

Here is the most explicit formula known for $\operatorname{sur}(m,n)$:

Theorem 2.4.17. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$\operatorname{sur}(m,n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^m.$$

The most conceptual proof of Theorem 2.4.17 uses the Principle of Inclusion and Exclusion, which we have not learned yet; this proof will appear in Subsection 2.9.4[169]. But there is also an alternative proof, which requires nothing that we have not already seen:

Exercise 2.4.4. Prove Theorem 2.4.17 by strong induction on m, using Proposition 2.4.13.

Applying Theorem 2.4.17 to $n = 3$, we find that each $m \in \mathbb{N}$ satisfies

$$\begin{aligned}\operatorname{sur}(m,3) &= \sum_{i=0}^{3} (-1)^{3-i} \binom{3}{i} i^m = -\underbrace{0^m}_{=[m=0]} + 3 \cdot \underbrace{1^m}_{=1} - 3 \cdot 2^m + 3^m \\ &= 3^m - 3 \cdot 2^m + 3 - [m=0].\end{aligned}$$

Likewise, we can recover parts **(a)**, **(b)** and **(c)** of Proposition 2.4.12 by applying Theorem 2.4.17 to $n = 0$, $n = 1$ and $n = 2$, respectively.

The following exercise gives some variations on the formula in Theorem 2.4.17:

[169] This proof also appears in [18s-hw3s, Exercise 2 **(b)**].

Exercise 2.4.5. Let m be a positive integer. Let $n \in \mathbb{N}$.

(a) Prove that

$$\operatorname{sur}(m,n) = n \sum_{i=0}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^{m-1}.$$

(b) Prove that

$$\left\{ {m \atop n} \right\} = \sum_{i=0}^{n} (-1)^{n-i} \frac{i^m}{i!\,(n-i)!}.$$

2.5. $1^m + 2^m + ... + n^m$

We have still not proved Theorem 1.2.10. But we are getting close. The crucial tool will be the following fact:

Theorem 2.5.1. Let $k \in \mathbb{N}$ and $m \in \mathbb{N}$. Then,

$$k^m = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{k}{i}.$$

Proof of Theorem 2.5.1. We shall prove the theorem by double counting. Let us compute the # of all maps $f : [m] \to [k]$. We shall compute this # in two ways:

1st way: We have

$$\begin{aligned} (\#\text{ of maps } f : [m] \to [k]) &= (\#\text{ of maps from } [m] \text{ to } [k]) \\ &= k^m \end{aligned} \tag{170}$$

(by Theorem 2.4.1, applied to k, $[m]$ and $[k]$ instead of n, A and B).

2nd way: We can construct a map $f : [m] \to [k]$ by the following method:

- First, we choose the number $|f([m])|$ (this is the size of the image of f, i.e., the # of distinct values of f). This is an integer in $\{0, 1, \ldots, m\}$ [170]. Let us call this integer i.
- Then, we choose the set $f([m])$ (this is the set of all values of f). There are $\binom{k}{i}$ many choices for this (since $f([m])$ must be an i-element subset of $[k]$).
- Finally, we choose the map f itself. The image of this map f must be the already chosen i-element set $f([m])$. Thus, what we are choosing is essentially a surjection from the m-element set $[m]$ to the already chosen i-element set $f([m])$. Hence, there are $\operatorname{sur}(m,i)$ many choices here (by Proposition 2.4.11).

[170] since the set $f([m]) = f(\{1,2,\ldots,m\}) = \{f(1), f(2), \ldots, f(m)\}$ clearly has at most m elements

Thus, by the dependent product rule, we obtain

$$(\#\text{ of maps } f : [m] \to [k]) = \sum_{i=0}^{m} \binom{k}{i} \cdot \operatorname{sur}(m,i). \tag{171}$$

(See Exercise 2.5.1 below for a rigorous presentation of this proof.)
Comparing (170) with (171), we obtain

$$k^m = \sum_{i=0}^{m} \binom{k}{i} \cdot \operatorname{sur}(m,i) = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{k}{i}.$$

This proves Theorem 2.5.1. □

Exercise 2.5.1. Prove (171) rigorously.

Theorem 2.5.2. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} k^m = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{n+1}{i+1}.$$

Proof of Theorem 2.5.2. We have

$$\sum_{k=0}^{n} \underbrace{k^m}_{=\sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{k}{i} \text{ (by Theorem 2.5.1)}} = \underbrace{\sum_{k=0}^{n} \sum_{i=0}^{m}}_{=\sum_{i=0}^{m} \sum_{k=0}^{n} \text{ (here, we interchanged the summation signs, by the Fubini principle)}} \operatorname{sur}(m,i) \cdot \binom{k}{i} = \sum_{i=0}^{m} \underbrace{\sum_{k=0}^{n} \operatorname{sur}(m,i) \cdot \binom{k}{i}}_{=\operatorname{sur}(m,i) \cdot \sum_{k=0}^{n} \binom{k}{i}}$$

$$= \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \underbrace{\sum_{k=0}^{n} \binom{k}{i}}_{= \binom{0}{i} + \binom{1}{i} + \cdots + \binom{n}{i} = \binom{n+1}{i+1} \text{ (by Theorem 1.3.29, applied to } k=i)} = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{n+1}{i+1}.$$

This proves Theorem 2.5.2. □

Proof of Theorem 1.2.10. Forget that we fixed k. Instead, let m be a positive integer. Theorem 2.5.2 yields

$$\sum_{k=0}^{n} k^m = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{n+1}{i+1}.$$

Comparing this with

$$\sum_{k=0}^{n} k^m = \underbrace{0^m}_{\substack{=0 \\ \text{(since } m>0\text{)}}} + 1^m + 2^m + \cdots + n^m = 1^m + 2^m + \cdots + n^m = \sum_{i=1}^{n} i^m,$$

we obtain

$$\sum_{i=1}^{n} i^m = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{n+1}{i+1}.$$

Now, forget that we fixed m. We thus have proved that

$$\sum_{i=1}^{n} i^m = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{n+1}{i+1} \qquad \text{for each positive integer } m.$$

Renaming m as k in this statement, we conclude that

$$\sum_{i=1}^{n} i^k = \sum_{i=0}^{k} \operatorname{sur}(k,i) \cdot \binom{n+1}{i+1} \qquad \text{for each positive integer } k.$$

This proves Theorem 1.2.10. □

An alternative, combinatorial proof of Theorem 1.2.10 (by double counting) can be found in [Galvin17, Proposition 23.2] (but, in a sense, is merely a translation of our above proof into the language of counting).

Class of 2019-10-25

2.6. The Vandermonde convolution

2.6.1. The Vandermonde convolution theorem

The next theorem is one of the most fundamental identities for binomial coefficients:

Theorem 2.6.1 (The Vandermonde convolution, or the Chu–Vandermonde identity)**.** Let $n \in \mathbb{N}$ and $x, y \in \mathbb{R}$. Then,

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k} \tag{172}$$

$$= \sum_{k} \binom{x}{k}\binom{y}{n-k}. \tag{173}$$

Here, the summation sign "$\sum_k$" on the right hand side of (173) means a sum over all $k \in \mathbb{Z}$. (We are thus implicitly claiming that this sum over all $k \in \mathbb{Z}$ is well-defined, i.e., that it has only finitely many nonzero addends.)

Note that (172) is precisely Theorem 1.3.37.

Remark 2.6.2. Before proving Theorem 2.6.1, let us explain why the right hand sides of (172) and (173) are equal. Indeed, fix $n \in \mathbb{N}$ and $x, y \in \mathbb{R}$. Now, consider any $k \in \mathbb{Z}$. If $k < 0$, then we have $k \notin \mathbb{N}$ and thus $\binom{x}{k} = 0$ (by (43)), and thus the product $\binom{x}{k}\binom{y}{n-k}$ is 0. But if $k > n$, then we have $n - k \notin \mathbb{N}$ and thus $\binom{y}{n-k} = 0$ (again by (43)), and thus the product $\binom{x}{k}\binom{y}{n-k}$ is again 0. Thus, the product $\binom{x}{k}\binom{y}{n-k}$ is 0 whenever the integer k satisfies either $k < 0$ or $k > n$. In other words, $\binom{x}{k}\binom{y}{n-k} = 0$ whenever $k \notin \{0, 1, \ldots, n\}$ (because an integer k satisfies either $k < 0$ or $k > n$ if and only if it satisfies $k \notin \{0, 1, \ldots, n\}$). Therefore, even though the sums on the right hand sides of (172) and (173) differ in some addends, these addends in which they differ are all 0. Thus, these sums are equal.

We shall use the symbol "$\overset{0}{=}$" (an equality sign with a 0 on top of it) to describe situations like this. More specifically: If A and B are two sums that only differ in addends that are 0, then we will write $A \overset{0}{=} B$. (Of course, $A \overset{0}{=} B$ implies $A = B$, which is why we are using the equality sign.) Thus, the argument we have just made shows that

$$\sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k} \overset{0}{=} \sum_{k} \binom{x}{k}\binom{y}{n-k}.$$

Likewise,

$$\sum_{k=0}^{n} k \overset{0}{=} \sum_{k=1}^{n} k \qquad \text{for each } n \in \mathbb{N}.$$

Likewise, each $n \in \mathbb{N}$ satisfies

$$\sum_{k=0}^{n} \binom{n}{k} \overset{0}{=} \sum_{k=0}^{n+1} \binom{n}{k} \overset{0}{=} \sum_{k \in \mathbb{N}} \binom{n}{k} \overset{0}{=} \sum_{k \in \mathbb{Z}} \binom{n}{k}$$

(since $\binom{n}{k} = 0$ whenever $k \notin \{0, 1, \ldots, n\}$). Likewise, the equality that we spent the main part of our proof of Corollary 1.3.30 arguing can be written as

$$\binom{0}{k} + \binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} \overset{0}{=} \binom{k}{k} + \binom{k+1}{k} + \binom{k+2}{k} + \cdots + \binom{n}{k}.$$

We will give two proofs of Theorem 2.6.1 and a reference to a third one; but none of our two proofs will be complete right away. Instead, our first proof will only

prove Theorem 2.6.1 in the particular case when $x \in \mathbb{N}$, and our second proof will only prove Theorem 2.6.1 in the (even more particular) case when both x and y belong to $\mathbb{N}$. Later – in Subsection 2.6.3 – we will see how to regain the generality of Theorem 2.6.1 and transform these proofs into complete proofs of Theorem 2.6.1.

First proof of Theorem 1.3.37 for $x \in \mathbb{N}$ (informal version). Let $u \in \mathbb{R}$ and $v \in \mathbb{N}$. Then, Theorem 1.3.8 yields

$$\binom{u}{n} = \binom{u-1}{n-1} + \binom{u-1}{n}.$$

Let us now apply Theorem 1.3.8 again to each addend on the right hand side of this equation:

$$\begin{aligned}
\binom{u}{n} &= \underbrace{\binom{u-1}{n-1}}_{\substack{=\binom{u-2}{n-2}+\binom{u-2}{n-1} \\ \text{(by Theorem 1.3.8)}}} + \underbrace{\binom{u-1}{n}}_{\substack{=\binom{u-2}{n-1}+\binom{u-2}{n} \\ \text{(by Theorem 1.3.8)}}} \\
&= \underbrace{\binom{u-2}{n-2}}_{\substack{=\binom{u-3}{n-3}+\binom{u-3}{n-2} \\ \text{(by Theorem 1.3.8)}}} + 2\underbrace{\binom{u-2}{n-1}}_{\substack{=\binom{u-3}{n-2}+\binom{u-3}{n-1} \\ \text{(by Theorem 1.3.8)}}} + \underbrace{\binom{u-2}{n}}_{\substack{=\binom{u-3}{n-1}+\binom{u-3}{n} \\ \text{(by Theorem 1.3.8)}}} \\
&= \binom{u-3}{n-3} + 3\binom{u-3}{n-2} + 3\binom{u-3}{n-1} + \binom{u-3}{n} \\
&= \binom{u-4}{n-4} + 4\binom{u-4}{n-3} + 6\binom{u-4}{n-2} + 4\binom{u-4}{n-1} + \binom{u-4}{n} \\
&\qquad \left(\text{by applying Theorem 1.3.8 to each addend again}\right).
\end{aligned}$$

We can keep applying Theorem 1.3.8 like this indefinitely. After v steps, we obtain an equality of the form

$$\begin{aligned}
\binom{u}{n} &= \alpha_{v,v}\binom{u-v}{n-v} + \alpha_{v,v-1}\binom{u-v}{n-(v-1)} + \cdots + \alpha_{v,1}\binom{u-v}{n-1} + \alpha_{v,0}\binom{u-v}{n} \\
&= \sum_{k=0}^{v} \alpha_{v,k}\binom{u-v}{n-k}, \qquad (174)
\end{aligned}$$

where $\alpha_{v,0}, \alpha_{v,1}, \ldots, \alpha_{v,v}$ are certain numbers. Due to how we are combining terms, we see that these numbers satisfy

$$\alpha_{v,0} = 1, \qquad \alpha_{v,v} = 1 \qquad \text{and} \qquad \alpha_{v,i} = \alpha_{v-1,i} + \alpha_{v-1,i-1} \text{ for each } i \in [v-1]$$

(because both $\binom{u-(v-1)}{n-i}$ and $\binom{u-(v-1)}{n-(i-1)}$ spawn a $\binom{u-v}{n-i}$ term when rewritten using Theorem 1.3.8). This is a recurrence that allows us to compute

the $\alpha_{v,i}$ for all v and i; but more importantly, this is the same recurrence that the binomial coefficients $\binom{v}{i}$ satisfy:

$$\binom{v}{0} = 1, \qquad \binom{v}{v} = 1, \qquad \text{and} \qquad \binom{v}{i} = \binom{v-1}{i} + \binom{v-1}{i-1} \text{ for each } i \in [v-1]$$

(by Theorem 1.3.8). Hence, a straightforward induction on v shows that

$$\alpha_{v,k} = \binom{v}{k} \qquad \text{for each } k \in \{0, 1, \ldots, v\}.$$

Thus, (174) rewrites as

$$\binom{u}{n} = \sum_{k=0}^{v} \binom{v}{k} \binom{u-v}{n-k}.$$

Now, forget that we fixed u and v. We thus have proved the identity

$$\binom{u}{n} = \sum_{k=0}^{v} \binom{v}{k} \binom{u-v}{n-k} \tag{175}$$

for any $u \in \mathbb{R}$ and $v \in \mathbb{N}$.

Now, let $x \in \mathbb{N}$ and $y \in \mathbb{R}$. Applying (175) to $u = x + y$ and $v = x$, we get[171]

$$\begin{aligned}
\binom{x+y}{n} &= \sum_{k=0}^{x} \binom{x}{k} \binom{(x+y)-x}{n-k} = \sum_{k=0}^{x} \binom{x}{k} \binom{y}{n-k} \\
&\overset{0}{=} \sum_{k \in \mathbb{N}} \binom{x}{k} \binom{y}{n-k} \qquad \left(\text{since } \binom{x}{k} = 0 \text{ whenever } k > x \right) \\
&\overset{0}{=} \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \qquad \left(\text{since } \binom{y}{n-k} = 0 \text{ whenever } k > n \right).
\end{aligned}$$

Thus, (172) is proved. Hence, (173) follows as well[172]. This proves Theorem 2.6.1 for $x \in \mathbb{N}$. □

The above proof was informal, but it is easy to formalize:

Exercise 2.6.1. Transform the above informal proof of Theorem 2.6.1 into a rigorous proof. (Of course, this proof will still require $x \in \mathbb{N}$.)

Now, let us come to our second proof of Theorem 2.6.1. As I said, it is even less complete than the first one: it only covers the case when $x, y \in \mathbb{N}$. However, it is neater:

[171] Here, we are using the "$\overset{0}{=}$" notation that we introduced in Remark 2.6.2.

[172] because we have seen in Remark 2.6.2 that the right hand sides of (172) and of (173) are equal

Second proof of Theorem 2.6.1 for $x, y \in \mathbb{N}$ (sketched). Let $x, y \in \mathbb{N}$. We shall prove (172) by double counting. How many ways are there to choose an n-element subset of the set $\{1, 2, \ldots, x\} \cup \{-1, -2, \ldots, -y\}$? Let us answer this question in two ways:

1st way: The answer is $\binom{x+y}{n}$ (by Theorem 1.3.12, since $\{1, 2, \ldots, x\} \cup \{-1, -2, \ldots, -y\}$ is an $(x+y)$-element set).

2nd way: We choose an n-element subset of the set $\{1, 2, \ldots, x\} \cup \{-1, -2, \ldots, -y\}$ as follows:

- First, we decide how many positive elements our subset will have. Let's say it will have k positive elements (with $k \in \{0, 1, \ldots, n\}$).
- Then, we choose these k positive elements. (There are $\binom{x}{k}$ choices for them, since they must belong to the x-element set $\{1, 2, \ldots, x\}$.)
- Then, we choose the remaining $n-k$ negative elements of our subset. (There are $\binom{y}{n-k}$ choices for them, since they must belong to the y-element set $\{-1, -2, \ldots, -y\}$).

Thus, the answer is $\sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}$. (Formally speaking, this follows by applying the sum rule and the product rule.)

Now, we can compare the two answers we have found. We obtain $\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}$. This proves (172) when $x, y \in \mathbb{N}$. Hence, (173) follows as well[173] (for $x, y \in \mathbb{N}$). Therefore, Theorem 2.6.1 is proved for $x, y \in \mathbb{N}$. □

(See [19s, proof of Lemma 2.17.15] for a more detailed version of this proof.)

A third proof of Theorem 2.6.1 can be obtained by induction on n, using the absorption identity $\binom{y}{n} = \frac{y}{n}\binom{y-1}{n-1}$. See [Grinbe15, first proof of Theorem 3.29] for this proof. Unlike our first two proofs above, it proves Theorem 2.6.1 in full generality (without any extra assumptions on x and y); but on the flipside, it is somewhat laborious and unmemorable.

Before I explain how the above two proofs above can be extended to the general case ($x, y \in \mathbb{R}$), let me draw a couple conclusions from the theorem:

Corollary 2.6.3. Let $x \in \mathbb{R}$ and $y \in \mathbb{N}$. Then,

$$\sum_{k=0}^{y} \binom{x}{k}\binom{y}{k} = \binom{x+y}{y}.$$

[173] because we have seen in Remark 2.6.2 that the right hand sides of (172) and of (173) are equal

Proof of Corollary 2.6.3. We have

$$\sum_{k=0}^{y} \binom{x}{k} \underbrace{\binom{y}{k}}_{=\binom{y}{y-k} \text{ (by Theorem 1.3.11, applied to } n=y)} = \sum_{k=0}^{y} \binom{x}{k}\binom{y}{y-k} = \binom{x+y}{y}$$

(by (172), applied to $n = y$). This proves Corollary 2.6.3. □

Exercise 2.6.2. We have so far not proved Theorem 2.6.1 in full generality. However, our first proof of Theorem 2.6.1 above proves the particular case of Theorem 2.6.1 for $x \in \mathbb{N}$.

Give an alternative proof of Corollary 2.6.3 which relies only on this particular case.

Corollary 2.6.4. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Proof of Corollary 2.6.4. We have

$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k}^2 &= \sum_{k=0}^{n} \binom{n}{k}\binom{n}{k} = \binom{n+n}{n} \\ &\qquad \text{(by Corollary 2.6.3 (applied to } x = n \text{ and } y = n)) \\ &= \binom{2n}{n}.\end{aligned}$$

This proves Corollary 2.6.4. □

Remark 2.6.5. Corollary 2.6.4 gives an explicit formula for $\sum_{k=0}^{n} \binom{n}{k}^2$, while Corollary 1.3.27 gives an explicit formula for $\sum_{k=0}^{n} \binom{n}{k}^1$. Is there a formula for $\sum_{k=0}^{n} \binom{n}{k}^3$ as well? No explicit formula is known, but some recursions can be found. For example, if we set $a_n = \sum_{k=0}^{n} \binom{n}{k}^3$ for each $n \in \mathbb{N}$, then

$$(n+1)^2 a_{n+1} = \left(7n^2 + 7n + 2\right) a_n + 8n^2 a_{n-1} \qquad \text{for each } n \geq 1.$$

(See [Stanle01, Exercise 6.54 b] for this formula, which was found by Franel in 1894. Recursions like this, although increasingly more complicated, exist for all $\sum_{k=0}^{n} \binom{n}{k}^r$. Note that the sequence $(a_0, a_1, a_2, \ldots)$ is OEIS sequence A000172.)

The situation is somewhat nicer for alternating sums – i.e., sums of the forms $\sum_{k=0}^{n} (-1)^k \binom{n}{k}^r$. Indeed, there are simple formulas for these sums for all $r \in \{1, 2, 3\}$. We have already seen the formula for $r = 1$ (this is Proposition 1.3.28), and will soon see a formula for $r = 2$ (in Exercise 2.8.1 **(c)**). The formula for $r = 3$ is a special case of Dixon's identity ([Ward91, $(*)$]), which we may see later too.

Exercise 2.6.3. Explain why Exercise 2.1.1 **(a)** is also a particular case of Theorem 1.3.37.

[**Hint:** Apply Theorem 1.3.37 to $y = -1$.]

2.6.2. The polynomial identity trick

We shall next discuss a "simple" trick that will help us complete the first two proofs of Theorem 2.6.1 (i.e., to prove the theorem in full generality, not just for $x, y \in \mathbb{N}$). Essentially, this trick allows us to argue that if a certain kind of identity involving a variable x holds for all $x \in \mathbb{N}$, then it must also hold for all $x \in \mathbb{R}$. This is the "*polynomial identity trick*".

Let me begin with **a reminder on polynomials**. I will not formally define polynomials here (I might get to it later, in the chapter on generating functions), but merely recall the main features of this concept. Polynomials are not functions, but you can nevertheless substitute numbers into them. Informally, a *polynomial* (with real coefficients, in 1 variable X) is a "formal expression" of the form

$$\alpha X^a + \beta X^b + \gamma X^c + \cdots + \omega X^z \qquad \text{with } \alpha, \beta, \gamma, \ldots, \omega \in \mathbb{R} \text{ and } a, b, c, \ldots, z \in \mathbb{N}$$

– that is, a finite sum[174] of terms of the form

$$(\text{a real number}) \cdot X^{(\text{a nonnegative integer})}.$$

For example,

$$2X^3 + 7X^5, \qquad \frac{3}{2}X^1 + 6X^0, \qquad 7X^5, \qquad (-2)\,X^0, \qquad 0$$

are polynomials (where 0 is understood to be an empty sum). Two such expressions are understood to be equal to each other if they can be transformed into one another by the following rules:

[174] possibly an empty sum

- The terms can be swapped at will (i.e., we can replace $\varphi X^n + \psi X^m$ by $\psi X^m + \varphi X^n$).
- Terms involving the same power of X can be combined (i.e., we can replace $\varphi X^n + \psi X^n$ by $(\varphi + \psi) X^n$). This is called "combining like terms". The opposite operation (i.e., splitting a term) can also be done.
- Terms of the form $0X^m$ can be removed or introduced at will.

We write X^0 as 1 (so the term αX^0 is written as α), and we write X^1 as X.

If P is a polynomial, then we can write P as a finite sum $a_0X^0 + a_1X^1 + \cdots + a_nX^n$ for some $n \in \mathbb{N}$ and some real numbers $a_0, a_1, \ldots, a_n$. (Indeed, we can transform P into this form by swapping the terms until they are in the order of increasing exponents[175], then combining like terms until no two terms with the same exponent remain, and finally introducing $0X^m$ terms wherever necessary.) Moreover, the representation of P as such a sum is unique up to "trailing zeroes": We can always make n larger by introducing $0X^m$ terms (for example, $2X^0 + 7X^1$ can be rewritten as $2X^0 + 7X^1 + 0X^2$ or as $2X^0 + 7X^1 + 0X^2 + 0X^3$), but other than that the representation of P is unique.

We can also write a polynomial P as an infinite sum $a_0X^0 + a_1X^1 + a_2X^2 + \cdots$, where $a_0, a_1, a_2, \ldots$ are real numbers such that only finitely many of them are nonzero. (Indeed, we obtain this representation by writing P as a finite sum $a_0X^0 + a_1X^1 + \cdots + a_nX^n$ and then setting $a_{n+1} = a_{n+2} = a_{n+3} = \cdots = 0$.)

If P is written in such a form $a_0X^0 + a_1X^1 + a_2X^2 + \cdots$, then a_i is called the *i-th coefficient* of P (or the *coefficient* of X^i in P) whenever $i \in \mathbb{N}$.

The *zero polynomial* is the polynomial 0 (that is, the polynomial whose all coefficients are 0). A polynomial is said to be *nonzero* if it is not the zero polynomial.

Addition of polynomials is defined by just throwing their terms together: e.g.,

$$\left(\alpha X^a + \beta X^b\right) + \left(\gamma X^c + \delta X^d\right) = \alpha X^a + \beta X^b + \gamma X^c + \delta X^d.$$

Subtraction is defined like addition, except that the terms of the subtrahend get their signs flipped:

$$\left(\alpha X^a + \beta X^b\right) - \left(\gamma X^c + \delta X^d\right) = \alpha X^a + \beta X^b + (-\gamma) X^c + (-\delta) X^d.$$

Multiplication is defined by the distributivity law and the rule $(\alpha X^a)\left(\beta X^b\right) = (\alpha\beta) X^{a+b}$. For example,

$$\begin{aligned}
&\left(\alpha X^a + \beta X^b\right)\left(\gamma X^c + \delta X^d\right) \\
&= \underbrace{(\alpha X^a)(\gamma X^c)}_{=\alpha\gamma X^{a+c}} + \underbrace{(\alpha X^a)\left(\delta X^d\right)}_{=\alpha\delta X^{a+d}} + \underbrace{\left(\beta X^b\right)(\gamma X^c)}_{=\beta\gamma X^{b+c}} + \underbrace{\left(\beta X^b\right)\left(\delta X^d\right)}_{=\beta\delta X^{b+d}} \\
&= \alpha\gamma X^{a+c} + \alpha\delta X^{a+d} + \beta\gamma X^{b+c} + \beta\delta X^{b+d}.
\end{aligned}$$

[175] The "exponent" of a term βX^b is understood to be the integer b.

We cannot always divide a polynomial by another polynomial; but we can divide a polynomial by a nonzero real number. Namely, $\dfrac{P}{r}$ is defined to be $r^{-1} \cdot P$ whenever r is a nonzero real number and P is a polynomial. Furthermore, if $n \in \mathbb{N}$ and if P is a polynomial, then P^n (that is, the n-th power of P) is defined to be the product $\underbrace{PP\cdots P}_{n \text{ times}}$.

The *degree* of a nonzero polynomial P is the largest $i \in \mathbb{N}$ such that the i-th coefficient of P is nonzero. For example, the degree of $2X^2 + 7X^5 - X$ is 5. (We say that the degree of the zero polynomial 0 is $-\infty$.)

Substituting a number (or square matrix, or another polynomial) x into a polynomial $P = \alpha X^a + \beta X^b + \gamma X^c + \cdots$ yields $\alpha x^a + \beta x^b + \gamma x^c + \cdots$. This result is called $P(x)$.

The discussion of polynomials we just had is not fully rigorous and self-contained. We could make it rigorous by formally defining the notion of "formal expression", but we would have to verify that it behaves as nicely as we would hope for, meaning that the following facts are true (among others):

- The representation of a given polynomial P as a finite sum $a_0X^0 + a_1X^1 + \cdots + a_nX^n$ is unique up to "trailing zeroes".
- The representation of a given polynomial P as an infinite sum $a_0X^0 + a_1X^1 + a_2X^2 + \cdots$ is unique. (This is necessary to ensure that the i-th coefficient of P is well-defined.)
- Our definitions of addition, subtraction and multiplication of polynomials are well-defined. (This means, for example, that the product PQ does not depend on how P and Q are expressed. For example, if we "combine like terms" or remove a $0X^m$ term from P, then the product PQ also stays the same.)
- The result of substituting a number x into a polynomial P does not depend on how the polynomial is expressed.

All of these facts are true and can be proven, but it requires some work. Thus, it is more common to define polynomials in a different way, namely as infinite sequences $(a_0, a_1, a_2, \ldots)$ of real numbers having only finitely many nonzero entries. (Such a sequence $(a_0, a_1, a_2, \ldots)$ corresponds to the polynomial $a_0X^0 + a_1X^1 + a_2X^2 + \cdots$.) This definition of polynomials can be found in [Grinbe15, §1.5] or [Loehr11, Sections 7.1–7.3] or [19s, §7.4] or most good algebra textbooks; we will also outline it in the generating functions chapter of this course.

We shall silently identify each number u with the polynomial uX^0 (which is called a *constant polynomial*, and has degree 0 when $u \neq 0$ and degree $-\infty$ when $u = 0$).

Let us now discuss roots of polynomials:

Definition 2.6.6. A number x (say, a rational or real or complex number) is a *root* of a polynomial P if and only if $P(x) = 0$.

A crucial property of polynomials is that they cannot have too many roots (unless they are the zero polynomial):

Theorem 2.6.7. Let $n \in \mathbb{N}$. Then, a nonzero polynomial of degree $\leq n$ has $\leq n$ roots.

Here, "polynomial" means "polynomial with real coefficients in 1 variable X", and "root" means "real root". However, the same theorem can be stated using rational or complex numbers instead (and the same proofs apply).

Example 2.6.8. (a) The polynomial $X^2 - 2X - 3$ has degree 2; thus, Theorem 2.6.7 (applied to $n = 2$) shows that it has ≤ 2 roots. And indeed, it has 2 roots: 3 and -1.

(b) The polynomial $X^2 - 2X + 1$ has degree 2; thus, Theorem 2.6.7 (applied to $n = 2$) shows that it has ≤ 2 roots. And indeed, it has 1 root: 1. (We could say that 1 is a "double root" of this polynomial, since $X^2 - 2X + 1 = (X-1)^2$; but this requires the somewhat subtle concept of "double roots" and, more generally, "multiple roots", which I don't want to introduce here.)

Theorem 2.6.7 is often called the "easy half of the Fundamental Theorem of Algebra". We will not prove it here, but proofs of this theorem are not hard to find. I believe any good textbook on abstract algebra contains a proof of Theorem 2.6.7 somewhere. (In particular, proofs appear in [Goodma15, Corollary 1.8.24], [Joyce17, Theorem 1.58], [Walker87, Corollary 4.5.10], [CoLiOs15, Chapter 1, §5, Corollary 3], [19s, Theorem 7.6.11], [Elman22, Corollary 33.8] and [Knapp16, Corollary 1.14].)

The following corollary of Theorem 2.6.7 is almost trivial:

Corollary 2.6.9. If a polynomial P has infinitely many roots, then P is the zero polynomial.

(Again, "polynomial" means "polynomial with real coefficients in 1 variable X", and "root" means "real root" here.)

Proof of Corollary 2.6.9. Let P be a polynomial that has infinitely many roots. We must prove that P is the zero polynomial. Indeed, assume the contrary. Thus, P is nonzero. Let n be the degree of P. Thus, P is a nonzero polynomial of degree $\leq n$. Hence, Theorem 2.6.7 shows that P has $\leq n$ roots. But P has $> n$ roots (since P has infinitely many roots). The previous two sentences contradict each other. This contradiction shows that our assumption was false. Hence, Corollary 2.6.9 is proven. □

A corollary of this corollary will prove the most useful to us:

Corollary 2.6.10. Let P and Q be polynomials (with real coefficients in 1 variable X). Assume that

$$P(x) = Q(x) \qquad \text{for all } x \in \mathbb{N}. \tag{176}$$

Then, $P = Q$.

Proof of Corollary 2.6.10. Consider the polynomial $P - Q$. For each $x \in \mathbb{N}$, we have

$$(P - Q)(x) = P(x) - Q(x) = 0 \qquad \text{(by (176))}.$$

In other words, each $x \in \mathbb{N}$ is a root of $P - Q$. Hence, $P - Q$ has infinitely many roots (since there are infinitely many $x \in \mathbb{N}$). Thus, Corollary 2.6.9 (applied to $P - Q$ instead of P) shows that $P - Q$ is the zero polynomial. In other words, $P - Q = 0$. Hence, $P = Q$. This proves Corollary 2.6.10. □

2.6.3. Salvaging the proofs of Theorem 2.6.1

How does Corollary 2.6.10 help us prove Theorem 2.6.1? What do the binomial coefficients appearing in Theorem 2.6.1 have to do with polynomials?

To understand this, let us extend our definition of binomial coefficients somewhat:

Definition 2.6.11. In Definition 1.3.3, we defined the binomial coefficient $\binom{n}{k}$ whenever n and k are numbers. Let us now extend this definition to the case when n is a polynomial (although k should still be a number).

Since polynomials are not usually denoted by n, let me restate this definition: If P is any polynomial and k is any number, then $\binom{P}{k}$ is a polynomial defined by

$$\binom{P}{k} = \frac{P(P-1)(P-2)\cdots(P-k+1)}{k!} \qquad \text{if } k \in \mathbb{N}$$

and

$$\binom{P}{k} = 0 \qquad \text{if } k \notin \mathbb{N}.$$

Note the following fact:

Proposition 2.6.12. Let P be a polynomial, and let n and k be two numbers. Then, substituting n into the polynomial $\binom{P}{k}$ yields the number $\binom{P(n)}{k}$.

This proposition is intuitively clear (it is just saying that it does not matter whether we substitute n for X before computing the binomial coefficient $\binom{P}{k}$ or after it). For a formal proof, see [19s, Corollary 7.6.16 **(c)**].

Let us now come back to our first proof of Theorem 2.6.1. In that proof, we only showed that Theorem 2.6.1 holds for all $x \in \mathbb{N}$. We shall now extend it to all real values of x:

Completion of the first proof of Theorem 2.6.1. Fix $y \in \mathbb{R}$ and $n \in \mathbb{N}$. We have already proved that Theorem 2.6.1 holds for $x \in \mathbb{N}$. Thus, the equality

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \tag{177}$$

holds for all $x \in \mathbb{N}$. We now want to prove this equality for all $x \in \mathbb{R}$.

Define two polynomials P and Q (in 1 variable X, with real coefficients) by

$$P = \binom{X+y}{n} \qquad \text{and} \qquad Q = \sum_{k=0}^{n} \binom{X}{k} \binom{y}{n-k}.$$

These are well-defined polynomials, and can be written explicitly as follows:

$$P = \binom{X+y}{n} = \frac{(X+y)(X+y-1)(X+y-2)\cdots(X+y-n+1)}{n!}$$

and

$$Q = \sum_{k=0}^{n} \binom{X}{k} \binom{y}{n-k} = \sum_{k=0}^{n} \frac{X(X-1)(X-2)\cdots(X-k+1)}{k!} \binom{y}{n-k}.$$

Now, for each $x \in \mathbb{R}$, we have

$$P(x) = \binom{x+y}{n} \qquad \left(\text{by Proposition 2.6.12, since } P = \binom{X+y}{n}\right)$$

and

$$Q(x) = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} \qquad (\text{likewise}).$$

In view of these two equalities, we can rewrite (177) as

$$P(x) = Q(x).$$

Hence, we know that $P(x) = Q(x)$ holds for all $x \in \mathbb{N}$ (because we know that (177) holds for all $x \in \mathbb{N}$). Therefore, Corollary 2.6.10 yields $P = Q$. Thus, $P(x) = Q(x)$ for all $x \in \mathbb{R}$. In other words,

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}$$

for all $x \in \mathbb{R}$ (since $P(x) = \binom{x+y}{n}$ and $Q(x) = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}$ for each $x \in \mathbb{R}$). Thus, we have proved the equality (172) for all $x \in \mathbb{R}$. Hence, (173) holds for all $x \in \mathbb{R}$ as well[176]. Therefore, Theorem 2.6.1 is proved (this time for all values of x and y). $\square$

[176] because we have seen in Remark 2.6.2 that the right hand sides of (172) and of (173) are equal

Our use of Corollary 2.6.10 in the proof we just gave is an instance of what I call the "*polynomial identity trick*": We wanted to prove the equality $P(x) = Q(x)$ for all $x \in \mathbb{R}$, where P and Q were two given polynomials. We did this as follows: We first proved it for all $x \in \mathbb{N}$; then, we used this to conclude that $P = Q$ (by Corollary 2.6.10); finally we substituted x in $P = Q$ to obtain $P(x) = Q(x)$ for all $x \in \mathbb{R}$. What made this argument possible is that the equality that we were aiming to show (in our case, (177)) was an equality between two polynomials in x (that is, we could rewrite it as $P(x) = Q(x)$ for two polynomials P and Q). Corollary 2.6.10 allows us to use this kind of argument in proving any such equality. This is called the "polynomial identity trick" or (in [GrKnPa94, §5.1]) the "polynomial argument".

We can also salvage our second proof of Theorem 2.6.1 in a similar way. Here we need to apply the polynomial identity trick twice:

- *Step 1:* Fix $y \in \mathbb{N}$ and $n \in \mathbb{N}$. Use the same argument as before to prove that (177) holds for all $x \in \mathbb{R}$. Thus, (177) is proved for all $x \in \mathbb{R}$ and $y \in \mathbb{N}$.
- *Step 2:* Fix $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Use an analogous argument (using y instead of x) to prove that (177) holds for all $y \in \mathbb{R}$.

See [19s, §2.17.3] for the details of this argument[177], and [Grinbe15, Second proof of Theorem 3.30] for a different variant of this argument (using polynomials in 2 variables).

2.6.4. More consequences of the polynomial identity trick

The polynomial identity trick can be applied to several other identities. For example:

- Proposition 1.3.35 (the trinomial revision formula) says that

$$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b} \tag{178}$$

  for all $n, a, b \in \mathbb{R}$. Our second proof of this proposition (in Subsection 2.2.2) only showed that it holds for all $n \in \mathbb{N}$. But using the polynomial identity trick, we can now complete it to obtain a proof of Proposition 1.3.35 for all $n \in \mathbb{R}$: Namely, we fix $a, b \in \mathbb{R}$, and we rewrite the equality (178) as

$$P(n) = Q(n),$$

  where the polynomials P and Q are defined by

$$P = \binom{X}{a}\binom{a}{b} \qquad \text{and} \qquad Q = \binom{X}{b}\binom{X-b}{a-b}.$$

[177] I use $\mathbb{Q}$ instead of $\mathbb{R}$ in [19s, §2.17.3], but otherwise the argument proceeds exactly in the same way.

Our second proof of Proposition 1.3.35 thus shows that $P(n) = Q(n)$ for all $n \in \mathbb{N}$. Hence, using the polynomial identity trick, we conclude that $P(n) = Q(n)$ for all $n \in \mathbb{R}$. This completes the second proof of Proposition 1.3.35.

- Proposition 1.3.28 says that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n = 0] \tag{179}$$

holds for all $n \in \mathbb{N}$. Can we use the polynomial identity trick to generalize this to all $n \in \mathbb{R}$? No, because n appears as a summation bound on the left hand side, and it would make no sense to replace it by a non-integer number (because what would "$\sum_{k=0}^{\sqrt{2}}$" even mean?).

We could try to sneak past this issue by rewriting the left hand side somewhat. For any $n \in \mathbb{N}$, we can rewrite the identity (179) as

$$\sum_{k \in \mathbb{N}} (-1)^k \binom{n}{k} = [n = 0] \tag{180}$$

(because $\sum_{k=0}^{n} (-1)^k \binom{n}{k} \overset{0}{=} \sum_{k \in \mathbb{N}} (-1)^k \binom{n}{k}$). But even in this form, we cannot generalize it to $n \in \mathbb{R}$ using the polynomial identity trick, because the right hand side of (180) cannot be written as a polynomial in n. In other words, there exists no polynomial Q such that

$$Q(n) = [n = 0] \qquad \text{for all } n \in \mathbb{N}$$

(in fact, such a polynomial Q would have infinitely many roots, contradicting Corollary 2.6.9).

Note that we cannot generalize (180) to all $n \in \mathbb{R}$ in any way (by the polynomial identity trick or otherwise), because if we try to substitute $n = -1$ into (180), then the left hand side will become

$$\sum_{k \in \mathbb{N}} (-1)^k \underbrace{\binom{-1}{k}}_{\substack{=(-1)^k \\ \text{(by (47))}}} = \sum_{k \in \mathbb{N}} \underbrace{(-1)^k (-1)^k}_{\substack{=(-1)^{k+k}=1 \\ \text{(since } k+k=2k \text{ is even)}}} = \sum_{k \in \mathbb{N}} 1,$$

which is an ill-defined infinite sum (with infinitely many nonzero addends). More generally, for **any** $n \in \mathbb{R} \setminus \mathbb{N}$, the infinite sum $\sum_{k \in \mathbb{N}} (-1)^k \binom{n}{k}$ will have infinitely many nonzero addends (unlike for $n \in \mathbb{N}$).

- Theorem 2.5.1 claims that

$$k^m = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{k}{i} \tag{181}$$

for all $k \in \mathbb{N}$ and $m \in \mathbb{N}$. Can we use the polynomial identity trick to generalize this to all $k \in \mathbb{R}$? What about generalizing it to all $m \in \mathbb{R}$?

The answer to the second question is negative, because k^m is clearly not a polynomial in m (that is, there exists no polynomial P such that $P(m) = k^m$ for all $m \in \mathbb{N}$, where k is fixed). Thus, m has to remain a nonnegative integer. But the answer to the first question is positive. Indeed, if we fix $m \in \mathbb{N}$, then both sides of (181) are polynomials in k; that is, we can rewrite the equality (181) as

$$P(k) = Q(k), \qquad \text{where } P = X^m \text{ and } Q = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{X}{i}.$$

From Theorem 2.5.1, we know that this equality holds for all $k \in \mathbb{N}$. Thus, the polynomial identity trick shows that it holds for all $k \in \mathbb{R}$. Thus, we have proved that

$$k^m = \sum_{i=0}^{m} \operatorname{sur}(m,i) \cdot \binom{k}{i} \tag{182}$$

for all $k \in \mathbb{R}$ and $m \in \mathbb{N}$. This is a significant generalization of Theorem 2.5.1.

- Exercise 2.1.1 **(a)** claims the equality

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m}$$

for all $n \in \mathbb{R}$ and $m \in \mathbb{N}$. We cannot generalize this equality to $m \in \mathbb{R}$ (because, for example, $(-1)^m \binom{n-1}{m}$ is not a polynomial in m). But the polynomial identity trick shows that if we had only proved it for $n \in \mathbb{N}$, we could automatically conclude that it holds for all $n \in \mathbb{R}$ (since both sides are polynomials in n). (But we have no need for this, since we have proved it for all $n \in \mathbb{R}$ already.)

- We cannot generalize Theorem 1.3.29 to all $n \in \mathbb{R}$, because n appears as a summation bound on the left hand side. The polynomial identity trick does not help here, since the left hand side is not a polynomial in n. (The right hand side is, but this alone is not sufficient.) We also cannot generalize Theorem 1.3.29 to all $k \in \mathbb{R}$, because it would be false for $k = -1$ and $n = 0$ (and, of course, because $\binom{n+1}{k+1}$ is not a polynomial in k). (It would be true for all $k \neq -1$, but only because it would boil down to $0 = 0$ in the stupidest possible way when $k+1 \notin \mathbb{N}$.) For similar reasons, we cannot generalize Corollary 1.3.30.

Class of 2019-10-28

2.6.5. Mutating the Chu–Vandermonde identity

We shall next see some "mutated" versions of the Chu–Vandermonde identity (Theorem 2.6.1). Here, "mutated" means that these versions are obtained from the Chu–Vandermonde identity by transforming the binomial coefficients via the upper negation and symmetry identities[178]. One example of such a "mutated" version is Corollary 2.6.3, since that corollary was proved by applying the Chu–Vandermonde identity and rewriting one of the binomial coefficients using symmetry. Here is another (which we shall prove soon):

Proposition 2.6.13. Let $n, x, y \in \mathbb{N}$. Then,

$$\binom{n+1}{x+y+1} = \sum_{k=0}^{n} \binom{k}{x} \binom{n-k}{y}.$$

This proposition is often called the "upside-down Vandermonde convolution", since its right hand side is the right hand side of (172) with all binomial coefficients turned "upside down". It behaves rather differently in some aspects, however. In particular, (172) holds for all $x, y \in \mathbb{R}$, whereas Proposition 2.6.13 requires $x, y \in \mathbb{N}$ (and indeed, would be false for $n = 3$, $x = -1$ and $y = 2$). The polynomial identity trick cannot be used to generalize Proposition 2.6.13, since its right hand side is neither a polynomial in n nor a polynomial in x nor a polynomial in y.

We shall give two proofs of Proposition 2.6.13: one algebraic and one by double counting. The algebraic proof will explain why we call it a "mutated" Chu–Vandermonde identity; the double-counting proof will shine some light on its combinatorial meaning. Which is the "right" proof? You decide.

First proof of Proposition 2.6.13. This proof is a close relative of the proof given in [Grinbe15, proof of Proposition 3.32 **(f)**] (but is more direct).

We shall first show an auxiliary claim:

Claim 1: Let $k \in \{0, 1, \ldots, n\}$ be such that $k < x$ or $n - k < y$. Then,

$$\binom{k}{x} \binom{n-k}{y} = 0.$$

[*Proof of Claim 1:* Assume the contrary. Thus, $\binom{k}{x} \binom{n-k}{y} \neq 0$. Hence, $\binom{k}{x} \neq 0$ and $\binom{n-k}{y} \neq 0$. Note that $k \in \{0, 1, \ldots, n\}$, so that both k and $n - k$ are nonnegative integers. Thus, $k \in \mathbb{N}$ and $n - k \in \mathbb{N}$.

[178] i.e., Proposition 1.3.7 and Theorem 1.3.11

From $k \in \mathbb{N}$ and $\binom{k}{x} \neq 0$, we obtain $k \geq x$, because otherwise, Proposition 1.3.6 (applied to k and x instead of n and k) would yield $\binom{k}{x} = 0$.

From $n-k \in \mathbb{N}$ and $\binom{n-k}{y} \neq 0$, we obtain $n-k \geq y$, because otherwise, Proposition 1.3.6 (applied to $n-k$ and y instead of n and k) would yield $\binom{n-k}{y} = 0$.

We have thus found $k \geq x$ and $n-k \geq y$. This contradicts the assumption that $k < x$ or $n-k < y$. This contradiction shows that our assumption was wrong. Hence, Claim 1 is proven.]

We are in one of the following two cases:

Case 1: We have $n < x+y$.

Case 2: We have $n \geq x+y$.

Let us first consider Case 1. In this case, we have $n < x+y$. Therefore, each $k \in \{0,1,\ldots,n\}$ satisfies either $k < x$ or $n-k < y$ [179]. Hence, each $k \in \{0,1,\ldots,n\}$ satisfies

$$\binom{k}{x}\binom{n-k}{y} = 0 \tag{183}$$

(by Claim 1).

Now, $n < x+y$, thus $n+1 < x+y+1$. Thus, Proposition 1.3.6 (applied to $n+1$ and $x+y+1$ instead of n and k) yields $\binom{n+1}{x+y+1} = 0$. Comparing this with

$$\sum_{k=0}^{n} \underbrace{\binom{k}{x}\binom{n-k}{y}}_{\substack{=0 \\ \text{(by (183))}}} = \sum_{k=0}^{n} 0 = 0,$$

we obtain

$$\binom{n+1}{x+y+1} = \sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y}.$$

Thus, Proposition 2.6.13 is proven in Case 1.

Let us now consider Case 2. In this case, we have $n \geq x+y$. Thus, $n-y \geq x$. Thus, $x \leq n-y$, so that $0 \leq x \leq n-y \leq n$ (since $y \in \mathbb{N}$). Therefore, the integer interval $[x, n-y] = \{x, x+1, \ldots, n-y\}$ is a subset of $[0,n] = \{0,1,\ldots,n\}$. Thus, the elements $k \in \{0,1,\ldots,n\}$ that satisfy $k \geq x$ and $k \leq n-y$ are precisely the elements of $\{x, x+1, \ldots, n-y\}$.

Now, each $k \in \{0,1,\ldots,n\}$ satisfies

$$\text{either } (k \geq x \text{ and } n-k \geq y) \text{ or } (k < x \text{ or } n-k < y)$$

[179] *Proof.* Assume the contrary. Thus, neither $k < x$ nor $n-k < y$ holds. Hence, we have $k \geq x$ and $n-k \geq y$. Adding these two inequalities together, we obtain $k+(n-k) \geq x+y$. This contradicts $k+(n-k) = n < x+y$. This contradiction shows that our assumption was wrong. Qed.

(but not both of these statements simultaneously). Thus, we can split the sum $\sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y}$ as follows:[180]

$$\begin{aligned}
&\sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y} \\
&= \underbrace{\sum_{\substack{k\in\{0,1,\ldots,n\};\\ k\geq x \text{ and } n-k\geq y}}}_{\substack{= \sum\limits_{\substack{k\in\{0,1,\ldots,n\};\\ k\geq x \text{ and } k\leq n-y}} \\ \text{(since the inequality } n-k\geq y \\ \text{is equivalent to } k\leq n-y\text{)}}} \binom{k}{x}\binom{n-k}{y} + \sum_{\substack{k\in\{0,1,\ldots,n\};\\ k<x \text{ or } n-k<y}} \underbrace{\binom{k}{x}\binom{n-k}{y}}_{\substack{=0 \\ \text{(by Claim 1)}}} \\
&= \sum_{\substack{k\in\{0,1,\ldots,n\};\\ k\geq x \text{ and } k\leq n-y}} \binom{k}{x}\binom{n-k}{y} + \sum_{\substack{k\in\{0,1,\ldots,n\};\\ k<x \text{ or } n-k<y}} 0 \\
&= \sum_{\substack{k\in\{0,1,\ldots,n\};\\ k\geq x \text{ and } k\leq n-y}} \binom{k}{x}\binom{n-k}{y} \\
&= \sum_{k=x}^{n-y} \binom{k}{x}\binom{n-k}{y} \qquad (184)
\end{aligned}$$

(because the elements $k \in \{0,1,\ldots,n\}$ that satisfy $k \geq x$ and $k \leq n-y$ are precisely the elements of $\{x, x+1, \ldots, n-y\}$).

Now, fix $k \in \{x, x+1, \ldots, n-y\}$. Thus, $x \leq k \leq n-y$, so that $0 \leq x \leq k \leq n-y \leq n$. Thus, $k \in \mathbb{N}$ (since $0 \leq k$) and $n-k \in \mathbb{N}$ (since $k \leq n$). Theorem 1.3.11 (applied to k and x instead of n and k) yields

$$\begin{aligned}
\binom{k}{x} &= \binom{k}{k-x} = \binom{-(-k)}{k-x} \qquad (\text{since } k = -(-k)) \\
&= (-1)^{k-x}\binom{-k+k-x-1}{k-x} \\
&\qquad \left(\begin{array}{c}\text{by Proposition 1.3.7, applied to } -k \text{ and } k-x \\ \text{instead of } n \text{ and } k\end{array}\right) \\
&= (-1)^{k-x}\binom{-x-1}{k-x} \qquad (185)
\end{aligned}$$

(since $-k+k-x-1 = -x-1$). Furthermore, recall that $n-k \in \mathbb{N}$; hence,

[180] Here we are using the splitting rule (28), along with the fact that the "$\sum_{k=0}^{n}$" sign is a shorthand for "$\sum_{k\in\{0,1,\ldots,n\}}$".

Theorem 1.3.11 (applied to $n-k$ and y instead of n and k) yields

$$\begin{aligned}
\binom{n-k}{y} &= \binom{n-k}{n-k-y} = \binom{-(k-n)}{n-k-y} \qquad (\text{since } n-k = -(k-n)) \\
&= (-1)^{n-k-y}\binom{k-n+n-k-y-1}{n-k-y} \\
&\qquad \left(\begin{array}{c}\text{by Proposition 1.3.7, applied to } k-n \text{ and } n-k-y \\ \text{instead of } n \text{ and } k\end{array}\right) \\
&= (-1)^{n-k-y}\binom{-y-1}{n-y-k} \qquad (186)
\end{aligned}$$

(since $k-n+n-k-y-1 = -y-1$ and $n-k-y = n-y-k$). Multiplying the equalities (185) and (186), we obtain

$$\begin{aligned}
\binom{k}{x}\binom{n-k}{y} &= (-1)^{k-x}\binom{-x-1}{k-x}(-1)^{n-k-y}\binom{-y-1}{n-y-k} \\
&= \underbrace{(-1)^{k-x}(-1)^{n-k-y}}_{\substack{=(-1)^{(k-x)+(n-k-y)}=(-1)^{n-x-y} \\ (\text{since } (k-x)+(n-k-y)=n-x-y)}}\binom{-x-1}{k-x}\binom{-y-1}{n-y-k} \\
&= (-1)^{n-x-y}\binom{-x-1}{k-x}\binom{-y-1}{n-y-k}. \qquad (187)
\end{aligned}$$

Now, forget that we fixed k. We thus have proved the equality (187) for each

$k \in \{x, x+1, \ldots, n-y\}$. Now, (184) becomes

$$\begin{aligned}
&\sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y} \\
&= \sum_{k=x}^{n-y} \underbrace{\binom{k}{x}\binom{n-k}{y}}_{\substack{=(-1)^{n-x-y}\binom{-x-1}{k-x}\binom{-y-1}{n-y-k} \\ \text{(by (187))}}} = \sum_{k=x}^{n-y} (-1)^{n-x-y}\binom{-x-1}{k-x}\binom{-y-1}{n-y-k} \\
&= \underbrace{\sum_{k=0}^{n-y-x}}_{\substack{=\sum_{k=0}^{n-x-y} \\ \text{(since } n-y-x=n-x-y\text{)}}} (-1)^{n-x-y} \underbrace{\binom{-x-1}{(k+x)-x}}_{\substack{=\binom{-x-1}{k} \\ \text{(since } (k+x)-x=k\text{)}}} \underbrace{\binom{-y-1}{n-y-(k+x)}}_{\substack{=\binom{-y-1}{n-x-y-k} \\ \text{(since } n-y-(k+x)=n-x-y-k\text{)}}} \\
&\qquad \text{(here, we have substituted } k+x \text{ for } k \text{ in the sum)} \\
&= \sum_{k=0}^{n-x-y} (-1)^{n-x-y}\binom{-x-1}{k}\binom{-y-1}{n-x-y-k} \\
&= (-1)^{n-x-y} \sum_{k=0}^{n-x-y} \binom{-x-1}{k}\binom{-y-1}{n-x-y-k}. \qquad (188)
\end{aligned}$$

Let us now look at the sum on the right hand side of this equality more carefully. It is a sum of products of binomial coefficients, and this time the running index k of the sum appears only in the bottom arguments of these coefficients. This looks similar to the right hand side of (172), and indeed we can easily recognize the right hand side of (172) in our sum, with $n-x-y$, $-x-1$ and $-y-1$ substituted for n, x and y.

Let us see how this works in detail: We have $n-x-y \geq 0$ (since $n \geq x+y$) and thus $n-x-y \in \mathbb{N}$. Thus, (172) (applied to $n-x-y$, $-x-1$ and $-y-1$ instead of n, x and y) yields

$$\binom{(-x-1)+(-y-1)}{n-x-y} = \sum_{k=0}^{n-x-y} \binom{-x-1}{k}\binom{-y-1}{n-x-y-k}.$$

In view of $(-x-1)+(-y-1) = -(x+y+2)$, this rewrites as

$$\binom{-(x+y+2)}{n-x-y} = \sum_{k=0}^{n-x-y} \binom{-x-1}{k}\binom{-y-1}{n-x-y-k}. \qquad (189)$$

Thus, (188) becomes

$$\begin{aligned}
&\sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y} \\
&= (-1)^{n-x-y} \underbrace{\sum_{k=0}^{n-x-y} \binom{-x-1}{k}\binom{-y-1}{n-x-y-k}}_{=\binom{-(x+y+2)}{n-x-y} \text{ (by (189))}} \\
&= (-1)^{n-x-y} \underbrace{\binom{-(x+y+2)}{n-x-y}}_{=(-1)^{n-x-y}\binom{x+y+2+n-x-y-1}{n-x-y} \text{ (by Proposition 1.3.7, applied to } x+y+2 \text{ and } n-x-y \text{ instead of } n \text{ and } k)} \\
&= \underbrace{(-1)^{n-x-y}(-1)^{n-x-y}}_{=(-1)^{(n-x-y)+(n-x-y)}=1 \text{ (since } (n-x-y)+(n-x-y)=2(n-x-y) \text{ is even)}} \underbrace{\binom{x+y+2+n-x-y-1}{n-x-y}}_{=\binom{n+1}{n-x-y} \text{ (since } x+y+2+n-x-y-1=n+1)} \\
&= \binom{n+1}{n-x-y} = \binom{n+1}{(n+1)-(n-x-y)} \\
&\qquad \text{(by Theorem 1.3.11, applied to } n+1 \text{ and } n-x-y \text{ instead of } n \text{ and } k) \\
&= \binom{n+1}{x+y+1} \qquad (\text{since } (n+1)-(n-x-y) = x+y+1).
\end{aligned}$$

Thus, Proposition 2.6.13 is proven in Case 2.

We have now proved Proposition 2.6.13 in both Cases 1 and 2. Hence, Proposition 2.6.13 always holds. □

Second proof of Proposition 2.6.13 (sketched). We shall prove Proposition 2.6.13 by double counting. How many $(x+y+1)$-element subsets does the set $[n+1]$ have? Let us answer this question in two ways:

1st way: Theorem 1.3.12 (applied to $n+1$, $x+y+1$ and $[n+1]$ instead of n, k and S) shows that

$$\begin{aligned}
&(\#\text{ of } (x+y+1)\text{-element subsets of } [n+1]) \\
&= \binom{n+1}{x+y+1}. \qquad (190)
\end{aligned}$$

2nd way: Here is a weird procedure to construct an $(x+y+1)$-element subset U of $[n+1]$:

- First, we choose the $(x+1)$-st smallest element of the subset U. Let us call it m. Thus, $m \in [n+1]$.
- Then, we choose the x smallest elements of U. These x smallest elements must belong to the $(m-1)$-element set $\{1,2,\ldots,m-1\}$ (since they must be smaller than the $(x+1)$-st smallest element of U, which is m); thus, there are $\binom{m-1}{x}$ choices for them (by Theorem 1.3.12, applied to $m-1$, x and $\{1,2,\ldots,m-1\}$ instead of n, k and S).
- Finally, we choose the remaining y elements of U. These y elements must belong to the $(n-m+1)$-element set $\{m+1,m+2,\ldots,n+1\}$ (since they must be larger than the $(x+1)$-st smallest element of U, which is m); thus, there are $\binom{n-m+1}{y}$ choices for them (by Theorem 1.3.12, applied to $n-m+1$, y and $\{m+1,m+2,\ldots,n+1\}$ instead of n, k and S).

The total # of ways to make these decisions is clearly $\sum_{m\in[n+1]} \binom{m-1}{x}\binom{n-m+1}{y}$. Thus,

$$\begin{aligned}&(\#\text{ of } (x+y+1)\text{-element subsets of } [n+1])\\ &= \sum_{m\in[n+1]} \binom{m-1}{x}\binom{n-m+1}{y}. \end{aligned} \tag{191}$$

Now, comparing (190) with (191), we obtain

$$\begin{aligned}\binom{n+1}{x+y+1} &= \underbrace{\sum_{m\in[n+1]}}_{=\sum_{m=1}^{n+1}} \binom{m-1}{x} \underbrace{\binom{n-m+1}{y}}_{\substack{=\binom{n-(m-1)}{y}\\ \text{(since } n-m+1=n-(m-1))}} \\ &= \sum_{m=1}^{n+1} \binom{m-1}{x}\binom{n-(m-1)}{y} = \sum_{k=0}^{n} \binom{k}{x}\binom{n-k}{y}\end{aligned}$$

(here, we have substituted k for $m-1$ in the sum). Thus, Proposition 2.6.13 is proved again. □

Exercise 2.6.4. Explain why Theorem 1.3.29 is a particular case of Proposition 2.6.13.

There are several other "mutated versions" of the Chu–Vandermonde identity. Two of them are given in the following exercises:

Exercise 2.6.5. Let $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$. Show that

$$\binom{x-y}{n} = \sum_{k=0}^{n} (-1)^k \binom{x}{n-k} \binom{k+y-1}{k}.$$

Exercise 2.6.6. Let $x \in \mathbb{N}$, $y \in \mathbb{R}$ and $n \in \mathbb{N}$. Prove that

$$\binom{y-x-1}{n-x} = \sum_{k=0}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k}.$$

The following two exercises can be solved entirely algebraically, using the Chu–Vandermonde identity and the trinomial revision formula alone:

Exercise 2.6.7. Let $a, b \in \mathbb{N}$ and $x \in \mathbb{R}$. Prove that

$$\binom{x}{a}\binom{x}{b} = \sum_{i=a}^{a+b} \binom{i}{a} \binom{a}{a+b-i} \binom{x}{i}.$$

Exercise 2.6.8. Let $a, b \in \mathbb{N}$ and $x, y \in \mathbb{R}$. Prove that

$$\sum_{i=0}^{\min\{a,b\}} \binom{x+y+i}{i} \binom{x}{a-i} \binom{y}{b-i} = \binom{x+b}{a} \binom{y+a}{b}.$$

[**Hint:** Apply the Chu–Vandermonde identity thrice and each of Propositions 1.3.35 and 2.2.4 once.]

Exercise 2.6.9. Fix a real $x \in \mathbb{R}$ and a nonnegative integer $n \in \mathbb{N}$. For any $u, v \in \mathbb{R}$, we define

$$F_{x,n}(u,v) = \sum_{i=0}^{n} \binom{x+u}{n-i} \binom{u+i}{i} \binom{v}{i}.$$

Prove that

$$F_{x,n}(u,v) = F_{x,n}(v,u) \qquad \text{for any } u, v \in \mathbb{R}.$$

[**Hint:** Apply both the Chu–Vandermonde identity and Corollary 2.6.3.]

2.7. Counting subsets again

One of the most important facts we have seen so far was Theorem 1.3.12, which said that if S is an n-element set and $k \in \mathbb{R}$, then

$$\binom{n}{k} = (\#\text{ of } k\text{-element subsets of } S).$$

We have proved this fact by induction on n. We shall now re-prove it using the sum rule applied "backwards". The underlying idea of the argument can be summarized by the saying "to count sheep, first count the legs and then divide by 4". In our case, the sheep will be the k-element subsets of S, and their legs will be *injective k-tuples* of elements of S (i.e., k-tuples $(s_1, s_2, \ldots, s_k) \in S^k$ such that $s_1, s_2, \ldots, s_k$ are distinct). More precisely, an injective k-tuple $(s_1, s_2, \ldots, s_k) \in S^k$ will be considered a "leg" of a sheep W if and only if $W = \{s_1, s_2, \ldots, s_k\}$. What is so useful about this definition of "legs" is that

- the legs are easier to count than the sheep, and
- each sheep has the same number of legs (although not 4).

This trick for counting is sometimes called the "multijection principle"[181], but it requires no new theorems; the sum rule is all we need.

Here are the details. First, let us define the injective k-tuples – the "legs" of our "sheep":

Definition 2.7.1. Let S be a set. Let $k \in \mathbb{N}$.
(a) A k-tuple $(s_1, s_2, \ldots, s_k) \in S^k$ is said to be *injective* if $s_1, s_2, \ldots, s_k$ are distinct.
(b) Let S^k_{inj} be the set of all injective k-tuples $(s_1, s_2, \ldots, s_k) \in S^k$. This is a subset of S^k.

For example, the 3-tuple $(3, 2, 5)$ is injective (since $3, 2, 5$ are distinct), whereas the 3-tuple $(4, 2, 4)$ is not (since $4 = 4$).

In probability theory, injective k-tuples are called "ordered k-samples without replacement" (while arbitrary k-tuples are called "ordered k-samples with replacement").

Warning: Some authors also refer to injective k-tuples $(s_1, s_2, \ldots, s_k) \in S^k$ as *k-permutations* of S. But this is not the meaning that the word "permutation" has in this text!

We promised that the injective k-tuples (the "legs") would be easy to count; let us do this:

Proposition 2.7.2. Let S be a finite set. Let $k \in \mathbb{N}$. Then, $\left|S^k_{\text{inj}}\right| = |S|^{\underline{k}}$.

Here, we are using the falling factorial notation $n^{\underline{k}}$ (as defined in Definition 2.4.2).

It is easy to prove Proposition 2.7.2 using the "dependent product rule"[182]. However, we have already made more or less the same argument when we proved The-

[181] or "strategic overcounting" (but there is yet another trick that shares this name)

[182] Just argue that an injective k-tuple $(s_1, s_2, \ldots, s_k) \in S^k_{\text{inj}}$ can be constructed by first choosing its first entry s_1 (there are $|S|$ many choices), then choosing its second entry s_2 (there are $|S| - 1$ many choices, since s_2 has to be distinct from s_1), then choosing its third entry s_3 (there are $|S| - 2$ many choices, since s_3 has to be distinct from the two distinct elements s_1 and s_2), and so on, and therefore the total # of injective k-tuples $(s_1, s_2, \ldots, s_k) \in S^k_{\text{inj}}$ must be $|S| \cdot (|S| - 1) \cdot (|S| - 2) \cdot \cdots \cdot (|S| - k + 1) = |S|^{\underline{k}}$.

orem 2.4.4, so instead of doing it again, I find it easier to piggyback on Theorem 2.4.4:

Proof of Proposition 2.7.2. Note that S is a $|S|$-element set, whereas $[k]$ is a k-element set.

The injective k-tuples $(s_1, s_2, \ldots, s_k) \in S^k$ are in one-to-one correspondence with the injective maps from $[k]$ to S. More precisely: If f is an injective map from $[k]$ to S, then the k-tuple $(f(1), f(2), \ldots, f(k)) \in S^k$ is injective (since the injectivity of f forces the values $f(1), f(2), \ldots, f(k)$ to be distinct) and thus belongs to S^k_{inj}. Thus, we can define a map

$$\begin{aligned} \alpha : \{\text{injective maps from } [k] \text{ to } S\} &\to S^k_{\text{inj}}, \\ f &\mapsto (f(1), f(2), \ldots, f(k)). \end{aligned}$$

This map α simply sends every injective map $f : [k] \to S$ to its list of values. It is easy to see that this map α is a bijection[183]. Thus, the bijection principle yields

$$|\{\text{injective maps from } [k] \text{ to } S\}| = \left|S^k_{\text{inj}}\right|.$$

Hence,

$$\begin{aligned} \left|S^k_{\text{inj}}\right| &= |\{\text{injective maps from } [k] \text{ to } S\}| \\ &= (\#\text{ of injective maps from } [k] \text{ to } S) = |S|^{\underline{k}} \end{aligned}$$

(by Theorem 2.4.4, applied to $m = k$, $n = |S|$, $A = [k]$ and $B = S$). This proves Proposition 2.7.2. □

We shall now apply this to obtain a second proof of Theorem 1.3.12, as promised:

Second proof of Theorem 1.3.12 (sketched). We must prove the equality

$$\binom{n}{k} = (\#\text{ of } k\text{-element subsets of } S).$$

[183] Indeed, α has an inverse, which can be constructed as follows: For each injective k-tuple $\mathbf{s} = (s_1, s_2, \ldots, s_k) \in S^k_{\text{inj}}$, we let $f_{\mathbf{s}} : [k] \to S$ be the map that sends $1, 2, \ldots, k$ to $s_1, s_2, \ldots, s_k$, respectively. This map $f_{\mathbf{s}}$ is injective (since its values $s_1, s_2, \ldots, s_k$ are distinct (because $(s_1, s_2, \ldots, s_k)$ is an injective k-tuple)), and thus belongs to $\{\text{injective maps from } [k] \text{ to } S\}$. Hence, we can define a map

$$\begin{aligned} \beta : S^k_{\text{inj}} &\to \{\text{injective maps from } [k] \text{ to } S\}, \\ \mathbf{s} &\mapsto f_{\mathbf{s}}. \end{aligned}$$

It is straightforward to see that the maps α and β are mutually inverse. Hence, the map α is invertible, i.e., bijective, i.e., a bijection.

If $k \notin \mathbb{N}$, then both sides of this equality are 0 (because S has no k-element subsets when $k \notin \mathbb{N}$), and thus the equality is clearly true. Hence, for the rest of this proof, we WLOG assume that $k \in \mathbb{N}$.

We have $|S| = n$ (since S is an n-element set).

For each injective k-tuple $\mathbf{s} = (s_1, s_2, \ldots, s_k) \in S^k_{\text{inj}}$, we let $\operatorname{set} \mathbf{s}$ denote the set $\{s_1, s_2, \ldots, s_k\}$ of all entries of $\mathbf{s}$. This set $\operatorname{set} \mathbf{s}$ is a k-element set (because $s_1, s_2, \ldots, s_k$ are distinct[184]) and a subset of S (because $s_1, s_2, \ldots, s_k$ are elements of S [185]), and thus is a k-element subset of S.

In our informal discussion above, $\operatorname{set} \mathbf{s}$ was playing the role of the "sheep" whose "leg" is the k-tuple $\mathbf{s}$. Now, how many "legs" does a "sheep" have? Let us find out.

Let us fix a k-element subset W of S. Thus, $|W| = k$ (since W is a k-element set). The following observation is easy:

> *Observation 1:* The injective k-tuples $\mathbf{s} \in S^k_{\text{inj}}$ satisfying $\operatorname{set} \mathbf{s} = W$ are precisely the injective k-tuples in W^k_{inj}.

[*Proof of Observation 1:* We must prove the following two claims:

> *Claim 1.1:* Every injective k-tuple $\mathbf{s} \in S^k_{\text{inj}}$ satisfying $\operatorname{set} \mathbf{s} = W$ is an injective k-tuple in W^k_{inj}.
>
> *Claim 1.2:* Every injective k-tuple in W^k_{inj} is an injective k-tuple $\mathbf{s} \in S^k_{\text{inj}}$ satisfying $\operatorname{set} \mathbf{s} = W$.

[*Proof of Claim 1.1:* Let $\mathbf{s} \in S^k_{\text{inj}}$ be an injective k-tuple satisfying $\operatorname{set} \mathbf{s} = W$. We must prove that $\mathbf{s}$ is an injective k-tuple in W^k_{inj}.

Write the k-tuple $\mathbf{s}$ as $\mathbf{s} = (s_1, s_2, \ldots, s_k)$. Then, $\operatorname{set} \mathbf{s} = \{s_1, s_2, \ldots, s_k\}$ (by the definition of $\operatorname{set} \mathbf{s}$), so that $\{s_1, s_2, \ldots, s_k\} = \operatorname{set} \mathbf{s} = W$. Hence, the elements $s_1, s_2, \ldots, s_k$ belong to W (because they clearly belong to $\{s_1, s_2, \ldots, s_k\}$). Therefore, $(s_1, s_2, \ldots, s_k) \in W^k$. In other words, $\mathbf{s} \in W^k$ (since $\mathbf{s} = (s_1, s_2, \ldots, s_k)$). Since the k-tuple $\mathbf{s}$ is injective, this shows that $\mathbf{s} \in W^k_{\text{inj}}$. Hence, $\mathbf{s}$ is an injective k-tuple in W^k_{inj}. This completes the proof of Claim 1.1.]

[*Proof of Claim 1.2:* Let $\mathbf{w}$ be an injective k-tuple in W^k_{inj}. We must prove that $\mathbf{w}$ is an injective k-tuple $\mathbf{s} \in S^k_{\text{inj}}$ satisfying $\operatorname{set} \mathbf{s} = W$. In other words, we must prove that $\mathbf{w}$ is an injective k-tuple that belongs to S^k_{inj} and satisfies $\operatorname{set} \mathbf{w} = W$.

We have $\mathbf{w} \in W^k_{\text{inj}} \subseteq W^k \subseteq S^k$ (since $W \subseteq S$). Thus, $\mathbf{w}$ is an injective k-tuple in S^k; in other words, $\mathbf{w} \in S^k_{\text{inj}}$. Now, write the k-tuple $\mathbf{w}$ in the form $\mathbf{w} = (w_1, w_2, \ldots, w_k)$. Then, $w_1, w_2, \ldots, w_k \in W$ (since $(w_1, w_2, \ldots, w_k) = \mathbf{w} \in W^k_{\text{inj}} \subseteq W^k$), so that $\{w_1, w_2, \ldots, w_k\}$ is a subset of W. Moreover, the k-tuple $(w_1, w_2, \ldots, w_k) = \mathbf{w}$ is injective; in other words, $w_1, w_2, \ldots, w_k$ are distinct. Thus, $\{w_1, w_2, \ldots, w_k\}$ is a k-element set. In other words, $|\{w_1, w_2, \ldots, w_k\}| = k$. Hence, $|\{w_1, w_2, \ldots, w_k\}| = k = |W|$ (since $|W| = k$). Hence, Theorem 1.4.7 **(c)** (applied to $A = W$ and $B = \{w_1, w_2, \ldots, w_k\}$) yields $\{w_1, w_2, \ldots, w_k\} = W$.

[184] since $(s_1, s_2, \ldots, s_k)$ is an injective k-tuple

[185] since $(s_1, s_2, \ldots, s_k) \in S^k_{\text{inj}} \subseteq S^k$

Now, from $\mathbf{w} = (w_1, w_2, \ldots, w_k)$, we obtain $\operatorname{set} \mathbf{w} = \{w_1, w_2, \ldots, w_k\}$ (by the definition of $\operatorname{set} \mathbf{w}$), so that $\operatorname{set} \mathbf{w} = \{w_1, w_2, \ldots, w_k\} = W$. Thus, altogether, we have shown that $\mathbf{w}$ is an injective k-tuple that belongs to S^k_{inj} and satisfies $\operatorname{set} \mathbf{w} = W$. This proves Claim 1.2.]

Combining Claim 1.1 with Claim 1.2, we obtain precisely the claim of Observation 1. Hence, Observation 1 is proven.]

Now, Observation 1 shows that

$$\begin{aligned}
&\left(\#\text{ of injective } k\text{-tuples } \mathbf{s} \in S^k_{\text{inj}} \text{ satisfying } \operatorname{set} \mathbf{s} = W\right) \\
&= \left(\#\text{ of injective } k\text{-tuples in } W^k_{\text{inj}}\right) \\
&= \left|W^k_{\text{inj}}\right| \qquad \left(\text{since all elements of } W^k_{\text{inj}} \text{ are injective } k\text{-tuples}\right) \\
&= |W|^{\underline{k}} \qquad (\text{by Proposition 2.7.2, applied to } W \text{ instead of } S) \\
&= k^{\underline{k}} \qquad (\text{since } |W| = k) \\
&= k! \qquad (192)
\end{aligned}$$

(by Proposition 2.4.3 **(d)**, applied to k instead of n).

Now, forget that we fixed W. We thus have proved (192) for each k-element subset W of S.

Now, recall that for each injective k-tuple $\mathbf{s} \in S^k_{\text{inj}}$, we have defined a k-element subset $\operatorname{set} \mathbf{s}$ of S. In other words, there is a map

$$\begin{aligned}
\left\{\text{injective } k\text{-tuples } \mathbf{s} \in S^k_{\text{inj}}\right\} &\to \{k\text{-element subsets of } S\}, \\
\mathbf{s} &\mapsto \operatorname{set} \mathbf{s}.
\end{aligned}$$

Hence, the sum rule (Theorem 1.2.5) shows that

$$\begin{aligned}
&\left(\#\text{ of injective } k\text{-tuples } \mathbf{s} \in S^k_{\text{inj}}\right) \\
&= \sum_{\substack{W \text{ is a } k\text{-element} \\ \text{subset of } S}} \underbrace{\left(\#\text{ of injective } k\text{-tuples } \mathbf{s} \in S^k_{\text{inj}} \text{ satisfying } \operatorname{set} \mathbf{s} = W\right)}_{\substack{=k! \\ (\text{by (192)})}} \\
&= \sum_{\substack{W \text{ is a } k\text{-element} \\ \text{subset of } S}} k! = (\#\text{ of } k\text{-element subsets of } S) \cdot k!.
\end{aligned}$$

Comparing this equality with

$$\begin{aligned}
&\left(\#\text{ of injective } k\text{-tuples } \mathbf{s} \in S^k_{\text{inj}}\right) \\
&= \left|S^k_{\text{inj}}\right| \qquad \left(\text{since all elements of } S^k_{\text{inj}} \text{ are injective } k\text{-tuples}\right) \\
&= |S|^{\underline{k}} \qquad (\text{by Proposition 2.7.2}) \\
&= n^{\underline{k}} \qquad (\text{since } |S| = n) \\
&= k! \cdot \binom{n}{k} \qquad (\text{by Proposition 2.4.3 } \textbf{(c)}),
\end{aligned}$$

we obtain

$$k! \cdot \binom{n}{k} = (\#\text{ of } k\text{-element subsets of } S) \cdot k!.$$

We can divide both sides of this equality by $k!$ (since $k! = 1 \cdot 2 \cdot \cdots \cdot k$ is clearly a nonzero integer), and thus obtain

$$\binom{n}{k} = (\#\text{ of } k\text{-element subsets of } S).$$

Hence, Theorem 1.3.12 is proved again. □

Class of 2019-10-30

2.8. Another use of polynomials

We have already seen how binomial identities (i.e., identities that involve binomial coefficients) can be proved using the "polynomial identity trick". This is not the only application of polynomials to proving binomial identities. We shall now see another application (which is actually a foretaste of a comprehensive method – the method of *generating functions*), in which polynomials are not merely evaluated at numbers, but also compared coefficientwise. This application will be (yet) another proof of the Chu–Vandermonde identity (specifically, (172)). As in our second proof of Theorem 2.6.1, we will only prove it in the case when $x, y \in \mathbb{N}$, but as we already know, the polynomial identity trick allows us to extend such a proof to the general case more or less automatically, so we don't lose any generality by restricting ourselves to such a case.

Before we come to this new proof of the Chu–Vandermonde identity, let us state a simple lemma:

Lemma 2.8.1. Let $p \in \mathbb{N}$. Then,

$$(1+X)^p = \sum_{m \in \mathbb{N}} \binom{p}{m} X^m$$

(an equality between polynomials in 1 variable X with real coefficients). Here, the sum on the right hand side is infinite, but it is well-defined because only finitely many of its addends are nonzero.

Proof of Lemma 2.8.1 (sketched). We have stated Theorem 1.3.24 only for the case when x and y are real numbers; however, it also holds when x and y are polynomials (and the same proof that we gave applies in this case). Thus, we can apply Theorem 1.3.24 to $n = p$, $x = X$ and $y = 1$. We thus obtain[186]

$$(X+1)^p = \sum_{k=0}^{p} \binom{p}{k} X^k \underbrace{1^{p-k}}_{=1} = \sum_{k=0}^{p} \binom{p}{k} X^k \overset{0}{=} \sum_{k \in \mathbb{N}} \binom{p}{k} X^k.$$

[186]See Remark 2.6.2 for the meaning of the "$\overset{0}{=}$" sign.

Here, the "$\overset{0}{=}$" sign is owed to the fact that all integers k satisfying $k > p$ satisfy $\binom{p}{k} = 0$ (by Proposition 1.3.6, applied to $n = p$) and thus $\binom{p}{k} X^k = 0$. This also shows that the infinite sum $\sum_{k \in \mathbb{N}} \binom{p}{k} X^k$ has only finitely many nonzero addends, and thus is well-defined. Now,

$$(X+1)^p = \sum_{k \in \mathbb{N}} \binom{p}{k} X^k = \sum_{m \in \mathbb{N}} \binom{p}{m} X^m$$

(here, we have renamed the summation index k as m). In view of $X + 1 = 1 + X$, we can rewrite this as

$$(1+X)^p = \sum_{m \in \mathbb{N}} \binom{p}{m} X^m.$$

This proves Lemma 2.8.1. □

Fourth proof of Theorem 2.6.1 for $x, y \in \mathbb{N}$ (sketched). Assume that $x, y \in \mathbb{N}$. We shall only prove the equality (172) (since we have already seen how to derive (173) from it).

Rename x and y as a and b. Thus, $a, b \in \mathbb{N}$, and we must prove the equality

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}. \tag{193}$$

Let us work with polynomials in one variable X, with real coefficients. Lemma 2.8.1 (applied to $p = a$) yields

$$(1+X)^a = \sum_{m \in \mathbb{N}} \binom{a}{m} X^m = \sum_{i \in \mathbb{N}} \binom{a}{i} X^i$$

(here, we have renamed the summation index m as i). Similarly,

$$(1+X)^b = \sum_{j \in \mathbb{N}} \binom{b}{j} X^j.$$

Multiplying these two equalities, we obtain

$$
\begin{aligned}
&(1+X)^a \cdot (1+X)^b \\
&= \left(\sum_{i \in \mathbb{N}} \binom{a}{i} X^i \right) \cdot \left(\sum_{j \in \mathbb{N}} \binom{b}{j} X^j \right) \\
&= \sum_{i \in \mathbb{N}} \underbrace{\binom{a}{i} X^i \sum_{j \in \mathbb{N}} \binom{b}{j} X^j}_{= \sum_{j \in \mathbb{N}} \binom{a}{i} X^i \binom{b}{j} X^j} = \sum_{i \in \mathbb{N}} \sum_{j \in \mathbb{N}} \underbrace{\binom{a}{i} X^i \binom{b}{j} X^j}_{= \binom{a}{i}\binom{b}{j} X^{i+j}} \\
&= \sum_{i \in \mathbb{N}} \sum_{j \in \mathbb{N}} \binom{a}{i}\binom{b}{j} X^{i+j} = \sum_{(i,j) \in \mathbb{N}^2} \binom{a}{i}\binom{b}{j} X^{i+j} \\
&\qquad \left(\begin{array}{c} \text{by the first equality sign in Theorem 1.6.11,} \\ \text{since only finitely many } (i,j) \in \mathbb{N}^2 \text{ satisfy } \binom{a}{i}\binom{b}{j} X^{i+j} \neq 0 \end{array} \right) \\
&= \sum_{m \in \mathbb{N}} \sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=m}} \binom{a}{i}\binom{b}{j} \underbrace{X^{i+j}}_{\substack{= X^m \\ (\text{since } i+j=m)}} \\
&\qquad (\text{here, we have used the analogue of (37) for infinite sums}) \\
&= \sum_{m \in \mathbb{N}} \underbrace{\sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=m}} \binom{a}{i}\binom{b}{j} X^m}_{= \left(\sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=m}} \binom{a}{i}\binom{b}{j} \right) X^m} \\
&= \sum_{m \in \mathbb{N}} \left(\sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=m}} \binom{a}{i}\binom{b}{j} \right) X^m .
\end{aligned}
$$

Comparing this with

$$
\begin{aligned}
&(1+X)^a \cdot (1+X)^b \\
&= (1+X)^{a+b} \qquad \left(\begin{array}{c} \text{since the product rule for exponents, } u^a \cdot u^b = u^{a+b}, \\ \text{holds for polynomials just as it holds for numbers} \end{array} \right) \\
&= \sum_{m \in \mathbb{N}} \binom{a+b}{m} X^m \qquad (\text{by Lemma 2.8.1, applied to } p = a+b) ,
\end{aligned}
$$

we obtain

$$\sum_{m\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}^2; \\ i+j=m}} \binom{a}{i}\binom{b}{j} \right) X^m = \sum_{m\in\mathbb{N}} \binom{a+b}{m} X^m. \tag{194}$$

We can thus define a polynomial P by

$$P = \sum_{m\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}^2; \\ i+j=m}} \binom{a}{i}\binom{b}{j} \right) X^m = \sum_{m\in\mathbb{N}} \binom{a+b}{m} X^m.$$

Now, from $P = \sum_{m\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}^2; \\ i+j=m}} \binom{a}{i}\binom{b}{j} \right) X^m$, we obtain

$$(\text{the } n\text{-th coefficient of } P) = \sum_{\substack{(i,j)\in\mathbb{N}^2; \\ i+j=n}} \binom{a}{i}\binom{b}{j}. \tag{195}$$

Meanwhile, from $P = \sum_{m\in\mathbb{N}} \binom{a+b}{m} X^m$, we obtain

$$(\text{the } n\text{-th coefficient of } P) = \binom{a+b}{n}.$$

Comparing this with (195), we obtain

$$\binom{a+b}{n} = \sum_{\substack{(i,j)\in\mathbb{N}^2; \\ i+j=n}} \binom{a}{i}\binom{b}{j} = \sum_{k\in\{0,1,\ldots,n\}} \binom{a}{k}\binom{b}{n-k}$$

(here, we have substituted $(k, n-k)$ for (i,j) in the sum, since the map

$$\begin{aligned} \{0,1,\ldots,n\} &\to \left\{ (i,j) \in \mathbb{N}^2 \mid i+j=n \right\}, \\ k &\mapsto (k, n-k) \end{aligned}$$

is a bijection[187]). This is precisely the equality (193) (since the summation sign $\sum_{k=0}^{n}$ is a synonym for $\sum_{k\in\{0,1,\ldots,n\}}$). Thus, (193) holds. As we have said, this proves Theorem 2.6.1 in the case when $x, y \in \mathbb{N}$. □

[187] In informal terms, this is just saying that each pair $(i,j) \in \mathbb{N}^2$ of nonnegative integers satisfying $i+j=n$ has the form $(k, n-k)$ for a unique $k \in \{0,1,\ldots,n\}$ (namely, for $k=i$), and conversely, any pair of the latter form is a pair $(i,j) \in \mathbb{N}^2$ of nonnegative integers satisfying $i+j=n$.

The proof we just gave used polynomials, but not via the polynomial identity trick. Instead, we obtained an equality between two polynomials (viz., (194)), and then compared coefficients (i.e., argued that two equal polynomials have equal n-th coefficients). This relies on the fact that any polynomial has a well-defined n-th coefficient for each $n \in \mathbb{N}$, which does not depend on how the polynomial is expressed. This is a versatile tactic, and we will later apply it to more general objects than polynomials. But even when restricted to polynomials, it is rather useful. Instead of proving Theorem 2.6.1 again and again, we can apply it to obtain a new equality:

Exercise 2.8.1. **(a)** Prove that

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} \binom{n}{m-k} = \begin{cases} (-1)^{m/2} \binom{n}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases}$$

for any $n \in \mathbb{N}$ and any $m \in \mathbb{N}$.

(b) Prove that the claim of Exercise 2.8.1 **(a)** holds, more generally, for all $n \in \mathbb{R}$ (rather than only for $n \in \mathbb{N}$).

(c) Conclude that every $n \in \mathbb{N}$ satisfies

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^2 = \begin{cases} (-1)^{n/2} \binom{n}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

[**Hint:** For part **(a)**, compare coefficients in the equality $(1-X)^n \cdot (1+X)^n = \left(1-X^2\right)^n$ (expanded, once again, using the binomial formula). For part **(b)**, apply the polynomial identity trick.]

Exercise 2.8.1 **(c)**, in turn, can be used to derive another binomial identity:

Exercise 2.8.2. Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{n} (-2)^k \binom{n}{k} \binom{2n-k}{n-k} = \begin{cases} (-1)^{n/2} \binom{n}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

2.9. The Principle of Inclusion and Exclusion

We shall now come to an important tool for counting: the *Principle of Inclusion and Exclusion*. We shall first present this principle in four forms (Theorem 2.9.1, Theorem 2.9.6, Theorem 2.9.7 and Theorem 2.9.9); then we will prove it in Subsection 2.9.3 (after proving a simple but important identity in Subsection 2.9.2, which will help in our proofs), and show some applications in the remaining subsections.

2.9.1. The principles

We begin with some simple facts about unions and intersections of finite sets.

If A_1 and A_2 are two disjoint finite sets, then $|A_1 \cup A_2| = |A_1| + |A_2|$. (This is just the equality (4), with X and Y renamed as A_1 and A_2.) Is there a similar formula for $|A_1 \cup A_2|$ when A_1 and A_2 are not disjoint? Yes, if $|A_1 \cap A_2|$ is known. Namely,

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| \tag{196}$$

for any two finite sets A_1 and A_2. This is fairly easy to check. A similar but more complicated formula holds for 3 sets: namely,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ + |A_1 \cap A_2 \cap A_3| \end{aligned} \tag{197}$$

for any three finite sets A_1, A_2 and A_3. A further formula of the same kind holds for 4 sets: namely,

$$\begin{aligned} &|A_1 \cup A_2 \cup A_3 \cup A_4| \\ &= |A_1| + |A_2| + |A_3| + |A_4| \\ &\quad - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4| \\ &\quad + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\ &\quad - |A_1 \cap A_2 \cap A_3 \cap A_4| \end{aligned} \tag{198}$$

for any four finite sets A_1, A_2, A_3 and A_4. These three formulas (along with the trivial formula $|A_1| = |A_1|$ for a single set A_1) all are particular cases of one general fact, which expresses the size of the union of n finite sets through the sizes of their intersections (more precisely, of the intersection of each k of these sets):

Theorem 2.9.1 (Principle of Inclusion and Exclusion (union form))**.** Let $n \in \mathbb{N}$. Let $A_1, A_2, \ldots, A_n$ be n finite sets. Then,

$$\begin{aligned} &|A_1 \cup A_2 \cup \cdots \cup A_n| \\ &= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left| A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m} \right|. \end{aligned} \tag{199}$$

The nested sum on the right hand side of (199) is somewhat daunting, so let us

write it out: It is

$$\begin{aligned}
&\underbrace{|A_1| + |A_2| + \cdots + |A_n|}_{\substack{\text{the sizes of all } A_i \\ \text{(summed with + signs)}}} \\
&\quad \underbrace{- |A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_{n-1} \cap A_n|}_{\substack{\text{the sizes of all intersections } A_i \cap A_j \text{ (with } i<j\text{)} \\ \text{(summed with } - \text{ signs)}}} \\
&\quad \underbrace{+ |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \cdots + |A_{n-2} \cap A_{n-1} \cap A_n|}_{\substack{\text{the sizes of all intersections } A_i \cap A_j \cap A_k \text{ (with } i<j<k\text{)} \\ \text{(summed with + signs)}}} \\
&\quad \pm \cdots \\
&\quad + \underbrace{(-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|}_{\substack{\text{the size of the intersection } A_1 \cap A_2 \cap \cdots \cap A_n \\ \text{(summed with a + or } - \text{ sign depending on the parity of } n\text{)}}} .
\end{aligned}$$

Thus, it is a sum that contains the sizes of all possible intersections of some of the sets $A_1, A_2, \ldots, A_n$, each with a $+$ or $-$ sign depending on how many sets are being intersected. Clearly, the right hand sides of (196), (197) and (198) are the particular cases of this sum obtained for $n = 2$, $n = 3$ and $n = 4$, respectively.

Theorem 2.9.1 is known as the *Principle of Inclusion and Exclusion* (often abbreviated *PIE*) or the *Sylvester sieve formula*. We will not prove it right away, since this will become easier once we have restated it in a more abstract form. This abstract form (which also makes it more convenient to apply) relies on the following notation from set theory:

Definition 2.9.2. Let I be a nonempty set. For each $i \in I$, let A_i be a set. Then, $\bigcap_{i \in I} A_i$ denotes the set

$$\{x \mid x \in A_i \text{ for each } i \in I\}.$$

This set $\bigcap_{i \in I} A_i$ is called the intersection of all A_i with $i \in I$.

It is easy to see that if $I = \{i_1, i_2, \ldots, i_m\}$ is a finite set, and if A_i is a set for each $i \in I$, then

$$\bigcap_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m}. \tag{200}$$

Example 2.9.3. Let $I = [5]$. For each $i \in I$, let $A_i = [i-8, i] = \{i-8, i-7, \ldots, i-1, i\}$ (where we are using the notation from Definition 1.4.17).

Then,

$$\begin{aligned}\bigcap_{i\in I} A_i &= \underbrace{A_1}_{\substack{=[1-8,1]\\=[-7,1]}} \cap \underbrace{A_2}_{\substack{=[2-8,2]\\=[-6,2]}} \cap \underbrace{A_3}_{\substack{=[3-8,3]\\=[-5,3]}} \cap \underbrace{A_4}_{\substack{=[4-8,4]\\=[-4,4]}} \cap \underbrace{A_5}_{\substack{=[5-8,5]\\=[-3,5]}} \\ &= [-7,1] \cap [-6,2] \cap [-5,3] \cap [-4,4] \cap [-3,5] \\ &= [-3,1] = \{-3,-2,-1,0,1\}.\end{aligned}$$

Note the similarity between the notation $\bigcap_{i\in I} A_i$ (for the intersection of a family of sets) and the notation $\sum_{i\in I} a_i$ (for the sum of a finite family of numbers). However, in the notation $\bigcap_{i\in I} A_i$, the set I must be nonempty (unlike in $\sum_{i\in I} a_i$) but can be infinite (unlike in $\sum_{i\in I} a_i$, which is usually undefined when I is infinite).

We can now rewrite the right hand side of (199) as follows:

Proposition 2.9.4. Let $n \in \mathbb{N}$. Let $A_1, A_2, \ldots, A_n$ be n finite sets. Then,

$$\sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m)\in[n]^m;\\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m}\right| = \sum_{\substack{I\subseteq[n];\\ I\neq\varnothing}} (-1)^{|I|-1} \left|\bigcap_{i\in I} A_i\right|.$$

Example 2.9.5. Set $n = 3$ in Proposition 2.9.4. Then, the claim of Proposition 2.9.4 becomes

$$\begin{aligned}&(-1)^{1-1}(|A_1|+|A_2|+|A_3|) \\ &\quad+(-1)^{2-1}(|A_1\cap A_2|+|A_1\cap A_3|+|A_2\cap A_3|) \\ &\quad+(-1)^{3-1}|A_1\cap A_2\cap A_3| \\ &=(-1)^{|\{1\}|-1}\left|\bigcap_{i\in\{1\}} A_i\right|+(-1)^{|\{2\}|-1}\left|\bigcap_{i\in\{2\}} A_i\right|+(-1)^{|\{3\}|-1}\left|\bigcap_{i\in\{3\}} A_i\right| \\ &\quad+(-1)^{|\{1,2\}|-1}\left|\bigcap_{i\in\{1,2\}} A_i\right|+(-1)^{|\{1,3\}|-1}\left|\bigcap_{i\in\{1,3\}} A_i\right| \\ &\quad+(-1)^{|\{2,3\}|-1}\left|\bigcap_{i\in\{2,3\}} A_i\right|+(-1)^{|\{1,2,3\}|-1}\left|\bigcap_{i\in\{1,2,3\}} A_i\right|\end{aligned}$$

(since the subsets I of $[n]$ that satisfy $I \neq \varnothing$ are $\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}$). You can easily confirm this by checking that the addends on the left hand side (after the parentheses are expanded) are precisely the addends on the right hand side.

Proof of Proposition 2.9.4. We first claim the following:

Claim 1: Let $m \in \{1,2,\ldots,n\}$. Then,

$$\sum_{\substack{(i_1,i_2,\ldots,i_m)\in[n]^m;\\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m}\right| = \sum_{\substack{I\subseteq[n];\\ I\neq\varnothing;\\ |I|=m}} \left|\bigcap_{i\in I} A_i\right|.$$

[*Proof of Claim 1:* We have $m > 0$ (since $m \in \{1,2,\ldots,n\}$). Now, if I is a subset of $[n]$ that satisfies $|I| = m$, then it satisfies $I \neq \varnothing$ (since $|I| = m > 0$). Hence, the condition "$I \neq \varnothing$" under the summation sign $\sum_{\substack{I\subseteq[n];\\ I\neq\varnothing;\\ |I|=m}}$ is redundant (i.e., the sum does not change if we remove it). Thus,

$$\begin{aligned}\sum_{\substack{I\subseteq[n];\\ I\neq\varnothing;\\ |I|=m}} \left|\bigcap_{i\in I} A_i\right| &= \sum_{\substack{I\subseteq[n];\\ |I|=m}} \left|\bigcap_{i\in I} A_i\right| \\ &= \sum_{I\in\{m\text{-element subsets of } [n]\}} \left|\bigcap_{i\in I} A_i\right|. \end{aligned} \tag{201}$$

For any m-tuple $(i_1,i_2,\ldots,i_m) \in [n]^m$ satisfying $i_1 < i_2 < \cdots < i_m$, the set $\{i_1,i_2,\ldots,i_m\}$ is an m-element subset of $[n]$ [188]. Thus, the map

$$\begin{aligned}\left\{(i_1,i_2,\ldots,i_m) \in [n]^m \mid i_1 < i_2 < \cdots < i_m\right\} &\to \{m\text{-element subsets of } [n]\}, \\ (i_1,i_2,\ldots,i_m) &\mapsto \{i_1,i_2,\ldots,i_m\}\end{aligned}$$

is well-defined. Moreover, this map is bijective[189]. Hence, we can substitute

[188] *Proof.* Let $(i_1,i_2,\ldots,i_m) \in [n]^m$ be an m-tuple satisfying $i_1 < i_2 < \cdots < i_m$. Thus, $i_1,i_2,\ldots,i_m \in [n]$; hence, $\{i_1,i_2,\ldots,i_m\}$ is a subset of $[n]$. Moreover, the numbers $i_1,i_2,\ldots,i_m$ are distinct (since $i_1 < i_2 < \cdots < i_m$), and thus the set $\{i_1,i_2,\ldots,i_m\}$ has m elements. Hence, $\{i_1,i_2,\ldots,i_m\}$ is an m-element set. Therefore, $\{i_1,i_2,\ldots,i_m\}$ is an m-element subset of $[n]$.

[189] Indeed, this can easily be derived from Proposition 1.4.13.

$\{i_1, i_2, \ldots, i_m\}$ for I in the sum $\sum_{I \in \{m\text{-element subsets of } [n]\}} \left| \bigcap_{i \in I} A_i \right|$. We thus obtain

$$\begin{aligned}\sum_{I \in \{m\text{-element subsets of } [n]\}} \left| \bigcap_{i \in I} A_i \right| &= \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left| \underbrace{\bigcap_{i \in \{i_1,i_2,\ldots,i_m\}} A_i}_{\substack{= A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m} \\ \text{(by (200))}}} \right| \\ &= \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left| A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m} \right|.\end{aligned}$$

Hence, (201) becomes

$$\sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing; \\ |I| = m}} \left| \bigcap_{i \in I} A_i \right| = \sum_{I \in \{m\text{-element subsets of } [n]\}} \left| \bigcap_{i \in I} A_i \right| = \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left| A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m} \right|.$$

This proves Claim 1.]

Now, for any subset I of $[n]$ satisfying $I \neq \varnothing$, we have $|I| \in \{1, 2, \ldots, n\}$ [190].

[190] *Proof.* Let I be a subset of $[n]$ satisfying $I \neq \varnothing$. Then, Theorem 1.4.7 **(b)** (applied to $A = [n]$ and $B = I$) yields $|I| \leq |[n]| = n$. Also, $|I| > 0$ (since $I \neq \varnothing$) and thus $|I| \geq 1$. Combining this with $|I| \leq n$, we obtain $|I| \in \{1, 2, \ldots, n\}$, qed.

Hence, an application of (37) yields

$$\begin{aligned}
\sum_{\substack{I\subseteq[n];\\ I\neq\varnothing}} (-1)^{|I|-1} \left|\bigcap_{i\in I} A_i\right| &= \sum_{m\in\{1,2,\ldots,n\}} \sum_{\substack{I\subseteq[n];\\ I\neq\varnothing;\\ |I|=m}} \underbrace{(-1)^{|I|-1}}_{\substack{=(-1)^{m-1}\\ \text{(since } |I|=m\text{)}}} \left|\bigcap_{i\in I} A_i\right| \\
&= \sum_{m\in\{1,2,\ldots,n\}} \underbrace{\sum_{\substack{I\subseteq[n];\\ I\neq\varnothing;\\ |I|=m}} (-1)^{m-1} \left|\bigcap_{i\in I} A_i\right|}_{=(-1)^{m-1} \sum\limits_{\substack{I\subseteq[n];\\ I\neq\varnothing;\\ |I|=m}} \left|\bigcap\limits_{i\in I} A_i\right|} \\
&= \sum_{m\in\{1,2,\ldots,n\}} (-1)^{m-1} \underbrace{\sum_{\substack{I\subseteq[n];\\ I\neq\varnothing;\\ |I|=m}} \left|\bigcap_{i\in I} A_i\right|}_{= \sum\limits_{\substack{(i_1,i_2,\ldots,i_m)\in[n]^m;\\ i_1<i_2<\cdots<i_m}} \left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_m}\right| \text{ (by Claim 1)}} \\
&= \underbrace{\sum_{m\in\{1,2,\ldots,n\}}}_{=\sum\limits_{m=1}^{n}} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m)\in[n]^m;\\ i_1<i_2<\cdots<i_m}} \left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_m}\right| \\
&= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m)\in[n]^m;\\ i_1<i_2<\cdots<i_m}} \left|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_m}\right|.
\end{aligned}$$

This proves Proposition 2.9.4. □

We can now restate Theorem 2.9.6 as follows:

Theorem 2.9.6 (Principle of Inclusion and Exclusion (union form))**.** Let $n \in \mathbb{N}$. Let $A_1, A_2, \ldots, A_n$ be n finite sets. Then,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\substack{I\subseteq[n];\\ I\neq\varnothing}} (-1)^{|I|-1} \left|\bigcap_{i\in I} A_i\right|. \tag{202}$$

We will soon prove Theorem 2.9.6 (and thus conclude Theorem 2.9.1 from it). First, let us state yet another equivalent version of this principle:

Theorem 2.9.7 (Principle of Inclusion and Exclusion (complement form))**.** Let $n \in \mathbb{N}$. Let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Then,

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|. \tag{203}$$

Here, the "empty" intersection $\bigcap_{i \in \varnothing} A_i$ is understood to mean the set U.

Example 2.9.8. Let U be a finite set, and let A_1 and A_2 be two subsets of U. Then, Theorem 2.9.7 (applied to $n = 2$) says that

$$\begin{aligned}
|U \setminus (A_1 \cup A_2)| &= \sum_{I \subseteq [2]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right| \\
&= \underbrace{(-1)^{|\varnothing|}}_{=1} \left| \underbrace{\bigcap_{i \in \varnothing} A_i}_{\substack{=U \\ \text{(by definition)}}} \right| + \underbrace{(-1)^{|\{1\}|}}_{=-1} \left| \underbrace{\bigcap_{i \in \{1\}} A_i}_{=A_1} \right| \\
&\quad + \underbrace{(-1)^{|\{2\}|}}_{=-1} \left| \underbrace{\bigcap_{i \in \{2\}} A_i}_{=A_2} \right| + \underbrace{(-1)^{|\{1,2\}|}}_{=1} \left| \underbrace{\bigcap_{i \in \{1,2\}} A_i}_{=A_1 \cap A_2} \right| \\
&\qquad \left(\text{since the subsets of } [2] \text{ are } \varnothing, \{1\}, \{2\}, \{1,2\}\right) \\
&= |U| + (-1)\,|A_1| + (-1)\,|A_2| + |A_1 \cap A_2| \\
&= |U| - |A_1| - |A_2| + |A_1 \cap A_2|\,.
\end{aligned}$$

A remark is in order here. In Definition 2.9.2, we have defined $\bigcap_{i \in I} A_i$ for any **nonempty** set I. This definition cannot be extended to the case when $I = \varnothing$, because it would entail that $\bigcap_{i \in \varnothing} A_i$ should be the set of **all** objects whatsoever, but there is no such set[191]. However, in order for the right hand side of (203) to make sense, we need a well-defined set $\bigcap_{i \in I} A_i$ for all $I \subseteq [n]$, including $I = \varnothing$. Thus, we need to define $\bigcap_{i \in \varnothing} A_i$ somehow. It turns out that defining $\bigcap_{i \in \varnothing} A_i$ to be U is the right thing to do (in this particular situation). It is justified here, because all of the sets involved are subsets of U, so "all objects" can be interpreted as "all elements of U"

[191] See [LeLeMe16, §8.3] for an explanation.

(and then the set of all objects really becomes U). This is, by the way, the reason why we chose the letter U in Theorem 2.9.7; it stands for "universe".

Finally, let us restate Theorem 2.9.7 in an equivalent form that is slightly easier to actually use, because it shuns the notation $\bigcap_{i \in I} A_i$ (and thus avoids having to define it separately for $I = \varnothing$):

Theorem 2.9.9 (Principle of Inclusion and Exclusion (complement form, simplified))**.** Let $n \in \mathbb{N}$. Let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Then,

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \{ s \in U \mid s \in A_i \text{ for all } i \in I \} \right|.$$

Note that the addend corresponding to $I = \varnothing$ on the right hand side of this equality is simply $|U|$ [192].

2.9.2. The cancellation lemma

We have now stated the Principle of Inclusion and Exclusion in four forms (Theorem 2.9.1, Theorem 2.9.6, Theorem 2.9.7 and Theorem 2.9.9). Soon we shall prove them. First, we state a crucial theorem that will serve as an auxiliary tool in the proofs:

Proposition 2.9.10. Let S be a finite set. Then,

$$\sum_{I \subseteq S} (-1)^{|I|} = [S = \varnothing].$$

Once again, we are using the Iverson bracket notation here (see Definition 1.3.15).

Example 2.9.11. The subsets of $\{1,2\}$ are $\varnothing$, $\{1\}$, $\{2\}$ and $\{1,2\}$. Thus, applying Proposition 2.9.10 to $S = \{1,2\}$, we find

$$\underbrace{(-1)^{|\varnothing|}}_{=1} + \underbrace{(-1)^{|\{1\}|}}_{=-1} + \underbrace{(-1)^{|\{2\}|}}_{=-1} + \underbrace{(-1)^{|\{1,2\}|}}_{=1} = [\{1,2\} = \varnothing].$$

[192] *Proof.* This addend is

$$\underbrace{(-1)^{|\varnothing|}}_{=1} \left| \underbrace{\{ s \in U \mid s \in A_i \text{ for all } i \in \varnothing \}}_{\substack{=\{s \in U\} \\ \text{(because each } s \in U \text{ satisfies } (s \in A_i \text{ for all } i \in \varnothing) \\ \text{(indeed, this is vacuously true, since there exists no } i \in \varnothing))}} \right| = \left| \underbrace{\{ s \in U \}}_{=U} \right| = |U|.$$

Indeed, both sides of this equality are 0 (the left hand side because the addends cancel; the right hand side because $\{1,2\} \neq \varnothing$).

First proof of Proposition 2.9.10. This will be similar to the proof of Theorem 1.4.1 that we gave in Subsection 1.4.2.

We have $S = \varnothing$ if and only if $|S| = 0$. In other words, "$S = \varnothing$" and "$|S| = 0$" are two equivalent logical statements. Hence, Exercise 1.3.3 **(a)** (applied to $\mathcal{A} =$ ("$S = \varnothing$") and $\mathcal{B} =$ ("$|S| = 0$")) yields $[S = \varnothing] = [|S| = 0]$.

Let $n = |S|$. Hence, S is an n-element set. If I is any subset of S, then Theorem 1.4.7 **(b)** (applied to $A = S$ and $B = I$) yields $|I| \leq |S| = n$ and therefore $|I| \in \{0, 1, \ldots, n\}$. Hence, an application of (37) yields

$$\begin{aligned}
&\sum_{I \subseteq S} (-1)^{|I|} \\
&= \sum_{k \in \{0,1,\ldots,n\}} \sum_{\substack{I \subseteq S; \\ |I| = k}} \underbrace{(-1)^{|I|}}_{\substack{= (-1)^k \\ \text{(since } |I| = k\text{)}}} = \sum_{k \in \{0,1,\ldots,n\}} \underbrace{\sum_{\substack{I \subseteq S; \\ |I| = k}} (-1)^k}_{\substack{= (\#\text{ of subsets } I \text{ of } S \text{ satisfying } |I| = k) \cdot (-1)^k}} \\
&= \underbrace{\sum_{k \in \{0,1,\ldots,n\}}}_{= \sum_{k=0}^{n}} \underbrace{(\#\text{ of subsets } I \text{ of } S \text{ satisfying } |I| = k)}_{\substack{= (\#\text{ of } k\text{-element subsets of } S) \\ = \binom{n}{k} \\ \text{(by Theorem 1.3.12)}}} \cdot (-1)^k \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n = 0] \qquad \text{(by Proposition 1.3.28)} \\
&= [|S| = 0] \qquad (\text{since } n = |S|) \\
&= [S = \varnothing] \qquad (\text{since } [S = \varnothing] = [|S| = 0]).
\end{aligned}$$

This proves Proposition 2.9.10. □

Second proof of Proposition 2.9.10. If $S = \varnothing$, then Proposition 2.9.10 holds[193]. Hence, for the rest of this proof, we WLOG assume that we don't have $S = \varnothing$. Thus, $S \neq \varnothing$.

[193] *Proof.* Assume that $S = \varnothing$. Thus, there exists exactly one subset of S, namely the empty set $\varnothing$. Hence, the sum $\sum_{I \subseteq S} (-1)^{|I|}$ has exactly one addend, namely the addend for $I = \varnothing$. Thus, this sum simplifies as follows:

$$\sum_{I \subseteq S} (-1)^{|I|} = (-1)^{|\varnothing|} = 1 \qquad (\text{since } |\varnothing| = 0 \text{ is even}).$$

Comparing this with

$$[S = \varnothing] = 1 \qquad (\text{since } S = \varnothing),$$

we obtain $\sum_{I \subseteq S} (-1)^{|I|} = [S = \varnothing]$. Hence, Proposition 2.9.10 is proven under the assumption that $S = \varnothing$.

Hence, there exists some $g \in S$. Consider this g. (We can have many choices for g, but we just pick one.)

Each subset I of S must satisfy either $g \in I$ or $g \notin I$ (but not both at the same time). Hence, we can split the sum $\sum_{I \subseteq S} (-1)^{|I|}$ as follows:

$$\sum_{I \subseteq S} (-1)^{|I|} = \sum_{\substack{I \subseteq S; \\ g \in I}} (-1)^{|I|} + \sum_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I|}. \tag{204}$$

We shall now "set the two sums on the right hand side up to fight each other".

Each subset J of S satisfies $J \cup \{g\} \subseteq S$ (because $g \in S$) and $g \in J \cup \{g\}$ (obviously). Thus, the map[194]

$$\begin{aligned} \{I \subseteq S \mid g \notin I\} &\to \{I \subseteq S \mid g \in I\}, \\ J &\mapsto J \cup \{g\} \end{aligned}$$

is well-defined. The map

$$\begin{aligned} \{I \subseteq S \mid g \in I\} &\to \{I \subseteq S \mid g \notin I\}, \\ K &\mapsto K \setminus \{g\} \end{aligned}$$

is also well-defined. These two maps are mutually inverse[195], and thus are bijections. Hence, in particular, the map

$$\begin{aligned} \{I \subseteq S \mid g \notin I\} &\to \{I \subseteq S \mid g \in I\}, \\ J &\mapsto J \cup \{g\} \end{aligned}$$

is a bijection. Thus, we can substitute $J \cup \{g\}$ for I in the sum $\sum_{\substack{I \subseteq S; \\ g \in I}} (-1)^{|I|}$. We thus obtain

$$\begin{aligned} \sum_{\substack{I \subseteq S; \\ g \in I}} (-1)^{|I|} &= \sum_{\substack{J \subseteq S; \\ g \notin J}} \underbrace{(-1)^{|J \cup \{g\}|}}_{\substack{=(-1)^{|J|+1} \\ \text{(since } |J \cup \{g\}| = |J|+1 \\ \text{(because } g \notin J))}} = \sum_{\substack{J \subseteq S; \\ g \notin J}} \underbrace{(-1)^{|J|+1}}_{=-(-1)^{|J|}} = -\sum_{\substack{J \subseteq S; \\ g \notin J}} (-1)^{|J|} \\ &= -\sum_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I|} \end{aligned} \tag{205}$$

[194] The notation "$\{I \subseteq S \mid g \notin I\}$" means "the set of all subsets I of S satisfying $g \notin I$". Similarly, the notation "$\{I \subseteq S \mid g \in I\}$" means "the set of all subsets I of S satisfying $g \in I$".

[195] because of the following two (easily proven) facts:

- Every subset J of S satisfying $g \notin J$ must satisfy $(J \cup \{g\}) \setminus \{g\} = J$.
- Every subset K of S satisfying $g \in K$ must satisfy $(K \setminus \{g\}) \cup \{g\} = K$.

(here, we have renamed the summation index J as I).

Now, (204) becomes

$$\sum_{I\subseteq S}(-1)^{|I|} = \underbrace{\sum_{\substack{I\subseteq S;\\ g\in I}}(-1)^{|I|}}_{=-\sum\limits_{\substack{I\subseteq S;\\ g\notin I}}(-1)^{|I|} \text{ (by (205))}} + \sum_{\substack{I\subseteq S;\\ g\notin I}}(-1)^{|I|} = -\sum_{\substack{I\subseteq S;\\ g\notin I}}(-1)^{|I|} + \sum_{\substack{I\subseteq S;\\ g\notin I}}(-1)^{|I|} = 0.$$

Comparing this with

$$[S=\varnothing] = 0 \qquad (\text{since } S\neq\varnothing),$$

we obtain $\sum\limits_{I\subseteq S}(-1)^{|I|} = [S=\varnothing]$. This proves Proposition 2.9.10. □

We note that there is a generalization of Proposition 2.9.10, which we will not use anytime soon but which is nevertheless rather useful:

Proposition 2.9.12. Let S be a finite set. Let T be a subset of S. Then,

$$\sum_{\substack{I\subseteq S;\\ T\subseteq I}}(-1)^{|I|} = (-1)^{|T|}\,[S=T].$$

Exercise 2.9.1. Prove Proposition 2.9.12.

Clearly, Proposition 2.9.10 is the particular case of Proposition 2.9.12 when $T=\varnothing$ (since every subset I of S satisfies $\varnothing\subseteq I$).

2.9.3. The proofs

Class of 2019-11-01

We are now ready to prove the Principle of Inclusion and Exclusion in all its forms. We begin with Theorem 2.9.9:

Proof of Theorem 2.9.9. We shall use the Iverson bracket notation (see Definition 1.3.15).

Here is the plan: We will approach the sum

$$\sum_{I\subseteq[n]}(-1)^{|I|}\,|\{s\in U \mid s\in A_i \text{ for all } i\in I\}| \tag{206}$$

by looking at each particular $s\in U$ and computing how often s is "counted" in this sum. In other words, instead of computing (206) directly, we shall compute the

sum $\sum_{I \subseteq [n]} (-1)^{|I|} [s \in A_i \text{ for all } i \in I]$ for a single $s \in U$ first. Then, we will sum it over all $s \in U$, and obtain (206), because of Proposition 1.6.3 **(b)**.

Here are the details: Fix $s \in U$. Define a subset S of $[n]$ by

$$S = \{i \in [n] \mid s \in A_i\}.$$

Thus, S is the set of all $i \in [n]$ such that $s \in A_i$. Hence, $S = \varnothing$ holds if and only if there exists no $i \in [n]$ such that $s \in A_i$. Thus, we have the following chain of logical equivalences:

$$\begin{aligned}
(S = \varnothing) &\iff (\text{there exists no } i \in [n] \text{ such that } s \in A_i) \\
&\iff (\text{we have } s \notin A_i \text{ for all } i \in [n]) \\
&\iff (s \notin A_1 \cup A_2 \cup \cdots \cup A_n) \\
&\iff (s \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)) \qquad (\text{since } s \in U).
\end{aligned}$$

Thus, "$S = \varnothing$" and "$s \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)$" are two equivalent logical statements. Hence, Exercise 1.3.3 **(a)** (applied to $\mathcal{A} = (\text{"}S = \varnothing\text{"})$ and $\mathcal{B} = (\text{"}s \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)\text{"})$) yields

$$[S = \varnothing] = [s \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)]. \tag{207}$$

On the other hand, let I be any subset of $[n]$. Then, we have the following chain of logical equivalences:

$$\begin{aligned}
&(s \in A_i \text{ for each } i \in I) \\
\iff &(i \in S \text{ for each } i \in I) \\
&\qquad \left(\begin{array}{c} \text{because for any given } i \in I, \text{ the statement "} s \in A_i \text{"} \\ \text{is equivalent to "} i \in S \text{" (by the definition of } S) \end{array} \right) \\
\iff &(I \subseteq S).
\end{aligned}$$

Thus, "$s \in A_i$ for each $i \in I$" and "$I \subseteq S$" are two equivalent logical statements. Consequently, Exercise 1.3.3 **(a)** (applied to $\mathcal{A} = (\text{"}s \in A_i \text{ for each } i \in I\text{"})$ and $\mathcal{B} = (\text{"}I \subseteq S\text{"})$) yields

$$[s \in A_i \text{ for each } i \in I] = [I \subseteq S]. \tag{208}$$

Forget that we fixed I. We thus have proved (208) for each subset I of $[n]$.

Now,

$$\sum_{I\subseteq[n]} (-1)^{|I|} \underbrace{[s \in A_i \text{ for each } i \in I]}_{\substack{=[I\subseteq S] \\ \text{(by (208))}}}$$

$$= \sum_{I\subseteq[n]} (-1)^{|I|} [I \subseteq S]$$

$$= \underbrace{\sum_{\substack{I\subseteq[n]; \\ I\subseteq S}}}_{\substack{=\sum_{I\subseteq S} \\ \text{(since } S\subseteq[n], \\ \text{and thus any subset } I \text{ of } S \\ \text{is a subset of } [n]\text{)}}} (-1)^{|I|} \underbrace{[I \subseteq S]}_{\substack{=1 \\ \text{(since } I\subseteq S\text{)}}} + \sum_{\substack{I\subseteq[n]; \\ \text{not } I\subseteq S}} (-1)^{|I|} \underbrace{[I \subseteq S]}_{\substack{=0 \\ \text{(since we don't have } I\subseteq S\text{)}}}$$

$$\text{(since each subset } I \text{ of } [n] \text{ satisfies either } I \subseteq S \text{ or not } I \subseteq S\text{)}$$

$$= \sum_{I\subseteq S} (-1)^{|I|} + \underbrace{\sum_{\substack{I\subseteq[n]; \\ \text{not } I\subseteq S}} (-1)^{|I|} 0}_{=0} = \sum_{I\subseteq S} (-1)^{|I|} = [S = \varnothing] \qquad \text{(by Proposition 2.9.10)}$$

$$= [s \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)] \tag{209}$$

(by (207)).

Forget that we fixed s. We thus have proved (209) for each $s \in U$. Now, if I is any subset of $[n]$, then

$$\begin{aligned} &|\{s \in U \mid s \in A_i \text{ for all } i \in I\}| \\ &= (\#\text{ of } s \in U \text{ that satisfy } (s \in A_i \text{ for all } i \in I)) \\ &= \sum_{s\in U} [s \in A_i \text{ for all } i \in I] \end{aligned} \tag{210}$$

(by Proposition 1.6.3 **(b)**, applied to $S = U$ and $\mathcal{A}(s) = (\text{“}s \in A_i \text{ for all } i \in I\text{”})$). Hence,

$$\sum_{I\subseteq[n]} (-1)^{|I|} \underbrace{|\{s \in U \mid s \in A_i \text{ for all } i \in I\}|}_{\substack{=\sum_{s\in U} [s\in A_i \text{ for all } i\in I] \\ \text{(by (210))}}}$$

$$= \sum_{I\subseteq[n]} (-1)^{|I|} \sum_{s\in U} [s \in A_i \text{ for all } i \in I] = \underbrace{\sum_{I\subseteq[n]} \sum_{s\in U}}_{=\sum_{s\in U} \sum_{I\subseteq[n]}} (-1)^{|I|} [s \in A_i \text{ for all } i \in I]$$

$$= \sum_{s\in U} \underbrace{\sum_{I\subseteq[n]} (-1)^{|I|} [s \in A_i \text{ for all } i \in I]}_{\substack{=[s\in U\setminus(A_1\cup A_2\cup\cdots\cup A_n)] \\ \text{(by (209))}}} = \sum_{s\in U} [s \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)]\,.$$

On the other hand, Proposition 1.6.3 **(a)** (applied to U and $U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)$ instead of S and T) yields

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{s \in U} [s \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)] .$$

Comparing these two equalities, we obtain

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \{s \in U \mid s \in A_i \text{ for all } i \in I\} \right| .$$

This proves Theorem 2.9.9. □

Let us next derive Theorem 2.9.7 from Theorem 2.9.9:

Proof of Theorem 2.9.7. In order to derive this from Theorem 2.9.9, we need to show the following fact:

Statement 1: Let I be a subset of $[n]$. Then,

$$\bigcap_{i \in I} A_i = \{s \in U \mid s \in A_i \text{ for all } i \in I\} .$$

[*Proof of Statement 1:* We are in one of the following two cases:
Case 1: We have $I = \varnothing$.
Case 2: We have $I \neq \varnothing$.

Let us first consider Case 1. In this case, we have $I = \varnothing$. Hence, $\bigcap_{i \in I} A_i = \bigcap_{i \in \varnothing} A_i = U$ (since we defined $\bigcap_{i \in \varnothing} A_i$ to be U in Theorem 2.9.7). Comparing this with

$$\begin{aligned}
&\{s \in U \mid s \in A_i \text{ for all } i \in I\} \\
&= \{s \in U \mid s \in A_i \text{ for all } i \in \varnothing\} \qquad (\text{since } I = \varnothing) \\
&= \{s \in U\} \qquad \left(\begin{array}{c} \text{since each } s \in U \text{ satisfies } (s \in A_i \text{ for all } i \in \varnothing) \\ \text{(indeed, this is vacuously true, since there exists no } i \in \varnothing) \end{array} \right) \\
&= U,
\end{aligned}$$

we obtain $\bigcap_{i \in I} A_i = \{s \in U \mid s \in A_i \text{ for all } i \in I\}$. Thus, Statement 1 is proved in Case 1.

Let us next consider Case 2. In this case, we have $I \neq \varnothing$. Thus, the set I is nonempty. Hence, the definition of $\bigcap_{i \in I} A_i$ yields

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for each } i \in I\} .$$

But I is nonempty; thus, there exists some $j \in I$. Consider this j. From $j \in I$, we obtain $\bigcap_{i \in I} A_i \subseteq A_j$ (since the intersection of a family of sets is clearly contained in

each of these sets). But A_j is a subset of U (since $A_1, A_2, \ldots, A_n$ are subsets of U). Hence, $A_j \subseteq U$, so that $\bigcap_{i \in I} A_i \subseteq A_j \subseteq U$ and thus $U \cap \left(\bigcap_{i \in I} A_i \right) = \bigcap_{i \in I} A_i$. Hence,

$$\begin{aligned}
\bigcap_{i \in I} A_i &= U \cap \underbrace{\left(\bigcap_{i \in I} A_i \right)}_{= \{x \mid x \in A_i \text{ for each } i \in I\}} \\
&= U \cap \{x \mid x \in A_i \text{ for each } i \in I\} = \{x \in U \mid x \in A_i \text{ for each } i \in I\} \\
&= \{x \in U \mid x \in A_i \text{ for all } i \in I\} = \{s \in U \mid s \in A_i \text{ for all } i \in I\}
\end{aligned}$$

(here, we have renamed the index x as s). Thus, Statement 1 is proved in Case 2.

We have now proved Statement 1 in both Cases 1 and 2. Hence, Statement 1 is always proved.]

Now, Theorem 2.9.9 yields

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \{s \in U \mid s \in A_i \text{ for all } i \in I\} \right|.$$

Comparing this with

$$\sum_{I \subseteq [n]} (-1)^{|I|} \left| \underbrace{\bigcap_{i \in I} A_i}_{\substack{= \{s \in U \mid s \in A_i \text{ for all } i \in I\} \\ \text{(by Statement 1)}}} \right| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \{s \in U \mid s \in A_i \text{ for all } i \in I\} \right|,$$

we obtain

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|.$$

This proves Theorem 2.9.7. □

We can now derive Theorem 2.9.6 from this:

Proof of Theorem 2.9.6. Let U be the set $A_1 \cup A_2 \cup \cdots \cup A_n$. Then, $A_1, A_2, \ldots, A_n$ are subsets of U. The set $U = A_1 \cup A_2 \cup \cdots \cup A_n$ is finite (since $A_1, A_2, \ldots, A_n$ are finite). From $U = A_1 \cup A_2 \cup \cdots \cup A_n$, we obtain $U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n) = \varnothing$ and thus $|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = |\varnothing| = 0$.

Let us agree to understand the "empty" intersection $\bigcap_{i \in \varnothing} A_i$ to mean the set U.

Then, Theorem 2.9.7 yields

$$\begin{aligned}
&|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right| \\
&= \underbrace{(-1)^{|\varnothing|}}_{\substack{=1 \\ (\text{since } |\varnothing|=0 \\ \text{is even})}} \left| \underbrace{\bigcap_{i \in \varnothing} A_i}_{=U} \right| + \sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} \underbrace{(-1)^{|I|}}_{=-(-1)^{|I|-1}} \left| \bigcap_{i \in I} A_i \right| \\
&\qquad (\text{here, we have split off the addend for } I = \varnothing \text{ from the sum}) \\
&= \left| \underbrace{U}_{=A_1 \cup A_2 \cup \cdots \cup A_n} \right| + \underbrace{\sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} \left(- (-1)^{|I|-1} \right) \left| \bigcap_{i \in I} A_i \right|}_{= - \sum\limits_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap\limits_{i \in I} A_i \right|} \\
&= |A_1 \cup A_2 \cup \cdots \cup A_n| - \sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|.
\end{aligned}$$

Comparing this with $|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = 0$, we obtain

$$|A_1 \cup A_2 \cup \cdots \cup A_n| - \sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| = 0.$$

In other words,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|.$$

This proves Theorem 2.9.6. □

Proof of Theorem 2.9.1. Theorem 2.9.6 yields

$$\begin{aligned}
|A_1 \cup A_2 \cup \cdots \cup A_n| &= \sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| \\
&= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1, i_2, \ldots, i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left| A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_m} \right|
\end{aligned}$$

(by Proposition 2.9.4). This proves Theorem 2.9.1. □

We thus have proved all three forms of the Principle of Inclusion and Exclusion. We notice that Theorem 2.9.6 also appears in [Smid09] (with a proof by induction), in [Galvin17, Theorem 16.1] (with two proofs) and in [Grinbe15, Theorem 3.42] (in a slightly more general form). Likewise, Theorem 2.9.7 also appears in [White10], in [Galvin17, (12)] and in [Grinbe15, Theorem 3.43] (again, in a slightly more general form). Several generalizations of the Principle can be found in [Grinbe15, Theorems 3.44, 3.45 and 3.46].

The following exercise provides an analogue of Theorem 2.9.1 with the roles of $\cup$ and $\cap$ swapped:

Exercise 2.9.2. Let n be a positive integer. Let $A_1, A_2, \ldots, A_n$ be n finite sets. Prove that

$$\left|A_1 \cap A_2 \cap \cdots \cap A_n\right| = \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m)\in[n]^m; \\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|.$$

We shall now explore some applications of the Principle of Inclusion and Exclusion.

2.9.4. Application: Surjections

Let us recall the numbers $\operatorname{sur}(m,n)$ we introduced in Definition 2.4.9. We have proved two recursive formulas for them in Subsection 2.4.5; but we left a more explicit formula (Theorem 2.4.17) without an appropriately elucidating proof[196]. It is now time to give such a proof using Theorem 2.9.9:

Proof of Theorem 2.4.17. Recall that $\operatorname{sur}(m,n)$ is the # of surjective maps from $[m]$ to $[n]$ (by Definition 2.4.9). In order to compute this using Theorem 2.9.9, we want to find a finite set ("universe") U and n subsets $A_1, A_2, \ldots, A_n$ of U such that

$$U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n) = \{\text{surjective maps from } [m] \text{ to } [n]\}. \tag{211}$$

We find them as follows: We define

$$U = [n]^{[m]} = \{\text{maps from } [m] \text{ to } [n]\}. \tag{212}$$

This is a finite set. Thus, the elements $f \in U$ are the maps $f : [m] \to [n]$. For each $i \in \{1,2,\ldots,n\}$, we define a subset A_i of U by

$$A_i = \{\text{maps } f : [m] \to [n] \mid i \notin f([m])\}. \tag{213}$$

(This is the set of all maps $f : [m] \to [n]$ which never take i as a value.) Then, $A_1, A_2, \ldots, A_n$ are n subsets of U. Let us check that they satisfy (211).

[196] unless you count the inductive proof in Exercise 2.4.4 as a such

Indeed, we have

$$\begin{aligned}
&\{\text{surjective maps from } [m] \text{ to } [n]\} \\
&= \{\text{maps } f : [m] \to [n] \mid f \text{ is surjective}\} \\
&= \{\text{maps } f : [m] \to [n] \mid \text{every } i \in [n] \text{ is taken as a value by } f\} \qquad (214)
\end{aligned}$$

(because a map $f : [m] \to [n]$ is surjective if and only if every $i \in [n]$ is taken as a value by f). But from (213), we obtain

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{\text{maps } f : [m] \to [n] \mid \text{at least one } i \in [n] \text{ satisfies } i \notin f([m])\}$$

and thus

$$\begin{aligned}
&U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n) \\
&= \underbrace{U}_{\substack{=\{\text{maps from } [m] \text{ to } [n]\} \\ =\{\text{maps } f:[m]\to[n]\}}} \\
&\qquad \setminus \{\text{maps } f : [m] \to [n] \mid \text{at least one } i \in [n] \text{ satisfies } i \notin f([m])\} \\
&= \{\text{maps } f : [m] \to [n]\} \\
&\qquad \setminus \{\text{maps } f : [m] \to [n] \mid \text{at least one } i \in [n] \text{ satisfies } i \notin f([m])\} \\
&= \{\text{maps } f : [m] \to [n] \mid \text{every } i \in [n] \text{ satisfies } i \in f([m])\} \\
&\qquad \left(\begin{array}{c} \text{since the negation of the statement} \\ \text{“at least one } i \in [n] \text{ satisfies } i \notin f([m])\text{”} \\ \text{is “every } i \in [n] \text{ satisfies } i \in f([m])\text{”} \end{array} \right) \\
&= \{\text{maps } f : [m] \to [n] \mid \text{every } i \in [n] \text{ is taken as a value by } f\} \\
&\qquad \left(\begin{array}{c} \text{since the statement “every } i \in [n] \text{ satisfies } i \in f([m])\text{”} \\ \text{means the same as “every } i \in [n] \text{ is taken as a value by } f\text{”} \end{array} \right) \\
&= \{\text{surjective maps from } [m] \text{ to } [n]\} \qquad (215)
\end{aligned}$$

(by (214)). Thus, (211) is indeed satisfied.

Now, (215) yields

$$\begin{aligned}
&|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| \\
&= |\{\text{surjective maps from } [m] \text{ to } [n]\}| \\
&= (\#\text{ of surjective maps from } [m] \text{ to } [n]) = \operatorname{sur}(m,n) \qquad (216)
\end{aligned}$$

(since $\operatorname{sur}(m,n)$ was defined as the # of surjective maps from $[m]$ to $[n]$).

In order to apply Theorem 2.9.9 successfully, we want to understand the sets $\{s \in U \mid s \in A_i \text{ for all } i \in I\}$ (or at least their sizes). But this is easy: If I is a subset of $[n]$, then

$$\begin{aligned}
&\{s \in U \mid s \in A_i \text{ for all } i \in I\} \\
&= \{\text{maps } f : [m] \to [n] \mid f([m]) \subseteq [n] \setminus I\}. \qquad (217)
\end{aligned}$$

[*Proof of (217):* Let I be a subset of $[n]$. We have

$$\begin{aligned}
&\{s \in U \mid s \in A_i \text{ for all } i \in I\} \\
&= \{s \in U \mid s \in A_i \text{ for each } i \in I\} \\
&= \{f \in U \mid f \in A_i \text{ for each } i \in I\} \qquad \text{(here, we have renamed the index } s \text{ as } f\text{)} \\
&= \{\text{maps } f : [m] \to [n] \mid f \in A_i \text{ for each } i \in I\} \qquad (218) \\
&\qquad \text{(since the elements } f \in U \text{ are the maps } f : [m] \to [n]\text{)}.
\end{aligned}$$

But if $f : [m] \to [n]$ is any map, then we have the following chain of logical equivalences:

$$\begin{aligned}
&(f \in A_i \text{ for each } i \in I) \\
&\iff (i \notin f([m]) \text{ for each } i \in I) \\
&\qquad \text{(because an } i \in I \text{ satisfies } f \in A_i \text{ if and only if } i \notin f([m]) \text{ (by (213)))} \\
&\iff (\text{none of the elements of } I \text{ is contained in } f([m])) \\
&\iff (\text{the sets } f([m]) \text{ and } I \text{ are disjoint}) \\
&\iff (f([m]) \text{ is disjoint from } I) \\
&\iff (f([m]) \subseteq [n] \setminus I)
\end{aligned}$$

(because $f([m])$ is a subset of $[n]$, and thus is disjoint from I if and only if $f([m]) \subseteq [n] \setminus I$). In light of this equivalence, we can rewrite (218) as

$$\{s \in U \mid s \in A_i \text{ for all } i \in I\} = \{\text{maps } f : [m] \to [n] \mid f([m]) \subseteq [n] \setminus I\}.$$

This proves (217).]

Now, if I is a subset of $[n]$, then

$$\begin{aligned}
&|\{s \in U \mid s \in A_i \text{ for all } i \in I\}| \\
&= |\{\text{maps } f : [m] \to [n] \mid f([m]) \subseteq [n] \setminus I\}| \qquad \text{(by (217))} \\
&= (\#\text{ of maps } f : [m] \to [n] \text{ satisfying } f([m]) \subseteq [n] \setminus I) \\
&= |[n] \setminus I|^{|[m]|} \qquad \text{(by Exercise 2.4.1 } \textbf{(a)}\text{, applied to } A = [m],\ B = [n] \text{ and } C = I\text{)} \\
&= (|[n]| - |I|)^{|[m]|} \qquad \left(\begin{array}{c} \text{since } |[n] \setminus I| = |[n]| - |I| \\ \text{(by Theorem 1.4.7 } \textbf{(a)}\text{, since } I \text{ is a subset of } [n]\text{)} \end{array}\right) \\
&= (n - |I|)^m \qquad \text{(since } |[n]| = n \text{ and } |[m]| = m\text{)}. \qquad (219)
\end{aligned}$$

Now, let us note that each subset I of $[n]$ satisfies $|I| \in \{0, 1, \ldots, n\}$ (since Theo-

rem 1.4.7 **(b)** yields $|I| \leq |[n]| = n$). Theorem 2.9.9 yields

$$\begin{aligned}
&|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{\left|\{s \in U \mid s \in A_i \text{ for all } i \in I\}\right|}_{\substack{=(n-|I|)^m \\ \text{(by (219))}}} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (n-|I|)^m = \sum_{k=0}^{n} \sum_{\substack{I \subseteq [n]; \\ |I|=k}} \underbrace{(-1)^{|I|} (n-|I|)^m}_{\substack{=(-1)^k (n-k)^m \\ \text{(since } |I|=k\text{)}}} \\
&\qquad \left(\begin{array}{c} \text{by an application of (37), since} \\ \text{each subset } I \text{ of } [n] \text{ satisfies } |I| \in \{0,1,\ldots,n\} \end{array} \right) \\
&= \sum_{k=0}^{n} \underbrace{\sum_{\substack{I \subseteq [n]; \\ |I|=k}} (-1)^k (n-k)^m}_{=(\text{\# of subsets } I \text{ of } [n] \text{ satisfying } |I|=k) \cdot (-1)^k (n-k)^m} \\
&= \sum_{k=0}^{n} \underbrace{(\text{\# of subsets } I \text{ of } [n] \text{ satisfying } |I| = k)}_{\substack{=(\text{\# of } k\text{-element subsets of } [n]) = \binom{n}{k} \\ \text{(by Theorem 1.3.12, applied to } S=[n]\text{)}}} \cdot (-1)^k (n-k)^m \\
&= \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k (n-k)^m = \sum_{k=0}^{n} \underbrace{(-1)^k}_{\substack{=(-1)^{n-(n-k)} \\ \text{(since } k=n-(n-k)\text{)}}} \underbrace{\binom{n}{k}}_{\substack{=\binom{n}{n-k} \\ \text{(by Theorem 1.3.11)}}} (n-k)^m \\
&= \sum_{k=0}^{n} (-1)^{n-(n-k)} \binom{n}{n-k} (n-k)^m = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^m
\end{aligned}$$

(here, we have substituted i for $n-k$ in the sum). Comparing this with (216), we obtain

$$\operatorname{sur}(m,n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^m.$$

This proves Theorem 2.4.17. □

2.9.5. Application: Derangements

In Definition 1.7.4, we defined the notion of a derangement; in Definition 1.7.7, we introduced the notation D_n for the # of derangements of $[n]$. We now intend to use the Principle of Inclusion and Exclusion to obtain a formula for D_n – namely, the formula from Theorem 1.7.9 **(d)**.

We shall use the following notation (which is fairly widespread in abstract algebra):

Definition 2.9.13. Let X be any set. Then, the set of all permutations of X is denoted by S_X.

Thus, if X is a finite set, then

$$S_X = \{\text{permutations of } X\}$$

and therefore

$$|S_X| = (\#\text{ of permutations of } X) = |X|! \tag{220}$$

(by Theorem 1.7.2, applied to $n = |X|$), since X is an $|X|$-element set.

In order to count the derangements of $[n]$ for some $n \in \mathbb{N}$, we can try to apply Theorem 2.9.9 to

$$U = S_{[n]} \qquad \text{and} \qquad A_i = \left\{\sigma \in S_{[n]} \mid \sigma(i) = i\right\}.$$

This would shift our problem to the computation of $|\{s \in U \mid s \in A_i \text{ for all } i \in I\}|$ for subsets I of $[n]$. The following proposition will help us do so:

Proposition 2.9.14. Let X be a set. Let I be a subset of X. Then, there is a bijection

$$\text{from } \{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\} \text{ to } S_{X \setminus I}.$$

Example 2.9.15. For this example, set $X = [4]$ and $I = \{1,3\}$. Then, Proposition 2.9.14 claims that there is a bijection

$$\text{from } \left\{\sigma \in S_{[4]} \mid \sigma(i) = i \text{ for each } i \in \{1,3\}\right\} \text{ to } S_{\{2,4\}}$$

(since $X \setminus I = [4] \setminus \{1,3\} = \{2,4\}$). Let us check this: The permutations $\sigma \in S_{[4]}$ satisfying $(\sigma(i) = i \text{ for each } i \in \{1,3\})$ are

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

(in two-line notation). Meanwhile, the permutations of $\{2,4\}$ are

$$\begin{pmatrix} 2 & 4 \\ 2 & 4 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}$$

(in two-line notation). Thus, there is a bijection from the former two permutations (i.e., from the set $\left\{\sigma \in S_{[4]} \mid \sigma(i) = i \text{ for each } i \in \{1,3\}\right\}$) to the latter two permutations (i.e., to the set $S_{\{2,4\}}$): Namely, the bijection is "throw away the values at 1 and at 3" or, more formally, "restrict the permutation to the subset $\{2,4\}$".

The following proof of Proposition 2.9.14 generalizes the bijection we have found in this example:

Proof of Proposition 2.9.14 (sketched). Here is the rough idea of the proof: If a permutation $\sigma \in S_X$ satisfies ($\sigma(i) = i$ for each $i \in I$), then it has to map each element of I to itself, and therefore must permute the remaining elements of X among themselves (i.e., it must send any element of $X \setminus I$ to an element of $X \setminus I$), since it would otherwise fail to be injective. Thus, a permutation $\sigma \in S_X$ satisfying ($\sigma(i) = i$ for each $i \in I$) is "nothing but" a permutation of the set $X \setminus I$ (since the requirement ($\sigma(i) = i$ for each $i \in I$) uniquely determines its values on the set I). This is not rigorous, because strictly speaking a permutation of X cannot be a permutation of $X \setminus I$ (after all, the former has domain X while the latter only has domain $X \setminus I$). Here is a rigorous version of the argument we just made:

To each permutation $\sigma \in S_X$ satisfying ($\sigma(i) = i$ for each $i \in I$), we can assign a permutation $\widetilde{\sigma}$ of $X \setminus I$ by letting

$$\widetilde{\sigma}(p) = \sigma(p) \qquad \text{for each } p \in X \setminus I.$$

[197] This defines a map

$$A : \{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\} \to S_{X \setminus I}, \quad \sigma \mapsto \widetilde{\sigma}.$$

Conversely, to each permutation τ of $X \setminus I$, we can assign a permutation $\widehat{\tau} \in S_X$ satisfying ($\widehat{\tau}(i) = i$ for each $i \in I$) by setting

$$\widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{for each } p \in X.$$

[198] This defines a map

$$B : S_{X \setminus I} \to \{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}, \quad \tau \mapsto \widehat{\tau}.$$

The maps A and B are well-defined and mutually inverse[199]. Hence, they are bijections. Thus, there is a bijection from the set $\{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}$ to the set $S_{X \setminus I}$ (namely, A). This proves Proposition 2.9.14. □

[197] Why is this map $\widetilde{\sigma}$ well-defined, and why is it really a permutation of $X \setminus I$? Try to answer these questions (and similar questions that we leave unanswered in this proof) on your own, or look up the answers in the solution to Exercise 2.9.3 below.

[198] Once again: This should be proved! (Proving this is part of Exercise 2.9.3 below.)

[199] Once again: This should be proved! (Proving this is part of Exercise 2.9.3 below.)

Exercise 2.9.3. Fill in the missing details in the above (sketched) proof of Proposition 2.9.14.

Corollary 2.9.16. Let $n \in \mathbb{N}$. Let X be an n-element set. Let I be a subset of X. Then,

$$|\{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}| = (n - |I|)!.$$

Proof of Corollary 2.9.16. The set X is finite (since it is an n-element set). Hence, its subset $X \setminus I$ is finite as well. Moreover, I is a subset of X; thus, Theorem 1.4.7 **(a)** (applied to $A = X$ and $B = I$) yields

$$|X \setminus I| = \underbrace{|X|}_{\substack{=n \\ \text{(since } X \text{ is} \\ \text{an } n\text{-element set)}}} - |I| = n - |I|.$$

Proposition 2.9.14 shows that there is a bijection

$$\text{from } \{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\} \text{ to } S_{X \setminus I}.$$

Hence, the bijection principle yields

$$|\{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}| = \left|S_{X \setminus I}\right| = |X \setminus I|!$$

(by (220), applied to $X \setminus I$ instead of X). In view of $|X \setminus I| = n - |I|$, this rewrites as

$$|\{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}| = (n - |I|)!$$

This proves Corollary 2.9.16. □

We can now prove Theorem 1.7.9 **(d)**:

*Proof of Theorem 1.7.9 **(d)**.* Let $n \in \mathbb{N}$. Set $U = S_{[n]}$. For each $i \in [n]$, we define a set

$$A_i = \left\{\sigma \in S_{[n]} \mid \sigma(i) = i\right\}. \tag{221}$$

This set A_i is a subset of $S_{[n]} = U$. Thus, we have found n subsets $A_1, A_2, \ldots, A_n$ of U. We claim that

$$U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n) = \{\text{derangements of } [n]\}. \tag{222}$$

[*Proof of (222):* Let σ be a permutation of $[n]$. Hence, $\sigma \in S_{[n]}$ (by the definition of $S_{[n]}$). Hence, for any $i \in [n]$, we have the equivalence $(\sigma \in A_i) \iff (\sigma(i) = i)$ (by (221)). Thus, we have the following equivalence:

$$\begin{aligned} &(\text{there exists no } i \in [n] \text{ such that } \sigma \in A_i) \\ &\iff (\text{there exists no } i \in [n] \text{ such that } \sigma(i) = i). \end{aligned} \tag{223}$$

But a fixed point of σ is defined to be an element $i \in [n]$ such that $\sigma(i) = i$. Hence, we have the following chain of equivalences:

$$\begin{aligned}
&(\sigma \text{ has no fixed points}) \\
&\iff (\text{there exists no } i \in [n] \text{ such that } \sigma(i) = i) \\
&\iff (\text{there exists no } i \in [n] \text{ such that } \sigma \in A_i) \qquad \text{(by (223))} \\
&\iff (\sigma \notin A_i \text{ for all } i \in [n]) \\
&\iff (\sigma \notin A_1 \cup A_2 \cup \cdots \cup A_n). \qquad (224)
\end{aligned}$$

Forget that we fixed σ. We thus have proved the equivalence (224) for each permutation σ of $[n]$.

Recall that a derangement of $[n]$ is defined as a permutation of $[n]$ that has no fixed points. Hence,

$$\begin{aligned}
&\{\text{derangements of } [n]\} \\
&= \{\text{permutations of } [n] \text{ that have no fixed points}\} \\
&= \{\sigma \text{ is a permutation of } [n] \mid \sigma \text{ has no fixed points}\} \\
&= \{\sigma \text{ is a permutation of } [n] \mid \sigma \notin A_1 \cup A_2 \cup \cdots \cup A_n\} \\
&\qquad \text{(by the equivalence (224))} \\
&= \left\{\sigma \in S_{[n]} \mid \sigma \notin A_1 \cup A_2 \cup \cdots \cup A_n\right\} \\
&\qquad \left(\text{since the permutations of } [n] \text{ are the elements of } S_{[n]}\right) \\
&= \underbrace{S_{[n]}}_{=U} \setminus (A_1 \cup A_2 \cup \cdots \cup A_n) = U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n).
\end{aligned}$$

This proves (222).]

Now, (222) yields

$$\begin{aligned}
&|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| \\
&= |\{\text{derangements of } [n]\}| \\
&= (\#\text{ of derangements of } [n]) = D_n \qquad (225)
\end{aligned}$$

(since D_n was defined as the # of derangements of $[n]$).

In order to apply Theorem 2.9.9 successfully, we want to understand the sets $\{s \in U \mid s \in A_i \text{ for all } i \in I\}$ (or at least their sizes). But this is easy: If I is a subset of $[n]$, then

$$\begin{aligned}
&\{s \in U \mid s \in A_i \text{ for all } i \in I\} \\
&= \left\{\sigma \in S_{[n]} \mid \sigma(i) = i \text{ for each } i \in I\right\}. \qquad (226)
\end{aligned}$$

[*Proof of (226):* Let I be a subset of $[n]$. We have

$$\begin{aligned}
&\{s \in U \mid s \in A_i \text{ for all } i \in I\} \\
&= \{s \in U \mid s \in A_i \text{ for each } i \in I\} \\
&= \{\sigma \in U \mid \sigma \in A_i \text{ for each } i \in I\} \\
&\qquad\qquad \text{(here, we have renamed the index } s \text{ as } \sigma\text{)} \\
&= \left\{\sigma \in S_{[n]} \mid \sigma \in A_i \text{ for each } i \in I\right\} \qquad \left(\text{since } U = S_{[n]}\right) \\
&= \left\{\sigma \in S_{[n]} \mid \sigma(i) = i \text{ for each } i \in I\right\}
\end{aligned}$$

(because for each $\sigma \in S_{[n]}$ and each $i \in I$, we have the equivalence $(\sigma \in A_i) \iff (\sigma(i) = i)$ [200]). This proves (226).]

Now, if I is a subset of $[n]$, then

$$\begin{aligned}
&|\{s \in U \mid s \in A_i \text{ for all } i \in I\}| \\
&= \left|\left\{\sigma \in S_{[n]} \mid \sigma(i) = i \text{ for each } i \in I\right\}\right| \qquad \text{(by (226))} \\
&= (n - |I|)! \qquad (227)
\end{aligned}$$

(by Corollary 2.9.16, applied to $X = [n]$).

Now, let us note that each subset I of $[n]$ satisfies $|I| \in \{0, 1, \ldots, n\}$ (since Theo-

[200] by (221)

rem 1.4.7 **(b)** yields $|I| \leq |[n]| = n$). Theorem 2.9.9 yields

$$\begin{aligned}
&|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{\left|\{s \in U \mid s \in A_i \text{ for all } i \in I\}\right|}_{\substack{=(n-|I|)! \\ \text{(by (227))}}} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (n-|I|)! = \sum_{k=0}^{n} \sum_{\substack{I \subseteq [n]; \\ |I|=k}} \underbrace{(-1)^{|I|} (n-|I|)!}_{\substack{=(-1)^k (n-k)! \\ \text{(since } |I|=k\text{)}}} \\
&\qquad \left(\begin{array}{c} \text{by an application of (37), since} \\ \text{each subset } I \text{ of } [n] \text{ satisfies } |I| \in \{0,1,\ldots,n\} \end{array} \right) \\
&= \sum_{k=0}^{n} \underbrace{\sum_{\substack{I \subseteq [n]; \\ |I|=k}} (-1)^k (n-k)!}_{=(\text{\# of subsets } I \text{ of } [n] \text{ satisfying } |I|=k) \cdot (-1)^k (n-k)!} \\
&= \sum_{k=0}^{n} \underbrace{(\text{\# of subsets } I \text{ of } [n] \text{ satisfying } |I| = k)}_{\substack{=(\text{\# of } k\text{-element subsets of } [n]) = \binom{n}{k} \\ \text{(by Theorem 1.3.12, applied to } S=[n]\text{)}}} \cdot (-1)^k (n-k)! \\
&= \sum_{k=0}^{n} \underbrace{\binom{n}{k}}_{\substack{= \frac{n!}{k! \cdot (n-k)!} \\ \text{(by Theorem 1.3.9)}}} \cdot (-1)^k (n-k)! = \sum_{k=0}^{n} \underbrace{\frac{n!}{k! \cdot (n-k)!} \cdot (-1)^k (n-k)!}_{=(-1)^k \frac{n!}{k!}} \\
&= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}.
\end{aligned}$$

Comparing this with (225), we obtain

$$D_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}.$$

This proves Theorem 1.7.9 **(d)**. □

Exercise 2.9.4. Prove parts **(a)**, **(b)** and **(c)** of Theorem 1.7.9.

2.9.6. Application: Euler's totient function

We recall two standard notions from elementary number theory (see, e.g., [19s, §2.9 and §2.10]):

- The *greatest common divisor* of two positive integers a and b is defined to be the greatest positive integer that divides both a and b. It is denoted by $\gcd(a,b)$. For example, $\gcd(4,6) = 2$ and $\gcd(3,7) = 1$ and $\gcd(10,25) = 5$.
- Two positive integers a and b are said to be *coprime* (or *relatively prime*) if $\gcd(a,b) = 1$.
- A positive integer a is said to be *coprime to* a positive integer b if $\gcd(a,b) = 1$ (that is, if a and b are coprime).

(These definitions can be extended to arbitrary integers, if we set $\gcd(0,0) = 0$ (despite 0 not literally being the greatest common divisor of 0 and 0). But we will only need them for positive integers.)

We now define a function that has many uses in number theory (see, e.g., [19s, §2.14]):

Definition 2.9.17. The function $\phi : \{1,2,3,\ldots\} \to \mathbb{N}$ (called *Euler's totient function* or *Euler's ϕ-function*) is defined by

$$\phi(u) = (\#\text{ of all } m \in [u] \text{ that are coprime to } u).$$

See [Tou17] for a history of this function (and an attempt at explaining its name).

Example 2.9.18. **(a)** The definition of ϕ yields

$$\phi(2) = (\#\text{ of all } m \in [2] \text{ that are coprime to } 2). \tag{228}$$

Among the elements $1,2$ of $[2]$, only 1 is coprime to 2 (since $\gcd(1,2) = 1$ and $\gcd(2,2) = 2$). Thus, the # of all $m \in [2]$ that are coprime to 2 is 1. Hence, (228) becomes

$$\phi(2) = 1.$$

(b) The definition of ϕ yields

$$\phi(4) = (\#\text{ of all } m \in [4] \text{ that are coprime to } 4). \tag{229}$$

Among the elements $1,2,3,4$ of $[4]$, only 1 and 3 are coprime to 4 (since $\gcd(1,4) = 1$, $\gcd(2,4) = 2$, $\gcd(3,4) = 1$ and $\gcd(4,4) = 4$). Thus, the # of all $m \in [4]$ that are coprime to 4 is 2. Hence, (229) becomes

$$\phi(4) = 2.$$

(c) Likewise,

$$\phi(6) = 2,$$

since the only elements among $1,2,3,4,5,6$ that are coprime to 6 are 1 and 5.

(d) Likewise,

$$\phi(7) = 6,$$

since the only elements among $1,2,3,4,5,6,7$ that are coprime to 7 are $1,2,3,4,5,6$.

(e) Likewise,

$$\phi(12) = 4,$$

since the only elements among $1,2,3,4,5,6,7,8,9,10,11,12$ that are coprime to 12 are $1,5,7,11$.

Here is a table of the first 15 values of ϕ:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\cdots$
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	$\cdots$

.

The function ϕ can, of course, be seen as a sequence of integers (namely, the sequence $(\phi(1), \phi(2), \phi(3), \ldots)$). As such, it appears in the OEIS as OEIS sequence A000010.

Here are two neat (but inconsequential, at least for us) exercises on the function ϕ (which can be solved essentially combinatorially):

Exercise 2.9.5. Let $n \in \mathbb{N}$ satisfy $n > 2$. Prove that $\phi(n)$ is even.

Exercise 2.9.6. Let $n \in \mathbb{N}$ satisfy $n > 1$. Prove that

$$\sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \text{ is coprime to } n}} i = n\phi(n)/2.$$

We shall apply the Principle of Inclusion and Exclusion to proving the following "explicit" formula for $\phi(u)$:

Theorem 2.9.19. Let u be a positive integer. Let $p_1, p_2, \ldots, p_n$ be the distinct primes that divide u. Then,

$$\phi(u) = u \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right).$$

Example 2.9.20. Let $u = 18$. What does Theorem 2.9.19 say in this case? The distinct primes that divide u are 2 and 3 (since $u = 18 = 2 \cdot 3^2$). Hence, we can apply Theorem 2.9.19 to $n = 2$, $p_1 = 2$ and $p_2 = 3$. We thus obtain

$$\phi(u) = u \cdot \prod_{i=1}^{2} \left(1 - \frac{1}{p_i}\right) = u \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right).$$

In view of $u = 18$, this rewrites as

$$\phi(18) = 18 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6.$$

This is easy to verify by actually counting all $m \in [18]$ that are coprime to 18.

There are many ways to prove Theorem 2.9.19; for example, one can be found in [19s, §2.16.3]. We shall give a combinatorial proof that uses the Principle of Inclusion and Exclusion as well as a few elementary lemmas. The first lemma is a pair of simple identities:

Lemma 2.9.21. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be any n numbers. Then:

(a) We have

$$\sum_{I \subseteq [n]} \prod_{i \in I} a_i = (1 + a_1)(1 + a_2) \cdots (1 + a_n).$$

(b) We have

$$\sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} a_i = (1 - a_1)(1 - a_2) \cdots (1 - a_n).$$

Example 2.9.22. If $n = 3$, then Lemma 2.9.21 **(a)** says that

$$1 + a_1 + a_2 + a_3 + a_1a_2 + a_1a_3 + a_2a_3 + a_1a_2a_3 = (1 + a_1)(1 + a_2)(1 + a_3).$$

This is no surprise: The left hand side is what you obtain if you expand the right hand side.

Exercise 2.9.7. Prove Lemma 2.9.21.

The remaining lemmas that we will need come from elementary number theory. The first is a simple counting exercise:[201]

Lemma 2.9.23. Let u and v be two positive integers such that v divides u. Then,

$$(\#\text{ of } m \in [u] \text{ such that } v \text{ divides } m) = u/v.$$

Proof of Lemma 2.9.23 (sketched). The positive integers u and v have the property that v divides u. Hence, u/v is a positive integer. Moreover, if $m \in [u]$, then $m \leq u$.

[201] In the following, we will (mostly) avoid using the symbol "|" for the word "divides" (in the notation "$a \mid b$"). Instead, we will just write out the word "divides". We will do this in order to avoid confusing expressions like "$\{m \in [u] \mid v \mid m\}$", because the symbol "|" is already used in set-builder notation (e.g., in "$\{m \in [u] \mid v \text{ divides } m\}$").

Hence, if $m \in [u]$ has the property that v divides m, then m/v is a positive integer satisfying $m/v \leq u/v$ (since $m \leq u$), and thus belongs to $[u/v]$. Hence, the map

$$A : \{m \in [u] \mid v \text{ divides } m\} \to [u/v], \\ m \mapsto m/v$$

is well-defined. Consider this map A.

On the other hand, if $j \in [u/v]$, then jv is an element of $[u]$ (because $j \in [u/v]$ yields $0 < j \leq u/v$ and thus $0 < jv \leq u$) and has the property that v divides jv. Hence, the map

$$B : [u/v] \to \{m \in [u] \mid v \text{ divides } m\}, \\ j \mapsto jv$$

is well-defined. Consider this map B.

The maps A and B are mutually inverse (since A divides the input by v, whereas B multiplies the input by v), and hence are bijections. Thus, the bijection principle yields

$$|\{m \in [u] \mid v \text{ divides } m\}| = |[u/v]| = u/v$$

(since u/v is a positive integer). Hence,

$$(\#\text{ of } m \in [u] \text{ such that } v \text{ divides } m) = |\{m \in [u] \mid v \text{ divides } m\}| = u/v.$$

This proves Lemma 2.9.23. □

The next lemma is a particular case of [19s, Exercise 2.10.3]:

Lemma 2.9.24. Let $c \in \mathbb{Z}$. Let $b_1, b_2, \ldots, b_k$ be k positive integers that are mutually coprime. ("Mutually coprime" means that b_i is coprime to b_j whenever $i \neq j$). Assume that $b_i \mid c$ for each $i \in \{1, 2, \ldots, k\}$. Then, $b_1 b_2 \cdots b_k \mid c$.

Using this lemma, we can easily see the following fact:

Lemma 2.9.25. Let $c \in \mathbb{Z}$. Let $b_1, b_2, \ldots, b_k$ be k distinct primes. Assume that $b_i \mid c$ for each $i \in \{1, 2, \ldots, k\}$. Then, $b_1 b_2 \cdots b_k \mid c$.

Exercise 2.9.8. Derive Lemma 2.9.25 from Lemma 2.9.24.

From Lemma 2.9.25, in turn, we can easily derive the following lemma:

Lemma 2.9.26. Let I be a finite set. For each $i \in I$, let p_i be a prime. Assume that all these primes p_i (for different $i \in I$) are distinct. Let m be an integer. Then, we have the equivalence

$$\left(p_j \text{ divides } m \text{ for each } j \in I\right) \iff \left(\prod_{i \in I} p_i \text{ divides } m\right). \tag{230}$$

Exercise 2.9.9. Prove Lemma 2.9.26.

The next lemma stems easily from the definition of a greatest common divisor:

Lemma 2.9.27. Let u be a positive integer. Let $p_1, p_2, \ldots, p_n$ be the distinct primes that divide u. Let m be a positive integer. Then, we have the equivalence

$$(m \text{ is coprime to } u) \iff ((p_i \text{ does not divide } m) \text{ for each } i \in [n]) .$$

Exercise 2.9.10. Prove Lemma 2.9.27.
[Hint: A well-known fact says that if $n > 1$ is an integer, then there exists at least one prime p such that $p \mid n$.]

We can now prove Theorem 2.9.19 using Theorem 2.9.9:

Proof of Theorem 2.9.19. Define a finite set U of positive integers by

$$U = [u] .$$

For each $i \in [n]$, define a subset A_i of U by

$$A_i = \{m \in U \mid p_i \text{ divides } m\} . \tag{231}$$

Thus, we have found n subsets $A_1, A_2, \ldots, A_n$ of U.
For any $m \in U$, we have the logical equivalence

$$(m \in A_i) \iff (p_i \text{ divides } m) \tag{232}$$

(by (231)), and thus we also have the logical equivalence

$$(m \notin A_i) \iff (p_i \text{ does not divide } m) . \tag{233}$$

We claim that

$$U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n) = \{m \in [u] \mid m \text{ is coprime to } u\} . \tag{234}$$

[*Proof of (234):* For any $m \in U$, we have the logical equivalence

$$(m \text{ is coprime to } u) \iff ((p_i \text{ does not divide } m) \text{ for each } i \in [n])$$

(by Lemma 2.9.27). Thus,

$$\begin{aligned} &\{m \in U \mid m \text{ is coprime to } u\} \\ &= \{m \in U \mid (p_i \text{ does not divide } m) \text{ for each } i \in [n]\} . \end{aligned} \tag{235}$$

But the definition of set difference yields

$$\begin{aligned}
&U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n) \\
&= \{m \in U \mid m \notin A_1 \cup A_2 \cup \cdots \cup A_n\} \\
&= \left\{ m \in U \mid \underbrace{m \notin A_i}_{\substack{\text{This is equivalent to} \\ \text{“}p_i \text{ does not divide } m\text{”} \\ \text{(by (233))}}} \quad \text{for each } i \in [n] \right\} \\
&= \{m \in U \mid (p_i \text{ does not divide } m) \text{ for each } i \in [n]\} \\
&= \{m \in U \mid m \text{ is coprime to } u\} \qquad \text{(by (235))} \\
&= \{m \in [u] \mid m \text{ is coprime to } u\} \qquad \text{(since } U = [u]\text{)}.
\end{aligned}$$

This proves (234).]

Now, the definition of ϕ yields

$$\begin{aligned}
\phi(u) &= (\#\text{ of all } m \in [u] \text{ that are coprime to } u) \\
&= |\{m \in [u] \mid m \text{ is coprime to } u\}| \\
&= |U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| \qquad (236)
\end{aligned}$$

(since (234) yields $\{m \in [u] \mid m \text{ is coprime to } u\} = U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)$).

In order to apply Theorem 2.9.9 successfully, we want to understand the sets $\{s \in U \mid s \in A_i \text{ for all } i \in I\}$ (or at least their sizes). But this is easy: If I is a subset of $[n]$, then

$$\begin{aligned}
&\{s \in U \mid s \in A_i \text{ for all } i \in I\} \\
&= \left\{ m \in [u] \mid \prod_{i \in I} p_i \text{ divides } m \right\}. \qquad (237)
\end{aligned}$$

[*Proof of (237):* Let I be a subset of $[n]$. We have

$$\begin{aligned}
&\{s \in U \mid s \in A_i \text{ for all } i \in I\} \\
&= \{s \in U \mid s \in A_i \text{ for each } i \in I\} \\
&= \{m \in U \mid m \in A_i \text{ for each } i \in I\} \\
&\qquad \text{(here, we have renamed the index } s \text{ as } m\text{)} \\
&= \{m \in U \mid p_i \text{ divides } m \text{ for each } i \in I\} \\
&\qquad \text{(due to the equivalence (232), which holds for every } m \in U\text{)} \\
&= \{m \in [u] \mid p_i \text{ divides } m \text{ for each } i \in I\} \qquad \text{(since } U = [u]\text{)} \\
&= \{m \in [u] \mid p_j \text{ divides } m \text{ for each } j \in I\} \\
&\qquad \text{(here, we have renamed the index } i \text{ as } j\text{)} \\
&= \left\{ m \in [u] \mid \prod_{i \in I} p_i \text{ divides } m \right\} \qquad \text{(by the equivalence (230))}.
\end{aligned}$$

This proves (237).]

As a consequence of (237), we can now easily see the following: If I is a subset of $[n]$, then

$$|\{s \in U \mid s \in A_i \text{ for all } i \in I\}| = u \cdot \prod_{i \in I} \frac{1}{p_i}. \tag{238}$$

[*Proof of (238):* Let I be a subset of $[n]$. All the primes p_i (for different $i \in I$) are distinct (since $p_1, p_2, \ldots, p_n$ are the distinct primes that divide u). Furthermore, p_j divides u for each $j \in I$ (for the same reason). But Lemma 2.9.26 (applied to $m = u$) shows that we have the equivalence

$$\left(p_j \text{ divides } u \text{ for each } j \in I\right) \Longleftrightarrow \left(\prod_{i \in I} p_i \text{ divides } u\right).$$

Hence, $\prod_{i \in I} p_i$ divides u (since p_j divides u for each $j \in I$). Thus, Lemma 2.9.23 (applied to $v = \prod_{i \in I} p_i$) yields that

$$\left(\#\text{ of } m \in [u] \text{ such that } \prod_{i \in I} p_i \text{ divides } m\right) = u / \left(\prod_{i \in I} p_i\right).$$

But (237) yields

$$\begin{aligned}
|\{s \in U \mid s \in A_i \text{ for all } i \in I\}| &= \left|\left\{m \in [u] \mid \prod_{i \in I} p_i \text{ divides } m\right\}\right| \\
&= \left(\#\text{ of } m \in [u] \text{ such that } \prod_{i \in I} p_i \text{ divides } m\right) \\
&= u / \left(\prod_{i \in I} p_i\right) = u \cdot \underbrace{\frac{1}{\prod_{i \in I} p_i}}_{= \prod_{i \in I} \frac{1}{p_i}} = u \cdot \prod_{i \in I} \frac{1}{p_i}.
\end{aligned}$$

This proves (238).]

Now, everything is in place. The equality (236) becomes

$$\begin{aligned}
\phi(u) &= |U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{|\{s \in U \mid s \in A_i \text{ for all } i \in I\}|}_{= u \cdot \prod_{i \in I} \frac{1}{p_i} \text{ (by (238))}} \qquad \text{(by Theorem 2.9.9)} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} u \cdot \prod_{i \in I} \frac{1}{p_i} = u \cdot \underbrace{\sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i}}_{= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right) \text{ (by Lemma 2.9.21 \textbf{(b)}, applied to } a_i = \frac{1}{p_i})} \\
&= u \cdot \underbrace{\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right)}_{= \prod_{i=1}^{n} \left(1-\frac{1}{p_i}\right)} = u \cdot \prod_{i=1}^{n} \left(1-\frac{1}{p_i}\right).
\end{aligned}$$

This proves Theorem 2.9.19. □

2.9.7. Other cancellation-type lemmas

Propositions 2.9.10 and 2.9.12 belong to a genre of results saying that certain sums simplify to 0 in most cases. The following exercises give other specimens of this kind of result:

Exercise 2.9.11. Let S be a finite set. Let T be any set. Prove that

$$\sum_{I \subseteq S} (-1)^{|I \setminus T|} = \begin{cases} 2^{|S|}, & \text{if } S \subseteq T; \\ 0, & \text{otherwise} \end{cases}.$$

Exercise 2.9.12. Let S be a finite set. Let X and Y be two **distinct** subsets of S. Prove that

$$\sum_{I \subseteq S} (-1)^{|X \cap I| + |Y \cap I|} = 0.$$

Class of 2019-11-04

2.10. Compositions and weak compositions

We already know how to count n-tuples of elements of a set A: They are the elements of A^n, so their number is $|A^n| = |A|^n$ (by Corollary 1.5.5). We shall now

turn to some subtler tuple-counting problems. Specifically, we will count tuples of integers with a given sum.

2.10.1. Compositions

How many ways are there to write 5 as a sum of 3 positive integers, if the order matters? In other words, how many 3-tuples (x_1, x_2, x_3) of positive integers satisfy $x_1 + x_2 + x_3 = 5$? The answer is that there are 6 such 3-tuples (i.e., there are 6 ways to write 5 as a sum of 3 positive integers), namely

$$(1,1,3), \quad (1,3,1), \quad (3,1,1), \quad (1,2,2), \quad (2,1,2), \quad (2,2,1).$$

Indeed,

$$5 = 1+1+3 = 1+3+1 = 3+1+1 = 1+2+2 = 2+1+2 = 2+2+1.$$

What if we replace 5 and 3 by two arbitrary nonnegative integers n and k ? In other words, how many k-tuples $(x_1, x_2, \ldots, x_k)$ of positive integers satisfy $x_1 + x_2 + \cdots + x_k = n$? The following theorem answers this question:

Theorem 2.10.1. Let $\mathbb{P} = \{1, 2, 3, \ldots\}$ be the set of all positive integers. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then,

$$\begin{aligned} &\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\ &= \binom{n-1}{n-k} \qquad (239) \\ &= \begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases}. \qquad (240) \end{aligned}$$

Before we prove Theorem 2.10.1, let us introduce some terminology for the tuples counted in it:

Definition 2.10.2. **(a)** A *composition* shall mean a tuple (i.e., a finite list) of positive integers.

(b) If $k \in \mathbb{N}$, then a *composition into k parts* shall mean a k-tuple of positive integers.

(c) If $n \in \mathbb{N}$, then a *composition of n* shall mean a tuple of positive integers whose sum is n.

(d) If $n \in \mathbb{N}$ and $k \in \mathbb{N}$, then a *composition of n into k parts* shall mean a k-tuple of positive integers whose sum is n.

Note that the compositions we have just defined have nothing to do with the composition $f \circ g$ of two maps f and g. The use of the same word for the two completely unrelated concepts is a historical accident.

Example 2.10.3. (a) The compositions of 5 into 3 parts are

$$(1,1,3)\,, \qquad (1,3,1)\,, \qquad (3,1,1)\,, \qquad (1,2,2)\,, \qquad (2,1,2)\,, \qquad (2,2,1)\,.$$

This is just a restatement of what we said before Theorem 2.10.1.

(b) The compositions of 3 are

$$(3)\,, \qquad (1,2)\,, \qquad (2,1)\,, \qquad (1,1,1)\,.$$

The first of these is a composition into 1 part; the last is a composition into 3 parts; the other two are compositions into 2 parts.

(c) The only composition of 0 is the 0-tuple $()$; it is a composition into 0 parts.

If $n \in \mathbb{N}$ and $k \in \mathbb{N}$, then the compositions of n into k parts are the k-tuples of positive integers whose sum is n. In other words, they are the k-tuples $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$ (where we are using the notation $\mathbb{P} = \{1, 2, 3, \ldots\}$). Hence, Theorem 2.10.1 can be restated as follows:

$$\begin{aligned}
&(\#\text{ of compositions of } n \text{ into } k \text{ parts}) \\
&= \binom{n-1}{n-k} \\
&= \begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k = 0]\,, & \text{if } n = 0 \end{cases}
\end{aligned}$$

for any $n \in \mathbb{N}$ and $k \in \mathbb{N}$.

We shall now outline a proof of Theorem 2.10.1, referring to [19f-hw0s, solution to Exercise 1 **(b)**] (where a similar argument is made in a slightly different proof) and to Exercise 2.10.1 for some missing details. A different proof will be given in Exercise 2.10.2 further below.

Proof of Theorem 2.10.1 (sketched). It is easy to see that Theorem 2.10.1 holds when $n = 0$ (see Exercise 2.10.1 **(b)** below for the proof). Thus, for the rest of this proof, we WLOG assume that $n \neq 0$. Hence, $n \geq 1$ (since $n \in \mathbb{N}$). Thus, $n - 1 \in \mathbb{N}$.

It is easy to see that Theorem 2.10.1 holds when $k = 0$ (see Exercise 2.10.1 **(c)** below for the proof). Thus, for the rest of this proof, we WLOG assume that $k \neq 0$. Hence, $k \geq 1$ (since $k \in \mathbb{N}$). Thus, $k - 1 \in \mathbb{N}$.

A k-tuple of positive integers whose sum is n is the same as a composition of n into k parts[202]. In other words, a k-tuple $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$ is the same as a composition of n into k parts[203]. Therefore,

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\
&= (\#\text{ of compositions of } n \text{ into } k \text{ parts})\,.
\end{aligned} \tag{241}$$

[202] since this is how a composition of n into k parts was defined in Definition 2.10.2 **(d)**

[203] since $\mathbb{P}$ is the set of all positive integers

Now, we define a map

$$C : \{\text{compositions of } n \text{ into } k \text{ parts}\} \to \{(k-1)\text{-element subsets of } [n-1]\}$$

by setting

$$\begin{aligned} C\left((a_1, a_2, \ldots, a_k)\right) &= \{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\} \\ &= \{a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{k-1}\} \\ &\qquad \text{for all compositions } (a_1, a_2, \ldots, a_k) \text{ of } n \text{ into } k \text{ parts.} \end{aligned}$$

It is easy to see that this map C is well-defined[204].

(For example, if $n = 10$ and $k = 3$, then applying the map C to the composition $(3, 5, 2)$ yields $C\left((3, 5, 2)\right) = \{3, 3+5\} = \{3, 8\}$.)

Next, we define a map

$$D : \{(k-1)\text{-element subsets of } [n-1]\} \to \{\text{compositions of } n \text{ into } k \text{ parts}\}$$

as follows: Let S be a $(k-1)$-element subset of $[n-1]$. Thus, Proposition 1.4.13 (applied to $m = k-1$) shows that there exists a unique $(k-1)$-tuple $(s_1, s_2, \ldots, s_{k-1})$ of integers satisfying $\{s_1, s_2, \ldots, s_{k-1}\} = S$ and $s_1 < s_2 < \cdots < s_{k-1}$. Consider this $(k-1)$-tuple, and extend it further to a $(k+1)$-tuple $(s_0, s_1, \ldots, s_k)$ by setting $s_0 = 0$ and $s_k = n$. Then, it is easy to see that $s_0 < s_1 < \cdots < s_k$ [205]. Now, set

$$D(S) = (s_1 - s_0, s_2 - s_1, \ldots, s_k - s_{k-1}).$$

This defines D. It is easy to see that this map D is well-defined[206].

Note that the map D depends on n. For example,

- if $n = 6$ and $k = 4$, then $D(\{2, 3, 5\}) = (2, 1, 2, 1)$; but

[204] *Proof.* We need to show that $\{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\}$ is actually a $(k-1)$-element subset of $[n-1]$ whenever $(a_1, a_2, \ldots, a_k)$ is a composition of n into k parts.

So let $(a_1, a_2, \ldots, a_k)$ be a composition of n into k parts. We must show that $\{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\}$ is a $(k-1)$-element subset of $[n-1]$. In [19f-hw0s, solution to Exercise 1 **(b)**, proof of the well-definedness of C], it is shown that $\{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\}$ is a subset of $[n-1]$. It thus remains to only show that this subset is a $(k-1)$-element subset.

The k-tuple $(a_1, a_2, \ldots, a_k)$ is a composition; thus, its entries $a_1, a_2, \ldots, a_k$ are positive integers. Hence, we have the chain of inequalities

$$a_1 < a_1 + a_2 < a_1 + a_2 + a_3 < \cdots < a_1 + a_2 + \cdots + a_{k-1}.$$

Thus, the $k-1$ numbers $a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{k-1}$ are distinct. In other words, the $k-1$ numbers $a_1 + a_2 + \cdots + a_i$ for $i \in [k-1]$ are distinct. Hence, the set $\{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\}$ is a $(k-1)$-element set. Since this set is a subset of $[n-1]$, we thus conclude that it is a $(k-1)$-element subset of $[n-1]$. This completes our proof.

[205] Indeed, this can be proved just as $s_0 < s_1 < \cdots < s_{k+1}$ is proved in [19f-hw0s, solution to Exercise 1 **(b)**, construction of the map D] (with the caveat that what we call k here corresponds to the $k+1$ in [19f-hw0s, solution to Exercise 1 **(b)**, construction of the map D]).

[206] This can be done as in [19f-hw0s, solution to Exercise 1 **(b)**, proof of the well-definedness of D].

- if $n = 7$ and $k = 4$, then $D(\{2,3,5\}) = (2,1,2,2)$.

Now, it is easy to check that the maps C and D are mutually inverse[207]. Thus, the map

$$C : \{\text{compositions of } n \text{ into } k \text{ parts}\} \to \{(k-1)\text{-element subsets of } [n-1]\}$$

is invertible, i.e., is a bijection. Hence, the bijection principle yields

$$\begin{aligned} &|\{\text{compositions of } n \text{ into } k \text{ parts}\}| \\ &= |\{(k-1)\text{-element subsets of } [n-1]\}| \\ &= (\#\text{ of } (k-1)\text{-element subsets of } [n-1]) \\ &= \binom{n-1}{k-1} \end{aligned} \tag{242}$$

(by Theorem 1.3.12, applied to $[n-1]$, $n-1$ and $k-1$ instead of S, n and k).

Now, (241) becomes

$$\begin{aligned} &\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\ &= (\#\text{ of compositions of } n \text{ into } k \text{ parts}) \\ &= |\{\text{compositions of } n \text{ into } k \text{ parts}\}| \\ &= \binom{n-1}{k-1} \qquad (\text{by (242)}) \\ &= \binom{n-1}{(n-1)-(k-1)} \qquad \left(\begin{array}{c}\text{by Theorem 1.3.11 (applied to } n-1 \text{ and } k-1 \\ \text{instead of } n \text{ and } k\text{), since } n-1 \in \mathbb{N}\end{array}\right) \\ &= \binom{n-1}{n-k} \qquad (\text{since } (n-1)-(k-1) = n-k). \end{aligned}$$

This proves (239). Comparing this with

$$\begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases} = \binom{n-1}{k-1} \qquad (\text{since } n > 0)$$

$$= \binom{n-1}{n-k},$$

we obtain (240). Thus, Theorem 2.10.1 is proved. □

Exercise 2.10.1. The purpose of this exercise is to supply some missing details for the above proof of Theorem 2.10.1.

[207] This can be done as in [19f-hw0s, solution to Exercise 1 **(b)**].

(a) Prove that any $n \in \mathbb{N}$ and $k \in \mathbb{N}$ satisfy

$$\binom{n-1}{n-k} = \begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases}.$$

(b) Prove that Theorem 2.10.1 holds for $n = 0$.
(c) Prove that Theorem 2.10.1 holds for $k = 0$.

Exercise 2.10.2. Prove Theorem 2.10.1 by induction on k.

2.10.2. Binary compositions

Let us now count the ways to write a given $n \in \mathbb{N}$ not as a sum of k positive integers, but as a sum of k elements of the set $\{0,1\}$:

Theorem 2.10.4. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then,

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \{0,1\}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) = \binom{k}{n}.$$

Proof of Theorem 2.10.4 (sketched). Here is the idea of the proof:

If $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ is a k-tuple, then each index $i \in [k]$ satisfies either $x_i = 0$ or $x_i = 1$; furthermore, the sum $x_1 + x_2 + \cdots + x_k$ of all entries of this k-tuple is precisely the number of indices $i \in [k]$ satisfying $x_i = 1$ (because each such index contributes a 1 to this sum, whereas all remaining indices contribute 0's).

Thus, in order to construct a k-tuple $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$, we just need to choose which n indices $i \in [k]$ will satisfy $x_i = 1$ (because then, the remaining $k - n$ indices $i \in [k]$ will necessarily satisfy $x_i = 0$). There are $\dbinom{k}{n}$ many options for this, since this boils down to choosing an n-element subset of $[k]$ (and Theorem 1.3.12 says that there are $\dbinom{k}{n}$ such subsets).

A formal version of this argument would proceed using the bijection principle. Namely, it would argue that the map

$$\left\{(x_1, x_2, \ldots, x_k) \in \{0,1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\} \to \{n\text{-element subsets of } [k]\},$$
$$(x_1, x_2, \ldots, x_k) \mapsto \{i \in [k] \mid x_i = 1\}$$

is a bijection; therefore, the bijection principle yields

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \{0,1\}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\
&= (\#\text{ of } n\text{-element subsets of } [k]) \\
&= \binom{k}{n} \qquad \text{(by Theorem 1.3.12, applied to } k \text{ and } n \text{ instead of } n \text{ and } k\text{)}.
\end{aligned}$$

□

Exercise 2.10.3. Prove Theorem 2.10.4 by induction on k.

2.10.3. Weak compositions

Let us next count the ways to write a given $n \in \mathbb{N}$ as a sum of k **nonnegative** integers:

Theorem 2.10.5. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then,

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\
&= \binom{n+k-1}{n} \qquad (243) \\
&= \begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases}. \qquad (244)
\end{aligned}$$

Remark 2.10.6. Tuples of nonnegative integers are called *weak compositions*. Thus, Theorem 2.10.5 can be considered as a formula for counting (certain) weak compositions.

Example 2.10.7. For $n = 2$ and $k = 3$, the k-tuples $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$ are

$$(0,0,2), \quad (0,2,0), \quad (2,0,0), \quad (0,1,1), \quad (1,0,1), \quad (1,1,0),$$

because

$$2 = 0+0+2 = 0+2+0 = 2+0+0 = 0+1+1 = 1+0+1 = 1+1+0.$$

Thus, their # is 6. This is exactly what (243) yields, since $\binom{2+3-1}{2} = \binom{4}{2} = 6$.

Proof of Theorem 2.10.5. Let $\mathbb{P}$ denote the set $\{1, 2, 3, \ldots\}$ of all positive integers.

If x is a nonnegative integer, then $x+1$ is a positive integer. In other words, if $x \in \mathbb{N}$, then $x+1 \in \mathbb{P}$. Hence, if a k-tuple $(x_1, x_2, \ldots, x_k)$ belongs to $\mathbb{N}^k$ and satisfies $x_1 + x_2 + \cdots + x_k = n$, then the k-tuple $(x_1+1, x_2+1, \ldots, x_k+1)$ belongs to $\mathbb{P}^k$ and satisfies

$$(x_1+1)+(x_2+1)+\cdots+(x_k+1) = \underbrace{(x_1+x_2+\cdots+x_k)}_{=n} + \underbrace{\underbrace{1+1+\cdots+1}_{k \text{ times}}}_{=k} = n+k.$$

Hence, the map

$$\begin{aligned} &\left\{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n\right\} \\ &\to \left\{(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \mid x_1 + x_2 + \cdots + x_k = n+k\right\}, \\ &(x_1, x_2, \ldots, x_k) \mapsto (x_1+1, x_2+1, \ldots, x_k+1) \end{aligned}$$

is well-defined. It is easy to see that this map is a bijection. Thus, the bijection principle yields

$$\begin{aligned} &\left|\left\{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}\right| \\ &= \left|\left\{(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \mid x_1 + x_2 + \cdots + x_k = n+k\right\}\right|. \end{aligned}$$

In other words,

$$\begin{aligned} &\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\ &= \left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n+k\right) \\ &= \binom{(n+k)-1}{(n+k)-k} \qquad \text{(by (239), applied to } n+k \text{ instead of } n) \\ &= \binom{n+k-1}{n} \qquad \text{(since } (n+k)-1 = n+k-1 \text{ and } (n+k)-k = n). \end{aligned}$$

This proves (243).

Continuing this computation, we obtain

$$\begin{aligned} &\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\ &= \binom{n+k-1}{n} = \begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases} \end{aligned}$$

(by Theorem 1.3.11 and an easy distinction of cases[208]). This proves (244). Thus, Theorem 2.10.5 is proven. □

[208] See Exercise 2.10.4 below for a detailed justification of the last equality sign.

Exercise 2.10.4. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Prove that

$$\binom{n+k-1}{n} = \begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases}.$$

The equality (243) also appears in [Grinbe15, Exercise 3.15] (with a proof by induction).

2.10.4. Other composition-like counting problems

Theorem 2.10.1, Theorem 2.10.5 and Theorem 2.10.4 are perhaps the three most important results about counting tuples of integers with a given sum. But there are many others. First of all, we can count compositions of n without specifying the number of parts:

Theorem 2.10.8. Let $n \in \mathbb{N}$. Then,

$$(\#\text{ of compositions of } n) = \begin{cases} 2^{n-1}, & \text{if } n > 0 \\ 1, & \text{if } n = 0 \end{cases}.$$

For the proof of Theorem 2.10.8, see [19f-hw0s, Exercise 1 **(b)**].

We may also want to count compositions of n whose entries belong to $\{1,2\}$ – that is, ways to write n as a sum of 1's and 2's. The answer turns out to be simple again:

Exercise 2.10.5. Let $n \in \mathbb{N}$.

A $\{1,2\}$-*composition of* n shall mean a composition $(x_1, x_2, \ldots, x_k)$ of n such that $x_1, x_2, \ldots, x_k \in \{1,2\}$.

For example, the $\{1,2\}$-compositions of 5 are

$$(1,1,1,1,1), \quad (1,1,1,2), \quad (1,1,2,1), \quad (1,2,1,1),$$
$$(2,1,1,1), \quad (2,2,1), \quad (2,1,2), \quad (1,2,2).$$

(a) Prove that

$$(\#\text{ of } \{1,2\}\text{-compositions of } n) = f_{n+1}$$

(where $(f_0, f_1, f_2, \ldots)$ denotes the Fibonacci sequence, as defined in Definition 1.1.10).

(b) Let $k \in \mathbb{N}$. A $\{1,2\}$-*composition of* n *into* k *parts* shall mean a composition $(x_1, x_2, \ldots, x_k)$ of n into k parts such that $x_1, x_2, \ldots, x_k \in \{1,2\}$.

Prove that

$$(\#\text{ of } \{1,2\}\text{-compositions of } n \text{ into } k \text{ parts}) = \binom{k}{n-k}.$$

Also, we can try to generalize Theorem 2.10.4 by replacing $\{0,1\}$ by $\{0,1,\ldots,p-1\}$ for a given $p \in \mathbb{N}$. Thus, we look for the # of $(x_1,x_2,\ldots,x_k) \in \{0,1,\ldots,p-1\}^k$ satisfying $x_1+x_2+\cdots+x_k=n$. The answer to this counting problem, however, will not be as simple as $\binom{k}{n}$:

Exercise 2.10.6. Let $p \in \mathbb{N}$. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$. Prove that

$$\left(\#\text{ of } (x_1,x_2,\ldots,x_k) \in \{0,1,\ldots,p-1\}^k \text{ satisfying } x_1+x_2+\cdots+x_k=n\right)$$
$$= \sum_{j=0}^{k} (-1)^j \binom{k}{j} \binom{n-pj+k-1}{n-pj}.$$

[**Hint:** Use the Principle of Inclusion and Exclusion, keeping in mind that $\{0,1,\ldots,p-1\} = \mathbb{N} \setminus \{i \in \mathbb{N} \mid i \geq p\}$.]

The next exercise is a simple-looking identity for binomial coefficients, which can be nicely solved using weak compositions despite not explicitly involving them:

Exercise 2.10.7. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Prove that

$$\sum_{i=0}^{k} \binom{n+i-1}{i} \binom{n}{k-2i} = \binom{n+k-1}{k}.$$

[**Hint:** Any nonnegative integer u can be written as $u = 2q+r$ for a unique $q \in \mathbb{N}$ and a unique $r \in \{0,1\}$. What does this mean for weak compositions of k into n parts?]

Exercise 2.10.8. Generalize Exercise 2.10.7 to all $n \in \mathbb{R}$.

Rather than count the compositions of an integer, we can also count them "with weight" – i.e., sum certain values over them. Perhaps the simplest such value is the length. Recall that the *length* of a tuple $(x_1,x_2,\ldots,x_k)$ is defined to be the integer k. In other words, the length of a tuple α is the $k \in \mathbb{N}$ such that α is a k-tuple. Thus, each composition has a well-defined length (since it is a tuple).

Exercise 2.10.9. Let n be a positive integer. Prove that the sum of the lengths of all compositions of n is $(n+1)\,2^{n-2}$.

2.11. Multisubsets

2.11.1. Definitions

The notion of a set is sufficiently versatile that it is often used as a foundation to build all of mathematics upon. But it has its limitations; in particular, a set

cannot contain multiple copies of the same element. (More precisely, a set S can either contain or not contain an element x; it makes no sense to ask "how often" it contains x.) Often, one wants to use a kind of collection that can contain elements with multiplicities[209]. The notion of a *multiset* addresses this need (at least if the multiplicities of the elements are nonnegative integers[210]). Rather than define this notion, we shall however introduce a slight modification thereof, namely the notion of a *multisubset* of a given set T:

Definition 2.11.1. Let T be a set.

(a) A *multisubset of* T is formally defined as a map $f : T \to \mathbb{N}$ such that only finitely many $t \in T$ satisfy $f(t) \neq 0$.

Informally, we regard such a map $f : T \to \mathbb{N}$ as a way to encode a "set with multiplicities" – namely, the "set" in which each $t \in T$ appears $f(t)$ many times.

(b) If f is a multisubset of T, and if $t \in T$, then the number $f(t)$ is called the *multiplicity* of t in f, and we say that the element t is contained in T exactly $f(t)$ times. If $f(t) = 0$, then we say that t is *not contained* in T, and we write $t \notin T$.

(c) Let $(a_1, a_2, \ldots, a_k)$ be a finite list of elements of T. (We don't require $a_1, a_2, \ldots, a_k$ to be distinct.) Then, $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ shall denote the multisubset of T in which each element $t \in T$ is contained as many times as it is contained in the list $(a_1, a_2, \ldots, a_k)$. In other words, $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ shall denote the multisubset f of T defined by

$$\begin{aligned} f(t) &= (\#\text{ of times } t \text{ appears in the list } (a_1, a_2, \ldots, a_k)) \\ &= (\#\text{ of } i \in [k] \text{ satisfying } a_i = t) \qquad \text{for each } t \in T. \end{aligned}$$

For example, if $T = [8]$, then the map from $[8]$ to $\mathbb{N}$ given in two-line notation as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 0 & 0 & 2 & 1 & 0 & 3 & 0 \end{pmatrix}$$

is a multisubset of $[8]$, namely the multisubset of $[8]$ in which 1 is contained 1 time, 4 is contained 2 times, 5 is contained 1 time, and 7 is contained 3 times (while the elements 2, 3, 6 and 8 are not contained in this multisubset). This multisubset can also be written as $\{1,4,4,5,7,7,7\}_{\text{multi}}$ or as $\{7,5,4,7,4,1,7\}_{\text{multi}}$ or in many other equivalent ways.

Note that $\{1,1\}_{\text{multi}} \neq \{1\}_{\text{multi}}$, despite $\{1,1\} = \{1\}$.

The requirement that "only finitely many $t \in T$ satisfy $f(t) \neq 0$" in Definition 2.11.1 **(a)** prevents us from having infinite multisubsets. Of course, if the set T is finite, then this requirement is automatically satisfied.

We note that many authors use the notation $\{\{a_1, a_2, \ldots, a_k\}\}$ instead of our notation $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ for a multisubset. However, the former notation can

[209] For example, the roots of a polynomial naturally come with multiplicities.

[210] There are also variants that allow infinite multiplicities.

be misunderstood to mean a set consisting of the set $\{a_1, a_2, \ldots, a_k\}$; thus we are avoiding it.

As we said, instead of defining multisubsets of a set T, we could have defined multisets in general.[211] We are preferring multisubsets of T here, as they are better adapted to counting purposes.

Definition 2.11.2. Let T be a set. If $f : T \to \mathbb{N}$ is a multisubset of T, then the *size* of this multisubset f is defined to be the nonnegative integer $\sum_{t \in T} f(t)$.

For example, the above-mentioned multisubset $\{1,4,4,5,7,7,7\}_{\text{multi}}$ of $[8]$ has size $1+2+1+3=7$. Note that the sum $\sum_{t \in T} f(t)$ in Definition 2.11.2 is well-defined, since we required in Definition 2.11.1 that only finitely many $t \in T$ satisfy $f(t) \neq 0$.

If $a_1, a_2, \ldots, a_k$ are k objects, then the set $\{a_1, a_2, \ldots, a_k\}$ doesn't always have size k; its size will be smaller than k if some of $a_1, a_2, \ldots, a_k$ are equal. But the multiset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ always has size k, as the following simple exercise shows:

Exercise 2.11.1. Let T be a set. Let $k \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_k$ be any k elements of T (not necessarily distinct). Prove that the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of T has size k.

2.11.2. Counting multisubsets of given size

A finite nonempty set T has infinitely many multisubsets, since any element can appear any number of times. Thus, counting all multisubsets of a given finite set T is not a promising combinatorial question. However, we get a finite number if we restrict ourselves to counting multisubsets with a given size:

Corollary 2.11.3. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Let T be a k-element set. Then,

$$(\#\text{ of multisubsets of } T \text{ having size } n) = \binom{n+k-1}{n}.$$

Example 2.11.4. The multisubsets of $[3]$ having size 2 are

$$\{1,1\}_{\text{multi}}, \quad \{1,2\}_{\text{multi}}, \quad \{1,3\}_{\text{multi}},$$
$$\{2,2\}_{\text{multi}}, \quad \{2,3\}_{\text{multi}}, \quad \{3,3\}_{\text{multi}}.$$

[211] The easiest way to define them is as follows: A *multiset* is a pair (S, f), where S is a finite set and $f : S \to \{1,2,3,\ldots\}$ is a map. The elements of S are considered to be the elements of this multiset, and the values $f(s)$ are understood to be their multiplicities (i.e., any element $s \in S$ is understood to appear $f(s)$ times in the multiset). This time, the map f must have target $\{1,2,3,\ldots\}$ rather than $\mathbb{N}$ (that is, it cannot have 0 in its image), since otherwise our multiset could have "ghost" elements s that are considered to be its elements but appear with multiplicity 0.

In terms of their definition, these multisubsets are the maps from $[3]$ to $\mathbb{N}$ with the two-line notations

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 2 \end{pmatrix},$$

respectively. Either way, we see that there are 6 of them, and this is what Corollary 2.11.3 predicts (because $\dbinom{2+3-1}{2} = 6$).

Proof of Corollary 2.11.3. Let $t_1, t_2, \ldots, t_k$ be the k elements of T, listed in some order (with no repetitions). Recall that a multisubset of T is the same as a map $f : T \to \mathbb{N}$ such that only finitely many $t \in T$ satisfy $f(t) \neq 0$ (according to Definition 2.11.1 **(a)**). In other words, a multisubset of T is the same as a map $f : T \to \mathbb{N}$ (because the property that "only finitely many $t \in T$ satisfy $f(t) \neq 0$" is automatically satisfied[212]). Moreover, if $f : T \to \mathbb{N}$ is a multisubset of T, then

$$\begin{aligned} (\text{the size of } f) &= \sum_{t \in T} f(t) \qquad \text{(by Definition 2.11.2)} \\ &= f(t_1) + f(t_2) + \cdots + f(t_k) \end{aligned}$$

(since $t_1, t_2, \ldots, t_k$ are the k elements of T). Hence, the multisubsets of T having size n are precisely the maps $f : T \to \mathbb{N}$ satisfying $f(t_1) + f(t_2) + \cdots + f(t_k) = n$. Clearly, such maps $f : T \to \mathbb{N}$ are uniquely determined by their lists of values $(f(t_1), f(t_2), \ldots, f(t_k)) \in \mathbb{N}^k$ (since $t_1, t_2, \ldots, t_k$ are the k elements of T). Thus, the map

$$\begin{aligned} \{\text{multisubsets of } T \text{ having size } n\} &\to \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n \right\}, \\ f &\mapsto (f(t_1), f(t_2), \ldots, f(t_k)) \end{aligned}$$

is a bijection. Hence, the bijection principle yields

$$\begin{aligned} &(\#\text{ of multisubsets of } T \text{ having size } n) \\ &= \left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n \right) \\ &= \binom{n+k-1}{n} \qquad \text{(by (243))}. \end{aligned}$$

This proves Corollary 2.11.3. □

[212] since T is finite

2.11.3. An application to lacunar subsets

We shall now outline an application of multisubsets. First, however, let us state two propositions, which are fairly obvious intuitively (even though proving them formally is somewhat time-consuming):[213]

Proposition 2.11.5. Let T be a set of integers. Let S be a multisubset of T. Then, there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers in T satisfying $\{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_k$.

Proposition 2.11.6. Let T be a set of integers. Let $m \in \mathbb{N}$. Let S be a multisubset of T having size m. Then, there exists a unique m-tuple $(s_1, s_2, \ldots, s_m)$ of integers in T satisfying $\{s_1, s_2, \ldots, s_m\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_m$.

Proposition 2.11.5 and Proposition 2.11.6 are multiset analogues of Proposition 1.4.11 and Proposition 1.4.13, respectively. The latter two propositions say that a finite set of integers has a unique **strictly** increasing list of elements; the former two say that a finite multiset of integers has a unique **weakly** increasing list of elements.

Exercise 2.11.2. Prove Proposition 2.11.5 and Proposition 2.11.6.

As an application of multisubsets, we shall sketch a solution to the following exercise (whose statement involves no multisubsets!):

Exercise 2.11.3. Let $m \in \mathbb{N}$ and $a, b \in \{0, 1, \ldots, m\}$. Prove that

$$\begin{aligned}&(\#\text{ of lacunar subsets of } [2m] \text{ with exactly } a \text{ even and } b \text{ odd elements})\\ &= \binom{m-a}{b} \cdot \binom{m-b}{a}.\end{aligned}$$

Exercise 2.11.3 originates in [MusPro07, Theorem 3] (although the authors of this paper forget to assume that $a, b \in \{0, 1, \ldots, m\}$). One might try to solve it using the dependent product rule, but this does not work: If we (say) first choose the b odd elements of our lacunar subset, then the # of ways to subsequently choose the remaining a even elements will depend on our chosen b odd elements. The exercise is too subtle for this method. I have outlined two solutions of Exercise 2.11.3 in [18s-hw2s, Exercise 3]. A simpler solution has been found by Musiker and Propp (in [MusPro07]) using multisubsets[214]. Before I sketch this solution, let me define a multiset analogue of the notion of the union of two disjoint sets:

[213] Note that a multisubset of a set T is defined as a map from T to $\mathbb{N}$, so you might expect me to use a letter like f or g for it. Nevertheless, I am using the uppercase letter S for it in Proposition 2.11.5 and Proposition 2.11.6, in order to stress the analogy to a subset of T (which is typically denoted by an uppercase letter).

[214] This solution is also sketched in [Stanle11, Exercise 1.10].

Definition 2.11.7. Let A and B be two disjoint sets. Let X be a multisubset of A. Let Y be a multisubset of B.

Then, $X \cup Y$ shall denote the multisubset of $A \cup B$ defined by

$$X \cup Y = \{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_\ell\}_{\text{multi}}, \tag{245}$$

where we have written X in the form $X = \{x_1, x_2, \ldots, x_k\}_{\text{multi}}$ and written Y in the form $Y = \{y_1, y_2, \ldots, y_\ell\}_{\text{multi}}$.

Here is a different (but equivalent) way to define this multisubset $X \cup Y$: Recall that a multisubset of A is the same as a map $f : A \to \mathbb{N}$. Thus, the multisubset X of A is a map $f : A \to \mathbb{N}$. Likewise, the multisubset Y of B is a map $g : B \to \mathbb{N}$. Now, define a map $h : A \cup B \to \mathbb{N}$ by setting

$$h(u) = \begin{cases} f(u), & \text{if } u \in A; \\ g(u), & \text{if } u \in B \end{cases} \qquad \text{for each } u \in A \cup B. \tag{246}$$

(This is well-defined, since no $u \in A \cup B$ can satisfy both $u \in A$ and $u \in B$ at the same time.) This map $h : A \cup B \to \mathbb{N}$ is a multisubset of $A \cup B$; we define $X \cup Y$ to be this multisubset.

The multisubset $X \cup Y$ of $A \cup B$ is called the *multiset union* of X and Y.

For example, the multiset union of the multisubset $\{1,2,2,4\}_{\text{multi}}$ of $\{1,2,3,4,5\}$ with the multisubset $\{6,6,8,9,9\}_{\text{multi}}$ of $\{6,7,8,9,10\}$ is the multisubset

$$\{1,2,2,4\}_{\text{multi}} \cup \{6,6,8,9,9\}_{\text{multi}} = \{1,2,2,4,6,6,8,9,9\}_{\text{multi}}$$

of $\{1,2,\ldots,10\}$.

Remark 2.11.8. Definition 2.11.7 can be extended to the case when A and B are not disjoint. However, there are two non-equivalent ways to do so. In other words, there are two different reasonable notions of $X \cup Y$ when A and B are not disjoint.

One of these two notions can be defined by the equality (245). Equivalently, it can be defined by regarding X and Y as maps $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$ (as in Definition 2.11.7), and defining $X \cup Y$ as the map $h : A \cup B \to \mathbb{N}$ given by

$$h(u) = \begin{cases} f(u), & \text{if } u \in A \setminus B; \\ g(u), & \text{if } u \in B \setminus A; \\ f(u) + g(u), & \text{if } u \in A \cap B \end{cases} \qquad \text{for each } u \in A \cup B.$$

For example, this definition entails that the multiset union of the multisubset $\{1,2,2,3\}_{\text{multi}}$ of $[3]$ with the multisubset $\{2,3,3,4\}_{\text{multi}}$ of $[4]$ is the multisubset

$$\{1,2,2,3\}_{\text{multi}} \cup \{2,3,3,4\}_{\text{multi}} = \{1,2,2,3,2,3,3,4\}_{\text{multi}} = \{1,2,2,2,3,3,3,4\}_{\text{multi}}$$

of $[4]$.

The second notion of $X \cup Y$ can be defined by regarding X and Y as maps $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$ (as in Definition 2.11.7), and defining $X \cup Y$ as the map $h' : A \cup B \to \mathbb{N}$ given by

$$h'(u) = \begin{cases} f(u), & \text{if } u \in A \setminus B; \\ g(u), & \text{if } u \in B \setminus A; \\ \max\{f(u), g(u)\}, & \text{if } u \in A \cap B \end{cases} \qquad \text{for each } u \in A \cup B$$

(where $\max S$ denotes the largest element of any given set $S \subseteq \mathbb{N}$). For example, this definition entails that the multiset union of the multisubset $\{1,2,2,3\}_{\text{multi}}$ of $[3]$ with the multisubset $\{2,3,3,4\}_{\text{multi}}$ of $[4]$ is the multisubset

$$\{1,2,2,3\}_{\text{multi}} \cup \{2,3,3,4\}_{\text{multi}} = \{1,2,2,3,3,4\}_{\text{multi}}$$

of $[4]$.

These two notions of $X \cup Y$ coincide when X and Y have no elements in common; otherwise, the first notion of $X \cup Y$ has larger size than the second. Note that the second notion (unlike the first) does not satisfy (245) in general.

It is easy to check that if A and B are two disjoint sets, then any multisubset of $A \cup B$ can be uniquely split up as a multiset union of a multisubset of A with a multisubset of B, in the following sense:

Lemma 2.11.9. Let A and B be two disjoint sets. Let Z be a multisubset of $A \cup B$. Then, there is a unique way to write Z in the form $X \cup Y$, where X is a multisubset of A and where Y is a multisubset of B. (In other words, there exists a unique pair (X, Y) such that X is a multisubset of A and Y is a multisubset of B and $Z = X \cup Y$.)

Proof of Lemma 2.11.9 (sketched). Let us view the multisubset Z of $A \cup B$ as a map $f : A \cup B \to \mathbb{N}$. Then, its restriction $f|_A : A \to \mathbb{N}$ is a multisubset of A, and its restriction $f|_B : B \to \mathbb{N}$ is a multisubset of B. If we denote these two restrictions by X and Y, we then have $Z = X \cup Y$. It is easy to see that this is the only way to write Z in the form $X \cup Y$, where X is a multisubset of A and where Y is a multisubset of B. Thus, Lemma 2.11.9 follows. □

The following is also rather obvious:

Lemma 2.11.10. Let A and B be two disjoint sets. Let X be a multisubset of A. Let Y be a multisubset of B. Then, the size of $X \cup Y$ is the sum of the sizes of X and Y.

We can now solve Exercise 2.11.3:

Solution to Exercise 2.11.3 (sketched). Let $g = m - a - b + 1$. It is easy to see that Exercise 2.11.3 is true if $g < 0$ [215]. Thus, for the rest of this solution, we WLOG assume that $g \geq 0$. Hence, $g \in \mathbb{N}$.

[215] *Proof.* Assume that $g < 0$. We must prove that Exercise 2.11.3 is true.

The set $[2g]$ is the union of its two disjoint g-element subsets

$$E := \{\text{even elements of } [2g]\} = \{2, 4, 6, \ldots, 2g\} \qquad \text{and}$$
$$O := \{\text{odd elements of } [2g]\} = \{1, 3, 5, \ldots, 2g-1\}.$$

Let S be a lacunar subset of $[2m]$ with exactly a even and b odd elements. Thus, $|S| = a+b$, so that we can write S uniquely in the form $S = \{s_1 < s_2 < \cdots < s_{a+b}\}$ (by Proposition 1.4.13). Let us consider these $s_1, s_2, \ldots, s_{a+b}$. Then, since S is lacunar, we have

$$s_1 - 0 \leq s_2 - 2 \leq s_3 - 4 \leq \cdots \leq s_{a+b} - 2(a+b-1) \tag{248}$$

[216]. Moreover, all the $a+b$ entries $s_i - 2(i-1)$ (for $i \in [a+b]$) of this chain of

---

We have

$$m - (a+b) = m - a - b = \underbrace{(m-a-b+1)}_{=g<0} - 1 < 0 - 1 = -1 < 0.$$

In other words, $m < a+b$. Thus, $a+b > m$.

However, Proposition 1.4.6 (applied to $n = 2m$) shows that the largest size of a lacunar subset of $[2m]$ is $\lceil 2m/2 \rceil$. In other words, the largest size of a lacunar subset of $[2m]$ is m (since $\left\lceil \underbrace{2m/2}_{=m} \right\rceil = \lceil m \rceil = m$). Therefore, any lacunar subset of $[2m]$ has size $\leq m$. In other words, no lacunar subset of $[2m]$ has size $> m$.

Hence, there exists no lacunar subset of $[2m]$ that contains exactly a even and b odd elements (because such a subset would have size $a+b > m$, but this would contradict the preceding sentence). In other words,

$$\begin{aligned}&(\#\text{ of lacunar subsets of } [2m] \text{ with exactly } a \text{ even and } b \text{ odd elements})\\ &= 0.\end{aligned} \tag{247}$$

On the other hand, $a \leq m$ (since $a \in \{0, 1, \ldots, m\}$), so that $m - a \geq 0$ and therefore $m - a \in \mathbb{N}$. Furthermore, $b > m - a$ (since $a + b > m$). Thus, Proposition 1.3.6 (applied to $m-a$ and b instead of n and k) yields $\binom{m-a}{b} = 0$. Therefore,

$$\underbrace{\binom{m-a}{b}}_{=0} \cdot \binom{m-b}{a} = 0.$$

Comparing this with (247), we obtain

$$\begin{aligned}&(\#\text{ of lacunar subsets of } [2m] \text{ with exactly } a \text{ even and } b \text{ odd elements})\\ &= \binom{m-a}{b} \cdot \binom{m-b}{a}.\end{aligned}$$

Hence, we have shown that Exercise 2.11.3 is true if $g < 0$.

[216] *Proof.* We must show that $s_i - 2(i-1) \leq s_{i+1} - 2i$ for each $i \in [a+b-1]$.

So let $i \in [a+b-1]$. Then, $s_i < s_{i+1}$ (since $s_1 < s_2 < \cdots < s_{a+b}$), so that $s_i \leq s_{i+1} - 1$ (since s_i

inequalities belong to the set $[2g]$ [217]. Hence, we can define the multisubset[218]

$$M_S := \{s_1 - 0 \leq s_2 - 2 \leq s_3 - 4 \leq \cdots \leq s_{a+b} - 2(a+b-1)\}_{\text{multi}}$$

of $[2g]$. This multisubset M_S has exactly a even and b odd elements[219] (since the integers $s_1 - 0, s_2 - 2, s_3 - 4, \ldots, s_{a+b} - 2(a+b-1)$ have the same parities[220] as the integers $s_1, s_2, s_3, \ldots, s_{a+b}$, respectively[221]). In other words, the multisubset M_S has exactly a elements from E and exactly b elements from O.

Recall that M_S is a multisubset of $[2g] = E \cup O$. Hence, we can (using Lemma 2.11.9) uniquely split M_S up as a multiset union $M_{S,\text{even}} \cup M_{S,\text{odd}}$, where

$$M_{S,\text{even}} \text{ is a multisubset of } E$$

and

$$M_{S,\text{odd}} \text{ is a multisubset of } O.$$

Moreover, the multisubset $M_{S,\text{even}}$ here has size a (since M_S has exactly a elements from E), and the multisubset $M_{S,\text{odd}}$ here has size b (since M_S has exactly b elements from O).

Forget that we fixed S. Thus, for each lacunar subset S of $[2m]$ with exactly a even and b odd elements, we have constructed a size-a multisubset $M_{S,\text{even}}$ of E

---

and s_{i+1} are integers). But recall that the set S is lacunar, and thus contains no two consecutive integers. If we had $s_i = s_{i+1} - 1$, then s_i and s_{i+1} would be two consecutive integers in S, which would contradict the previous sentence. Hence, we cannot have $s_i = s_{i+1} - 1$. Thus, we have $s_i \neq s_{i+1} - 1$. Combined with $s_i \leq s_{i+1} - 1$, this yields $s_i < s_{i+1} - 1$. Since s_i and $s_{i+1} - 1$ are integers, this entails $s_i \leq (s_{i+1} - 1) - 1 = s_{i+1} - 2$. Subtracting $2(i-1)$ from both sides of this inequality, we obtain $s_i - 2(i-1) \leq s_{i+1} - 2 - 2(i-1) = s_{i+1} - 2i$.

Now, forget that we fixed i. We thus have showed that $s_i - 2(i-1) \leq s_{i+1} - 2i$ for each $i \in [a+b-1]$. In other words,

$$s_1 - 0 \leq s_2 - 2 \leq s_3 - 4 \leq \cdots \leq s_{a+b} - 2(a+b-1).$$

[217] *Proof.* We must show that $s_i - 2(i-1) \in [2g]$ for each $i \in [a+b]$. So let us fix $i \in [a+b]$. Then, $1 \leq i \leq a+b$. Hence, $s_1 - 0 \leq s_i - 2(i-1) \leq s_{a+b} - 2(a+b-1)$ (by (248)). Hence, $s_i - 2(i-1) \geq s_1 - 0 = s_1 \geq 1$ (since $s_1 \in \{s_1 < s_2 < \cdots < s_{a+b}\} = S \subseteq [2m]$). Also, $s_{a+b} \leq 2m$ (since $s_{a+b} \in \{s_1 < s_2 < \cdots < s_{a+b}\} = S \subseteq [2m]$), and $s_i - 2(i-1) \leq \underbrace{s_{a+b}}_{\leq 2m} - 2(a+b-1) \leq 2m - 2(a+b-1) = 2\underbrace{(m-a-b+1)}_{=g} = 2g$. Combining $s_i - 2(i-1) \geq 1$ with $s_i - 2(i-1) \leq 2g$, we obtain $s_i - 2(i-1) \in \{1, 2, \ldots, 2g\} = [2g]$, qed.

[218] We are using an analogue of the notation from Definition 1.4.12 for multisets here: If T is a set of integers, and if $a_1, a_2, \ldots, a_k$ are k numbers from T, then the notation "$\{a_1 \leq a_2 \leq \cdots \leq a_k\}_{\text{multi}}$" shall denote the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of T and simultaneously assert that $a_1 \leq a_2 \leq \cdots \leq a_k$.

[219] counted with multiplicity

[220] The *parity* of an integer k is defined to be 0 if k is even and 1 if k is odd. Thus, two integers k and ℓ have the same parity if and only if they are either both even or both odd.

[221] because the former integers differ from the latter integers by a multiple of 2 (to wit: $s_i - 2(i-1)$ differs from s_i by $2(i-1)$).

and a size-b multisubset $M_{S,\mathrm{odd}}$ of O. Hence, we can define a map

$$\begin{aligned}&\{\text{lacunar subsets of } [2m] \text{ with exactly } a \text{ even and } b \text{ odd elements}\}\\&\to \{\text{size-}a \text{ multisubsets of } E\} \times \{\text{size-}b \text{ multisubsets of } O\},\\S &\mapsto \left(M_{S,\mathrm{even}}, M_{S,\mathrm{odd}}\right).\end{aligned}$$

This map is easily seen to be a bijection[222]. Hence, the bijection principle yields

$$\begin{aligned}&(\#\text{ of lacunar subsets of } [2m] \text{ with exactly } a \text{ even and } b \text{ odd elements})\\&= |\{\text{size-}a \text{ multisubsets of } E\} \times \{\text{size-}b \text{ multisubsets of } O\}|\\&= \underbrace{(\#\text{ of size-}a \text{ multisubsets of } E)}_{=(\#\text{ of multisubsets of } E \text{ having size } a)} \cdot \underbrace{(\#\text{ of size-}b \text{ multisubsets of } O)}_{=(\#\text{ of multisubsets of } O \text{ having size } b)}\\&\qquad \underbrace{=\binom{a+g-1}{a}}_{\substack{\text{(by Corollary 2.11.3,}\\ \text{applied to } a, g \text{ and } E \text{ instead of } n, k \text{ and } T)}} \qquad \underbrace{=\binom{b+g-1}{b}}_{\substack{\text{(by Corollary 2.11.3,}\\ \text{applied to } b, g \text{ and } O \text{ instead of } n, k \text{ and } T)}}\\&\qquad\qquad (\text{by the product rule})\\&= \underbrace{\binom{a+g-1}{a}}_{\substack{=\binom{m-b}{a}\\ (\text{since } a+g-1=m-b\\ (\text{because } g=m-a-b+1))}} \cdot \underbrace{\binom{b+g-1}{b}}_{\substack{=\binom{m-a}{b}\\ (\text{since } b+g-1=m-a\\ (\text{because } g=m-a-b+1))}}\\&= \binom{m-b}{a}\cdot\binom{m-a}{b} = \binom{m-a}{b}\cdot\binom{m-b}{a}.\end{aligned}$$

This solves Exercise 2.11.3. □

Note that, as a consequence of Exercise 2.11.3, we can obtain the following formula for Fibonacci numbers:

$$f_{2m+2} = \sum_{a=0}^{m}\sum_{b=0}^{m}\binom{m-a}{b}\cdot\binom{m-b}{a} \qquad \text{for all } m \in \mathbb{N}.$$

(See [18s-mt1s, solution to Exercise 3 **(f)**] for more details on how this is proved.)

[222] The inverse map sends any pair $(X, Y) \in \{\text{size-}a \text{ multisubsets of } E\} \times \{\text{size-}b \text{ multisubsets of } O\}$ to the lacunar subset S of $[2m]$ constructed as follows: Write the multiset union $X \cup Y$ in the form $X \cup Y = \{t_1 \le t_2 \le \cdots \le t_{a+b}\}_{\mathrm{multi}}$ (Proposition 2.11.6 guarantees that this can be done in a unique way), and define S by

$$S = \{t_1 + 0 < t_2 + 2 < t_3 + 4 < \cdots < t_{a+b} + 2(a+b-1)\}.$$

2.12. Multinomial coefficients

2.12.1. Definition and formulas

Let us next introduce another family of combinatorially meaningful numbers.

Definition 2.12.1. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$. Then, we define a rational number $\binom{n}{n_1, n_2, \ldots, n_k}$ by

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

This number $\binom{n}{n_1, n_2, \ldots, n_k}$ is called a *multinomial coefficient*.

Remark 2.12.2. **(a)** We are not defining $\binom{n}{n_1, n_2, \ldots, n_k}$ for negative or non-integer n. (This is in contrast to the notion of binomial coefficients $\binom{n}{k}$.)

(b) The notation $\binom{n}{n_1, n_2, \ldots, n_k}$ for multinomial coefficients may get mistaken for a binomial coefficient in the case when $k = 1$. However, in this trivial case, both notations lead to the same value (namely, 1) [223], and thus the ambiguity is harmless.

Example 2.12.3. We have $7 \in \mathbb{N}$ and $2, 3, 2 \in \mathbb{N}$ and $2 + 3 + 2 = 7$. Thus, Definition 2.12.1 yields

$$\binom{7}{2, 3, 2} = \frac{7!}{2! \cdot 3! \cdot 2!} = \frac{5040}{2 \cdot 6 \cdot 2} = 210.$$

Here are some algebraic properties of multinomial coefficients:

[223] In more details: Assume that $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ satisfy $n_1 + n_2 + \cdots + n_k = n$ and $k = 1$. Then, $n = n_1 + n_2 + \cdots + n_k = n_1$ (since $k = 1$), so that $n_1 = n$. Thus, the binomial coefficient $\binom{n}{n_1}$ satisfies $\binom{n}{n_1} = \binom{n}{n} = 1$ (by Exercise 1.3.2). But the definition of the multinomial coefficient $\binom{n}{n_1, n_2, \ldots, n_k}$ yields $\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!} = \frac{n!}{n_1!}$ (since $k = 1$), so that $\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1!} = 1$ (since $n = n_1$). Hence, both the binomial coefficient $\binom{n}{n_1}$ and the multinomial coefficient $\binom{n}{n_1, n_2, \ldots, n_k}$ equal 1 in this case.

Proposition 2.12.4. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$. Then:

(a) We have

$$\begin{aligned}\binom{n}{n_1, n_2, \ldots, n_k} &= \prod_{i=1}^{k} \binom{n - n_1 - n_2 - \cdots - n_{i-1}}{n_i} \\ &= \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots \underbrace{\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}}_{=1} \\ &= \prod_{i=1}^{k-1} \binom{n - n_1 - n_2 - \cdots - n_{i-1}}{n_i}.\end{aligned}$$

(b) We have $\dbinom{n}{n_1, n_2, \ldots, n_k} \in \mathbb{N}$.

Exercise 2.12.1. Prove Proposition 2.12.4.

2.12.2. Counting maps that take values a given number of times

Next, we shall give two combinatorial interpretations of multinomial coefficients:

Proposition 2.12.5. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$. Then, the # of maps $f : [n] \to [k]$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } f(a) = i) = n_i \qquad \text{for each } i \in [k]$$

is $\dbinom{n}{n_1, n_2, \ldots, n_k}$.

Example 2.12.6. We have $7 \in \mathbb{N}$ and $2, 3, 2 \in \mathbb{N}$ and $2 + 3 + 2 = 7$. Hence, Proposition 2.12.5 (applied to $n = 7$ and $k = 3$ and $(n_1, n_2, n_3) = (2, 3, 2)$) says that the # of maps $f : [7] \to [3]$ satisfying

$$\begin{aligned}&(\#\text{ of } a \in [n] \text{ such that } f(a) = 1) = 2 \qquad \text{and} \\ &(\#\text{ of } a \in [n] \text{ such that } f(a) = 2) = 3 \qquad \text{and} \\ &(\#\text{ of } a \in [n] \text{ such that } f(a) = 3) = 2\end{aligned}$$

is $\dbinom{7}{2, 3, 2} = 210$. In other words, it says that the # of maps $f : [7] \to [3]$ that take the value 1 exactly twice, take the value 2 exactly thrice, and take the value 3 exactly twice is 210. One such map is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 2 & 2 & 1 & 2 & 3 \end{pmatrix}$ (in two-line notation).

Class of 2019-11-06

Let us first give an informal way of proving Proposition 2.12.5:

Proof of Proposition 2.12.5 (informal version, sketched). A *relevant map* shall mean a map $f : [n] \to [k]$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } f(a) = i) = n_i \qquad \text{for each } i \in [k]. \tag{249}$$

Thus, we need to prove that the # of all relevant maps is $\dbinom{n}{n_1, n_2, \ldots, n_k}$.

A map $f : [n] \to [k]$ (not necessarily relevant) is uniquely determined if you know which elements of $[n]$ it sends to 1, which elements of $[n]$ it sends to 2, which elements of $[n]$ it sends to 3, and so on. In other words, a map $f : [n] \to [k]$ is uniquely determined if you know the k sets

$$\begin{aligned}
&\{a \in [n] \mid f(a) = 1\}, \\
&\{a \in [n] \mid f(a) = 2\}, \\
&\{a \in [n] \mid f(a) = 3\}, \\
&\ldots, \\
&\{a \in [n] \mid f(a) = k\}.
\end{aligned}$$

These k sets should be k disjoint subsets of $[n]$ [224], and their union must be $[n]$ [225]. If we want the map f to be relevant, then these k sets should have sizes $n_1, n_2, n_3, \ldots, n_k$, respectively[226].

Thus, the following algorithm can be used to construct any relevant map $f : [n] \to [k]$:

- First, choose the set $\{a \in [n] \mid f(a) = 1\}$. This must be a subset of $[n]$ having size n_1. In other words, this must be an n_1-element subset of the n-element set $[n]$. Thus, we have $\dbinom{n}{n_1}$ choices for it.
- Then, choose the set $\{a \in [n] \mid f(a) = 2\}$. This must be a subset of $[n]$ having size n_2 and disjoint from the already chosen set $\{a \in [n] \mid f(a) = 1\}$. In other words, this must be an n_2-element subset of the $(n - n_1)$-element set $[n] \setminus \{a \in [n] \mid f(a) = 1\}$. Thus, we have $\dbinom{n - n_1}{n_2}$ choices for it.

[224] Indeed, they must be disjoint, since any element a in the intersection of two of them would have two different values of $f(a)$ at the same time.

[225] since each $a \in [n]$ should have some value $f(a) \in [k]$ assigned to it, and thus lie in one of these k sets

[226] because the equality (249) says that $|\{a \in [n] \mid f(a) = i\}| = n_i$ for each $i \in [k]$

- Then, choose the set $\{a \in [n] \mid f(a) = 3\}$. This must be a subset of $[n]$ having size n_3 and disjoint from the two already chosen sets $\{a \in [n] \mid f(a) = 1\}$ and $\{a \in [n] \mid f(a) = 2\}$. In other words, this must be an n_3-element subset of the $(n - n_1 - n_2)$-element set $[n] \setminus \{a \in [n] \mid f(a) = 1\} \setminus \{a \in [n] \mid f(a) = 2\}$. Thus, we have $\binom{n - n_1 - n_2}{n_3}$ choices.
- And so on, until the last set $\{a \in [n] \mid f(a) = k\}$ has been chosen (for which we have $\binom{n - n_1 - n_2 - \cdots - n_{k-1}}{n_k}$ choices).

The dependent product rule thus shows that the total # of relevant maps is

$$\begin{aligned}
&\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} \\
&= \prod_{i=1}^{k} \binom{n-n_1-n_2-\cdots-n_{i-1}}{n_i} \\
&= \binom{n}{n_1, n_2, \ldots, n_k} \qquad \text{(by Proposition 2.12.4 \textbf{(a)})}.
\end{aligned}$$

Thus, Proposition 2.12.5 is proved. □

Exercise 2.12.2. Give a formal proof of Proposition 2.12.5 (using induction instead of the dependent product rule).

If A is any set and $n \in \mathbb{N}$, then the maps from $[n]$ to A are in bijection with the n-tuples of elements of A (as we have seen, e.g., in the proof of Theorem 1.5.7). Thus, any properties of the former can be restated in terms of the latter (and vice versa). For example, we can restate Proposition 2.12.5 in terms of n-tuples:

Proposition 2.12.7. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$. Then, the # of n-tuples $(u_1, u_2, \ldots, u_n) \in [k]^n$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } u_a = i) = n_i \qquad \text{for each } i \in [k] \tag{250}$$

is $\binom{n}{n_1, n_2, \ldots, n_k}$.

Note that the n-tuples $(u_1, u_2, \ldots, u_n) \in [k]^n$ satisfying (250) in Proposition 2.12.7 are simply the n-tuples of elements of $[k]$ that contain the entry 1 exactly n_1 many times, contain the entry 2 exactly n_2 many times, contain the entry 3 exactly n_3 many times, and so on.

Proof of Proposition 2.12.7 (sketched). We introduce some shorthand terminology: A *relevant n-tuple* shall mean an n-tuple $(u_1, u_2, \ldots, u_n) \in [k]^n$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } u_a = i) = n_i \qquad \text{for each } i \in [k].$$

Thus, we need to prove that the # of all relevant n-tuples is $\binom{n}{n_1, n_2, \ldots, n_k}$.

A *relevant map* shall mean a map $f : [n] \to [k]$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } f(a) = i) = n_i \qquad \text{for each } i \in [k].$$

Thus, Proposition 2.12.5 shows that the # of all relevant maps is $\binom{n}{n_1, n_2, \ldots, n_k}$.

Recall that $[k]^{[n]} = \{\text{maps from } [n] \text{ to } [k]\}$. Consider the map

$$\Phi : \{\text{relevant maps}\} \to \{\text{relevant } n\text{-tuples}\},$$
$$f \mapsto (f(1), f(2), \ldots, f(n)).$$

This map Φ sends each relevant map $f : [n] \to [k]$ to its list of values at the points[227] $1, 2, \ldots, n$. It is clear that this map Φ is a bijection[228]. Thus, the bijection principle yields

$$|\{\text{relevant maps}\}| = |\{\text{relevant } n\text{-tuples}\}|.$$

In other words,

$$(\#\text{ of all relevant maps}) = (\#\text{ of all relevant } n\text{-tuples}). \tag{251}$$

But we know that the # of all relevant maps is $\binom{n}{n_1, n_2, \ldots, n_k}$. Thus, (251) shows that the # of all relevant n-tuples is $\binom{n}{n_1, n_2, \ldots, n_k}$. This proves Proposition 2.12.7. □

2.12.3. Counting anagrams

For a second combinatorial interpretation of multinomial coefficients, we need the notion of an "anagram":

Definition 2.12.8. Let $n \in \mathbb{N}$. Let α be an n-tuple (of any objects). An *anagram* of α shall mean an n-tuple that can be obtained from α by permuting its entries.

In other words (more formally): Write α as $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Then, an anagram of α is an n-tuple of the form $\left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}\right)$, where σ is a permutation of $[n]$.

"Anagrams" are often called "permutations", but the latter terminology risks confusion with the notion of permutations defined in Definition 1.7.1.

[227] I am just using "point" as just a suggestive way of saying "element of $[n]$" here.

[228] Indeed, the definition of a "relevant map" requires the map to take the value i exactly n_i many times (for each $i \in [k]$), whereas the definition of a "relevant n-tuple" requires the n-tuple to contain the entry i exactly n_i many times (for each $i \in [k]$). It is clear that if we encode a map by its list of values, then the former requirement translates into the latter requirement.

Example 2.12.9. (a) The anagrams of the 3-tuple $(1,4,6)$ are $(1,4,6)$, $(1,6,4)$, $(4,1,6)$, $(4,6,1)$, $(6,1,4)$ and $(6,4,1)$.

(b) The anagrams of the 3-tuple $(1,4,1)$ are $(1,4,1)$, $(4,1,1)$ and $(1,1,4)$. (There are 6 ways to permute the 3 entries of $(1,4,1)$, but they only produce 3 different results.)

(c) The only anagram of the 3-tuple $(2,2,2)$ is $(2,2,2)$ itself. (All 6 ways of permuting the 3 entries of $(2,2,2)$ yield the same result.)

We can now interpret multinomial coefficients as counting anagrams:

Proposition 2.12.10. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$.

Let α be the n-tuple

$$\left(\underbrace{1,1,\ldots,1}_{n_1 \text{ times}}, \underbrace{2,2,\ldots,2}_{n_2 \text{ times}}, \ldots, \underbrace{k,k,\ldots,k}_{n_k \text{ times}} \right).$$

Then, the # of distinct anagrams of α (that is, n-tuples obtained from α by permuting its entries) is $\dbinom{n}{n_1, n_2, \ldots, n_k}$.

Example 2.12.11. How many anagrams does the word "anagram" have? (Here, we regard a word as a tuple of letters; it doesn't have to make any sense in English. For example, "nagrama" is an anagram of "anagram". And yes, a word counts as its own anagram.)

Equivalently, how many anagrams does the word "aaagmnr" have? (This is an equivalent question, because the words "anagram" and "aaagmnr" are anagrams of one another, and thus have the same set of anagrams.)

Equivalently, how many anagrams does the 7-tuple $(1,1,1,2,3,4,5)$ have? (This is an equivalent question, because $(1,1,1,2,3,4,5)$ is obtained from "aaagmnr" by replacing each letter by a number[229].)

Proposition 2.12.10 (applied to $n = 7$, $k = 5$ and $(n_1, n_2, \ldots, n_k) = (3,1,1,1,1)$) says that the answer to the last question is

$$\binom{7}{3,1,1,1,1} = \frac{7!}{3! \cdot 1! \cdot 1! \cdot 1! \cdot 1!} = \frac{7!}{3!} = 7 \cdot 6 \cdot 5 \cdot 4 = 840.$$

Thus, the word "anagram" has 840 anagrams.

Let us prove Proposition 2.12.10 informally:

[229] Namely, we replaced the letters "a", "g", "m", "n" and "r" by the numbers 1, 2, 3, 4 and 5, respectively. (It doesn't matter which letter we choose to replace by which number; the replacement merely has to guarantee that equal letters become equal numbers, while distinct letters become distinct numbers.)

Proof of Proposition 2.12.10 (informal version). If we permute the entries of an n-tuple, then the order of its entries will change (usually), but some things won't change: The number of times 1 appears as an entry won't change; the number of times 2 appears as an entry won't change; the number of times 3 appears as an entry won't change; and so on. Thus, if β is any anagram of α, and if $i \in [k]$ is arbitrary, then

$$\begin{aligned}(\#\text{ of times } i \text{ appears in } \beta) &= (\#\text{ of times } i \text{ appears in } \alpha) \\ &= n_i\end{aligned} \tag{252}$$

(since i appears n_i times in the n-tuple α). Hence, if β is an anagram of α, then

$$(\#\text{ of times } i \text{ appears in } \beta) = n_i \qquad \text{for each } i \in [k]\,. \tag{253}$$

Conversely, if $\beta \in [k]^n$ is an n-tuple that satisfies (253), then β is an anagram of α. Indeed, we can sort the entries of β in increasing order, thus obtaining an n-tuple of the form $\left(\underbrace{1,1,\ldots,1}_{\text{some \# of 1's}}, \underbrace{2,2,\ldots,2}_{\text{some \# of 2's}}, \ldots, \underbrace{k,k,\ldots,k}_{\text{some \# of } k\text{'s}}\right)$; but the equalities (253) show that the # of 1's in this n-tuple will be n_1, and the # of 2's will be n_2, and the # of 3's will be n_3, and so on, so that this n-tuple will be precisely $\left(\underbrace{1,1,\ldots,1}_{n_1 \text{ times}}, \underbrace{2,2,\ldots,2}_{n_2 \text{ times}}, \ldots, \underbrace{k,k,\ldots,k}_{n_k \text{ times}}\right) = \alpha$. This shows that α can be obtained by sorting β, and thus β is an anagram of α.

Combining our observations, we conclude that the anagrams of α are precisely the n-tuples $\beta \in [k]^n$ that satisfy (253). Renaming β as $(u_1, u_2, \ldots, u_n)$, we can rewrite this as follows: The anagrams of α are precisely the n-tuples $(u_1, u_2, \ldots, u_n) \in [k]^n$ that satisfy

$$(\#\text{ of times } i \text{ appears in } (u_1, u_2, \ldots, u_n)) = n_i \qquad \text{for each } i \in [k]\,.$$

In other words, the anagrams of α are precisely the n-tuples $(u_1, u_2, \ldots, u_n) \in [k]^n$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } u_a = i) = n_i \qquad \text{for each } i \in [k]\,.$$

But we know (from Proposition 2.12.7) that the # of such n-tuples is $\binom{n}{n_1, n_2, \ldots, n_k}$. Hence, we conclude that the # of distinct anagrams of α is $\binom{n}{n_1, n_2, \ldots, n_k}$. This proves Proposition 2.12.10. $\square$

To formalize the above proof of Proposition 2.12.10, we need to fill two gaps. The first is a rigorous justification of the equality (252) (assuming that β is an anagram of α). This can easily be done on a more general level:

Exercise 2.12.3. Let X be any set. Let $n \in \mathbb{N}$. Let $\alpha \in X^n$ be an n-tuple. Let β be an anagram of α. Let $i \in X$. Prove that

$$(\#\text{ of times } i \text{ appears in } \beta) = (\#\text{ of times } i \text{ appears in } \alpha)\,.$$

Applying Exercise 2.12.3 to $X = [k]$, we immediately obtain (252).

But there is a second gap in the above informal proof of Proposition 2.12.10 (at least from a formal point of view); indeed, we used the notion of "sorting" an n-tuple (when we said that "we can sort the entries of β in increasing order"). Behind this notion stands the fundamental but nontrivial fact that any n-tuple of integers (or, more generally, of real numbers) can be sorted into weakly increasing order by permuting its entries. This fact is not hard to prove (see, e.g., [Grinbe15, Proposition 6.40 **(a)**] and its proof in [Grinbe15, solution to Exercise 6.13]).

There is also a second way of closing this second gap. Indeed, we can avoid the notion of "sorting" altogether, and instead show the following fact (a converse to Exercise 2.12.3):

Exercise 2.12.4. Let X be any set. Let $n \in \mathbb{N}$. Let $\alpha \in X^n$ and $\beta \in X^n$ be two n-tuples. Assume that

$$(\#\text{ of times } i \text{ appears in } \beta) = (\#\text{ of times } i \text{ appears in } \alpha) \tag{254}$$

for each $i \in X$. Prove that β is an anagram of α.

Example 2.12.12. Let $X = \mathbb{Z}$ and $n = 5$ and $\alpha = (1, 4, 1, 2, 0)$ and $\beta = (2, 0, 1, 1, 4)$. Then, each integer appears as often in the 5-tuple α as it appears in the 5-tuple β. In other words, (254) holds for each $i \in X$. Hence, Exercise 2.12.4 shows that β is an anagram of α. And indeed, if we write α as $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$, then we can easily find a permutation σ of $[5]$ such that $\beta = \left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \alpha_{\sigma(3)}, \alpha_{\sigma(4)}, \alpha_{\sigma(5)}\right)$. (For example, the permutation given in two-line notation as $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$ will do.)

Once Exercise 2.12.4 is solved, we no longer have need for sorting. Instead, we can apply Exercise 2.12.4 to $X = [k]$, and thus conclude that if $\beta \in [k]^n$ is an n-tuple that satisfies (253), then β is an anagram of α. So the second gap in the above proof of Proposition 2.12.10 is filled again.

Note that Exercise 2.12.4 is a weaker version of [19s, Lemma 2.13.20].

Proposition 2.12.10 is somewhat restrictive in that it requires the entries of α to appear in weakly increasing order (which is why, in Exercise 2.12.11, we had to replace "anagram" by "aaagmnr" before we could apply the proposition). This requirement is insubstantial and can easily be lifted:

Proposition 2.12.13. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$.

Let $\alpha \in [k]^n$ be an n-tuple that satisfies

$$(\#\text{ of times } i \text{ appears in } \alpha) = n_i \qquad \text{for each } i \in [k]\,. \tag{255}$$

Then, the # of distinct anagrams of α (that is, n-tuples obtained from α by permuting its entries) is $\dbinom{n}{n_1, n_2, \ldots, n_k}$.

Exercise 2.12.5. Prove Proposition 2.12.13.

2.12.4. More formulas

We shall now state a few more basic properties of multinomial coefficients.

First, we observe that the multinomial coefficients generalize the binomial coefficients that you see in Pascal's triangle:

Proposition 2.12.14. Let $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$. Then,

$$\underbrace{\binom{n}{k}}_{\text{binomial coefficient}} = \underbrace{\binom{n}{k, n-k}}_{\text{multinomial coefficient}}\,.$$

Proof of Proposition 2.12.14. From $k \in \{0, 1, \ldots, n\}$, we obtain $k \leq n$ and thus $n - k \in \mathbb{N}$. Also, $k \in \{0, 1, \ldots, n\} \subseteq \mathbb{N}$. So we have $k, n-k \in \mathbb{N}$ and $k + (n-k) = n$. Thus, the multinomial coefficient $\dbinom{n}{k, n-k}$ is well-defined. Moreover, its definition yields

$$\binom{n}{k, n-k} = \frac{n!}{k!\,(n-k)!} = \frac{n!}{k! \cdot (n-k)!}.$$

Comparing this with

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \qquad \text{(by Theorem 1.3.9)}\,,$$

we obtain $\dbinom{n}{k} = \dbinom{n}{k, n-k}$. This proves Proposition 2.12.14. □

Let us prove some further properties of multinomial coefficients.

Proposition 2.12.15. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$. Let σ be a permutation of $[k]$. Then,

$$\binom{n}{n_1, n_2, \ldots, n_k} = \binom{n}{n_{\sigma(1)}, n_{\sigma(2)}, \ldots, n_{\sigma(k)}}.$$

Proof of Proposition 2.12.15. The map σ is a permutation of $[k]$, that is, a bijection from $[k]$ to $[k]$. Hence, the product $n_{\sigma(1)}!n_{\sigma(2)}!\cdots n_{\sigma(k)}!$ has the same factors as the product $n_1!n_2!\cdots n_k!$ (just in a different order). Thus, $n_{\sigma(1)}!n_{\sigma(2)}!\cdots n_{\sigma(k)}! = n_1!n_2!\cdots n_k!$. For similar reasons, we have $n_{\sigma(1)} + n_{\sigma(2)} + \cdots + n_{\sigma(k)} = n_1 + n_2 + \cdots + n_k$. Thus, $n_{\sigma(1)} + n_{\sigma(2)} + \cdots + n_{\sigma(k)} = n_1 + n_2 + \cdots + n_k = n$, so that the multinomial coefficient $\binom{n}{n_{\sigma(1)}, n_{\sigma(2)}, \ldots, n_{\sigma(k)}}$ is well-defined.

But the definition of the multinomial coefficient $\binom{n}{n_{\sigma(1)}, n_{\sigma(2)}, \ldots, n_{\sigma(k)}}$ yields

$$\begin{aligned}\binom{n}{n_{\sigma(1)}, n_{\sigma(2)}, \ldots, n_{\sigma(k)}} &= \frac{n!}{n_{\sigma(1)}!n_{\sigma(2)}!\cdots n_{\sigma(k)}!} = \frac{n!}{n_1!n_2!\cdots n_k!} \\ &\qquad \left(\text{since } n_{\sigma(1)}!n_{\sigma(2)}!\cdots n_{\sigma(k)}! = n_1!n_2!\cdots n_k!\right) \\ &= \binom{n}{n_1, n_2, \ldots, n_k}\end{aligned}$$

(since the multinomial coefficient $\binom{n}{n_1, n_2, \ldots, n_k}$ is defined to be $\frac{n!}{n_1!n_2!\cdots n_k!}$).

This proves Proposition 2.12.15. □

Theorem 2.12.16 (Recurrence of the multinomial coefficients)**.** Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n > 0$. Then,

$$\binom{n}{n_1, n_2, \ldots, n_k} = \sum_{i=1}^{k} \underbrace{\binom{n-1}{n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k}}_{\text{This should be interpreted as 0 if } n_i = 0}.$$

Exercise 2.12.6. Prove Theorem 2.12.16.

Just as we tabulated the binomial coefficients in Pascal's triangle, we can tabulate the multinomial coefficients $\binom{n}{n_1, n_2, \ldots, n_k}$ for a given value of k in a k-dimensional pyramid-like table, called "Pascal's pyramid" (see [Uecker17, p. 20, Figure 10] for a picture). Theorem 2.12.16 shows that each entry in this table (except for the $\binom{0}{0, 0, \ldots, 0} = 1$ at its apex) is the sum of its k upper neighbors (generalizing the analogous property of Pascal's triangle).

The following theorem generalizes the binomial formula (because of Proposition 2.12.14):

Theorem 2.12.17 (the multinomial formula)**.** Let $x_1, x_2, \ldots, x_k$ be k numbers. Let $n \in \mathbb{N}$. Then,

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{(n_1,n_2,\ldots,n_k)\in\mathbb{N}^k; \\ n_1+n_2+\cdots+n_k=n}} \binom{n}{n_1, n_2, \ldots, n_k} x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}.$$

Proof. LTTR. There are many ways to prove this: Either do it combinatorially using Proposition 2.12.5 (see [Galvin17, Theorem 11.7] for this proof); or use induction on n; or use induction on k (see [Grinbe15, Exercise 6.2] for this proof[230]). □

3. The twelvefold way

Let us look back at the counting problems we have so far been solving. We have counted subsets, tuples, maps, integers, tilings and more complicated combinations of these (such as tuples of subsets). While these problems were often interconnected (in particular, many of them were solved using the same methods, and bijections let us translate between differently looking objects), the problems themselves followed no system other than "what else can we count using the methods seen so far?". Historically, this has led to combinatorics being regarded more as a hodgepodge of problems and tricks rather than as a systematic theory.

To some extent, this is still the case, and it is not just an artifact of viewpoint; combinatorics really is a broad field with much less of a clear direction than many other mathematical subjects.[231] Nevertheless, there is more structure in combinatorics than meets the eye, and there have been several successful attempts to classify and organize the most common enumerative problems in a coherent theory. One of the most successful attempts of this kind is the *twelvefold way*, introduced in the 1960s by Gian-Carlo Rota under the name of "theory of distribution and occupancy" (or, less grandiloquently, "placing balls in boxes") and since popularized as the "twelvefold way".

3.1. What is the twelvefold way?

The *twelvefold way* is a collection of 12 standard counting problems (usually arranged as a table with 4 rows and 3 columns) that frequently appear in combina-

[230] Keep in mind that what we call $\binom{n}{n_1, n_2, \ldots, n_k}$ is denoted by $\mathbf{m}(n_1, n_2, \ldots, n_k)$ in [Grinbe15, Exercise 6.2].

[231] This is not entirely a bad thing: It means that an average result in combinatorics relies less on prior knowledge and mastery of complex theory than in most other pure-mathematical disciplines. Already early on in your journey, you have more directions to "branch out" into, and more results you can achieve without years of training but merely with a good dose of creativity and perseverance. But on the flip side, it means that said results will be less likely to be foundational to others' work after you. (And this does not spell significance for texts like this...)

torics (in the sense that many other counting problems can be reduced to them). Let us first introduce it informally, and then define it formally and study it in detail.

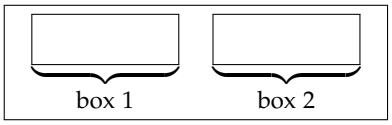
Convention 3.1.1. For the rest of Chapter 3, we fix two finite sets A and X. We shall refer to the elements of A as *balls*, and we shall refer to the elements of X as *boxes*. (The letters A and X have been chosen because "a" appears in "ball" while "x" appears in "box". I cannot use "B" for both sets...)

A *placement* shall mean a way to distribute all the balls $a \in A$ into the boxes $x \in X$. Rigorously, we can think of a placement as a map from A to X. More precisely, this is what we will call an "$L \to L$ *placement*"; other kinds of placements will be defined below.

How many $L \to L$ placements are there? Of course, there are $|X|^{|A|}$ many (by Theorem 2.4.1). But let us look at them more closely.

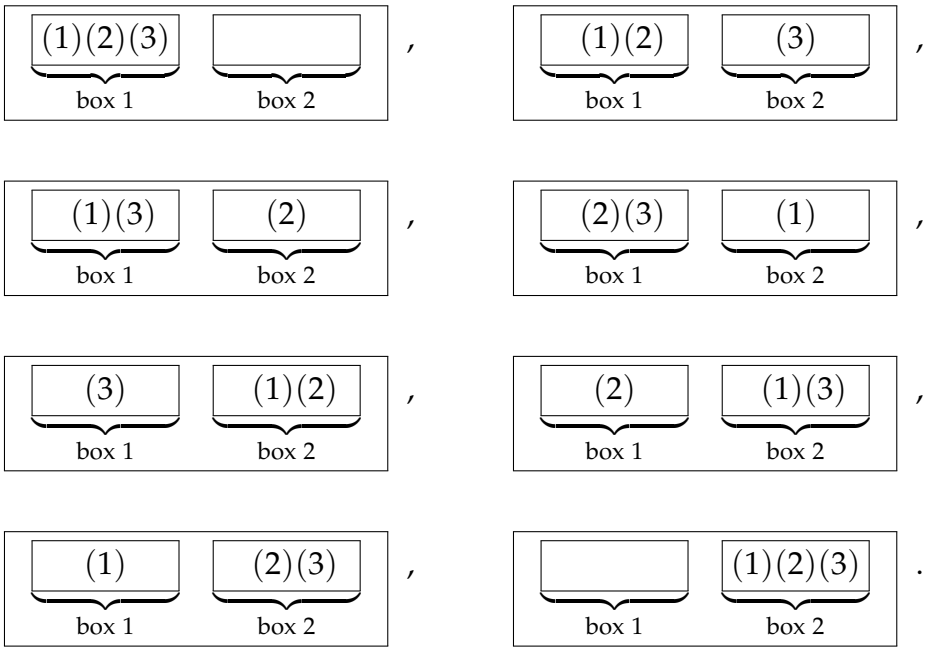
Example 3.1.2. Let $X = [2]$ and $A = [3]$, so that $|X| = 2$ and $|A| = 3$. Thus, we are trying to place 3 balls (called $1, 2, 3$) into 2 boxes (called $1, 2$).

We will draw such placements as follows: We will always draw the boxes in increasing order:

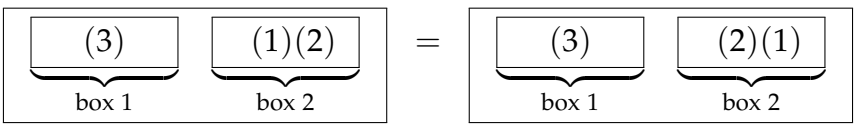


We draw each ball as a pair of parentheses with a number inside – so, for example, the ball 3 will be drawn as "(3)".

So the $L \to L$ placements of the balls $1, 2, 3 \in A$ in the boxes $1, 2 \in X$ are



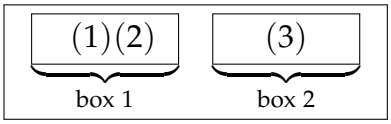
The order of balls **within** a single box does not matter:



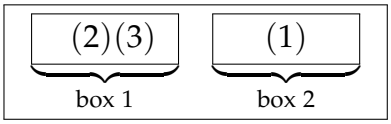
As we said, counting these $L \to L$ placements was easy. But we can consider the following variations of the problem:

- What if we require our maps $f : A \to X$ to be injective (i.e., each box contains ≤ 1 ball) or surjective (i.e., each box contains ≥ 1 ball)?
- What if the balls are unlabelled (i.e., indistinguishable)?

  For example, the two $L \to L$ placements

  and

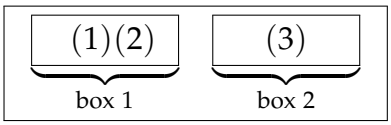
  were counted as different, because the former has ball 1 in box 1 whereas the latter has ball 1 in box 2. But if the balls are indistinguishable, then this difference disappears, and these placements become identical, thus reducing the count.

  Intuitively, it may be clear what "indistinguishable" means, but it is a bit tricky to make this mathematically rigorous. After all, if we define placements as maps, then we cannot just pretend that two different maps are equal because we "chose to think of the balls as indistinguishable". (There is no notion of a "set with indistinguishable elements" in mathematics.[232])

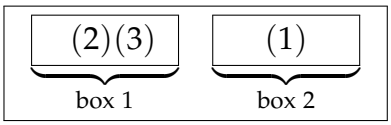
  We will make this rigorous using the notion of *equivalence classes* (which we will introduce in Section 3.3). These are sets of mutually equivalent objects (in our case, maps $f : A \to X$), where the word "equivalent" is understood with respect to a specific relation. Equivalent objects will contribute to the same equivalence class; thus, if we want to "count objects up to equivalence", all we will have to do is counting their equivalence classes. This is a valid and (once you have gotten used to it) fairly convenient rigorous alternative to "pretending" that equivalent objects are "the same".

  Here is how this general idea will be applied to our question about indistinguishable balls: We will say that two maps $f, g : A \to X$ are "*ball-equivalent*" if there is a permutation τ of the balls (i.e., formally: a permutation τ of the set A) that transforms one into the other (i.e., that satisfies $f = g \circ \tau$). Then, "*$U \to L$ placements*" (i.e., placements of unlabelled balls in labelled boxes) will be defined as the equivalence classes of ball-equivalence.

  For example, the two $L \to L$ placements

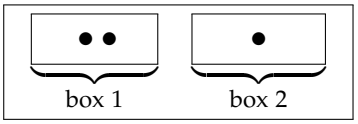
  and

[232] Actually, there is: the notion of a multiset, as defined in Section 2.11. However, it would only help us if we defined maps between multisets (as well as maps between multisets and sets), which we are not going to do (as it comes with its own difficulties).

are ball-equivalent, and therefore contribute to only 1 ball-equivalence class – i.e., they count as one and the same $U \to L$ placement.

We shall draw $U \to L$ placements in the same way as we draw $L \to L$ placements, but representing balls by "•" symbols (rather than by numbers in parentheses). Thus, the $U \to L$ placement that we have just discussed becomes

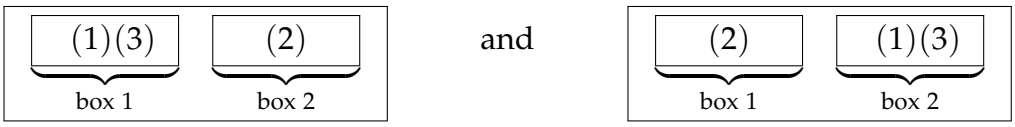


.

This shall visualize the fact that balls are indistinguishable.

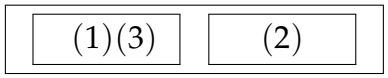
- What if the boxes are unlabelled (i.e., indistinguishable)?

  This can be made rigorous in a similar way, but using permutations of boxes instead of permutations of balls. This gives "*$L \to U$ placements*" (i.e., placements of labelled balls into unlabelled boxes). For example, the two $L \to L$ placements



  are "*box-equivalent*" (i.e., can be transformed into one another by permuting the boxes) and thus contribute to only 1 box-equivalence class – i.e., they count as one and the same $L \to U$ placement.

  We shall draw $L \to U$ placements in the same way as we draw $L \to L$ placements, but without marking the boxes as "box 1", "box 2" etc.. Thus, the $L \to U$ placement that we have just discussed becomes



.

- What if both the boxes and the balls are indistinguishable? This kind of placements will be called "*$U \to U$ placements*". We shall draw them in the same way as we draw $L \to L$ placements, but representing balls by "•" symbols and without marking the boxes.

We can combine these variations, by

- requiring f either to be arbitrary (i.e., not requiring anything about f), or to be injective, or to be surjective;
- counting $L \to L$ placements or $U \to L$ placements or $L \to U$ placements or $L \to L$ placements.

In total, we thus get $3 \cdot 4 = 12$ many different counting problems. We list them in a table:

	arbitrary	injective	surjective
$L \to L$	$\lvert X\rvert^{\lvert A\rvert}$		
$U \to L$			
$L \to U$			
$U \to U$			

Here:

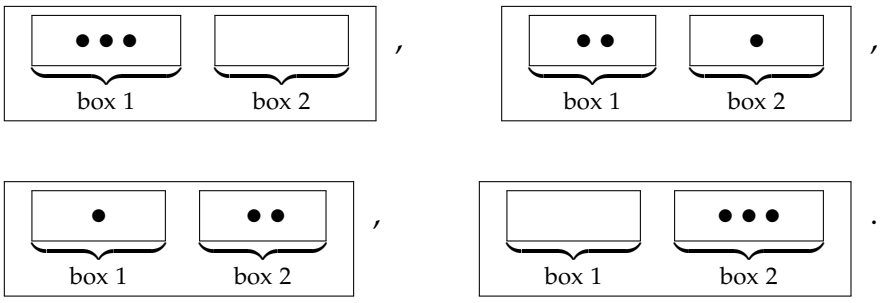
- The columns specify whether we are requiring f to be arbitrary or injective or surjective.
- The rows specify what kind of placements we are counting:
  - "$L \to L$" means "balls are labelled, boxes are labelled", so we are just counting maps $f : A \to X$.
  - "$U \to L$" means "balls are unlabelled, boxes are labelled".
  - "$L \to U$" means "balls are labelled, boxes are unlabelled".
  - "$U \to U$" means "balls are unlabelled, boxes are unlabelled".

Example 3.1.3. Let $X = [2]$ and $A = [3]$. Then, let us count how many placements of each kind we have:

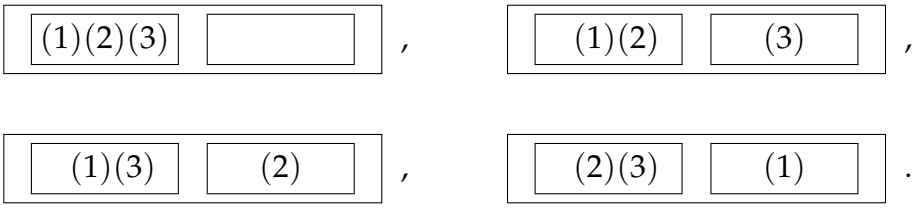
	arbitrary	injective	surjective
$L \to L$	8	0	6
$U \to L$	4	0	2
$L \to U$	4	0	3
$U \to U$	2	0	1

In fact:

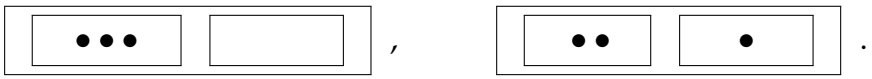
- The $U \to L$ placements are



- The $L \to U$ placements are



- The $U \to U$ placements are



In general, not every of the 12 questions in the table above has a closed-form answer. But each has, at least, a good recursive answer, and there is much to be learned from attempting to answer all the questions. We shall thus strive to fill in the whole "twelvefold way" table, row by row.

3.2. $L \to L$

We begin with the first row of the twelvefold way: the counting of $L \to L$ placements. Let us repeat how we defined them above:

Definition 3.2.1. An $L \to L$ *placement* from A to X is just a map from A to X. The value of this map at some $a \in A$ is called the *box in which ball a is placed*.

We can now count the $L \to L$ placements:

Proposition 3.2.2. We have

$$\begin{aligned}&(\#\text{ of } L \to L \text{ placements } A \to X)\\ &= (\#\text{ of maps from } A \text{ to } X) = |X|^{|A|}.\end{aligned}$$

Proof. The first equality sign follows from Definition 3.2.1. The second equality sign follows from Theorem 2.4.1 (applied to $m = |A|$, $n = |X|$ and $B = X$). □

Proposition 3.2.3. We have

$$\begin{aligned}&(\#\text{ of injective } L \to L \text{ placements } A \to X)\\ &= (\#\text{ of injective maps from } A \text{ to } X) = |X|^{\underline{|A|}}.\end{aligned}$$

Proof. The first equality sign follows from Definition 3.2.1. The second equality sign follows from Theorem 2.4.4 (applied to $m = |A|$, $n = |X|$ and $B = X$). □

Proposition 3.2.4. We have

$$\begin{aligned}&(\#\text{ of surjective } L \to L \text{ placements } A \to X)\\ &= (\#\text{ of surjective maps from } A \text{ to } X) = \operatorname{sur}\left(|A|, |X|\right).\end{aligned}$$

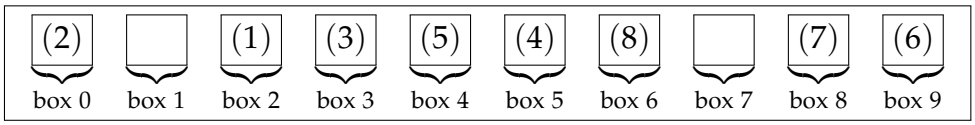
Proof. The first equality sign follows from Definition 3.2.1. The second equality sign follows from Theorem 2.4.11 (applied to $m = |A|$, $n = |X|$ and $B = X$). □

Example 3.2.5. Here are some typical counting problems that boil down to counting $L \to L$ placements:

- How many ways are there to assign grades (from a finite set X) to students (from a finite set A) ? These assignments are arbitrary $L \to L$ placements.
- How many ways are there to assign IP addresses to a given set of computers? These assignments are injective $L \to L$ placements, since IP addresses should be distinct and come from a well-specified set (say, {32-bit numbers} for IPv4 addresses).
- How many 8-digit telephone numbers are there with no 2 equal digits?

  Of course, these telephone numbers are precisely the injective 8-tuples $(i_1, i_2, \ldots, i_8) \in \{0, 1, \ldots, 9\}^8_{\text{inj}}$ (see Definition 2.7.1 for the meaning of these words), and thus Proposition 2.7.2 shows that there are $10^{\underline{8}}$ many of them.

  Alternatively, let us restate this counting problem in terms of $L \to L$ placements: The 8-digit telephone numbers with no 2 equal digits correspond to injective $L \to L$ placements with $A = [8]$ and $X = \{0, 1, \ldots, 9\}$; for example, the telephone number 20354986 corresponds to the $L \to L$ placement



  .

  Thus, the total # of such telephone numbers is $10^{\underline{8}} = 10 \cdot 9 \cdot \cdots \cdot 3 = 10!/2!$.

3.3. Equivalence relations

Now, we take a break from counting questions to build some theory that will help us rigorously formulate the other three rows of the twelvefold way (i.e., the notions of $U \to L$ placements, $L \to U$ placements, and $U \to U$ placements). These notions

depend on having "unlabelled balls" and/or "unlabelled boxes". What does it mean for balls, or boxes, to be unlabelled?

Rigorously, it means that we are counting **not** the maps $f : A \to X$ themselves, but rather their **equivalence classes** with respect to some relation.

We are going to explain what these are. First, let us introduce (or recall, depending on your background) the notions of *relations* and, in particular, *equivalence relations*.

Class of 2019-11-08

3.3.1. Relations

I will follow [19s, Chapter 3] in this subsection.

We will first define the notion of a *binary relation*. Roughly speaking, if S is a set, then a binary relation on S is a rule that associates some elements of S with some elements of S. For instance, equality is a binary relation on an arbitrary set S (associating each element of S with itself); divisibility is a binary relation on the set $\mathbb{Z}$ (associating each integer x with each integer y such that x is divisible by y); orthogonality is a binary relation on the set of all (straight) lines in the plane (associating each line with each line that is orthogonal to it). See Example 3.3.3 for some more examples.

In order to rigorously define the general notion of a binary relation, we encode it as a set of pairs of elements of S: namely, as the set of all pairs (x, y) such that our relation associates x with y. Since a set of pairs of elements of S is the same as a subset of $S \times S$, we thus arrive at the following definition:

Definition 3.3.1. Let S be a set. A *binary relation* on S is formally defined as a subset of $S \times S$. If R is a binary relation on S, and if (x, y) is a pair of two elements of S, then the statement "$(x, y) \in R$" will be written as "$x \ R \ y$". (This notation is called "writing R *infix*".)

Informally, a binary relation on S is understood to mean a statement "$x \ R \ y$" defined for every pair of elements $(x, y) \in S \times S$. For each pair $(x, y) \in S \times S$, this statement $x \ R \ y$ is either true or false.

The informal and the formal definitions of a binary relation are equivalent, because:

- Given a statement "$x \ R \ y$" defined for every pair $(x, y) \in S \times S$, we can encode it as a subset of $S \times S$, namely as the subset
$$\{(x, y) \in S \times S \mid x \ R \ y\}.$$
- Conversely, every subset T of $S \times S$ can be decoded into a statement defined for every pair $(x, y) \in S \times S$ (namely, the statement "$(x, y) \in T$").

Convention 3.3.2. In the following, we will abbreviate the words "*binary relation*" simply as "*relation*".

Relations can be found in droves all over mathematics; here are some basic examples:

Example 3.3.3. Let $S = \mathbb{Z}$.

(a) The relation $=$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\begin{aligned}\{(a,b) \in S \times S \mid a = b\} &= \{(c,c) \mid c \in S\} \\ &= \{\ldots, (-2,-2), (-1,-1), (0,0), (1,1), (2,2), \ldots\}.\end{aligned}$$

(b) The relation $<$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\{(a,b) \in S \times S \mid a < b\}.$$

For example, the pair $(2,3)$ belongs to this subset $<$ of $S \times S$, whereas the pairs $(2,2)$ and $(3,2)$ do not.

(c) The relation $\leq$ is a binary relation on S. For instance, it contains the pairs $(2,2)$ and $(2,3)$ but not $(3,2)$.

(d) The relation $\neq$ is a binary relation on S. As a subset of $S \times S$, this relation is $(S \times S) \setminus (=)$, where $(=)$ is the relation $=$ from Example 3.3.3 **(a)**.

(e) Fix $n \in \mathbb{Z}$. Define a binary relation $\underset{n}{\equiv}$ on $S = \mathbb{Z}$ by

$$\begin{aligned}\left(a \underset{n}{\equiv} b\right) &\iff (a \equiv b \bmod n) \iff (n \mid a-b) \\ &\iff (a = b + kn \text{ for some } k \in \mathbb{Z}).\end{aligned}$$

This relation $\underset{n}{\equiv}$ is called *congruence modulo n*. Note that the relation $\underset{0}{\equiv}$ is $=$.

When n is positive, we have $a \equiv b \bmod n$ if and only if $a\%n = b\%n$, where we are using the notation $c\%n$ for the remainder of an integer c upon division by n.

For $n = 1$, we have the chain of equivalences

$$\left(a \underset{1}{\equiv} b\right) \iff (1 \mid a-b) \iff \left(\frac{a-b}{1} \in \mathbb{Z}\right) \iff (a-b \in \mathbb{Z}) \iff (\text{true})$$

for any two integers a and b. Thus, the relation $\underset{1}{\equiv}$ contains every pair of two integers (i.e., we have $a \underset{1}{\equiv} b$ for all $(a,b) \in S \times S$). Hence, it equals the whole set $S \times S$ (when considered as a subset of $S \times S$).

The relation $\underset{2}{\equiv}$ associates every even integer with every even integer, and associates every odd integer with every odd integer. Besides these, it associates no integers. Thus, it associates two integers if and only if these two integers have the same parity.

(f) Define a binary relation N on S by

$$(a \ N \ b) \iff (\text{false}) .$$

That is, there is no pair $(a,b) \in S \times S$ such that $a \ N \ b$. As a subset of $S \times S$, this relation N is $\varnothing$.

(g) Define a binary relation A on S by

$$(a \ A \ b) \iff (\text{true}) .$$

That is, every pair $(a,b) \in S \times S$ satisfies $a \ A \ b$. As a subset of $S \times S$, this relation is $S \times S$ itself.

This relation A is identical with the relation $\underset{1}{\equiv}$ from Example 3.3.3 **(e)**; however, the way we have just defined it, we can just as well define an analogous relation A for every set S (not just for $S = \mathbb{Z}$), whereas the definition of $\underset{1}{\equiv}$ requires S to be $\mathbb{Z}$.

(h) The relation $\mid$ (also known as "divides") is a binary relation on S. For instance, the pair $(3, 12)$ belongs to this relation $\mid$, because $3 \mid 12$.

(i) The relation "is coprime to" is a binary relation on S. For example, it contains the pair $(3, 4)$, but not the pair $(2, 4)$.

There are other examples of relations on $\mathbb{Z}$, as well as relations on other sets. For example, if S is the set of all straight lines on the plane (in plane geometry), then "parallel" is a relation on S; so is "orthogonal".

3.3.2. Equivalence relations

We shall be particularly interested in a special class of relations: the *equivalence relations*. To define them, we first introduce three properties that some relations have:

Definition 3.3.4. Let R be a binary relation on a set S.

(a) We say that R is *reflexive* if every $a \in S$ satisfies $a \ R \ a$.

(b) We say that R is *symmetric* if every $a, b \in S$ satisfying $a \ R \ b$ satisfy $b \ R \ a$.

(c) We say that R is *transitive* if every $a, b, c \in S$ satisfying $a \ R \ b$ and $b \ R \ c$ satisfy $a \ R \ c$.

Example 3.3.5. Let S be the set $\mathbb{Z}$. Recall the relations on S introduced in Example 3.3.3.

(a) The relation $=$ is reflexive, symmetric and transitive. (For instance, the transitivity of $=$ means that every $a, b, c \in S$ satisfying $a = b$ and $b = c$ satisfy $a = c$. This is a very fundamental property of equality.)

(b) The relation $<$ is not reflexive, not symmetric but transitive.

(c) The relation $\leq$ is reflexive, not symmetric but transitive. (It is reflexive because every $a \in S$ satisfies $a \leq a$.)

(d) The relation $\neq$ is not reflexive, but symmetric. It is not transitive (e.g., we have $2 \neq 3$ and $3 \neq 2$, but $2 = 2$).

(e) For every $n \in \mathbb{Z}$, the congruence relation $\equiv_n$ is reflexive (since $n \mid a - a$), symmetric (since $n \mid a - b$ implies $n \mid b - a$) and transitive (since $n \mid a - b$ and $n \mid b - c$ imply $n \mid a - c$).

(f) The relation N is symmetric (vacuously) and transitive (vacuously), but not reflexive. ("Vacuously" means that the respective statements are vacuously true. For instance, in order to show that the relation N is symmetric, we must show that every $a, b \in S$ satisfying $a \ N \ b$ satisfy $b \ N \ a$. But this is vacuously true, since the antecedent $a \ N \ b$ never holds in the first place.)

(g) The relation A is reflexive, symmetric and transitive.

(h) The divisibility relation $\mid$ is reflexive but not symmetric. It is transitive (if $a \mid b$ and $b \mid c$, then $a \mid c$).

(i) The coprimality relation is symmetric but neither reflexive nor transitive.

We are now ready to define equivalence relations:

Definition 3.3.6. An *equivalence relation* on a set S means a relation on S that is reflexive, symmetric and transitive.

Among the relations discussed in Example 3.3.3, three are equivalence relations:

Example 3.3.7. Let S be any set. The relation $=$ on S is an equivalence relation.

Example 3.3.8. Let $n \in \mathbb{Z}$. Then, the congruence relation $\equiv_n$ on $\mathbb{Z}$ is an equivalence relation.

Example 3.3.9. Let S be any set. Let A be the binary relation on S defined by $(a \ A \ b) \iff (\text{true})$. (That is, we define A as in Example 3.3.3 **(g)**, but without requiring $S = \mathbb{Z}$.) Then, A is an equivalence relation.

Here are some further examples from plane geometry:

Example 3.3.10. The relation "parallel" on the set {lines in the plane} is an equivalence relation. But the relation "orthogonal" on the same set is not (since it is neither reflexive nor transitive).

Example 3.3.11. The relation "similar" on the set {triangles in the plane} is an equivalence relation.

Example 3.3.12. The relation "directly similar" (= similar with the same orientation) on {triangles in the plane} is an equivalence relation.

However, the relation "indirectly similar" (= similar with opposite orientation) on {triangles in the plane} is not an equivalence relation, because it is not reflexive.

The following example is very general:

Example 3.3.13. Let S and T be two sets. Let $f : S \to T$ be a map. Define a relation $\underset{f}{\equiv}$ on S by

$$\left(a \underset{f}{\equiv} b\right) \Longleftrightarrow \left(f\left(a\right) = f\left(b\right)\right).$$

(As a subset of $S \times S$, this relation is the set of all pairs $(a, b) \in S \times S$ that satisfy $f(a) = f(b)$.) This relation $\underset{f}{\equiv}$ is an equivalence relation. (For instance, its transitivity easily follows from the transitivity of equality: If $f(a) = f(b)$ and $f(b) = f(c)$, then $f(a) = f(c)$.)

Here is an informal example:

Example 3.3.14. Let S be $\{$all points on the landmass of the Earth$\}$. Define a relation $\sim$ on S by

$$\left(a \sim b\right) \Longleftrightarrow \left(\text{there is a land route from } a \text{ to } b\right).$$

Then, $\sim$ is an equivalence relation. (Its transitivity follows from the fact that two routes with a common endpoint can be combined to form a composite route.)

The following example is crucial in the construction of the rational number system:

Example 3.3.15. Let

$$S = \mathbb{Z} \times \left(\mathbb{Z} \setminus \{0\}\right) = \left\{\left(a_1, a_2\right) \in \mathbb{Z}^2 \mid a_1 \in \mathbb{Z} \text{ and } a_2 \in \mathbb{Z} \setminus \{0\}\right\}.$$

This is the set of all pairs of integers such that the second entry of the pair is nonzero.

Define a relation $\underset{*}{\sim}$ on S by

$$\left(\left(a_1, a_2\right) \underset{*}{\sim} \left(b_1, b_2\right)\right) \iff \left(a_1 b_2 = a_2 b_1\right).$$

This relation $\underset{*}{\sim}$ is an equivalence relation. (Let us check its transitivity: If α, β, γ are three elements of S satisfying $\alpha \underset{*}{\sim} \beta$ and $\beta \underset{*}{\sim} \gamma$, then we can write α, β, γ in the form $\alpha = (a_1, a_2)$ and $\beta = (b_1, b_2)$ and $\gamma = (c_1, c_2)$. Thus, $\alpha \underset{*}{\sim} \beta$ rewrites as $(a_1, a_2) \underset{*}{\sim} (b_1, b_2)$, which means that $a_1 b_2 = a_2 b_1$. Similarly, from $\beta \underset{*}{\sim} \gamma$, we obtain $b_1 c_2 = c_1 b_2$. Using these two equalities, we obtain

$$\underbrace{a_1 b_2}_{= a_2 b_1} c_2 = a_2 \underbrace{b_1 c_2}_{= c_1 b_2} = a_2 c_1 b_2.$$

We can cancel b_2 from this equality (since $(b_1, b_2) \in S$ entails $b_2 \neq 0$) and thus obtain $a_1 c_2 = a_2 c_1$. This means that $(a_1, a_2) \underset{*}{\sim} (c_1, c_2)$. That is, $\alpha \underset{*}{\sim} \gamma$ (since $\alpha = (a_1, a_2)$ and $\gamma = (c_1, c_2)$). This proves that the relation $\underset{*}{\sim}$ is transitive. The proofs of its reflexivity and its symmetry are easier.)

3.3.3. Equivalence classes

Given an equivalence relation on a set S, we can define certain special subsets of S that are known as its *equivalence classes*:

Definition 3.3.16. Let $\sim$ be an equivalence relation on a set S.
(a) For each $a \in S$, we define a subset $[a]_\sim$ of S by

$$[a]_\sim = \{b \in S \mid b \sim a\}.$$

This subset $[a]_\sim$ is called the *equivalence class of a* (for the relation $\sim$), or the *$\sim$-equivalence class of a*.
(b) The *equivalence classes of $\sim$* are defined to be the sets $[a]_\sim$ for $a \in S$. They are also known as the *$\sim$-equivalence classes*.

Example 3.3.17. Consider the relation $\underset{3}{\equiv}$ on $\mathbb{Z}$ (as defined in Example 3.3.3 **(e)**). We have

$$\begin{aligned}[5]_{\underset{3}{\equiv}} &= \left\{b \in \mathbb{Z} \mid b \underset{3}{\equiv} 5\right\} = \{b \in \mathbb{Z} \mid b \equiv 5 \bmod 3\} \\ &= \{5 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\}\end{aligned}$$

and

$$\begin{aligned}[3]_{\underset{3}{\equiv}} &= \left\{b \in \mathbb{Z} \mid b \underset{3}{\equiv} 3\right\} = \{b \in \mathbb{Z} \mid b \equiv 3 \bmod 3\} \\ &= \{3 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}\end{aligned}$$

and

$$\begin{aligned}[2]_{\underset{3}{\equiv}} &= \left\{b \in \mathbb{Z} \mid b \underset{3}{\equiv} 2\right\} = \{b \in \mathbb{Z} \mid b \equiv 2 \bmod 3\} \\ &= \{2 + 3k \mid k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\}.\end{aligned}$$

Note that $[2]_{\underset{3}{\equiv}} = [5]_{\underset{3}{\equiv}}$. This illustrates the general principle that different elements of S will often have the same $\sim$-equivalence class. (See Proposition 3.3.21 for general criteria for this to happen.)

Example 3.3.18. Let $n \in \mathbb{Z}$. Recall the relation $\underset{n}{\equiv}$ from Example 3.3.3 **(e)**. It is easy to see that its equivalence classes are (the sets of entries of) arithmetic progressions with difference n (and integer entries).

Let us now state some basic general properties of equivalence classes. For their proofs, see [19s, §3.3.2] or any sufficiently thorough introduction to proofs.

Proposition 3.3.19. Let $\sim$ be an equivalence relation on a set S. Let $a \in S$. Then,

$$[a]_{\sim} = \{b \in S \mid a \sim b\}.$$

Proposition 3.3.20. Let $\sim$ be an equivalence relation on a set S. Let $a \in S$. Then, $a \in [a]_{\sim}$.

Proposition 3.3.21. Let $\sim$ be an equivalence relation on a set S. Let $x, y \in S$.
(a) If $x \sim y$, then $[x]_{\sim} = [y]_{\sim}$.
(b) If not $x \sim y$, then $[x]_{\sim}$ and $[y]_{\sim}$ are disjoint.
(c) We have $x \sim y$ if and only if $x \in [y]_{\sim}$.
(d) We have $x \sim y$ if and only if $y \in [x]_{\sim}$.
(e) We have $x \sim y$ if and only if $[x]_{\sim} = [y]_{\sim}$.

As a consequence of Proposition 3.3.21 (specifically, of its parts **(a)** and **(b)**), any two $\sim$-equivalence classes are either identical or disjoint.

Example 3.3.22. Let

$$S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \left\{(a_1, a_2) \in \mathbb{Z}^2 \mid a_1 \in \mathbb{Z} \text{ and } a_2 \in \mathbb{Z} \setminus \{0\}\right\}.$$

Consider the relation $\underset{*}{\sim}$ on the set S defined by

$$\left((a_1, a_2) \underset{*}{\sim} (b_1, b_2)\right) \iff (a_1 b_2 = a_2 b_1).$$

As we know from Example 3.3.15, this relation $\underset{*}{\sim}$ is an equivalence relation. Its equivalence classes are the rational numbers! Indeed, this is how the rational numbers are rigorously defined; the standard notation $\dfrac{a_1}{a_2}$ for a rational number (obtained as a quotient of two integers a_1 and a_2) is merely a shorthand for the equivalence class $[(a_1, a_2)]_{\underset{*}{\sim}}$ of the pair (a_1, a_2). (See, e.g., [Warner71, §17] or [Loehr20, §6.6] or [Newste19, §B.2] or [Yashin15, §6] for the details of this definition.)

So the relation $\underset{*}{\sim}$ in Example 3.3.15 is not a nameless relation among many, but a rather important one: It tells us which pairs of integers give the same rational number (upon dividing the first entry by the second).

Example 3.3.23. Let S be the set $\{\text{all points on the landmass of the Earth}\}$, and consider the relation $\sim$ on S defined by

$$(a \sim b) \iff (\text{there is a land route from } a \text{ to } b)\,.$$

As we have seen above, this relation $\sim$ is an equivalence relation. The $\sim$-equivalence classes are the continents and islands (as long as we consider Europe and Asia to be one single continent).

Example 3.3.24. Let A be a set, and let $k \in \mathbb{N}$. Consider the set A^k, which consists of all k-tuples of elements of A. The relation $\underset{\text{perm}}{\sim}$ on A^k is defined as follows:

$$\left(\mathbf{p} \underset{\text{perm}}{\sim} \mathbf{q}\right) \iff (\mathbf{p} \text{ is an anagram of } \mathbf{q})$$
$$\iff (\mathbf{p} \text{ can be obtained from } \mathbf{q} \text{ by permuting the entries})\,.$$

For example, $(3,8,8,2) \underset{\text{perm}}{\sim} (8,3,2,8)$.

It is easy to see that the relation $\underset{\text{perm}}{\sim}$ is an equivalence relation. (See Exercise 3.3.1 below for the proof.)

The equivalence classes of $\underset{\text{perm}}{\sim}$ are called *unordered k-tuples* of elements of A. They are in bijection with size-k multisubsets of A: Namely, the equivalence class $\left[(a_1, a_2, \ldots, a_k)\right]_{\underset{\text{perm}}{\sim}}$ of a k-tuple $(a_1, a_2, \ldots, a_k) \in A^k$ corresponds to the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$. This fact is intuitively obvious (isn't a multisubset just a bunch of elements without a specific ordering?); a formal proof will be given in the solution to Exercise 3.3.2.

Example 3.3.25. Let $n \in \mathbb{Z}$. The equivalence classes of the relation $\underset{n}{\equiv}$ (which was defined in Example 3.3.3 **(e)**) are called "*integers modulo n*" (or, more precisely, "*residue classes of integers modulo n*"). The set of these equivalence classes is denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ or $\mathbb{Z}/n$ or Z_n or C_n (depending on author and context). In particular, the sets $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/24\mathbb{Z}$ have well-known meanings: they stand for the hours on a clock (a 12-hour clock or a 24-hour clock, respectively). For example, when you say "3 hours after 11 is 2", you are really saying that $11 + 3 \equiv 2 \bmod 12$ or, equivalently, $[11]_{\underset{12}{\equiv}} + [3]_{\underset{12}{\equiv}} = [2]_{\underset{12}{\equiv}}$ for an appropriate definition of addition of equivalence classes.

Exercise 3.3.1. Let A be a set, and let $k \in \mathbb{N}$. Prove that the relation $\underset{\text{perm}}{\sim}$ (defined in Example 3.3.24) is an equivalence relation on the set A^k.

Exercise 3.3.2. Let A be a set, and let $k \in \mathbb{N}$. Show that the unordered k-tuples of elements of A (defined as in Example 3.3.24) are in bijection with the size-k multisubsets of A. More precisely, show that the map

$$\{\text{unordered } k\text{-tuples of elements of } A\} \to \{\text{size-}k \text{ multisubsets of } A\},$$
$$[(a_1, a_2, \ldots, a_k)]_{\sim_{\text{perm}}} \mapsto \{a_1, a_2, \ldots, a_k\}_{\text{multi}}$$

is well-defined and bijective.

Next, we will define box-equivalence and ball-equivalence on placements of balls into boxes. Then, by taking equivalence classes, we will be able to make sense of "unlabelled balls" and "unlabelled boxes".

Class of 2019-11-11

3.3.4. Defining unlabelled boxes and balls

What does it mean for balls, or boxes, to be unlabelled (in the twelvefold way)?

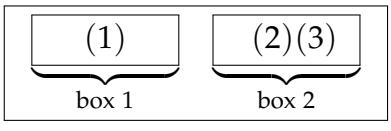
As we already mentioned, it means that we are counting **not** the maps $f : A \to X$, **but rather** their equivalence classes with respect to certain equivalence relations. Let us define these relations:

Definition 3.3.26. Let $f, g : A \to X$ be two maps (i.e., two $L \to L$ placements). Then:

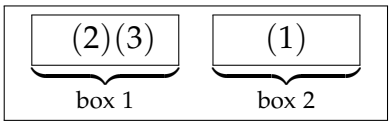
- We say that f is *box-equivalent* to g (this is written $f \overset{\text{box}}{\sim} g$) if and only if there exists a permutation σ of X such that $f = \sigma \circ g$ (in other words, f can be obtained from g by permuting boxes).
- We say that f is *ball-equivalent* to g (this is written $f \overset{\text{ball}}{\sim} g$) if and only if there exists a permutation τ of A such that $f = g \circ \tau$ (in other words, f can be obtained from g by permuting balls).
- We say that f is *box-ball-equivalent* to g (this is written $f \underset{\text{ball}}{\overset{\text{box}}{\sim}} g$) if and only if there exist a permutation σ of X and a permutation τ of A such that $f = \sigma \circ g \circ \tau$.

Thus, we have defined three relations $\overset{\text{box}}{\sim}$, $\overset{\text{ball}}{\sim}$ and $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ on the set of all maps from A to X.

Example 3.3.27. Let $A = [3]$ and $X = [2]$.
(a) The two $L \to L$ placements

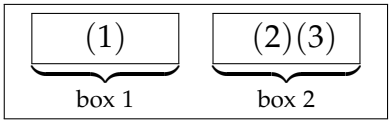


and

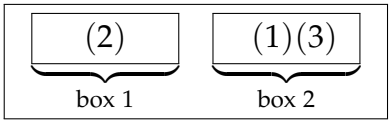


are box-equivalent to one another (since they can be obtained from one another by swapping the two boxes), but they are not ball-equivalent to one another (since a permutation of balls cannot change the fact that the first placement has 1 ball in the first box, whereas the second placement has 2).

(b) The two $L \to L$ placements

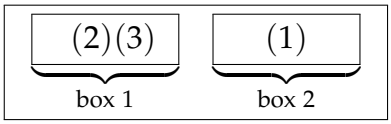


and

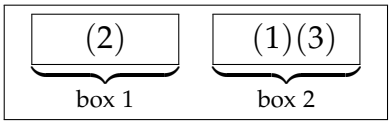


are ball-equivalent to one another (since they can be obtained from one another by swapping the balls 1 and 2), but they are not box-equivalent to one another (since a permutation of boxes cannot change the fact that balls 2 and 3 are together in a single box in the first placement, but not in the second).

(c) The two $L \to L$ placements

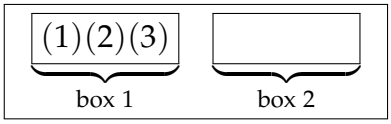


and

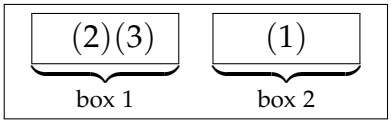


are box-ball-equivalent to one another (since they can be obtained from one another by swapping the two boxes and swapping balls 1 and 2). But they are neither box-equivalent nor ball-equivalent.

(d) The two $L \to L$ placements



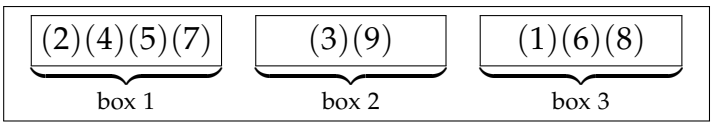
and



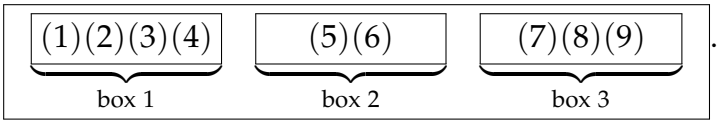
are not box-ball-equivalent to one another (since no permutation of boxes or of balls can change the fact that the first placement has an empty box, but the second does not).

Example 3.3.28. Here is a less trivial example of ball-equivalence: Let $X = [3]$ and $A = [9]$, and consider the two $L \to L$ placements

$f :=$



and $g :=$



.

(Thus, for instance, f is the map from A to X that sends $1,2,3,4,5,6,7,8,9$ to $3,1,2,1,1,3,1,3,2$, respectively.)

These two placements f and g are ball-equivalent. Indeed, f can be obtained from g by permuting the balls so that the balls $1,2,3,4,5,6,7,8,9$ become $2,4,5,7,3,9,1,6,8$. (In more formal terms: We have $f = g \circ \tau$, where τ is the permutation of A that sends $1,2,3,4,5,6,7,8,9$ to $2,4,5,7,3,9,1,6,8$, respectively.) Note that this permutation is far from unique, since the order of the balls inside a box is not fixed.

The ball-equivalence of f and g can also be seen without explicitly constructing the permutation. Indeed, it suffices to notice that each box has equally many balls in f as it has in g (for instance, box 1 has 4 balls in each of f and g); thus, any permutation τ of A that

- sends the balls in box 1 of g to the balls in box 1 of f;
- sends the balls in box 2 of g to the balls in box 2 of f;
- sends the balls in box 3 of g to the balls in box 3 of f

will have the property that $f = g \circ \tau$ and therefore will show that f and g are ball-equivalent. The specific permutation τ that we picked above is merely one of $4! \cdot 2! \cdot 3! = 288$ many possible choices.

Proposition 3.3.29. All three relations $\overset{\text{box}}{\sim}$, $\overset{\text{ball}}{\sim}$ and $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ are equivalence relations on the set $\{\text{maps } A \to X\}$.

This proposition should be fairly intuitive at this point, and its proof is a straightforward exercise in basic mathematical reasoning (specifically, the concepts of bijectivity and relations):

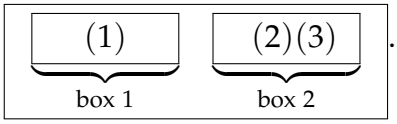
Exercise 3.3.3. Prove Proposition 3.3.29.

We can now rigorously define $U \to L$ placements, $L \to U$ placements and $U \to U$ placements:

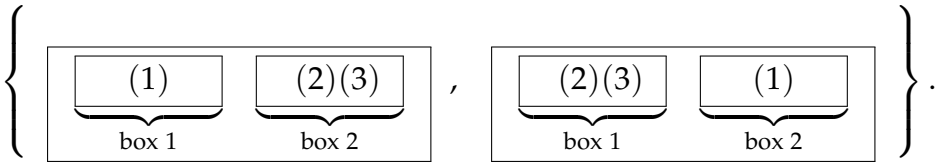
Definition 3.3.30.

- We define the $U \to L$ *placements* to be the $\overset{\text{ball}}{\sim}$-equivalence classes.
- We define the $L \to U$ *placements* to be the $\overset{\text{box}}{\sim}$-equivalence classes.
- We define the $U \to U$ *placements* to be the $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$-equivalence classes.

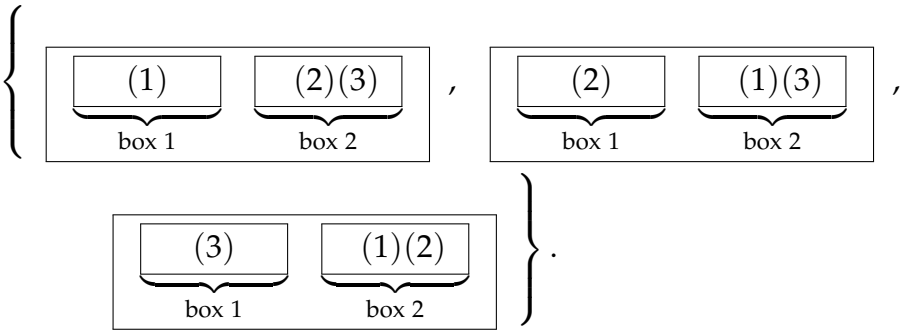
Example 3.3.31. As in Example 3.3.27, let $X = [2]$ and $A = [3]$. Let g be the $L \to L$ placement



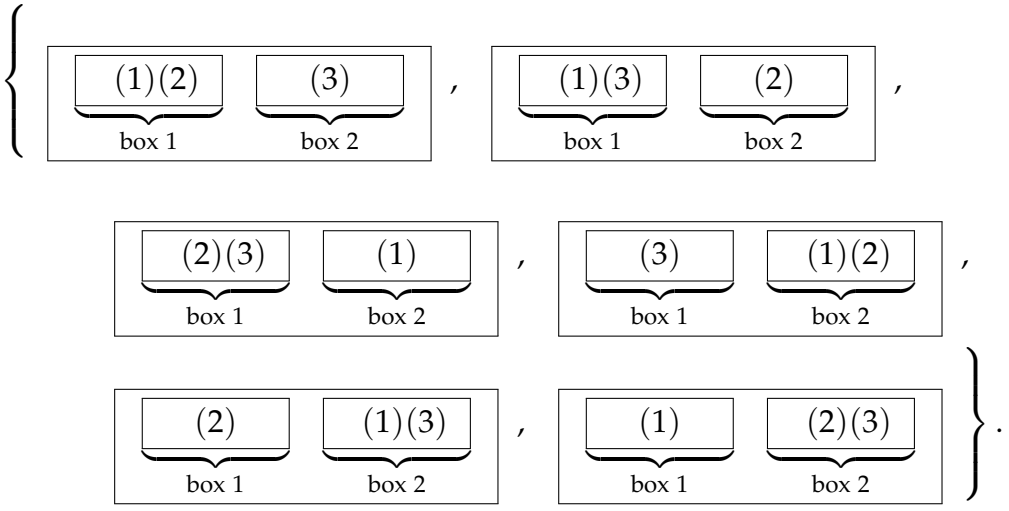
(a) The $\overset{\text{box}}{\sim}$-equivalence class of g is



(b) The $\overset{\text{ball}}{\sim}$-equivalence class of g is



(c) The $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$-equivalence class of g is



Let us briefly explain why Definition 3.3.30 matches our intuitive understanding of $U \to L$ placements, $L \to U$ placements and $U \to U$ placements. Indeed:

- According to Definition 3.3.30, a $U \to L$ placement is a $\overset{\text{ball}}{\sim}$-equivalence class – i.e., a set that consists of all $L \to L$ placements that can be obtained from a given $L \to L$ placement $f : A \to X$ by permuting balls. Thus, roughly speaking, a $U \to L$ placement is an $L \to L$ placement "up to permutation of balls". In other words, it is a placement of unlabelled balls in labelled boxes, in our intuitive sense.
- Similarly, an $L \to U$ placement is a placement of labelled balls in unlabelled boxes.
- Similarly, a $U \to U$ placement is a placement of unlabelled balls in unlabelled boxes.

Thus, we have put our notions of $U \to L$, $L \to U$ and $U \to U$ placements on a rigorous footing. Let us now define what it means for such a placement to be injective or surjective. This definition will rely on the following two facts:

Proposition 3.3.32. Let $f, g : A \to X$ be two maps that satisfy $f \overset{\text{box}}{\sim} g$ or $f \overset{\text{ball}}{\sim} g$ or $f \underset{\text{ball}}{\overset{\text{box}}{\sim}} g$. Then:
(a) If f is injective, then g is injective.
(b) If f is surjective, then g is surjective.

Corollary 3.3.33. Let C be a $U \to L$ placement or an $L \to U$ placement or a $U \to U$ placement. (In other words, let C be a $\overset{\text{ball}}{\sim}$-equivalence class or a $\overset{\text{box}}{\sim}$-equivalence class or a $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$-equivalence class.) Then:
(a) If C contains an injective map, then every map in C is injective.
(b) If C contains a surjective map, then every map in C is surjective.

Exercise 3.3.4. Prove Proposition 3.3.32 and Corollary 3.3.33.

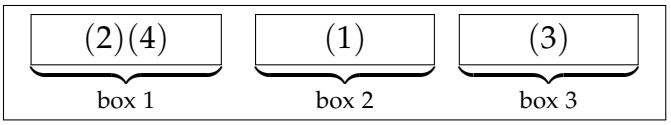
Definition 3.3.34. Let C be a $U \to L$ placement or an $L \to U$ placement or a $U \to U$ placement. (In other words, let C be a $\overset{\text{ball}}{\sim}$-equivalence class or a $\overset{\text{box}}{\sim}$-equivalence class or a $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$-equivalence class.) Then:
(a) We say that C is *injective* if C contains an injective map. (By Corollary 3.3.33 **(a)**, this condition entails that every map in C is injective.)
(b) We say that C is *surjective* if C contains a surjective map. (By Corollary 3.3.33 **(b)**, this condition entails that every map in C is surjective.)

Visually speaking, a placement of (labelled or unlabelled) balls in (labelled or unlabelled) boxes is

- **injective** if and only if each box contains **at most** one ball (i.e., no two balls lie in the same box);

- **surjective** if and only if each box contains **at least** one ball.

Example 3.3.35. (a) Let $A = [4]$ and $X = [3]$. Let f be the $L \to L$ placement

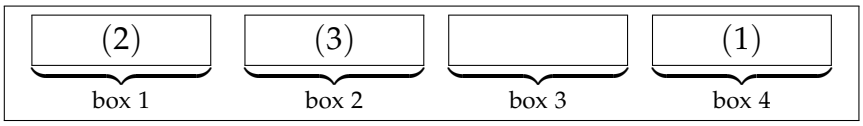


.

This $L \to L$ placement f is surjective (i.e., each box contains at least one ball). Thus, so are the $U \to L$ placement, the $L \to U$ placement and the $U \to U$ placement obtained from it (i.e., the equivalence classes $[f]_{\underset{\sim}{\text{ball}}}$, $[f]_{\underset{\sim}{\text{box}}}$ and $[f]_{\substack{\underset{\sim}{\text{box}} \\ \text{ball}}}$).

However, the $L \to L$ placement f is not injective (since box 1 contains two balls). Thus, neither are the $U \to L$ placement, the $L \to U$ placement and the $U \to U$ placement obtained from it (i.e., the equivalence classes $[f]_{\underset{\sim}{\text{ball}}}$, $[f]_{\underset{\sim}{\text{box}}}$ and $[f]_{\substack{\underset{\sim}{\text{box}} \\ \text{ball}}}$).

(b) Now, let $A = [3]$ and $X = [4]$ instead. Let g be the $L \to L$ placement

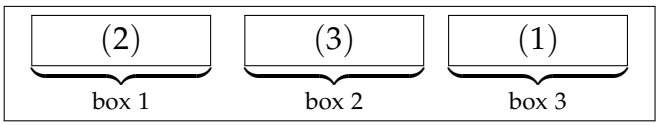


.

This $L \to L$ placement g is injective (i.e., each box contains at most one ball). Thus, so are the $U \to L$ placement, the $L \to U$ placement and the $U \to U$ placement obtained from it (i.e., the equivalence classes $[g]_{\underset{\sim}{\text{ball}}}$, $[g]_{\underset{\sim}{\text{box}}}$ and $[g]_{\substack{\underset{\sim}{\text{box}} \\ \text{ball}}}$).

However, the $L \to L$ placement g is not surjective (since box 3 contains no balls). Thus, neither are the $U \to L$ placement, the $L \to U$ placement and the $U \to U$ placement obtained from it (i.e., the equivalence classes $[g]_{\underset{\sim}{\text{ball}}}$, $[g]_{\underset{\sim}{\text{box}}}$ and $[g]_{\substack{\underset{\sim}{\text{box}} \\ \text{ball}}}$).

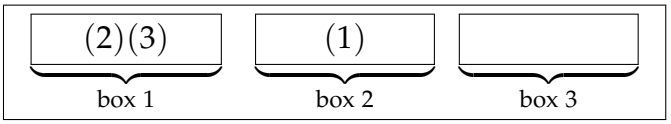
(c) Now, let $A = [3]$ and $X = [3]$. Let h be the $L \to L$ placement



.

This $L \to L$ placement h is both injective and surjective (since each box contains exactly one ball). Thus, so are the $U \to L$ placement, the $L \to U$ placement and the $U \to U$ placement obtained from it (i.e., the equivalence classes $[h]_{\underset{\sim}{\text{ball}}}$, $[h]_{\underset{\sim}{\text{box}}}$ and $[h]_{\substack{\underset{\sim}{\text{box}} \\ \text{ball}}}$).

(d) Finally, let $A = [3]$ and $X = [3]$. Let d be the $L \to L$ placement



.

This $L \to L$ placement d is neither injective nor surjective. Thus, the same holds for the $U \to L$ placement, the $L \to U$ placement and the $U \to U$ placement obtained from it (i.e., the equivalence classes $[d]_{\underset{\sim}{\text{ball}}}$, $[d]_{\underset{\sim}{\text{box}}}$ and $[d]_{\substack{\underset{\sim}{\text{box}} \\ \text{ball}}}$).

Example 3.3.36. In Example 3.3.27 **(d)**, the second $L \to L$ placement is surjective (and so are the $U \to L$ placement, the $L \to U$ placement and the $U \to U$ placement obtained from it), but the first is not.

Finally, some words about counting. Recall the following crucial general fact about equivalence classes (Proposition 3.3.21 **(e)**):

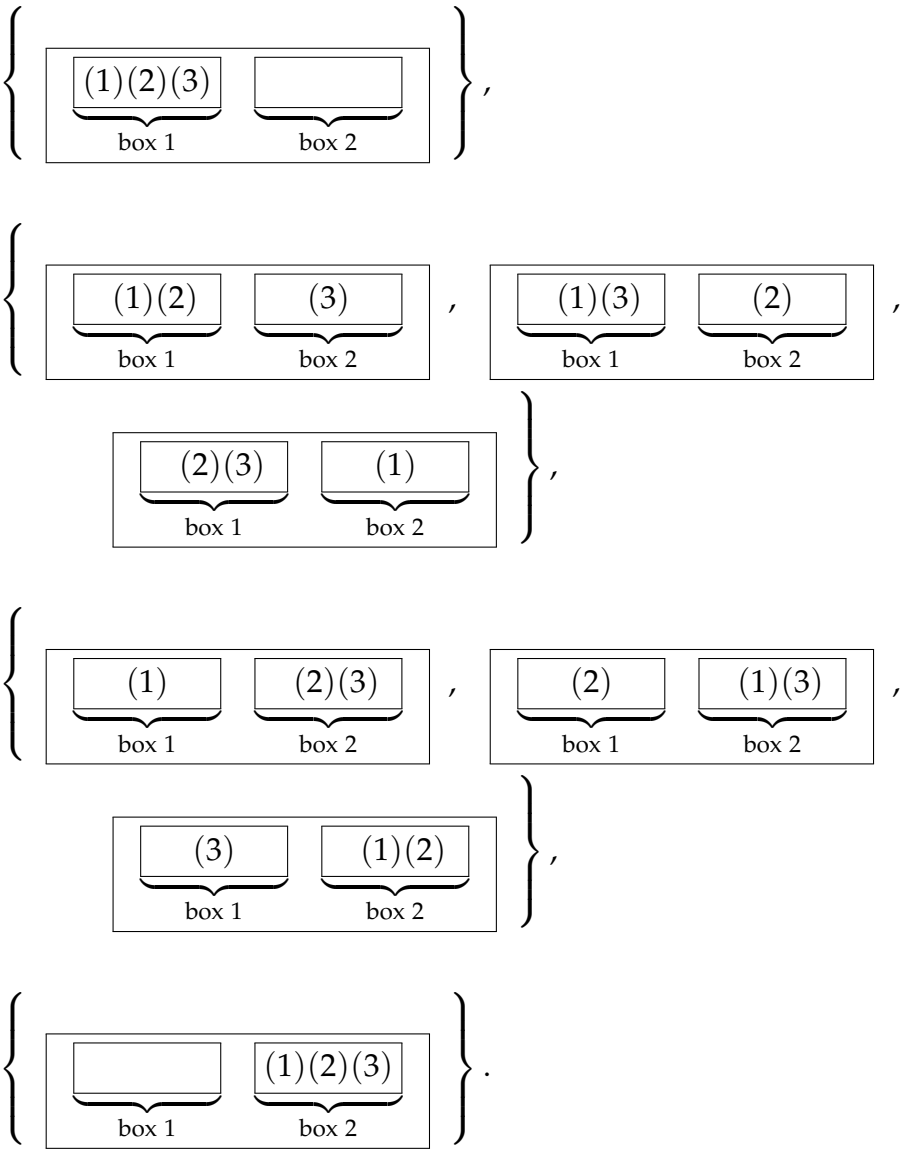
Proposition 3.3.37. Let $\sim$ be an equivalence relation on a set S. Let $x \in S$ and $y \in S$. Then, $x \sim y$ if and only if the $\sim$-equivalence classes of x and y are identical (that is, $[x]_\sim = [y]_\sim$).

Thus, "counting elements of S up to equivalence" means counting $\sim$-equivalence classes. For instance, "counting maps from A to X up to $\overset{\text{ball}}{\sim}$-equivalence" means counting $\overset{\text{ball}}{\sim}$-equivalence classes (aka $U \to L$ placements).

3.4. $U \to L$

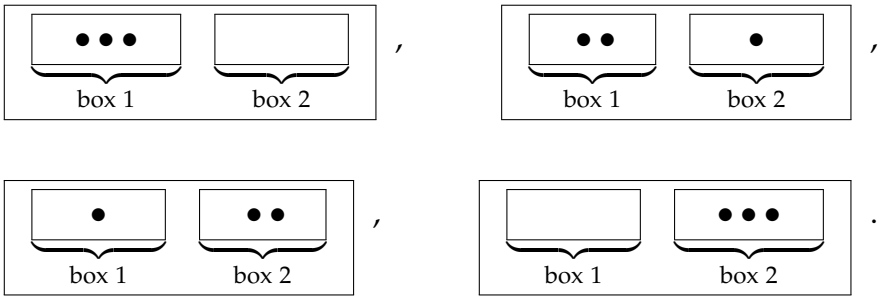
Recall that the $U \to L$ placements are the $\overset{\text{ball}}{\sim}$-equivalence classes. We shall now count them.

Example 3.4.1. For $X = [2]$ and $A = [3]$, there are 4 different $U \to L$ placements:



Convention 3.4.2. When visualizing a $U \to L$ placement, we will just draw the balls as circles, without putting any numbers in them (since the balls are meant to be unlabelled, i.e., their precise identities do not matter). So the four $U \to L$ placements for $X = [2]$ and $A = [3]$ are (shown here in the same order as in

Example 3.4.1)



Now, we are ready to count the $U \to L$ placements in the general case:

Unpolished stuff starts here

Proposition 3.4.3. We have

$$\begin{aligned}
&(\#\text{ of } U \to L \text{ placements } A \to X) \\
&= \left(\#\text{ of } \left(x_1, x_2, \ldots, x_{|X|}\right) \in \mathbb{N}^{|X|} \text{ satisfying } x_1 + x_2 + \cdots + x_{|X|} = |A|\right) \\
&= \binom{|A| + |X| - 1}{|A|}.
\end{aligned}$$

Proof. The second equality sign follows from (243).

It remains to prove the first equality sign. First, we WLOG assume that $X = [|X|]$ (so the boxes are labelled $1, 2, \ldots, |X|$). Then, consider the bijection

$$\{U \to L \text{ placements } A \to X\} \to \left\{\left(x_1, x_2, \ldots, x_{|X|}\right) \in \mathbb{N}^{|X|} \mid x_1 + x_2 + \cdots + x_{|X|} = |A|\right\}$$

that sends each $U \to L$ placement $\boxed{\boxed{a_1 \text{ balls}}\ \boxed{a_2 \text{ balls}}\ \cdots\ \boxed{a_{|X|} \text{ balls}}}$ to the $|X|$-tuple $\left(a_1, a_2, \ldots, a_{|X|}\right)$. (More rigorously: The $\overset{\text{ball}}{\sim}$-equivalence class of a map $f : A \to X$ is sent to the $|X|$-tuple

$$\left(\left|f^{-1}(1)\right|, \left|f^{-1}(2)\right|, \ldots, \left|f^{-1}(|X|)\right|\right),$$

where

$$f^{-1}(x) := \{a \in A \mid f(a) = x\}.$$

To see that this is a bijection, we need to show that if $f, g : A \to X$ are two maps such that

$$\left|f^{-1}(x)\right| = \left|g^{-1}(x)\right| \qquad \text{for all } x \in X,$$

then $f \overset{\text{ball}}{\sim} g$.)

Thus, the bijection principle yields

$$\begin{aligned}&(\#\text{ of } U \to L \text{ placements } A \to X)\\ &= \left(\#\text{ of } \left(x_1, x_2, \ldots, x_{|X|}\right) \in \mathbb{N}^{|X|} \text{ satisfying } x_1 + x_2 + \cdots + x_{|X|} = |A|\right).\end{aligned}$$

This is exactly the first equality sign of Proposition 3.4.3. □

Recall: An $L \to L$ placement is surjective if and only if each box has at least one ball in it.

We define surjectivity of $U \to L$ placements in the same way. Thus, a $\overset{\text{ball}}{\sim}$-equivalence class is a surjective $U \to L$ placement if and only if all its elements are surjective maps.

Proposition 3.4.4. We have

$$\begin{aligned}&(\#\text{ of surjective } U \to L \text{ placements } A \to X)\\ &= \left(\#\text{ of } \left(x_1, x_2, \ldots, x_{|X|}\right) \in \mathbb{P}^{|X|} \text{ satisfying } x_1 + x_2 + \cdots + x_{|X|} = |A|\right)\\ &= \binom{|A|-1}{|A|-|X|}.\end{aligned}$$

Proof. The first equality sign is proved similarly to the first equality sign in Proposition 3.4.3.

The second equality sign follows from (239). □

Recall: An $L \to L$ placement is injective if and only if each box has at most one ball in it.

We define injectivity of $U \to L$ placements in the same way. Thus, a $\overset{\text{ball}}{\sim}$-equivalence class is an injective $U \to L$ placement if and only if all its elements are injective maps.

Proposition 3.4.5. We have

$$\begin{aligned}&(\#\text{ of injective } U \to L \text{ placements } A \to X)\\ &= \left(\#\text{ of } \left(x_1, x_2, \ldots, x_{|X|}\right) \in \{0,1\}^{|X|} \text{ satisfying } x_1 + x_2 + \cdots + x_{|X|} = |A|\right)\\ &= \binom{|X|}{|A|}.\end{aligned}$$

Proof. The first equality sign is proved similarly to the first equality sign in Proposition 3.4.3.

The second equality sign follows from Theorem 2.10.4. □

Thus, our "twelvefold way" table now looks as follows:

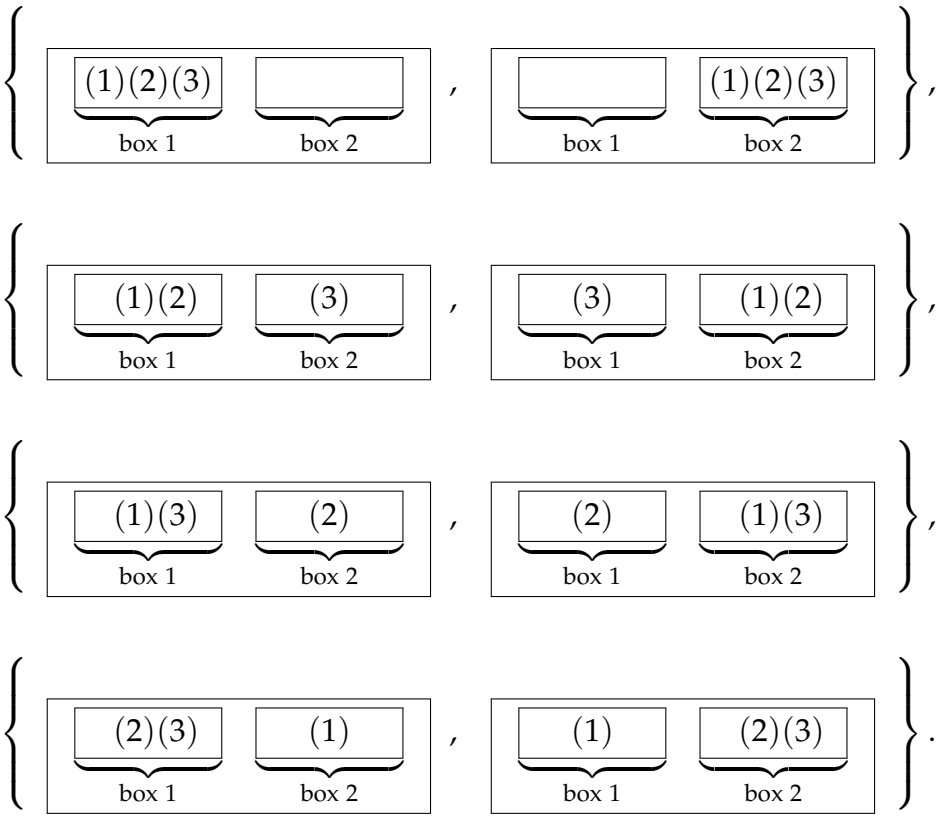
	arbitrary	injective	surjective
$L \to L$	$\lvert X\rvert^{\lvert A\rvert}$	$\lvert X\rvert^{\underline{\lvert A\rvert}}$	$\operatorname{sur}(\lvert X\rvert, \lvert A\rvert)$
$U \to L$	$\binom{\lvert A\rvert + \lvert X\rvert - 1}{\lvert A\rvert}$	$\binom{\lvert X\rvert}{\lvert A\rvert}$	$\binom{\lvert A\rvert - 1}{\lvert A\rvert - \lvert X\rvert}$
$L \to U$			
$U \to U$			

.

3.5. $L \to U$

Recall: The $L \to U$ placements are the $\overset{\text{box}}{\sim}$-equivalence classes. They are placements of labelled balls in unlabelled boxes.

Example 3.5.1. For $X = [2]$ and $A = [3]$, there are 4 different $L \to U$ placements:

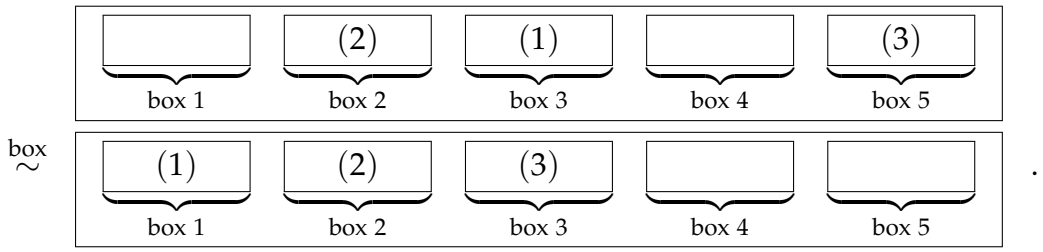


Proposition 3.5.2. We have

$$(\#\text{ of injective } L \to U \text{ placements } A \to X) = [\lvert A\rvert \leq \lvert X\rvert].$$

Proof. If $|A| > |X|$, then the Pigeonhole Principle shows that no such placements exist, and thus (# of injective $L \to U$ placements) $= 0$.

Now assume that $|A| \leq |X|$. WLOG assume that $X = [|X|]$, so that the boxes are labelled $1, 2, \ldots, |X|$. Thus, injective $L \to U$ placements do exist: for example, we can place each ball i into box i (thus leaving the last $|X| - |A|$ many boxes empty). Furthermore, any two injective $L \to U$ placements are identical. (Indeed, any such placement consists of one box with ball 1, one box with ball 2, one box with ball 3, and so on, totalling to $|A|$ many boxes filled with 1 ball each, and furthermore $|X| - |A|$ many empty boxes. It is clear that this uniquely describes it as an $L \to U$ placement, because any two $L \to L$ placements of this form can be turned into one another by a permutation of the boxes. For example,



.

Thus, any two injective $L \to U$ placements are identical.) Hence, the total # of injective $L \to U$ placements is 1. But this is precisely $[|A| \leq |X|]$, since $|A| \leq |X|$. $\square$

Recall: If $n \in \mathbb{N}$ and $k \in \mathbb{N}$, then $\left\{ n \atop k \right\} := \operatorname{sur}(n,k)/k!$ is called a **Stirling number of the second kind**.

Proposition 3.5.3. We have

$$(\text{\# of surjective } L \to U \text{ placements } A \to X) = \left\{ |A| \atop |X| \right\} = \frac{\operatorname{sur}(|A|, |X|)}{|X|!}.$$

Proof. The crux of the proof is the following claim:

> *Claim 1:* Each $\overset{\text{box}}{\sim}$-equivalence class of surjective maps (i.e., each surjective $L \to U$ placement) contains exactly $|X|!$ many maps $A \to X$.

[*Proof of Claim 1:* Consider the $\overset{\text{box}}{\sim}$-equivalence class of some surjective map $g : A \to X$. The elements of this class are all the maps of the form $\sigma \circ g$ with σ a permutation of X. There are $|X|!$ many permutations of X, and they all lead to **distinct** maps $\sigma \circ g$ (because if you know $\sigma \circ g$ and you have an $x \in X$, then you can tell what $\sigma(x)$ is by looking at a ball placed in box x by g, and checking which box contains this ball in $\sigma \circ g$). Thus, there are exactly $|X|!$ many distinct maps $\sigma \circ g$ in the class of g. This proves Claim 1.]

Now, Proposition 2.4.11 yields

$$\begin{aligned}
&\operatorname{sur}\left(|A|,|X|\right) \\
&= \left(\#\text{ of surjections } A \to X\right) \\
&= \sum_{\substack{C \text{ is a } \overset{\text{box}}{\sim}\text{-equivalence} \\ \text{class of surjections}}} \underbrace{|C|}_{\substack{=|X|! \\ \text{(by Claim 1)}}} \qquad \left(\begin{array}{c}\text{here, we have split the sum} \\ \text{according to the } \overset{\text{box}}{\sim}\text{-equivalence class}\end{array}\right) \\
&= \sum_{\substack{C \text{ is a } \overset{\text{box}}{\sim}\text{-equivalence} \\ \text{class of surjections}}} |X|! = \left(\#\text{ of } \overset{\text{box}}{\sim}\text{-equivalence classes of surjections}\right) \cdot |X|!.
\end{aligned}$$

Thus, dividing by $|X|!$, we obtain

$$\begin{aligned}
&\left(\#\text{ of } \overset{\text{box}}{\sim}\text{-equivalence classes of surjections}\right) \\
&= \operatorname{sur}\left(|A|,|X|\right) / |X|! = \left\{ {|A| \atop |X|} \right\}
\end{aligned}$$

(since $\left\{ {|A| \atop |X|} \right\}$ was defined to be $\operatorname{sur}\left(|A|,|X|\right) / |X|!$). This proves Proposition 3.5.3 (since the $\overset{\text{box}}{\sim}$-equivalence classes of surjections are precisely the surjective $L \to U$ placements $A \to X$). □

Class of 2019-11-13

Proposition 3.5.4. We have

$$\left(\#\text{ of } L \to U \text{ placements } A \to X\right) = \left\{ {|A| \atop 0} \right\} + \left\{ {|A| \atop 1} \right\} + \cdots + \left\{ {|A| \atop |X|} \right\}.$$

Proof. We can prove a better claim: For each $k \in \{0,1,\ldots,|X|\}$, we have

$$\left(\#\text{ of } L \to U \text{ placements with exactly } k \text{ nonempty boxes}\right) = \left\{ {|A| \atop k} \right\}.$$

(This is not hard to see, because in an $L \to U$ placement, we can WLOG assume that all empty boxes are at the end, and thus we can simply ignore the empty boxes.)

Adding these equalities up for all $k \in \{0,1,\ldots,|X|\}$, we obtain precisely the claim of Proposition 3.5.4. (Details LTTR.) □

Thus, our table now looks as follows:

	arbitrary	injective	surjective
$L \to L$	$\lvert X\rvert^{\lvert A\rvert}$	$\lvert X\rvert^{\underline{\lvert A\rvert}}$	$\operatorname{sur}(\lvert X\rvert, \lvert A\rvert)$
$U \to L$	$\binom{\lvert A\rvert + \lvert X\rvert - 1}{\lvert A\rvert}$	$\binom{\lvert X\rvert}{\lvert A\rvert}$	$\binom{\lvert A\rvert - 1}{\lvert A\rvert - \lvert X\rvert}$
$L \to U$	$\left\{ {\lvert A\rvert \atop 0} \right\} + \left\{ {\lvert A\rvert \atop 1} \right\} + \cdots + \left\{ {\lvert A\rvert \atop \lvert X\rvert} \right\}$	$[\lvert A\rvert \leq \lvert X\rvert]$	$\left\{ {\lvert A\rvert \atop \lvert X\rvert} \right\}$
$U \to U$			

.

Let us say a few words about an equivalent version of surjective $L \to U$ placements: the set partitions.

Definition 3.5.5. Let S be a set.

(a) A **set partition** of S is a set $\mathcal{F}$ of disjoint nonempty subsets of S such that the union of these subsets is S.

In other words, a set partition of S is a set $\{S_1, S_2, \ldots, S_k\}$ of nonempty subsets of S such that each element of S lies in exactly one S_i. (Here, we are assuming that S is finite.)

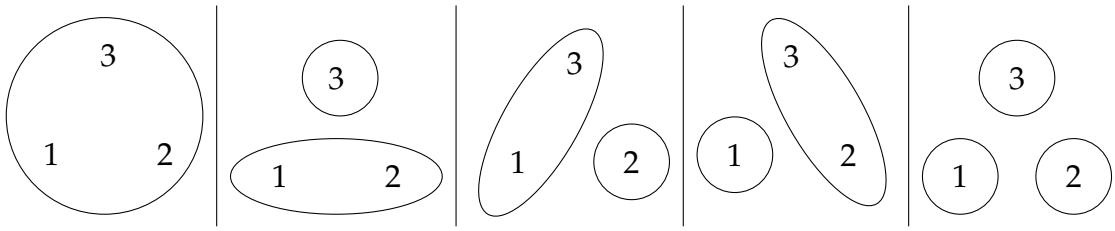
(b) If $\mathcal{F}$ is a set partition of S, then the elements of $\mathcal{F}$ are called the **parts** (or **blocks**) of $\mathcal{F}$. Keep in mind that they are subsets of S.

(c) If a set partition $\mathcal{F}$ of S has k parts, then we say that $\mathcal{F}$ is a **set partition of S into k parts**.

Example 3.5.6. Here are all set partitions of the set $[3] = \{1,2,3\}$:

$$\{\{1,2,3\}\}, \quad \{\{1,2\},\{3\}\}, \quad \{\{1,3\},\{2\}\}, \quad \{\{2,3\},\{1\}\}, \quad \{\{1\},\{2\},\{3\}\}.$$

And here are the same set partitions, drawn as pictures (each part of the set partition corresponds to a blob):



Proposition 3.5.7. Let A be an n-element set. Let $k \in \mathbb{N}$. Then,

$$(\#\text{ of set partitions of } A \text{ into } k \text{ parts}) = \left\{ {n \atop k} \right\}.$$

Proof. Let $X = [k]$. Then, there is a bijection

$$\{\text{set partitions of } A \text{ into } k \text{ parts}\} \to \{\text{surjective } L \to U \text{ placements } A \to X\},$$
$$\{S_1, S_2, \ldots, S_k\} \mapsto (\text{all elements in } S_i \text{ go into box } i).$$

(This is well-defined, because the resulting $L \to U$ placement does not depend on the order in which we have listed the blocks of our set partition; any two orders lead to $\overset{\text{box}}{\sim}$-equivalent maps.) Now, it remains to recall the bijection principle and apply Proposition 3.5.3. □

Recall that we have shown a bunch of properties of $\operatorname{sur}(m,n)$. Since $\left\{ {m \atop n} \right\} = \operatorname{sur}(m,n)/n!$, we can translate them into properties of $\left\{ {m \atop n} \right\}$:

Proposition 3.5.8. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$.

(a) We have $\left\{ {n \atop 0} \right\} = [n = 0]$.

(b) We have $\left\{ {0 \atop k} \right\} = [k = 0]$.

(c) We have $\left\{ {n \atop k} \right\} = 0$ if $k > n$.

(d) We have $\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}$ if $n > 0$ and $k > 0$.

(e) We have $\left\{ {n \atop k} \right\} = \sum_{j=0}^{n-1} \binom{n}{j} \left\{ {j \atop k-1} \right\} / k$ if $k > 0$.

(f) We have $\left\{ {n \atop k} \right\} = \frac{1}{k!} \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n$.

Proof. **(a)** Follows from Proposition 2.4.12 **(a)**.
(b) Follows from Proposition 2.4.12 **(d)**.
(c) Follows from Proposition 2.4.12 **(f)**.
(d) Follows from Proposition 2.4.14.
(e) Follows from Proposition 2.4.13.
(f) Follows from Theorem 2.4.17. □

Remark 3.5.9. Let $n \in \mathbb{N}$. The **n-th Bell number** $B(n)$ is defined as the # of all set partitions of $[n]$. Thus, Proposition 3.5.3 yields

$$B(n) = \left\{ {n \atop 0} \right\} + \left\{ {n \atop 1} \right\} + \cdots + \left\{ {n \atop n} \right\}.$$

For example, $B(3) = 5$.

There is no explicit formula for $B(n)$, but there is a recurrence relation:

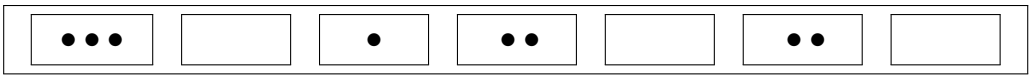
$$B(n+1) = \sum_{i=0}^{n} \binom{n}{i} B(i).$$

See [Guicha20, Theorem 1.4.3] for a proof of this recurrence relation, and [18s-hw3s, §0.3.2] for more about the Bell numbers.

3.6. $U \to U$ and integer partitions

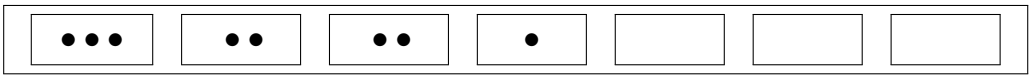
It remains to count $U \to U$ placements.

A $U \to U$ placement looks like this:



,

with the understanding that the boxes, too, are interchangeable. Thus, we can order the boxes by decreasing number of balls:



.

You can encode this $U \to U$ placement by a sequence of numbers, which say how many balls lie in each box:

$$(3,2,2,1,0,0,0)\,.$$

The decreasing order makes this sequence unique.

Let us introduce a name for such sequences, more precisely, for such sequences that don't contain zeroes:

Definition 3.6.1. A **partition** of an integer n is a weakly decreasing list $(a_1, a_2, \ldots, a_k)$ of positive integers whose sum is n (that is, $a_1 \geq a_2 \geq \cdots \geq a_k > 0$ and $a_1 + a_2 + \cdots + a_k = n$).

Instead of "partition", we can also say "integer partition".

The positive integers $a_1, a_2, \ldots, a_k$ are called the **parts** of the partition $(a_1, a_2, \ldots, a_k)$.

If a partition of n has k parts, then we say that it is a **partition of n into k parts**.

Example 3.6.2. The partitions of 5 are

$$(5)\,, \quad (4,1)\,, \quad (3,2)\,, \quad (3,1,1)\,,$$
$$(2,2,1)\,, \quad (2,1,1,1)\,, \quad (1,1,1,1,1)\,.$$

The partition $(2,2,1)$ is a partition of 5 into 3 parts.

Remark 3.6.3. A partition of n is the same as a weakly decreasing composition of n.

Definition 3.6.4. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then, we set

$$p_k(n) = (\#\text{ of partitions of } n \text{ into } k \text{ parts})\,.$$

Example 3.6.5. We have

$$p_0(5) = 0, \qquad p_1(5) = 1, \qquad p_2(5) = 2, \qquad p_3(5) = 2,$$
$$p_4(5) = 1, \qquad p_5(5) = 1, \qquad p_k(5) = 0 \text{ for } k > 5.$$

Proposition 3.6.6. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$.
(a) We have $p_k(n) = 0$ when $n < 0$.
(b) We have $p_k(n) = 0$ when $k > n$.
(c) We have $p_0(n) = [n = 0]$.
(d) We have $p_1(n) = [n > 0]$.
(e) We have $p_k(n) = p_k(n-k) + p_{k-1}(n-1)$ when $k \geq 1$.
(f) We have $p_2(n) = \lfloor n/2 \rfloor$ if $n \in \mathbb{N}$.

Proof. **(a)** A sum of positive integers is never negative. Thus, there exist no partitions of n when $n < 0$.

(b) If $(a_1, a_2, \ldots, a_k)$ is a partition of n into k parts, then

$$n = \underbrace{a_1}_{\geq 1} + \underbrace{a_2}_{\geq 1} + \cdots + \underbrace{a_k}_{\geq 1} \geq \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} = k.$$

Thus, no such partition exists if $k > n$.

(c) A partition of n into 0 parts is a 0-tuple of positive integers whose sum is n. But the sum of a 0-tuple is always 0. Hence, such a partition exists only for $n = 0$, and is unique. Thus, $p_0(n) = 1$ if $n = 0$ and is 0 otherwise.

(d) If $n > 0$, then there is only one partition of n into 1 part, namely the 1-tuple (n). If $n = 0$, then there is no partition of n into 1 part.

(e) Assume that $k \geq 1$. Let us call a partition of n

- **red** if 1 is a part of it;
- **green** if 1 is not a part of it.

Any red partition of n must end with a 1 (since it contains a 1 but is weakly decreasing). Thus, the map

$$\{\text{red partitions of } n \text{ into } k \text{ parts}\} \to \{\text{partitions of } n-1 \text{ into } k-1 \text{ parts}\},$$
$$(a_1, a_2, \ldots, a_{k-1}, 1) \mapsto (a_1, a_2, \ldots, a_{k-1})$$

is well-defined. It is easy to see that this map is a bijection. Hence, the bijection principle yields

$$(\#\text{ of red partitions of } n \text{ into } k \text{ parts})$$
$$= (\#\text{ of partitions of } n-1 \text{ into } k-1 \text{ parts}) = p_{k-1}(n-1).$$

All parts of a green partition of n are > 1 (since they are positive integers and $\neq 1$). Thus, the map

$$\{\text{green partitions of } n \text{ into } k \text{ parts}\} \to \{\text{partitions of } n-k \text{ into } k \text{ parts}\}$$
$$(a_1, a_2, \ldots, a_k) \mapsto (a_1 - 1, a_2 - 1, \ldots, a_k - 1)$$

is well-defined. It is easy to see that this map is a bijection. Hence, the bijection principle yields

$$(\#\text{ of green partitions of } n \text{ into } k \text{ parts})$$
$$= (\#\text{ of partitions of } n-k \text{ into } k \text{ parts}) = p_k(n-k).$$

Adding these two equalities together, we get the claim of **(e)**.

(f) Let $n \in \mathbb{N}$. Then, the partitions of n into 2 parts are

$$(n-1,1), \quad (n-2,2), \quad (n-3,3), \quad \ldots, \quad (\lceil n/2 \rceil, \lfloor n/2 \rfloor)$$

(where $\lceil x \rceil$ denotes the ceiling of the real number x). So there are $\lfloor n/2 \rfloor$ many of them. □

Here is a table of the numbers $p_k(n)$ for small values of k and n:

$p_k(n)$	$n=0$	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$	$n=9$
$k=0$	1	0	0	0	0	0	0	0	0	0
$k=1$	0	1	1	1	1	1	1	1	1	1
$k=2$	0	0	1	1	2	2	3	3	4	4
$k=3$	0	0	0	1	1	2	3	4	5	7
$k=4$	0	0	0	0	1	1	2	3	5	6
$k=5$	0	0	0	0	0	1	1	2	3	5
$k=6$	0	0	0	0	0	0	1	1	2	3
$k=7$	0	0	0	0	0	0	0	1	1	2
$k=8$	0	0	0	0	0	0	0	0	1	1
$k=9$	0	0	0	0	0	0	0	0	0	1

Proposition 3.6.7. We have

$$(\#\text{ of surjective } U \to U \text{ placements } A \to X) = p_{|X|}(|A|).$$

Proof. Proof idea: Encode a surjective $U \to U$ placement $A \to X$ as a partition of $|A|$ into $|X|$ parts: namely the partition $\left(a_1, a_2, \ldots, a_{|X|}\right)$, where

$$a_i = (\#\text{ of balls in the box with the } i\text{-th largest \# of balls}).$$

This is a bijection. □

Proposition 3.6.8. We have

$$(\#\text{ of injective } U \to U \text{ placements } A \to X) = [|A| \leq |X|]\,.$$

Proof. This follows from Proposition 3.5.2. □

Proposition 3.6.9. We have

$$(\#\text{ of } U \to U \text{ placements } A \to X) = p_0(|A|) + p_1(|A|) + \cdots + p_{|X|}(|A|)\,.$$

Proof. Similar to the proof of Proposition 3.5.4. □

Thus, we have obtained a full table of answers to the "twelvefold way" counting problems:

	arbitrary	injective	surjective
$L \to L$	$\lvert X\rvert^{\lvert A\rvert}$	$\lvert X\rvert^{\underline{\lvert A\rvert}}$	$\operatorname{sur}(\lvert X\rvert, \lvert A\rvert)$
$U \to L$	$\binom{\lvert A\rvert + \lvert X\rvert - 1}{\lvert A\rvert}$	$\binom{\lvert X\rvert}{\lvert A\rvert}$	$\binom{\lvert A\rvert - 1}{\lvert A\rvert - \lvert X\rvert}$
$L \to U$	$\left\{ {\lvert A\rvert \atop 0} \right\} + \left\{ {\lvert A\rvert \atop 1} \right\} + \cdots + \left\{ {\lvert A\rvert \atop \lvert X\rvert} \right\}$	$[\lvert A\rvert \leq \lvert X\rvert]$	$\left\{ {\lvert A\rvert \atop \lvert X\rvert} \right\}$
$U \to U$	$p_0(\lvert A\rvert) + p_1(\lvert A\rvert) + \cdots + p_{\lvert X\rvert}(\lvert A\rvert)$	$[\lvert A\rvert \leq \lvert X\rvert]$	$p_{\lvert X\rvert}(\lvert A\rvert)$

.

By the way, what happens if we add an extra column for "bijective"? Here is this column:

	bijective
$L \to L$	$[\lvert A\rvert = \lvert X\rvert] \cdot \lvert X\rvert!$
$U \to L$	$[\lvert A\rvert = \lvert X\rvert]$
$L \to U$	$[\lvert A\rvert = \lvert X\rvert]$
$U \to U$	$[\lvert A\rvert = \lvert X\rvert]$

.

(See [17f-hw1s, Exercise 7] for the proofs.) So that's not a very interesting column.

Class of 2019-11-15

3.7. Integer partitions (an introduction)

Recall that we have set

$$p_k(n) := (\#\text{ of partitions of } n \text{ into } k \text{ parts})$$

for all $n \in \mathbb{Z}$ and $k \in \mathbb{N}$.

Proposition 3.6.6 **(e)** says that

$$p_k(n) = p_k(n-k) + p_{k-1}(n-k) \qquad \text{for all } n \in \mathbb{Z} \text{ and } k \geq 1.$$

Let us also set

$$p(n) := (\#\text{ of partitions of } n)$$

for all $n \in \mathbb{Z}$. Then,

$$p(n) = p_0(n) + p_1(n) + \cdots + p_n(n) \qquad \text{for each } n \in \mathbb{Z}$$

(by Proposition 3.6.6 **(b)**).

Let us now count partitions with some more special properties.

Definition 3.7.1. Let $n \in \mathbb{Z}$.

(a) Let

$$\begin{aligned} p_{\text{odd}}(n) &= (\#\text{ of partitions of } n \text{ into odd parts}) \\ &= (\#\text{ of partitions } (a_1, a_2, \ldots, a_k) \text{ of } n \text{ such that all } a_i \text{ are odd}). \end{aligned}$$

(b) Let

$$\begin{aligned} p_{\text{dist}}(n) &= (\#\text{ of partitions of } n \text{ into distinct parts}) \\ &= (\#\text{ of partitions } (a_1, a_2, \ldots, a_k) \text{ of } n \text{ such that } a_1 > a_2 > \cdots > a_k). \end{aligned}$$

Example 3.7.2. **(a)** We have

$$p_{\text{odd}}(7) = |\{(7), (5,1,1), (3,3,1), (3,1,1,1,1), (1,1,1,1,1,1,1)\}| = 5.$$

(b) We have

$$p_{\text{dist}}(7) = |\{(7), (6,1), (5,2), (4,3), (4,2,1)\}| = 5.$$

The following theorem is due to Euler:

Theorem 3.7.3. Let $n \in \mathbb{Z}$. Then, $p_{\text{odd}}(n) = p_{\text{dist}}(n)$.

Proof. Here is a rough outline. See [Andrew16] or [Galvin17, Proposition 18.1] for a more detailed version (albeit with a slightly different version of the bijection).

We construct a map

$$A : \{\text{partitions of } n \text{ into odd parts}\} \to \{\text{partitions of } n \text{ into distinct parts}\}$$

which transforms a partition as follows: Repeatedly merge two equal parts until no more equal parts can be found. "Merging two equal parts" means replacing two

equal parts a, a by the single part $2a$, and (if necessarily) rearranging the resulting tuple back into weakly decreasing order.

(*Examples:* Let us compute $A(5,5,3,1,1,1)$:

$$\left(\underline{5,5},3,1,1,1\right) \to \left(10,3,\underline{1,1},1\right) \to (10,3,2,1)$$

(where we underline equal entries that are about to get merged). Thus, $A(5,5,3,1,1,1) = (10,3,2,1)$.

Let us compute $A(5,3,1,1,1,1)$:

$$\left(5,3,\underline{1,1},1,1\right) \to \left(5,3,2,\underline{1,1}\right) \to \left(5,3,\underline{2,2}\right) \to (5,4,3).$$

Thus, $A(5,3,1,1,1,1) = (5,4,3)$.)

Why is this map A well-defined? This is not obvious.

Our definition of A was non-deterministic: It tells us to merge equal parts; but it does not tell us which equal parts to choose first (and there can be several choices). Thus, we have to prove that the result of our many merges does not depend on the order in which we do the merges.

One way to prove this is using something called the **diamond lemma**. Another way is by writing the parts of the partitions in binary (this is what Andrews does in [Andrew16]; he doesn't even talk about merging).

The inverse of A transforms a partition by repeatedly splitting even parts into two equal pieces.

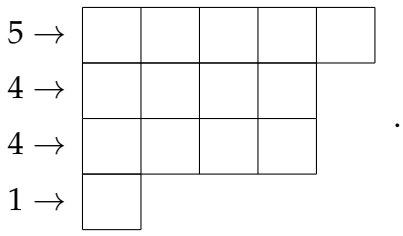
(The map A is called the Glaisher bijection; there are several other bijections that work.) □

Proposition 3.7.4. Let $n \in \mathbb{Z}$ and $k > 0$. Then,

$$p_k(n) = (\#\text{ of partitions of } n \text{ whose largest part is } k).$$

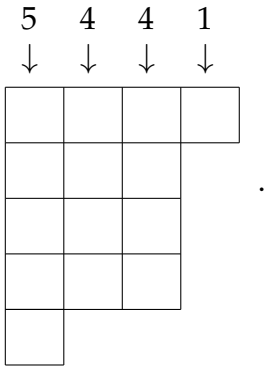
Example 3.7.5. We have $p_3(5) = (\#\text{ of partitions of 5 whose largest part is 3})$ (indeed, both numbers are 2). Indeed, the partitions of 5 into 3 parts are $(3,1,1)$ and $(2,2,1)$.

Proof. Picture proof: e.g., let $n = 14$ and $k = 4$. Start with the partition $\lambda = (5,4,4,1)$ of n into k parts. Draw a table of k left-aligned rows, where the length of each row equals the corresponding part of λ:



.

Now, flip the table across the main diagonal (i.e., the diagonal going from the top-left to the bottom-right), so that the rows become columns and vice versa:



.

The lengths of the rows of the resulting table again form a partition of n. The largest part of this new partition is k (because our original table had k rows, so the flipped table has k columns). In our example, this new partition is $(4,3,3,3,1)$.

Thus, we obtain a map

$$\{\text{partitions of } n \text{ into } k \text{ parts}\} \to \{\text{partitions of } n \text{ whose largest part is } k\},$$

which transforms a partition by flipping its table.

This map is a bijection; indeed, its inverse map is defined in the same way. This bijection is called **conjugation of partitions**. The bijection principle now yields the proposition.

(Note: The table that we constructed above is called the **Young diagram** of λ, or the **Ferrers diagram** of λ.) □

Definition 3.7.6. For any $k \in \mathbb{Z}$, define $w_k \in \mathbb{N}$ by

$$w_k = \frac{(3k-1)\,k}{2}.$$

This is called a **pentagonal number**.

Theorem 3.7.7 (Euler's recursion for the partition numbers)**.** For each $n > 0$, we have

$$\begin{aligned} &p(n) \\ &= p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) \pm \cdots \\ &= \sum_{\substack{k \in \mathbb{Z}; \\ k \neq 0}} (-1)^{k-1} p(n - w_k). \end{aligned}$$

We might get to prove this later on, using the technique of **generating functions**.

There is, of course, much more to say about partitions. See [Wilf09] or [AndEri04] for two introductions.

3.8. Odds and ends

Here are some random counting exercises.

Exercise 3.8.1. Given n persons ($n > 0$) and k tasks ($k > 0$).

(a) What is the # of ways to assign a task to each person such that each task has at least 1 person working on it?

(b) What if we additionally want to choose a leader for each task (among the people assigned to this task)?

(c) What if, instead, we want to choose a vertical hierarchy (between all people working on the task) for each task? (A "vertical hierarchy" means a ranking of all people working on the task, with no ties.)

Example: Assume $n = 8$ and $k = 3$. Let our 8 people be $1, 2, 3, 4, 5, 6, 7, 8$, and let our 3 tasks be A, B, C.

(a) One option is

task	people working on it
A	$1, 2, 5$
B	3
C	$4, 6, 7, 8$

(b) One option is

task	people working on it
A	$1, 2, 5$ with leader 2
B	3 with leader 3
C	$4, 6, 7, 8$ with leader 7

(c) One option is

task	people working on it
A	$1 > 5 > 2$
B	3
C	$7 > 8 > 4 > 6$

(where the "$>$" signs stand for "is ranked above").

Proof. (Solution sketch.)

(a) $\operatorname{sur}(n, k)$.

Proof. Choosing such an arrangement is tantamount to choosing a surjection $\{\text{people}\} \to \{\text{tasks}\}$.

(b) $n^{\underline{k}} \cdot k^{n-k}$.

Proof. First, choose a leader for each task. There are $n^{\underline{k}}$ options for this (since the leaders have to be distinct). Then, every of the remaining $n - k$ people joins one of

the k leaders. There are k^{n-k} options for this.

(c) $n! \cdot \binom{n-1}{k-1}$.

Proof. First, order all the n people in some way. There are $n!$ options for this. Then, split this ordering into k nonempty chunks (corresponding to the k tasks). There are $\binom{n-1}{k-1}$ options for this, since we need to put $k-1$ separators into the $n-1$ positions between two consecutive people in our ordering. □

Class of 2019-11-18

4. Permutations

4.1. Introduction

We will now talk about permutations in more detail. For deeper treatments, see [Bona22], [Sagan01] and [Stanle11, Chapter 1]. See also [Grinbe15, Chapter 5] for a detailed exposition of the basics.

Recall: A **permutation** of a set X is a bijection from X to X.

4.2. Definitions

Definition 4.2.1. Let $n \in \mathbb{N}$. Let S_n be the set of all permutations of $[n]$. This set S_n is called the **n-th symmetric group**. It is closed under composition (i.e., for any $\alpha \in S_n$ and $\beta \in S_n$, we have $\alpha \circ \beta \in S_n$) and under inverses (i.e., for any $\sigma \in S_n$, we have $\sigma^{-1} \in S_n$), and contains the identity map $\mathrm{id}_{[n]}$.

Definition 4.2.2. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. We introduce two notations for σ:

(a) The **one-line notation** of σ is the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. (Conventionally, authors use square brackets for it, but we use parentheses.)

(b) The **cycle digraph** of σ is defined (informally) as follows:

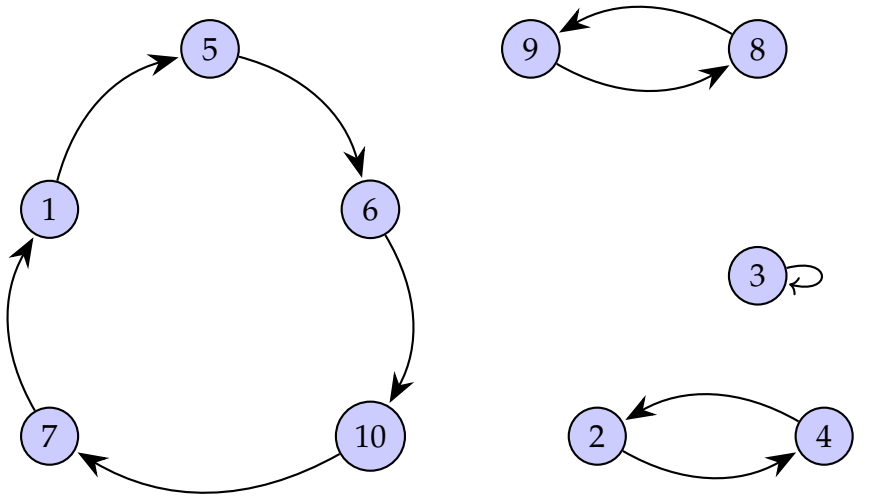
For each $i \in [n]$, draw a point ("node") labelled i.

For each $i \in [n]$, draw an arrow ("arc") from the node labelled i to the node labelled $\sigma(i)$.

The result is called the **cycle digraph** of σ.

Example 4.2.3. Let $\sigma : [10] \to [10]$ be the map that sends the elements $1,2,3,4,5,6,7,8,9,10$ to $5,4,3,2,6,10,1,9,8,7$, respectively. Then, σ is a bijection, hence a permutation of $[10]$. The one-line notation of σ is $(5,4,3,2,6,10,1,9,8,7)$.

The cycle digraph of σ is



.

4.3. Transpositions and cycles

Definition 4.3.1. **(a)** Let i and j be two distinct elements of a set X.

Then, the **transposition** $t_{i,j}$ is the permutation of X that sends i to j, sends j to i, and leaves all other elements in their places.

If $X = [n]$ for some $n \in \mathbb{N}$, and if $i < j$, then the one-line notation of $t_{i,j}$ is

$$\left(\underbrace{1,2,\ldots,i-1}_{\text{integers from 1 to } i-1}, j, \underbrace{i+1,i+2,\ldots,j-1}_{\text{integers from } i+1 \text{ to } j-1}, i, \underbrace{j+1,j+2,\ldots,n}_{\text{integers from } j+1 \text{ to } n} \right).$$

(b) Let $n \in \mathbb{N}$ and $i \in [n-1]$. Then, the **simple transposition** s_i is defined by $s_i = t_{i,i+1} \in S_n$. So a simple transposition is a transposition that swaps two consecutive integers.

Convention 4.3.2. If α and β are two permutations of a set X, then we write $\alpha\beta$ for $\alpha \circ \beta$.

Also, if α is any permutation of X, then we set $\alpha^i := \underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{i \text{ times}}$ for each $i \in \mathbb{N}$. If $i = 0$, this is understood to be id_X.

Proposition 4.3.3. Let $n \in \mathbb{N}$.

(a) We have $s_i^2 = \mathrm{id}$ for all $i \in [n-1]$. (Recall: $s_i^2 = s_i \circ s_i$.)

(b) We have $s_i s_j = s_j s_i$ for all $i, j \in [n-1]$ with $|i-j| > 1$.

(c) We have $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} = t_{i,i+2}$ for all $i \in [n-2]$. (This is known as "the braid relation for permutations".)

Proof. Straightforward verification that both sides send each $k \in [n]$ to the same value. (The "hardest" part is part **(c)**, which is proved in [Grinbe15, solution to Exercise 5.1 **(a)**].) $\square$

Definition 4.3.4. Let $n \in \mathbb{N}$. Let w_0 be the permutation in S_n that sends each $i \in [n]$ to $n+1-i$.

In other words, it "reflects" all numbers from 1 to n across the middle of $[n]$. It is the unique strictly decreasing permutation of $[n]$.

Example 4.3.5. If $n = 5$, then $w_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ in two-line notation, and $w_0 = (5,4,3,2,1)$ in one-line notation.

Definition 4.3.6. Let X be a set. Let $i_1, i_2, \ldots, i_k$ be k distinct elements of X. Then,

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$$

means the permutation of X that sends $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $i_3 \mapsto i_4$, $\ldots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$ and leaves all other elements of X unchanged. This is called a **k-cycle**.

Remark 4.3.7. People often write $(i_1, i_2, \ldots, i_k)$ for $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$. (But we won't.)

Example 4.3.8. Let $X = [8]$. Then, the permutation $\operatorname{cyc}_{2,6,5}$ of $[8]$ has two-line notation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 6 & 3 & 4 & 2 & 5 & 7 & 8 \end{pmatrix}$.

Remark 4.3.9. A permutation α is called an **involution** if $\alpha^2 = \mathrm{id}$. For example, all transpositions $t_{i,j}$ are involutions. Also, both id and w_0 are involutions. But k-cycles with $k > 2$ are not involutions.

Proposition 4.3.10. Let $n \in \mathbb{N}$.

(a) For any k distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, we have

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k} = \underbrace{t_{i_1,i_2} t_{i_2,i_3} \cdots t_{i_{k-1},i_k}}_{k-1 \text{ transpositions}}.$$

(b) For any $i \in [n]$ and $k \in \mathbb{N}$ such that $i + k - 1 \leq n$, we have

$$\operatorname{cyc}_{i,i+1,\ldots,i+k-1} = s_i s_{i+1} \cdots s_{i+k-2}.$$

(c) For any $i \in [n]$, we have $\operatorname{cyc}_i = \mathrm{id}$.

(d) For any distinct $i, j \in [n]$, we have $\operatorname{cyc}_{i,j} = t_{i,j}$.

(e) For any k distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$, we have

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k} = \operatorname{cyc}_{i_k,i_1,i_2,\ldots,i_{k-1}}.$$

(f) For any k distinct elements $i_1, i_2, \ldots, i_k$ of $[n]$ and any $\sigma \in S_n$, then

$$\sigma \operatorname{cyc}_{i_1,i_2,\ldots,i_k} \sigma^{-1} = \operatorname{cyc}_{\sigma(i_1),\sigma(i_2),\ldots,\sigma(i_k)}.$$

(g) If i and j are two integers satisfying $1 \leq i < j \leq n$, then

$$\begin{aligned} t_{i,j} &= s_i s_{i+1} \cdots s_{j-1} \cdots s_{i+1} s_i \\ &\qquad \left(\begin{array}{c} \text{this is a product starting at } s_i\text{, then walking up to } s_{j-1} \\ \text{and back down to } s_i \end{array} \right) \\ &= s_{j-1} s_{j-2} \cdots s_i \cdots s_{j-2} s_{j-1} \\ &\qquad \left(\begin{array}{c} \text{this is a product starting at } s_{j-1}\text{, then walking down to } s_i \\ \text{and back up to } s_{j-1} \end{array} \right). \end{aligned}$$

(h) We have

$$\begin{aligned} w_0 &= \operatorname{cyc}_{1,2,\ldots,n} \operatorname{cyc}_{1,2,\ldots,n-1} \cdots \operatorname{cyc}_1 \\ &= (s_1 s_2 \cdots s_{n-1}) (s_1 s_2 \cdots s_{n-2}) \cdots (s_1 s_2) s_1 \\ &= \operatorname{cyc}_1 \operatorname{cyc}_{2,1} \operatorname{cyc}_{3,2,1} \cdots \operatorname{cyc}_{n,n-1,\ldots,1} \\ &= s_1 (s_2 s_1) (s_3 s_2 s_1) \cdots (s_{n-1} s_{n-2} \cdots s_1). \end{aligned}$$

Proof. All of these are doable with some bookkeeping and induction.

(a) This is [Grinbe15, Exercise 5.16].

(b) This follows from part **(a)**.

(c), **(d)** and **(e)** are obvious consequences of the definitions.

(f) This is [Grinbe15, Exercise 5.17 **(a)**].

(g) This can be proved by induction on $j - i$ or otherwise. Perhaps the quickest way, however, is using part **(a)**: To show that $t_{i,j} = s_i s_{i+1} \cdots s_{j-1} \cdots s_{i+1} s_i$, we notice that part **(a)** yields

$$s_i s_{i+1} \cdots s_{j-1} = t_{i,i+1} t_{i+1,i+2} \cdots t_{j-1,j} = \operatorname{cyc}_{i,i+1,\ldots,j} \qquad \text{(by part \textbf{(a)})}$$

and

$$s_{j-2} s_{j-3} \cdots s_{i+1} s_i = t_{j-1,j-2} t_{j-2,j-3} \cdots t_{i+2,i+1} t_{i+1,i} = \operatorname{cyc}_{j-1,j-2,\ldots,i+1,i} \qquad \text{(by part \textbf{(a)})}.$$

Now,

$$\begin{aligned} &s_i s_{i+1} \cdots s_{j-1} \cdots s_{i+1} s_i \\ &= \underbrace{\left(s_i s_{i+1} \cdots s_{j-1}\right)}_{=\operatorname{cyc}_{i,i+1,\ldots,j}} \underbrace{\left(s_{j-2} s_{j-3} \cdots s_{i+1} s_i\right)}_{=\operatorname{cyc}_{j-1,j-2,\ldots,i+1,i}} \\ &= \operatorname{cyc}_{i,i+1,\ldots,j} \operatorname{cyc}_{j-1,j-2,\ldots,i+1,i} = t_{i,j} \qquad \text{(this is easy to check)}. \end{aligned}$$

This proves the first equality sign of part **(g)**; the second is proved similarly.

(h) TODO. For now, see [18s]. □

4.4. Inversions and lengths

Definition 4.4.1. Let $n \in \mathbb{N}$ and $\sigma \in S_n$.

(a) An **inversion** of σ is a pair (i,j) of elements of $[n]$ such that $i < j$ and $\sigma(i) > \sigma(j)$.

(b) The **length** (or **Coxeter length**) of σ is the # of inversions of σ. It is called $\ell(\sigma)$.

(In LaTeX, you can obtain the symbol "ℓ" by typing "`\ell`". If you just type "`l`", then you get the less remarkable letter "l".)

Example 4.4.2. Let $\pi = (3,1,4,2) \in S_4$ (in one-line notation).

The inversions of π are

$$(1,4) \qquad \left(\text{since } 1 < 4 \text{ and } \underbrace{\pi(1)}_{=3} > \underbrace{\pi(4)}_{=2} \right) \qquad \text{and}$$

$$(3,4) \qquad \left(\text{since } 3 < 4 \text{ and } \underbrace{\pi(3)}_{=4} > \underbrace{\pi(4)}_{=2} \right) \qquad \text{and}$$

$$(1,2) \qquad \left(\text{since } 1 < 2 \text{ and } \underbrace{\pi(1)}_{=3} > \underbrace{\pi(2)}_{=1} \right).$$

So the length of π is 3.

Remark 4.4.3. If $\sigma \in S_n$, then $0 \leq \ell(\sigma) \leq \binom{n}{2}$.

The only $\sigma \in S_n$ with $\ell(\sigma) = 0$ is id.

The only $\sigma \in S_n$ with $\ell(\sigma) = \binom{n}{2}$ is w_0.

Inbetween, there are many permutations with a given $\ell(\sigma)$.

Class of 2019-11-20

Remark 4.4.4. If $n \in \mathbb{N}$, then the permutations of $[n]$ can be represented as the vertices of an $(n-1)$-dimensional polyhedron in n-dimensional space. Namely, each permutation σ of $[n]$ gives rise to the point $(\sigma(1), \sigma(2), \ldots, \sigma(n)) \in \mathbb{R}^n$, and the convex hull of all these points is the polyhedron. This is called the **permutahedron**.

Proposition 4.4.5. For every $\sigma \in S_n$, we have $\ell\left(\sigma^{-1}\right) = \ell(\sigma)$.

Proof. Recall: An inversion of σ is a pair $(i,j) \in [n] \times [n]$ such that $i < j$ and $\sigma(i) > \sigma(j)$. An inversion of σ^{-1} is a pair $(u,v) \in [n] \times [n]$ such that $u < v$ and $\sigma^{-1}(u) > \sigma^{-1}(v)$.

The map

$$\{\text{inversions of } \sigma\} \to \left\{\text{inversions of } \sigma^{-1}\right\},$$
$$(i,j) \mapsto (\sigma(j), \sigma(i))$$

is well-defined and bijective (its inverse map sends each $(u,v) \in \left\{\text{inversions of } \sigma^{-1}\right\}$ to $\left(\sigma^{-1}(v), \sigma^{-1}(u)\right)$). So the bijection principle yields $\ell(\sigma) = \ell\left(\sigma^{-1}\right)$.

(For details, see [Grinbe15, Exercise 5.2 **(f)**].) □

Recall from last time

- the transpositions $t_{i,j}$ (swapping i with j while leaving all other numbers unchanged), and
- the simple transpositions $s_i = t_{i,i+1}$.

Proposition 4.4.6. Let $n \in \mathbb{N}$, $\sigma \in S_n$ and $k \in [n-1]$.

(a) We have

$$\ell(\sigma \circ s_k) = \begin{cases} \ell(\sigma)+1, & \text{if } \sigma(k) < \sigma(k+1); \\ \ell(\sigma)-1, & \text{if } \sigma(k) > \sigma(k+1). \end{cases}$$

(b) We have

$$\ell(s_k \circ \sigma) = \begin{cases} \ell(\sigma)+1, & \text{if } \sigma^{-1}(k) < \sigma^{-1}(k+1); \\ \ell(\sigma)-1, & \text{if } \sigma^{-1}(k) > \sigma^{-1}(k+1). \end{cases}$$

[**Note:** $\sigma^{-1}(i)$ is the **position** in which i appears in the one-line notation of σ. For example, if $\sigma = (5,1,2,3,6,4)$ in one-line notation, then $\sigma^{-1}(6) = 5$.]

Proof. **(b)** How do the inversions of $s_k \circ \sigma$ differ from the inversions of σ ?

I claim that they are the same, except that (when we go from σ to $s_k \circ \sigma$)

- if $\sigma^{-1}(k) < \sigma^{-1}(k+1)$, then we gain a new inversion $\left(\sigma^{-1}(k), \sigma^{-1}(k+1)\right)$;
- if $\sigma^{-1}(k) > \sigma^{-1}(k+1)$, then we lose an existing inversion $\left(\sigma^{-1}(k+1), \sigma^{-1}(k)\right)$.

For example, let

$$n = 7 \qquad \text{and} \qquad \sigma = (6,2,4,1,7,3,5) \qquad \text{and} \qquad k = 4.$$

Thus, $\sigma^{-1}(k) < \sigma^{-1}(k+1)$ and $s_k \circ \sigma = (6,2,5,1,7,3,4)$. So we gain a new inversion $(3,7)$ since $5 > 4$, but all other inversions remain the same.

For another example, let

$$n = 7 \qquad \text{and} \qquad \sigma = (3,1,4,2,7,6,5) \qquad \text{and} \qquad k = 2.$$

Thus, $\sigma^{-1}(k) > \sigma^{-1}(k+1)$ and $s_k \circ \sigma = (2,1,4,3,7,6,5)$. So we lose the inversion $(1,4)$ since $3 > 2$, but all other inversions remain the same.

Thus, when going from σ to $s_k \circ \sigma$, the # of inversions increases by 1 if $\sigma^{-1}(k) < \sigma^{-1}(k+1)$ and decreases by 1 if $\sigma^{-1}(k) > \sigma^{-1}(k+1)$. This is precisely the claim of **(b)**.

(a) Apply part **(b)** to σ^{-1} instead of σ. We get

$$\begin{aligned}
\ell\left(s_k \circ \sigma^{-1}\right) &= \begin{cases} \ell\left(\sigma^{-1}\right) + 1, & \text{if } \left(\sigma^{-1}\right)^{-1}(k) < \left(\sigma^{-1}\right)^{-1}(k+1); \\ \ell\left(\sigma^{-1}\right) - 1, & \text{if } \left(\sigma^{-1}\right)^{-1}(k) > \left(\sigma^{-1}\right)^{-1}(k+1) \end{cases} \\
&= \begin{cases} \ell(\sigma) + 1, & \text{if } \sigma(k) < \sigma(k+1); \\ \ell(\sigma) - 1, & \text{if } \sigma(k) > \sigma(k+1) \end{cases}
\end{aligned}$$

(since $\ell\left(\sigma^{-1}\right) = \ell(\sigma)$ (by previous Proposition) and $\left(\sigma^{-1}\right)^{-1} = \sigma$). On the other hand, the previous Proposition yields

$$\begin{aligned}
\ell\left(s_k \circ \sigma^{-1}\right) &= \ell\left(\underbrace{\left(s_k \circ \sigma^{-1}\right)^{-1}}_{\substack{=\left(\sigma^{-1}\right)^{-1} \circ (s_k)^{-1} \\ (\text{since } (\alpha\circ\beta)^{-1} = \beta^{-1}\circ\alpha^{-1})}}\right) = \ell\left(\underbrace{\left(\sigma^{-1}\right)^{-1}}_{=\sigma} \circ \underbrace{(s_k)^{-1}}_{\substack{=s_k \\ (\text{since } s_k \circ s_k = \mathrm{id})}}\right) \\
&= \ell(\sigma \circ s_k).
\end{aligned}$$

Comparing these equalities, we get

$$\ell(\sigma \circ s_k) = \begin{cases} \ell(\sigma) + 1, & \text{if } \sigma(k) < \sigma(k+1); \\ \ell(\sigma) - 1, & \text{if } \sigma(k) > \sigma(k+1). \end{cases}$$

(See [Grinbe15, Exercise 5.2 **(a)**] for a similar proof in more detail.) □

Remark 4.4.7. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Let $i, j \in [n]$ be such that $i < j$ and $\sigma(i) > \sigma(j)$. Is

$$\ell\left(\sigma \circ t_{i,j}\right) < \ell(\sigma) \ ?$$

It's not obvious, but the answer is "yes". See [Grinbe15, Exercise 5.20].

Recall: A **simple transposition** in S_n means one of the transpositions $s_1, s_2, \ldots, s_{n-1}$. We shall occasionally abbreviate "simple transposition" as "**simple**".

Theorem 4.4.8. Let $n \in \mathbb{N}$ and $\sigma \in S_n$.

(a) We can write σ as a composition of $\ell(\sigma)$ simples.

(b) The number $\ell(\sigma)$ is the smallest $p \in \mathbb{N}$ such that we can write σ as a composition of p simples.

[**Keep in mind:** The composition of 0 simples is id.]

Example 4.4.9. Let $\sigma \in S_4$ be the permutation $(4,1,3,2)$ (in one-line notation). How can we represent σ as a composition of simples? There are several ways to do so, for example

$$\sigma = \underbrace{s_2 \circ s_3 \circ s_2}_{=s_3 \circ s_2 \circ s_3} \circ s_1 = s_3 \circ s_2 \circ \underbrace{s_3 \circ s_1}_{=s_1 \circ s_3} = s_3 \circ s_2 \circ s_1 \circ s_3$$
$$= s_2 \circ s_1 \circ s_1 \circ s_3 \circ s_2 \circ s_1 = \cdots.$$

The shortest of these representations involve 4 simples, as the Theorem above predicts (since $\ell(\sigma) = 4$).

Proof. (Proof of Theorem.)

(a) Induction on $\ell(\sigma)$.

Induction base: If $\ell(\sigma) = 0$, then $\sigma = \mathrm{id}$, so we can write σ as a composition of 0 simples.

Induction step: Fix $h \in \mathbb{N}$. Assume (as the IH) that Theorem **(a)** holds for $\ell(\sigma) = h$.

Now, let $\sigma \in S_n$ be such that $\ell(\sigma) = h+1$.

Hence, $\ell(\sigma) = h+1 > 0$, so $\sigma \neq \mathrm{id}$.

Therefore, there exists some $k \in [n-1]$ such that $\sigma(k) > \sigma(k+1)$ (because otherwise, we would have $\sigma(1) \leq \sigma(2) \leq \cdots \leq \sigma(n)$, and this would imply $\ell(\sigma) = 0$, whence $\sigma = \mathrm{id}$). Fix such a k.

Part **(a)** of the previous proposition yields

$$\ell(\sigma \circ s_k) = \begin{cases} \ell(\sigma)+1, & \text{if } \sigma(k) < \sigma(k+1); \\ \ell(\sigma)-1, & \text{if } \sigma(k) > \sigma(k+1) \end{cases} = \underbrace{\ell(\sigma)}_{=h+1} - 1$$
$$= (h+1) - 1 = h.$$

Thus, the IH (applied to $\sigma \circ s_k$ instead of σ) shows that we can write $\sigma \circ s_k$ as a composition of $\ell(\sigma \circ s_k) = h$ simples:

$$\sigma \circ s_k = s_{i_1} \circ s_{i_2} \circ \cdots \circ s_{i_h} \qquad \text{for some } i_1, i_2, \ldots, i_h \in [n-1].$$

Composing both sides of this equality with $(s_k)^{-1}$, we obtain

$$\sigma = \left(s_{i_1} \circ s_{i_2} \circ \cdots \circ s_{i_h}\right) \circ \underbrace{(s_k)^{-1}}_{=s_k}$$
$$= \left(s_{i_1} \circ s_{i_2} \circ \cdots \circ s_{i_h}\right) \circ s_k = s_{i_1} \circ s_{i_2} \circ \cdots \circ s_{i_h} \circ s_k.$$

This shows that we can write σ as a composition of $h+1 = \ell(\sigma)$ simples. Thus, Theorem **(a)** holds for $\ell(\sigma) = h+1$. This completes the induction step, and so Theorem **(a)** is proved by induction.

[The idea behind this proof is known as "bubblesort".]

(b) Omitted.

(For details, see [Grinbe15, Exercise 5.2 **(g)**].) □

Corollary 4.4.10. Let $n \in \mathbb{N}$.

(a) We have $\ell(\sigma \circ \tau) \equiv \ell(\sigma) + \ell(\tau) \bmod 2$ for all $\sigma \in S_n$ and $\tau \in S_n$. (In other words, if $\ell(\sigma \circ \tau)$ is even, then $\ell(\sigma) + \ell(\tau)$ is even, and the same for "odd".)

(b) We have $\ell(\sigma \circ \tau) \leq \ell(\sigma) + \ell(\tau)$.

(c) If $\sigma = s_{k_1} \circ s_{k_2} \circ \cdots \circ s_{k_q}$, then $q \geq \ell(\sigma)$ and $q \equiv \ell(\sigma) \bmod 2$.

Example 4.4.11. Let $n = 4$ and $\sigma = (3,2,1,4)$ and $\tau = (3,1,4,2)$ in one-line notation. Then, $\ell(\sigma) = 3$ and $\ell(\tau) = 3$. Now, $\sigma \circ \tau = (1,3,4,2)$ has $\ell(\sigma \circ \tau) = 2$.

Corollary **(a)** says $\ell(\sigma \circ \tau) \equiv \ell(\sigma) + \ell(\tau) \bmod 2$. In other words, $2 \equiv 3 + 3 \bmod 2$.

Corollary **(b)** says $\ell(\sigma \circ \tau) \leq \ell(\sigma) + \ell(\tau)$. In other words, $2 \leq 3 + 3$.

Proof. (Proof of Corollary) See [Grinbe15, Exercises 5.2 and 5.3]. (Or do it yourself, e.g., by induction on $\ell(\sigma)$.) □

Proposition 4.4.12. Let $n \in \mathbb{N}$.

(a) We have $\ell(s_k) = 1$ for any $k \in [n-1]$.

(b) We have $\ell\left(t_{i,j}\right) = 2|i-j| - 1$ for any distinct $i, j \in [n]$.

(c) We have $\ell\left(\mathrm{cyc}_{i,i+1,\ldots,i+k-1}\right) = k-1$ for all i, k.

(d) We have $\ell\left(\mathrm{cyc}_{i_1,i_2,\ldots,i_k}\right) \geq k-1$ for all distinct $i_1, i_2, \ldots, i_k \in [n]$.

(e) We have $\ell(\mathrm{id}) = 0$ and $\ell(w_0) = \binom{n}{2}$. (Recall: w_0 is the "reflection across the middle of $[n]$".)

Proof. **(a)** follows from **(b)**.

(b) is [Grinbe15, Exercise 5.10 **(a)**], but also easy to check.

(c) and **(d)** are parts of [Grinbe15, Exercise 5.17].

(e) is trivial. □

Class of 2019-11-25

Remark 4.4.13. For a given k and n, how many $\sigma \in S_n$ have length k ?

- The # of $\sigma \in S_n$ having $\ell(\sigma) = 0$ is 1 (namely, just $\sigma = \mathrm{id}$).
- The # of $\sigma \in S_n$ having $\ell(\sigma) = 1$ is $n-1$ (namely, just $\sigma = s_k$ with $k \in [n-1]$).

- The # of $\sigma \in S_n$ having $\ell(\sigma) = 2$ is $(n-1)(n+1)/2$. (Exercise.)

What about the general case?
There is no explicit formula, but there is a generating function:

Proposition 4.4.14. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned}
&\sum_{w \in S_n} x^{\ell(w)} \\
&= \prod_{i=1}^{n-1} \left(1 + x + x^2 + \cdots + x^i\right) \\
&= (1+x) \cdot \left(1 + x + x^2\right) \cdot \left(1 + x + x^2 + x^3\right) \cdot \cdots \cdot \left(1 + x + x^2 + \cdots + x^{n-1}\right).
\end{aligned}$$

Example 4.4.15. Applying this to $n = 3$, we obtain

$$\sum_{w \in S_3} x^{\ell(w)} = (1+x) \cdot \left(1 + x + x^2\right).$$

Let us check this:

$$\begin{aligned}
\sum_{w \in S_3} x^{\ell(w)} &= x^{\ell(1,2,3)} + x^{\ell(1,3,2)} + x^{\ell(2,1,3)} + x^{\ell(2,3,1)} + x^{\ell(3,1,2)} + x^{\ell(3,2,1)} \\
&\qquad \text{(where we are writing each permutation in one-line notation)} \\
&= x^0 + x^1 + x^1 + x^2 + x^2 + x^3 = x^0 + 2x^1 + 2x^2 + x^3 \\
&= (1+x) \cdot \left(1 + x + x^2\right).
\end{aligned}$$

Proof. The proposition is [Grinbe15, Corollary 5.53], and a proof appears in [Grinbe15, solution to Exercise 5.18]. □

4.5. Descents

Definition 4.5.1. Let $n \in \mathbb{N}$ and $\sigma \in S_n$.
A **descent** of σ means a $k \in [n-1]$ such that $\sigma(k) > \sigma(k+1)$.
The **descent set** of σ, denoted $\operatorname{Des}\sigma$, is the set of all descents of σ.

Example 4.5.2. Let $\pi \in S_4$ be the permutation with one-line notation $(3,1,4,2)$. Then, 1 is a descent of π (since $\pi(1) = 3 > 1 = \pi(2)$), and so is 3, but not 2. Thus, $\operatorname{Des}\pi = \{1,3\}$.

Exercise 4.5.1. Fix $n \geq 4$.
(a) How many $\sigma \in S_n$ have 0 descents?
(b) How many $\sigma \in S_n$ have 1 descent?
(c) How many $\sigma \in S_n$ have $n-1$ descents?
(d) How many $\sigma \in S_n$ satisfy $1 \in \operatorname{Des}\sigma$ (that is, $\sigma(1) > \sigma(2)$) ?
(e) How many $\sigma \in S_n$ satisfy $1,2 \in \operatorname{Des}\sigma$ (that is, $\sigma(1) > \sigma(2) > \sigma(3)$) ?
(f) How many $\sigma \in S_n$ satisfy $1,3 \in \operatorname{Des}\sigma$ (that is, $\sigma(1) > \sigma(2)$ and $\sigma(3) > \sigma(4)$) ?

Proof. (Solution sketch.) **(a)** The answer is 1 (namely, $\sigma = \mathrm{id}$).
(d) The answer is $\dfrac{n!}{2}$.
First proof: The map

$$\{\sigma \in S_n \mid \sigma(1) > \sigma(2)\} \to \{\sigma \in S_n \mid \sigma(1) < \sigma(2)\}, \quad \sigma \mapsto \sigma \circ s_1$$

is bijective. So each of the 2 sets is half as large as S_n (because each $\sigma \in S_n$ satisfies either $\sigma(1) > \sigma(2)$ or $\sigma(1) < \sigma(2)$). But $|S_n| = n!$.
Second proof: To construct a $\sigma \in S_n$ satisfying $\sigma(1) > \sigma(2)$, we can proceed as follows:

- Choose the **set** $\{\sigma(1), \sigma(2)\}$. There are $\dbinom{n}{2}$ options.
- Thus, $\sigma(1)$ and $\sigma(2)$ are already uniquely determined, because they have to satisfy $\sigma(1) > \sigma(2)$.
- Choose $\sigma(3), \sigma(4), \ldots, \sigma(n)$. There are $(n-2)!$ options.

$\Longrightarrow$ The total # is $\dbinom{n}{2} \cdot (n-2)! = \dfrac{n!}{2!} = \dfrac{n!}{2}$.
(e) The answer is $\dfrac{n!}{3!}$.
For the detailed proof, see [18s-mt1s, solution to Exercise 2 **(b)**].
(f) The answer is $\dfrac{n!}{2! \cdot 2!} = \dfrac{n!}{4}$.
For the detailed proof, see [18s-mt1s, solution to Exercise 2 **(a)**].
More generally, you can ask how many permutations $\sigma \in S_n$ have a given bunch of numbers in their descent set. A similar question is answered in [18f-hw4s, Exercise 4 **(a)**].
(b) First of all, fix $i \in [n-1]$. How many $\sigma \in S_n$ have $\operatorname{Des}\sigma = \{i\}$?
In other words, how many $\sigma \in S_n$ satisfy

$$\sigma(1) < \sigma(2) < \cdots < \sigma(i) > \sigma(i+1) < \sigma(i+2) < \cdots < \sigma(n).$$

We have

$$(\#\text{ of } \sigma \in S_n \text{ such that } \sigma(1) < \sigma(2) < \cdots < \sigma(i) \text{ and } \sigma(i+1) < \sigma(i+2) < \cdots < \sigma(n)) = \binom{n}{i}$$

(because in order to construct such a σ, it suffices to choose the i-element subset $\{\sigma(1), \sigma(2), \ldots, \sigma(i)\}$ of $[n]$). Thus,

$$\begin{aligned}
&(\#\text{ of } \sigma \in S_n \text{ such that } \sigma(1) < \sigma(2) < \cdots < \sigma(i) > \sigma(i+1) < \sigma(i+2) < \cdots < \sigma(n)) \\
&= \underbrace{(\#\text{ of } \sigma \in S_n \text{ such that } \sigma(1) < \sigma(2) < \cdots < \sigma(i) \text{ and } \sigma(i+1) < \sigma(i+2) < \cdots < \sigma(n))}_{= \binom{n}{i}} \\
&- \underbrace{(\#\text{ of } \sigma \in S_n \text{ such that } \sigma(1) < \sigma(2) < \cdots < \sigma(i) < \sigma(i+1) < \sigma(i+2) < \cdots < \sigma(n))}_{=1} \\
&= \binom{n}{i} - 1.
\end{aligned}$$

Now, forget that we fixed i. Summing this over all $i \in [n-1]$, we get

$$\begin{aligned}
&(\#\text{ of } \sigma \in S_n \text{ that have exactly 1 descent}) \\
&= \sum_{i=1}^{n-1} \left(\binom{n}{i} - 1 \right) = \underbrace{\sum_{i=1}^{n-1} \binom{n}{i}}_{=2^n-2} - (n-1) = 2^n - 2 - (n-1) = 2^n - (n+1).
\end{aligned}$$

(c) Only 1 permutation $\sigma \in S_n$ has $n-1$ descents, namely w_0. □

4.6. Signs

Definition 4.6.1. Let $n \in \mathbb{N}$. The **sign** of a permutation $\sigma \in S_n$ is $(-1)^{\ell(\sigma)}$.
It is called $(-1)^{\sigma}$ or $\operatorname{sgn}(\sigma)$ or $\operatorname{sign}(\sigma)$ or $\varepsilon(\sigma)$.

Proposition 4.6.2. Let $n \in \mathbb{N}$.
(a) We have $(-1)^{\mathrm{id}} = 1$.
(b) We have $(-1)^{t_{i,j}} = -1$.
(c) We have $(-1)^{\mathrm{cyc}_{i_1,i_2,\ldots,i_k}} = (-1)^{k-1}$ for any $k \geq 1$ and any distinct $i_1, i_2, \ldots, i_k \in [n]$.
(d) We have $(-1)^{\sigma\circ\tau} = (-1)^{\sigma} \cdot (-1)^{\tau}$ for any $\sigma, \tau \in S_n$. (In the lingo of abstract algebra, this is saying "The sign is a group homomorphism from S_n to $\{1, -1\}$".)
(e) We have $(-1)^{\sigma_1\circ\sigma_2\circ\cdots\circ\sigma_p} = (-1)^{\sigma_1}(-1)^{\sigma_2}\cdots(-1)^{\sigma_p}$ for any $\sigma_1, \sigma_2, \ldots, \sigma_p \in S_n$.

(f) We have $(-1)^{\sigma^{-1}} = (-1)^{\sigma}$ for any $\sigma \in S_n$. (The LHS has to be read as $(-1)^{\left(\sigma^{-1}\right)}$.)

(g) We have

$$(-1)^{\sigma} = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \qquad \text{for each } \sigma \in S_n.$$

(h) If $x_1, x_2, \ldots, x_n$ are any numbers, and $\sigma \in S_n$, then

$$\prod_{1 \leq i < j \leq n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right) = (-1)^{\sigma} \prod_{1 \leq i < j \leq n} \left(x_i - x_j\right).$$

Proof. Most of this follows easily from what we have proved above, but here are references to complete proofs:

(a) This is [Grinbe15, Proposition 5.15 **(a)**].
(b) This is [Grinbe15, Exercise 5.10 **(b)**].
(c) This is [Grinbe15, Exercise 5.17 **(d)**].
(d) This is [Grinbe15, Proposition 5.15 **(c)**].
(e) This is [Grinbe15, Proposition 5.28].
(f) This is [Grinbe15, Proposition 5.15 **(d)**].
(g) This is [Grinbe15, Exercise 5.13 **(c)**].
(h) This is [Grinbe15, Exercise 5.13 **(a)**]. □

Definition 4.6.3. Let $n \in \mathbb{N}$. A permutation $\sigma \in S_n$ is said to be

- **even** if $(-1)^{\sigma} = 1$ (that is, if $\ell(\sigma)$ is even);
- **odd** if $(-1)^{\sigma} = -1$ (that is, if $\ell(\sigma)$ is odd).

Corollary 4.6.4. Let $n \geq 2$. Then,

$$(\#\text{ of even } \sigma \in S_n) = (\#\text{ of odd } \sigma \in S_n) = n!/2.$$

Proof. The map

$$\{\text{even } \sigma \in S_n\} \to \{\text{odd } \sigma \in S_n\}, \quad \sigma \mapsto \sigma \circ s_1$$

is a bijection. (See [Grinbe15, Exercise 5.4] for details.) □

Example 4.6.5. The 15-game

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 15 & 14 & \end{array} \longrightarrow \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & \end{array}$$

(via swaps of the empty cell with the neighboring square ("slides")) is unsolvable.

Why?

Proof sketch.

(a) Let us first consider the 3×3-analogue:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 8 & 7 & \end{array} \longrightarrow \begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & \end{array}.$$

This is also impossible.

Proof: For each position P, let σ_P be the permutation of $[8]$ whose one-line notation is what you get if you read P row by row from left to right.

$$P = \begin{array}{ccc} a & b & c \\ d & e & \\ f & g & h \end{array} \mapsto \sigma_P = (a,b,c,d,e,f,g,h) \text{ (in one-line notation).}$$

Now, a slide changes σ_P **either** not at all **or** by multiplying it with a $\underbrace{\text{3-cycle}}_{\substack{\text{cyc}_{p,q,r} \\ \text{for some } p,q,r}}$ (that is, σ_P becomes $\sigma_P \circ \text{cyc}_{p,q,r}$). Thus, the sign of σ_P never changes (since 3-cycles have sign 1). Thus, the 3×3-game is unsolvable (since the initial position and the target position have different signs of σ_P).

(b) Now to the 4×4-version.

The sign of σ_P is no longer invariant. Instead, every vertical slide flips the sign of σ_P. Therefore,

$$(-1)^{\sigma_P} \cdot (-1)^{\text{which row has an empty square}}$$

is invariant. This again proves that the game is unsolvable, because the initial and target positions have different values of this invariant.

Remark 4.6.6. For any $n \in \mathbb{N}$, the set of all even permutations $\sigma \in S_n$ is called the **alternating group** A_n.

2019-12-04 notes

5. Lattice paths (brief introduction)

We shall say a few words about lattice paths. See [18f, Chapter 6] for more, and see [Kratte17] for much more.

Definition 5.0.1. The **integer lattice** (or, for short, **lattice**) is the set $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$.

Its elements are called **points**; indeed, any element $(a, b) \in \mathbb{Z}^2$ can be identified with the point with coordinates a and b on the plane.

Points can be added and subtracted entrywise: e.g.,

$$(a, b) - (c, d) = (a - c, b - d) .$$

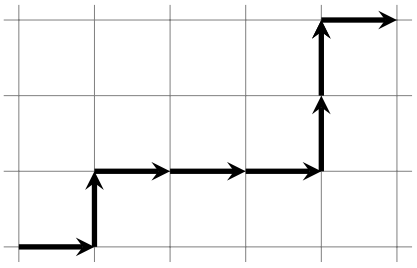
If $(a, b) \in \mathbb{Z}^2$ and $(c, d) \in \mathbb{Z}^2$ are two points, then a **lattice path** (for short, **LP**) from (a, b) to (c, d) means

- (informally) a path from (a, b) to (c, d) that uses only 2 kinds of steps:
  - "up-steps" (U) going $(p, q) \mapsto (p, q + 1)$;
  - "right-steps" (R) going $(p, q) \mapsto (p + 1, q)$.
- (rigorously) a tuple $(v_0, v_1, \ldots, v_n)$ of points $v_i \in \mathbb{Z}^2$ such that

$$v_0 = (a, b) \qquad \text{and} \qquad v_n = (c, d)$$

$$\text{and} \qquad v_i - v_{i-1} \in \left\{ \underbrace{(0, 1)}_{\text{up-step}}, \ \underbrace{(1, 0)}_{\text{right-step}} \right\} \qquad \text{for each } i \in [n] .$$

Example 5.0.2. The following picture shows an LP from $(0, 0)$ to $(5, 3)$:



Formally speaking, this LP is the 9-tuple

$$((0, 0) , (1, 0) , (1, 1) , (2, 1) , (3, 1) , (4, 1) , (4, 2) , (4, 3) , (5, 3)) .$$

Its "step sequence" (i.e., the sequence of the directions of its steps) is $RURRRUUR$ (meaning that its first step is a right-step, its second step is an up-step, its third step is a right-step, and so on).

Note that any LP is uniquely determined by its starting point and its "step sequence".

Proposition 5.0.3. Let $(a,b) \in \mathbb{Z}^2$ and $(c,d) \in \mathbb{Z}^2$ be two points. Then,

$$(\#\text{ of LPs from } (a,b) \text{ to } (c,d)) = \begin{cases} \dbinom{c+d-a-b}{c-a}, & \text{if } c+d \geq a+b; \\ 0, & \text{if } c+d < a+b \end{cases}.$$

Proof. In each LP, the x-coordinates of the points weakly increase at each step, and so do the y-coordinates. Thus, LPs from (a,b) to (c,d) can only exist when $c \geq a$ and $d \geq b$.

Furthermore, each step of a LP increases

$$(\text{x-coordinate}) + (\text{y-coordinate})$$

by exactly 1 (in the sense that if (x_i, y_i) and (x_{i+1}, y_{i+1}) are two consecutive points on an LP, then $x_{i+1} + y_{i+1} = (x_i + y_i) + 1$). Hence, each LP $(v_0, v_1, \ldots, v_n)$ from (a,b) to (c,d) must have $n = c+d-a-b$. Thus, if $c+d < a+b$, then the # of LPs from (a,b) to (c,d) is 0. Otherwise, the bijection

$$\{\text{LPs from } (a,b) \text{ to } (c,d)\} \to \{(c-a)\text{-element subsets of } [c+d-a-b]\}, \\ (v_0, v_1, \ldots, v_n) \mapsto \{i \in [n] \mid v_i - v_{i-1} = (1,0)\}$$

shows that the # of LPs is $\dbinom{c+d-a-b}{c-a}$. □

Definition 5.0.4. Let $\mathbf{v} = (v_0, v_1, \ldots, v_n)$ be a LP from (a,b) to (c,d). Let $p \in \mathbb{Z}^2$. We say that $p \in \mathbf{v}$ (in words: p **lies on** $\mathbf{v}$) if $p \in \{v_0, v_1, \ldots, v_n\}$.

Exercise 5.0.1. Find the # of LPs $\mathbf{v}$ from $(0,0)$ to $(6,6)$ such that $(2,2) \in \mathbf{v}$.

Proof. (Solution sketch.) Each such $\mathbf{v}$ consists of a LP from $(0,0)$ to $(2,2)$ and a LP from $(2,2)$ to $(6,6)$. Thus, the product rule yields

$$(\#\text{ of LPs } \mathbf{v} \text{ from } (0,0) \text{ to } (6,6) \text{ such that } (2,2) \in \mathbf{v}) \\ = \underbrace{(\#\text{ of LPs from } (0,0) \text{ to } (2,2))}_{= \binom{2+2-0-0}{2-0}} \cdot \underbrace{(\#\text{ of LPs from } (2,2) \text{ to } (6,6))}_{= \binom{6+6-2-2}{6-2}}.$$

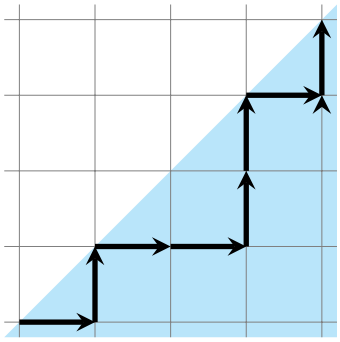
□

We shall now introduce a special class of LPs:

Definition 5.0.5. A LP $\mathbf{v}$ is said to be **Catalan** if $x \geq y$ for each $(x, y) \in \mathbf{v}$.
(Visually, this means that $\mathbf{v}$ never strays above the diagonal $x = y$.)

(In [18f], I say "legal" instead of "Catalan".)

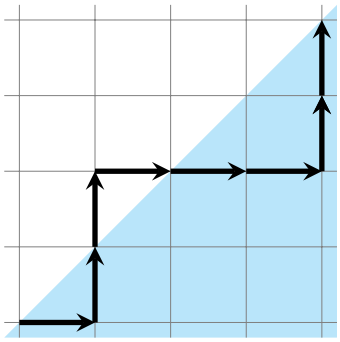
Example 5.0.6. The following picture shows a Catalan LP from $(0, 0)$ to $(4, 4)$:



.

(Here, the region shaded cyan is the set of all $(x, y) \in \mathbb{R}^2$ satisfying $x \geq y$; this is the region in which a Catalan LP must stay.)

The following LP from $(0, 0)$ to $(4, 4)$ is **not** Catalan:



.

Definition 5.0.7. If $n, m \in \mathbb{Z}$, then we set

$$L_{n,m} = (\text{\# of Catalan LPs from } (0,0) \text{ to } (n,m)).$$

Proposition 5.0.8. **(a)** We have $L_{n,m} = L_{n-1,m} + L_{n,m-1}$ for any $n \in \mathbb{Z}$ and $m \in \mathbb{Z}$ satisfying $n \geq m$ and $(n, m) \neq (0, 0)$.

(b) If $n \in \mathbb{N}$ and $m \in \mathbb{N}$ satisfy $n < m$, then $L_{n,m} = 0$.

(c) If $n \in \mathbb{N}$ and $m \in \mathbb{N}$ satisfy $n \geq m - 1$, then

$$L_{n,m} = \binom{n+m}{m} - \binom{n+m}{m-1}.$$

(d) If $n \in \mathbb{N}$ and $m \in \mathbb{N}$ satisfy $n \geq m - 1$, then

$$L_{n,m} = \frac{n+1-m}{n+1}\binom{n+m}{m}.$$

(e) For any $n \in \mathbb{N}$, we have

$$L_{n,n} = \frac{1}{n+1}\binom{2n}{n}.$$

Proof. Main idea: Recall the notion of "upsided tuples" from MT3 exercise 4. There is a bijection

$$\begin{aligned}&\{\text{Catalan LPs from } (0,0) \text{ to } (n,m)\}\\ &\to \{\text{upsided } (n+m)\text{-tuples } (i_1,i_2,\ldots,i_{n+m}) \text{ with } i_1+i_2+\cdots+i_{n+m}=n\},\\ &(v_0,v_1,\ldots,v_{n+m}) \mapsto (i_1,i_2,\ldots,i_{n+m}), \qquad \text{where } i_k = [v_k - v_{k-1} = (1,0)].\end{aligned}$$

Thus, the claims of **(b)** and **(c)** follow from MT3 exercise 4. The claim of **(d)** follows by simple algebra from **(c)**. The claim of **(e)** follows by applying **(d)** to $m = n$. The claim of **(a)** follows by looking at the last step of a Catalan LP. □

Definition 5.0.9. For any $n \in \mathbb{N}$, the number $L_{n,n} = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1}$ is called the ***n*-th Catalan number** and is denoted by C_n.

A whole book ([Stanle15]) has been written about Catalan numbers. A few other places where they appear are:

- Let us say that a permutation $\sigma \in S_n$ is **123-avoiding** if there exist no $i < j < k$ in $[n]$ such that $\sigma(i) < \sigma(j) < \sigma(k)$. Then, the # of 123-avoiding permutations $\sigma \in S_n$ is C_n.
- Consider all possible ways to fully parenthesize a given expression $a_1 + a_2 + \cdots + a_n$. For example, for $n = 4$, these are

  $$\begin{aligned}&(a_1+a_2)+(a_3+a_4), \qquad &&(a_1+(a_2+a_3))+a_4,\\ &a_1+((a_2+a_3)+a_4), \qquad &&a_1+(a_2+(a_3+a_4)),\\ &((a_1+a_2)+a_3)+a_4.\end{aligned}$$

  For any $n \in \mathbb{N}$, there are C_{n-1} ways to do this.
- Fix an $n \geq 3$, and a convex n-gon G_n. How many ways are there to triangulate G_n (i.e., to subdivide G_n into triangles whose vertices are vertices of G_n) ?

  The answer is C_{n-2}.

There are several variations on Catalan numbers and Catalan LPs, such as ***r*-Catalan numbers**.

6. Generating functions (introduction)

We have already seen a few generating functions. Here are two more examples.

Basic idea: Any sequence $(a_0, a_1, a_2, \ldots)$ of numbers gives rise to a "power series" $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$, called its "**generating function**". What exactly it is is a question that would take us a while (see [Loehr11, Chapter 7 (in the 1st edition)] or [Niven69] or [19s, Chapter 7]), but let us just calculate with these generating functions as if they were polynomials in x. (Of course, they are not literally polynomials in x, since they can have infinitely many nonzero coefficients.)

Example 1. Recall the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ with

$$f_0 = 0, \qquad f_1 = 1, \qquad f_n = f_{n-1} + f_{n-2}.$$

Consider its gf (= generating function)

$$\begin{aligned} F(x) &= f_0 + f_1 x + f_2 x^2 + \cdots \\ &= 0 + 1x + 1x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \cdots . \end{aligned}$$

Then,

$$\begin{aligned} F(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + \cdots \\ &= \underbrace{0 + 1x}_{=x} + \underbrace{\left(f_1 + f_0\right) x^2 + \left(f_2 + f_1\right) x^3 + \left(f_3 + f_2\right) x^4 + \cdots}_{\substack{= \left(f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right) \\ + \left(f_0 x^2 + f_1 x^3 + f_2 x^4 + \cdots\right)}} \\ &= x + \underbrace{\left(f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right)}_{\substack{= f_0 x + f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots \\ \text{(since } f_0 = 0\text{)}}} + \left(f_0 x^2 + f_1 x^3 + f_2 x^4 + \cdots\right) \\ &= x + \underbrace{\left(f_0 x + f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right)}_{= xF(x)} + \underbrace{\left(f_0 x^2 + f_1 x^3 + f_2 x^4 + \cdots\right)}_{= x^2 F(x)} \\ &= x + xF(x) + x^2 F(x). \end{aligned}$$

Solving this equation for $F(x)$, we get

$$F(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \phi x)(1 - \psi x)}$$

where $\phi = \dfrac{1 + \sqrt{5}}{2}$ and $\psi = \dfrac{1 - \sqrt{5}}{2}$ are the "golden ratios". Applying partial fraction decomposition to the RHS, we obtain

$$F(x) = \frac{x}{(1 - \phi x)(1 - \psi x)} = \frac{1}{\sqrt{5}} \cdot \frac{1}{1 - \phi x} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1 - \psi x}.$$

Now, what are the coefficients of $\dfrac{1}{1-\alpha x}$ for $\alpha \in \mathbb{C}$?

Well:

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots,$$

because

$$\begin{aligned}
&(1-x)\left(1 + x + x^2 + x^3 + \cdots\right) \\
&= \left(1 + x + x^2 + x^3 + \cdots\right) - x\left(1 + x + x^2 + x^3 + \cdots\right) \\
&= \left(1 + x + x^2 + x^3 + \cdots\right) - \left(x + x^2 + x^3 + \cdots\right) = 1.
\end{aligned}$$

If we substitute αx for x here, we obtain

$$\begin{aligned}
\frac{1}{1-\alpha x} &= 1 + \alpha x + (\alpha x)^2 + (\alpha x)^3 + \cdots \\
&= 1 + \alpha x + \alpha^2 x^2 + \alpha^3 x^3 + \cdots.
\end{aligned}$$

Thus, our formula for $F(x)$ becomes

$$\begin{aligned}
F(x) &= \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\phi x} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\psi x} \\
&= \frac{1}{\sqrt{5}} \cdot \left(1 + \phi x + \phi^2 x^2 + \phi^3 x^3 + \cdots\right) - \frac{1}{\sqrt{5}} \cdot \left(1 + \psi x + \psi^2 x^2 + \psi^3 x^3 + \cdots\right) \\
&= \frac{1-1}{\sqrt{5}} + \frac{\phi - \psi}{\sqrt{5}} x + \frac{\phi^2 - \psi^2}{\sqrt{5}} x^2 + \frac{\phi^3 - \psi^3}{\sqrt{5}} x^3 + \cdots.
\end{aligned}$$

Now, comparing coefficients before x^n, we get

$$f_n = \frac{\phi^n - \psi^n}{\sqrt{5}} \qquad \text{for each } n \in \mathbb{N}.$$

This is exactly Binet's formula. Unlike the first time we saw it, we now have a motivated "proof" of it.

However, of course, this is only a proof if we can explain

- what a power series is;
- what x is;
- why we can divide by power series like $1 - x - x^2$;
- why we can substitute αx for x into a power series;
- why we can expand infinite sums;
- ...

This is done nicely in [Loehr11, Chapter 7 (in the 1st edition)] and [19s, Chapter 7] and [21s] and in most detailed textbooks on abstract algebra.

[18f, Chapter 8] gives a quick overview. So does [Niven69]. Many applications are found in [Wilf09].

7. Solutions and references to the exercises

This chapter contains solutions to the exercises not solved in the text, or references to places where these solutions can be found.

7.1. Solution to Exercise 1.3.1

Exercise 1.3.1 appears in [17f-hw2s, Exercise 1 **(a)**] and in [Grinbe15, Exercise 3.2 **(a)**]. The following solution is taken from [17f-hw2s]:

Solution to Exercise 1.3.1. We have

$$(2n)! = 1 \cdot 2 \cdot \cdots \cdot (2n) = \prod_{k \in \{1,2,\ldots,2n\}} k = \underbrace{\left(\prod_{\substack{k \in \{1,2,\ldots,2n\}; \\ k \text{ is even}}} k \right)}_{\substack{= 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (2n) \\ = \prod_{i=1}^{n} (2i) \\ = 2^n \prod_{i=1}^{n} i}} \underbrace{\left(\prod_{\substack{k \in \{1,2,\ldots,2n\}; \\ k \text{ is odd}}} k \right)}_{= 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}$$

$$\left(\begin{array}{c} \text{here, we have split the product } \prod_{k \in \{1,2,\ldots,2n\}} k \text{ into one product} \\ \text{containing all even } k \text{ and one product containing all odd } k \end{array} \right)$$

$$= 2^n \underbrace{\left(\prod_{i=1}^{n} i \right)}_{= 1 \cdot 2 \cdot \cdots \cdot n = n!} \cdot (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1))$$

$$= 2^n n! \cdot (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) .$$

Dividing this equality by $2^n n!$, we obtain

$$\frac{(2n)!}{2^n n!} = 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1) = (2n-1) \cdot (2n-3) \cdot \cdots \cdot 1.$$

This solves Exercise 1.3.1. □

7.2. Solution to Exercise 1.3.2

Solution to Exercise 1.3.2. Theorem 1.3.11 (applied to $k = n$) yields

$$\binom{n}{n} = \binom{n}{n-n} = \binom{n}{0} \qquad (\text{since } n - n = 0)$$
$$= 1 \qquad (\text{by (44)}) .$$

This solves Exercise 1.3.2. □

7.3. Reference to solution to Exercise 1.3.3

Parts **(a)**, **(b)**, **(c)**, **(d)** and **(e)** of Exercise 1.3.3 appear (with solution) in [17f-hw1s, Exercise 1] and in [Grinbe15, Exercise 3.12]. Thus, it remains to solve part **(f)**:

Solution to Exercise 1.3.3 (f). **(f)** We shall show that

$$[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_n] = [\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_n] \tag{256}$$

for each $n \in \{0, 1, \ldots, k\}$.

[*Proof of (256):* We shall prove (256) by induction on n:

Induction base: The conjunction $\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_0$ of no statements is a true statement (by definition), and thus its truth value is 1. In other words, $[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_0] = 1$. Comparing this with $[\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_0] = (\text{empty product}) = 1$, we obtain $[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_0] = [\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_0]$. In other words, (256) holds for $n = 0$. This completes the induction base.

Induction step: Let $m \in \{0, 1, \ldots, k\}$ be positive. Assume that (256) holds for $n = m - 1$. We must prove that (256) holds for $n = m$ as well.

We have assumed that (256) holds for $n = m - 1$. In other words, we have

$$[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}] = [\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_{m-1}] .$$

But the statement $\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_m$ is equivalent to $(\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}) \wedge \mathcal{A}_m$ [233]. Hence, Exercise 1.3.3 **(a)** (applied to $\mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_m$ and $\mathcal{B} = (\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}) \wedge \mathcal{A}_m$) yields

$$\begin{aligned}
&[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_m] \\
&= [(\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}) \wedge \mathcal{A}_m] \\
&= \underbrace{[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}]}_{=[\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_{m-1}]} [\mathcal{A}_m] \\
&\qquad (\text{by Exercise 1.3.3 } \textbf{(c)}, \text{ applied to } \mathcal{A} = \mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1} \text{ and } \mathcal{B} = \mathcal{A}_m) \\
&= ([\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_{m-1}]) \cdot [\mathcal{A}_m] \\
&= [\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_m] .
\end{aligned}$$

In other words, (256) holds for $n = m$. This completes the induction step. Thus, the induction proof of (256) is complete.]

Now, (256) (applied to $n = k$) yields $[\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_k] = [\mathcal{A}_1] \cdot [\mathcal{A}_2] \cdot \cdots \cdot [\mathcal{A}_k]$. This solves Exercise 1.3.3 **(f)**. □

[233] Make sure you understand why this is true even for $m = 1$! (In this case, it comes helpful that the conjunction $\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_0$ of no statements was defined to be a true statement, so that $(\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_0) \wedge \mathcal{A}_1$ is equivalent to $\mathcal{A}_1$.)

7.4. Solution to Exercise 1.3.4

In order to solve Exercise 1.3.4, we must prove Lemma 1.3.17 without using Theorem 1.3.12. Here is such a proof:

Second proof of Lemma 1.3.17. Forget that we fixed n and k. We shall prove Lemma 1.3.17 by induction on n:

Induction base: For each $k \in \mathbb{Z}$, we have

$$\begin{aligned}\binom{0}{k} &= [k=0] && \text{(by Lemma 1.3.14)}\\ &\in \{0,1\} && \text{(since } [\mathcal{A}] \in \{0,1\} \text{ for any statement } \mathcal{A}\text{)}\\ &\subseteq \mathbb{N}.\end{aligned}$$

Thus, we have $\binom{0}{k} \in \mathbb{N}$ for each $k \in \mathbb{Z}$. In other words, Lemma 1.3.17 holds for $n = 0$. Thus, the induction base is complete.

Induction step: Let m be a positive integer. Assume that Lemma 1.3.17 holds for $n = m-1$. We must prove that Lemma 1.3.17 holds for $n = m$.

Let $k \in \mathbb{Z}$. Recall that Lemma 1.3.17 holds for $n = m-1$ (by our assumption). Thus, Lemma 1.3.17 (applied to $m-1$ instead of n) yields $\binom{m-1}{k} \in \mathbb{N}$. Also, Lemma 1.3.17 (applied to $m-1$ and $k-1$ instead of n and k) yields $\binom{m-1}{k-1} \in \mathbb{N}$ (because Lemma 1.3.17 holds for $n = m-1$). Now, Theorem 1.3.8 (applied to $n = m$) yields

$$\binom{m}{k} = \underbrace{\binom{m-1}{k-1}}_{\in \mathbb{N}} + \underbrace{\binom{m-1}{k}}_{\in \mathbb{N}} \in \mathbb{N}$$

(since the sum of two elements of $\mathbb{N}$ is always an element of $\mathbb{N}$).

Forget that we fixed k. We thus have proven that $\binom{m}{k} \in \mathbb{N}$ for each $k \in \mathbb{Z}$. In other words, Lemma 1.3.17 holds for $n = m$. This completes the induction step. Thus, the inductive proof of Lemma 1.3.17 is finished. □

7.5. Reference to solution to Exercise 1.3.5

Proposition 1.3.33 is proved in [17f-hw2s, Exercise 1 **(b)**], in [Grinbe15, Exercise 3.2 **(b)**] and in [18f-hw3s, Exercise 3 **(a)**].

7.6. Solution to Exercise 1.3.6

First solution to Exercise 1.3.6. If $n = 0$, then Exercise 1.3.6 holds[234]. Hence, for the rest of this solution, we can WLOG assume that $n \neq 0$. Assume this. Combining $n \neq 0$ with $n \in \mathbb{N}$, we obtain $n \in \{1, 2, 3, \ldots\}$, so that $n - 1 \in \mathbb{N}$.

We have

$$\sum_{k=0}^{n} k\binom{n}{k} = \underbrace{0\binom{n}{0}}_{=0} + \sum_{k=1}^{n} k \underbrace{\binom{n}{k}}_{\substack{=\frac{n}{k}\binom{n-1}{k-1} \\ \text{(by Proposition 1.3.36,} \\ \text{applied to } n \text{ and } k \\ \text{instead of } m \text{ and } n)}} \qquad \left(\begin{array}{c}\text{here, we have split off the} \\ \text{addend for } k = 0 \text{ from the sum}\end{array}\right)$$

$$= \sum_{k=1}^{n} \underbrace{k \cdot \frac{n}{k}}_{=n} \binom{n-1}{k-1} = \sum_{k=1}^{n} n\binom{n-1}{k-1}$$

$$= \sum_{k=0}^{n-1} n\binom{n-1}{k} \qquad \left(\begin{array}{c}\text{here, we have substituted } k \\ \text{for } k-1 \text{ in the sum}\end{array}\right)$$

$$= n \underbrace{\sum_{k=0}^{n-1} \binom{n-1}{k}}_{\substack{=2^{n-1} \\ \text{(by Corollary 1.3.27,} \\ \text{applied to } n-1 \text{ instead of } n)}} \qquad \text{(by an application of (32))}$$

$$= n \cdot 2^{n-1}.$$

This solves Exercise 1.3.6. □

Second solution to Exercise 1.3.6. The following solution uses the same "Little Gauss" trick that you have seen in the second proof of Theorem 1.2.1, except that we are

[234] *Proof.* Assume that $n = 0$. Then, $\sum_{k=0}^{n} k\binom{n}{k} = \sum_{k=0}^{0} k\binom{0}{k} = 0\binom{0}{0} = 0$. Comparing this with $\underbrace{n}_{=0} \cdot 2^{n-1} = 0$, we obtain $\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}$. Thus, we have solved Exercise 1.3.6 under the assumption that $n = 0$.

now using the summation sign. We have

$$2 \cdot \sum_{k=0}^{n} k\binom{n}{k} = \sum_{k=0}^{n} k\binom{n}{k} + \sum_{k=0}^{n} k\binom{n}{k} = \sum_{k=0}^{n} k\binom{n}{k} + \sum_{k=0}^{n} (n-k) \underbrace{\binom{n}{n-k}}_{=\binom{n}{k}} \quad \text{(by Theorem 1.3.11)}$$

$$= \sum_{k=0}^{n} k\binom{n}{k} + \sum_{k=0}^{n} (n-k)\binom{n}{k} = \sum_{k=0}^{n} \underbrace{\left(k\binom{n}{k} + (n-k)\binom{n}{k}\right)}_{=(k+(n-k))\binom{n}{k}}$$

(here, we have substituted $n-k$ for k in the second sum)

(by an application of (31))

$$= \sum_{k=0}^{n} \underbrace{(k+(n-k))}_{=n}\binom{n}{k} = \sum_{k=0}^{n} n\binom{n}{k} = n \underbrace{\sum_{k=0}^{n}\binom{n}{k}}_{=2^n} \quad \text{(by Corollary 1.3.27)}$$

(by an application of (32))

$$= n \cdot 2^n.$$

Dividing both sides of this equality by 2, we obtain $\sum_{k=0}^{n} k\binom{n}{k} = n \cdot \underbrace{2^n/2}_{=2^{n-1}} = n \cdot 2^{n-1}$.

This solves Exercise 1.3.6 again. □

Another solution to Exercise 1.3.6 can be found in Section 1.6: The claim of the exercise comes out (as Corollary 1.6.5) of comparing the results of two different solutions to Exercise 1.6.1.

7.7. Solution to Exercise 1.4.1

In order to solve Exercise 1.4.1, we must prove Theorem 1.4.1.

First proof of Theorem 1.4.1. Forget that we fixed n and S.

We proceed by induction on n:

Induction base: If S is a 0-element set, then $S = \varnothing$ and thus

$$\begin{aligned}(\#\text{ of subsets of } S) &= (\#\text{ of subsets of } \varnothing) \\ &= 1 \qquad \left(\begin{array}{c}\text{since the empty set } \varnothing \text{ has only one subset,} \\ \text{namely the empty subset } \varnothing\end{array}\right) \\ &= 2^0 \qquad \left(\text{since } 2^0 = 1\right).\end{aligned}$$

In other words, for any 0-element set S, we have $(\#\text{ of subsets of } S) = 2^0$. Thus, Theorem 1.4.1 is proven for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume (as the induction hypothesis) that Theorem 1.4.1 holds for $n = m$.

Let S be an $(m+1)$-element set. We must prove that

$$(\#\text{ of subsets of } S) = 2^{m+1}.$$

The set S is an $(m+1)$-element set; thus, its size is $|S| = m+1 \geq 1 > 0$. Hence, the set S is nonempty, i.e., there exists a $t \in S$. Fix such a t.

Now, we shall call a subset of S

- **red** if it contains t, and
- **green** if it does not contain t.

Thus, each subset of S is either red or green (but not both at the same time). Thus, by the sum rule, we have

$$(\#\text{ of subsets of } S) = (\#\text{ of red subsets of } S) + (\#\text{ of green subsets of } S)\,.$$

We shall now compute the two addends on the right hand side.

The green subsets of S are the subsets of S that don't contain t. In other words, the green subsets of S are exactly the subsets of $S \setminus \{t\}$. Hence,

$$(\#\text{ of green subsets of } S) = (\#\text{ of subsets of } S \setminus \{t\})\,. \tag{257}$$

But S is an $(m+1)$-element set, and thus $S \setminus \{t\}$ is an m-element set (since $t \in S$). Hence, our induction hypothesis shows that Theorem 1.4.1 can be applied to m and $S \setminus \{t\}$ instead of n and S. We thus obtain

$$(\#\text{ of subsets of } S \setminus \{t\}) = 2^m.$$

Hence, (257) becomes

$$(\#\text{ of green subsets of } S) = (\#\text{ of subsets of } S \setminus \{t\}) = 2^m. \tag{258}$$

What about the red subsets?

Informally, a similar argument works: The red subsets of S are not exactly the subsets of $S \setminus \{t\}$, but they "correspond to" the latter in a specific way. Namely, since the red subsets of S are required to contain t, the only "information" that a red subset of S really "carries" is what other elements (other than t) it contains. In other words, each red subset R of S "corresponds to" the subset $R \setminus \{t\}$ of $S \setminus \{t\}$.

Formally, this can be restated as follows: The map

$$\begin{aligned} f : \{\text{red subsets of } S\} &\to \{\text{subsets of } S \setminus \{t\}\}\,, \\ R &\mapsto R \setminus \{t\} \end{aligned}$$

is well-defined and is a bijection.[235] Therefore, the bijection principle (applied to the bijection f) yields

$$|\{\text{red subsets of } S\}| = |\{\text{subsets of } S \setminus \{t\}\}|.$$

In other words,

$$(\#\text{ of red subsets of } S) = (\#\text{ of subsets of } S \setminus \{t\}). \tag{259}$$

But $S \setminus \{t\}$ is an m-element set. Hence, our induction hypothesis shows that Theorem 1.4.1 can be applied to m and $S \setminus \{t\}$ instead of n and S. We thus obtain

$$(\#\text{ of subsets of } S \setminus \{t\}) = 2^m.$$

Hence, (259) becomes

$$(\#\text{ of red subsets of } S) = (\#\text{ of subsets of } S \setminus \{t\}) = 2^m. \tag{260}$$

Now, we can finish our computation of $(\#\text{ of subsets of } S)$ that we started above:

$$\begin{aligned}(\#\text{ of subsets of } S) &= \underbrace{(\#\text{ of red subsets of } S)}_{\substack{=2^m \\ \text{(by (260))}}} + \underbrace{(\#\text{ of green subsets of } S)}_{\substack{=2^m \\ \text{(by (258))}}} \\ &= 2^m + 2^m = 2 \cdot 2^m = 2^{m+1}.\end{aligned}$$

Now, forget that we fixed S. We thus have shown that every $(m+1)$-element set S satisfies

$$(\#\text{ of subsets of } S) = 2^{m+1}.$$

In other words, Theorem 1.4.1 holds for $n = m+1$. This completes the induction step, and thus the proof of Theorem 1.4.1. □

7.8. Solution to Exercise 1.4.2

In order to solve Exercise 1.4.2, we need to prove Proposition 1.4.13.

Proof of Proposition 1.4.13. The set S has size $|S| = m$ (since it is an m-element set). Thus, it is finite. Hence, Proposition 1.4.11 yields that there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers satisfying $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$. Consider this tuple, and denote it by $(t_1, t_2, \ldots, t_p)$. Thus, $(t_1, t_2, \ldots, t_p)$ is the unique tuple of integers satisfying $\{t_1, t_2, \ldots, t_p\} = S$ and $t_1 < t_2 < \cdots < t_p$. From $t_1 < t_2 < \cdots < t_p$, we conclude that the p numbers $t_1, t_2, \ldots, t_p$ are distinct. Hence, the set $\{t_1, t_2, \ldots, t_p\}$ has size p. In other words, $|\{t_1, t_2, \ldots, t_p\}| = p$. In view of $\{t_1, t_2, \ldots, t_p\} = S$, this rewrites as $|S| = p$. Comparing this with $|S| = m$, we obtain $p = m$.

[235] This can be showed in the same way as we proved the corresponding claim in our proof of Theorem 1.3.12.

Recall that the tuple $(t_1, t_2, \ldots, t_p)$ is a p-tuple of integers satisfying $\{t_1, t_2, \ldots, t_p\} = S$ and $t_1 < t_2 < \cdots < t_p$. In view of $p = m$, we can rewrite this as follows: The tuple $(t_1, t_2, \ldots, t_m)$ is an m-tuple of integers satisfying $\{t_1, t_2, \ldots, t_m\} = S$ and $t_1 < t_2 < \cdots < t_m$. Hence, there exists **at least one** m-tuple $(s_1, s_2, \ldots, s_m)$ of integers satisfying $\{s_1, s_2, \ldots, s_m\} = S$ and $s_1 < s_2 < \cdots < s_m$ (namely, the m-tuple $(t_1, t_2, \ldots, t_m)$). Furthermore, there exists **at most one** such m-tuple $(s_1, s_2, \ldots, s_m)$ [236]. Combining the claims of the preceding two sentences, we conclude that there exists a **unique** m-tuple $(s_1, s_2, \ldots, s_m)$ of integers satisfying $\{s_1, s_2, \ldots, s_m\} = S$ and $s_1 < s_2 < \cdots < s_m$. This proves Proposition 1.4.13. □

7.9. Reference to solution to Exercise 1.4.6

Exercise 1.4.6 is [17f-hw1s, Exercise 5].

7.10. Reference to solution to Exercise 1.4.7

Exercise 1.4.7 is [17f-hw1s, Exercise 6].

7.11. Reference to solution to Exercise 1.4.8

Exercise 1.4.8 is [17f-hw3s, Exercise 3].

7.12. Reference to solution to Exercise 1.5.1

Parts **(a)**, **(b)** and **(c)** of Exercise 1.5.1 are [17f-hw3s, Exercise 1].

Part **(d)** of Exercise 1.5.1 is [19f-hw2s, Exercise 2].

Part **(e)** of Exercise 1.5.1 is [19f-mt1s, Exercise 2].

7.13. Reference to solution to Exercise 1.5.2

Exercise 1.5.2 is [17f-hw3s, Exercise 4].

7.14. Reference to solution to Exercise 2.1.1

Exercise 2.1.1 **(a)** is essentially [18f-hw2s, Exercise 4]. (More precisely, [18f-hw2s, Exercise 4] is the particular case of Exercise 2.1.1 **(a)** where n is assumed to be a positive integer. However, the first two solutions to [18f-hw2s, Exercise 4] apply

[236] *Proof.* Recall that $(t_1, t_2, \ldots, t_p)$ is the **unique** tuple $(s_1, s_2, \ldots, s_k)$ of integers satisfying $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$. Hence, if $(s_1, s_2, \ldots, s_k)$ is any tuple of integers satisfying $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$, then $(s_1, s_2, \ldots, s_k)$ must equal $(t_1, t_2, \ldots, t_p)$. Applying this to $k = m$, we conclude that if $(s_1, s_2, \ldots, s_m)$ is any m-tuple of integers satisfying $\{s_1, s_2, \ldots, s_m\} = S$ and $s_1 < s_2 < \cdots < s_m$, then $(s_1, s_2, \ldots, s_m)$ must equal $(t_1, t_2, \ldots, t_p)$. Thus, there exists **at most one** such m-tuple $(s_1, s_2, \ldots, s_m)$.

just as well to the general case. Only the third solution to [18f-hw2s, Exercise 4] really requires n to be a positive integer.)

Let us solve Exercise 2.1.1 **(b)** now. In order to do so, we need to prove Proposition 1.3.28 again:

*Alternative proof of Proposition 1.3.28 using Exercise 2.1.1 **(a)**.* If $n = 0$, then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0}^{0} (-1)^k \binom{0}{k} = \underbrace{(-1)^0}_{=1} \underbrace{\binom{0}{0}}_{\substack{=1 \\ \text{(by (44))}}} = 1$$

$$= [n = 0] \qquad (\text{since } [n = 0] = 1 \text{ (because } n = 0)).$$

Thus, Proposition 1.3.28 is proved in the case when $n = 0$. Hence, for the rest of this proof, we WLOG assume that $n \neq 0$. Thus, $[n = 0] = 0$. Also, n is a positive integer (since $n \in \mathbb{N}$ and $n \neq 0$), and thus $n - 1 \in \mathbb{N}$. Furthermore, $n > n - 1$. Hence, Proposition 1.3.6 (applied to $n - 1$ and n instead of n and k) yields $\binom{n-1}{n} = 0$. Now, Exercise 2.1.1 **(a)** (applied to $m = n$) yields

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = (-1)^n \underbrace{\binom{n-1}{n}}_{=0} = 0 = [n = 0]$$

(since $[n = 0] = 0$). This proves Proposition 1.3.28. □

Thus, Exercise 2.1.1 **(b)** is solved.

7.15. Reference to solution to Exercise 2.2.1

Exercise 2.2.1 is [17f-hw2s, Exercise 2].

7.16. Solution to Exercise 2.2.2

In order to solve Exercise 2.2.2, we need to prove Theorem 2.2.2. Let us now do this:

Proof of Theorem 2.2.2. The set $X \times Y$ is finite (since X and Y are finite). Thus, the set S is finite (since S is a subset of $X \times Y$).

The elements of S are pairs $(x, y) \in X \times Y$ with $x \in X$ and $y \in Y$ (since S is a subset of $X \times Y$). Let $f : S \to X$ be the map that sends each pair $(x, y) \in S$ to its first entry $x \in X$. Then, Theorem 1.2.5 (applied to $W = X$) yields

$$|S| = \sum_{w \in X} (\#\text{ of } s \in S \text{ satisfying } f(s) = w). \tag{261}$$

Now, fix $w \in X$. We have assumed that for each $x \in X$, there are precisely a_2 many elements $y \in Y$ such that $(x,y) \in S$. Applying this to $x = w$, we conclude that there are precisely a_2 many elements $y \in Y$ such that $(w,y) \in S$. In other words,

$$(\#\text{ of elements } y \in Y \text{ such that } (w,y) \in S) = a_2. \tag{262}$$

We shall next prove that

$$(\#\text{ of elements } y \in Y \text{ such that } (w,y) \in S) = (\#\text{ of } s \in S \text{ satisfying } f(s) = w).$$

Indeed, this will follow from the bijection principle, once we have set up the appropriate bijections. Let us do this now:

If y is an element of Y satisfying $(w,y) \in S$, then the pair (w,y) is an $s \in S$ satisfying $f(s) = w$ (since the definition of f yields $f((w,y)) = w$). Hence, the map

$$\begin{aligned} \alpha : \{y \in Y \mid (w,y) \in S\} &\to \{s \in S \mid f(s) = w\}, \\ y &\mapsto (w,y) \end{aligned}$$

is well-defined.

On the other hand, recall again that the elements of S are pairs $(x,y) \in X \times Y$ with $x \in X$ and $y \in Y$. In other words, they are pairs $(u,v) \in X \times Y$ with $u \in X$ and $v \in Y$. If (u,v) is an element s of S satisfying $f(s) = w$, then v is an element $y \in Y$ such that $(w,y) \in S$ [237]. Hence, the map

$$\begin{aligned} \beta : \{s \in S \mid f(s) = w\} &\to \{y \in Y \mid (w,y) \in S\}, \\ (u,v) &\mapsto v \end{aligned}$$

is well-defined.

It is straightforward to see that our maps α and β are mutually inverse[238]. Thus, α and β are bijections. Hence, the bijection principle yields

$$|\{y \in Y \mid (w,y) \in S\}| = |\{s \in S \mid f(s) = w\}|.$$

[237] *Proof.* Let (u,v) be an element s of S satisfying $f(s) = w$. Thus, $(u,v) \in S$ and $f((u,v)) = w$. But the definition of f yields $f((u,v)) = u$, so that $u = f((u,v)) = w$. Hence, $(u,v) = (w,v)$, so that $(w,v) = (u,v) \in S$. In other words, v is an element $y \in Y$ such that $(w,y) \in S$.

[238] *Proof.* We need to show that $\alpha \circ \beta = \mathrm{id}$ and $\beta \circ \alpha = \mathrm{id}$. The second of these two equalities is easy to check; we thus only need to prove the first one.

Let s be an element of S satisfying $f(s) = w$. Write s in the form $s = (u,v)$ for some $u \in U$ and $v \in V$. (We can do this, since every element of S has this form.) Now, $f(s) = w$ rewrites as $f((u,v)) = w$ (since $s = (u,v)$), so that $w = f((u,v)) = u$ (by the definition of f). Hence, $(w,v) = (u,v) = s$. But the definition of β yields $\beta((u,v)) = v$. This rewrites as $\beta(s) = v$ (since $s = (u,v)$). Applying the map α to both sides of this equality, we obtain

$$\begin{aligned} \alpha(\beta(s)) &= \alpha(v) = (w,v) \qquad \text{(by the definition of } \alpha) \\ &= s. \end{aligned}$$

Thus, $(\alpha \circ \beta)(s) = \alpha(\beta(s)) = s = \mathrm{id}(s)$.

Forget that we fixed s. We thus have showed that $(\alpha \circ \beta)(s) = \mathrm{id}(s)$ for each $s \in S$ satisfying $f(s) = w$. In other words, $\alpha \circ \beta = \mathrm{id}$. This completes our proof that α and β are mutually inverse (since $\beta \circ \alpha = \mathrm{id}$).

In other words,

$$(\#\text{ of elements } y \in Y \text{ such that } (w,y) \in S) = (\#\text{ of } s \in S \text{ satisfying } f(s) = w).$$

Comparing this with (262), we find

$$(\#\text{ of } s \in S \text{ satisfying } f(s) = w) = a_2. \tag{263}$$

Now, forget that we fixed w. We thus have proved (263) for each $w \in X$. Thus, (261) becomes

$$|S| = \sum_{w \in X} \underbrace{(\#\text{ of } s \in S \text{ satisfying } f(s) = w)}_{\substack{=a_2 \\ \text{(by (263))}}} = \sum_{w \in X} a_2 = \underbrace{|X|}_{=a_1} \cdot a_2 = a_1 a_2.$$

This proves Theorem 2.2.2. □

7.17. Reference to solution to Exercise 2.2.3

Exercise 2.2.3 is [17f-hw1s, Exercise 3].

7.18. Solution to Exercise 2.2.4

In order to solve Exercise 2.2.4, we must prove Proposition 2.2.4.

Proof of Proposition 2.2.4. We are in one of the following three cases:
Case 1: We have $b \notin \mathbb{N}$.
Case 2: We have $b \in \mathbb{N}$ and $a \notin \mathbb{N}$.
Case 3: We have $b \in \mathbb{N}$ and $a \in \mathbb{N}$.

Let us first consider Case 1. In this case, we have $b \notin \mathbb{N}$. Hence, (43) (applied to a and b instead of n and k) yields $\binom{a}{b} = 0$. Likewise, (43) (applied to $n-a+b$ and b instead of n and k) yields $\binom{n-a+b}{b} = 0$. Now, comparing $\binom{n}{a}\underbrace{\binom{a}{b}}_{=0} = 0$ with $\binom{n}{a-b}\underbrace{\binom{n-a+b}{b}}_{=0} = 0$, we obtain $\binom{n}{a}\binom{a}{b} = \binom{n}{a-b}\binom{n-a+b}{b}$. Hence, Proposition 2.2.4 is proved in Case 1.

Let us now consider Case 2. In this case, we have $b \in \mathbb{N}$ and $a \notin \mathbb{N}$. Hence, $a-b \notin \mathbb{N}$ (because if we had $a-b \in \mathbb{N}$, then we would have $a = \underbrace{(a-b)}_{\in\mathbb{N}} + \underbrace{b}_{\in\mathbb{N}} \in \mathbb{N}$, which would contradict $a \notin \mathbb{N}$). Thus, (43) (applied to $k = a-b$) yields $\binom{n}{a-b} = 0$. Moreover, (43) (applied to $k = a$) yields $\binom{n}{a} = 0$ (since $a \notin \mathbb{N}$). Now,

comparing $\underbrace{\binom{n}{a}}_{=0}\binom{a}{b} = 0$ with $\underbrace{\binom{n}{a-b}}_{=0}\binom{n-a+b}{b} = 0$, we obtain $\binom{n}{a}\binom{a}{b} = \binom{n}{a-b}\binom{n-a+b}{b}$. Hence, Proposition 2.2.4 is proved in Case 2.

Finally, let us consider Case 3. In this case, we have $b \in \mathbb{N}$ and $a \in \mathbb{N}$. Therefore, Theorem 1.3.11 (applied to a and b instead of n and k) yields $\binom{a}{b} = \binom{a}{a-b}$. Multiplying this equality by $\binom{n}{a}$, we find

$$\begin{aligned}\binom{n}{a}\binom{a}{b} &= \binom{n}{a}\binom{a}{a-b} = \binom{n}{a-b}\binom{n-(a-b)}{a-(a-b)} \\ &\qquad \text{(by Proposition 1.3.35, applied to } a-b \text{ instead of } b\text{)} \\ &= \binom{n}{a-b}\binom{n-a+b}{b} \qquad \text{(since } n-(a-b) = n-a+b \text{ and } a-(a-b) = b\text{)}.\end{aligned}$$

Thus, Proposition 2.2.4 is proved in Case 3.

We have now proved Proposition 2.2.4 in all three cases 1, 2 and 3. Thus, Proposition 2.2.4 always holds. □

7.19. Solution to Exercise 2.4.1

Solution to Exercise 2.4.1. **(a)** Informally speaking, the claim of Exercise 2.4.1 **(a)** is obvious: The maps $f : A \to B$ satisfying $f(A) \subseteq C$ are "the same as" the maps from A to C, since their values belong to C; thus, the # of the former maps equals the # of the latter maps, which is $|C|^{|A|}$ (by Theorem 2.4.1, applied to C instead of B).

But from a rigorous point of view, this argument is not precise; the maps $f : A \to B$ satisfying $f(A) \subseteq C$ are not literally maps from A to C, even though their values belong to C (unless, of course, $C = B$). In fact, a map (as defined nowadays) "knows" what its domain and its codomain are; thus, two maps with different codomains cannot be equal, even if they have the same domain and the same value on each element of this domain.

Thus, we need to slightly refine our argument. If $f : A \to B$ is a map satisfying $f(A) \subseteq C$, then we can define a map

$$\begin{aligned} f\mid^{C} : A &\to C, \\ a &\mapsto f(a) \end{aligned}$$

(because each $a \in A$ satisfies $f(a) \in f(A) \subseteq C$). This map $f\mid^{C}$ may be called the *corestriction* of f to C. (Unlike a restriction, it has the same domain as A but a different codomain. Informally, you can think of $f\mid^{C}$ as being the map f "wearing

a tighter cloak".) Thus, the map

$$\begin{aligned} &\{\text{maps } f : A \to B \text{ satisfying } f(A) \subseteq C\} \to \{\text{maps from } A \text{ to } C\}, \\ &\qquad f \mapsto f\mid^{C} \end{aligned} \tag{264}$$

is well-defined. Conversely, if g is any map from A to C, then we can define a map

$$\begin{aligned} g\mid^{B} : A &\to B, \\ a &\mapsto g(a) \end{aligned}$$

(because each $a \in A$ satisfies $g(a) \in C \subseteq B$), and this map $g\mid^{B}$ is a map $f : A \to B$ satisfying $f(A) \subseteq C$ (since $\left(g\mid^{B}\right)(A) = g(A) \subseteq C$). Thus, the map

$$\begin{aligned} &\{\text{maps from } A \text{ to } C\} \to \{\text{maps } f : A \to B \text{ satisfying } f(A) \subseteq C\}, \\ &\qquad g \mapsto g\mid^{B} \end{aligned} \tag{265}$$

is well-defined. Note that neither of the two maps (264) and (265) changes the values of the map they are being applied to; all they change is the codomain. Thus, it is clear that the two maps (264) and (265) are mutually inverse; hence, they are bijections. Thus, the bijection principle yields

$$|\{\text{maps } f : A \to B \text{ satisfying } f(A) \subseteq C\}| = |\{\text{maps from } A \text{ to } C\}|.$$

In other words,

$$(\#\text{ of maps } f : A \to B \text{ satisfying } f(A) \subseteq C) = (\#\text{ of maps from } A \text{ to } C) = |C|^{|A|}$$

(by Theorem 2.4.1, applied to C, $|A|$ and $|C|$ instead of B, m and n). This solves Exercise 2.4.1 **(a)**.

(b) In the above solution to Exercise 2.4.1 **(a)**, we have defined a map $f\mid^{C} : A \to C$ for each map $f : A \to B$ satisfying $f(A) \subseteq C$. Thus, in particular, the map $f\mid^{C} : A \to C$ is defined for each map $f : A \to B$ satisfying $f(A) = C$ (because $f(A) = C$ implies $f(A) \subseteq C$). Moreover, it is easy to see that if $f : A \to B$ is a map satisfying $f(A) = C$, then the map $f\mid^{C} : A \to C$ is surjective (because its image is $\left(f\mid^{C}\right)(A) = f(A) = C$). Hence, the map

$$\begin{aligned} &\{\text{maps } f : A \to B \text{ satisfying } f(A) = C\} \to \{\text{surjective maps from } A \text{ to } C\}, \\ &\qquad f \mapsto f\mid^{C} \end{aligned} \tag{266}$$

is well-defined. Conversely, if g is any surjective map from A to C, then the map $g\mid^{B}$ can be defined as in our above solution to Exercise 2.4.1 **(a)**; this latter map $g\mid^{B}$ is a map $f : A \to B$ satisfying $f(A) = C$ (since $\left(g\mid^{B}\right)(A) = g(A) = C$ (because g is surjective)). Thus, the map

$$\begin{aligned} &\{\text{surjective maps from } A \text{ to } C\} \to \{\text{maps } f : A \to B \text{ satisfying } f(A) = C\}, \\ &\qquad g \mapsto g\mid^{B} \end{aligned} \tag{267}$$

is well-defined. It is easy to see that the two maps (266) and (267) are mutually inverse[239]; hence, they are bijections. Thus, the bijection principle yields

$$|\{\text{maps } f : A \to B \text{ satisfying } f(A) = C\}| = |\{\text{surjective maps from } A \text{ to } C\}|.$$

In other words,

$$(\#\text{ of maps } f : A \to B \text{ satisfying } f(A) = C) = (\#\text{ of surjective maps from } A \text{ to } C).$$

This solves Exercise 2.4.1 **(b)**. □

7.20. Solution to Exercise 2.4.2

Solution to Exercise 2.4.2. We need to prove the equalities (168) and (169) rigorously. The equality (168) can be proved either using the sum rule or using the product rule; the equality (169) can only be proved using the sum rule[240]. Thus, in order to be maximally consistent, we shall prove both equalities using the sum rule.

[*Proof of (168):* If $f : [m] \to [n]$ is a red surjection, then $f(m)$ is some element of $[n]$ (since $m \in \{1, 2, \ldots, m\} = [m]$). Thus, the sum rule yields

$$\begin{aligned}&(\#\text{ of red surjections } f : [m] \to [n])\\ &= \sum_{i \in [n]} (\#\text{ of red surjections } f : [m] \to [n] \text{ such that } f(m) = i). \end{aligned} \tag{268}$$

But let $i \in [n]$. Then, the map

$$\{\text{red surjections } f : [m] \to [n] \text{ such that } f(m) = i\} \to \{\text{surjections from } [m-1] \text{ to } [n]\},$$
$$f \mapsto f|_{[m-1]}$$

is well-defined (because if $f : [m] \to [n]$ is a red surjection, then its restriction $f|_{[m-1]} : [m-1] \to [n]$ is "still" a surjection), and is a bijection[241]. Thus, the bijection principle yields

$$\begin{aligned}&(\#\text{ of red surjections } f : [m] \to [n] \text{ such that } f(m) = i)\\ &= (\#\text{ of surjections from } [m-1] \text{ to } [n])\\ &= \operatorname{sur}(m-1, n)\end{aligned} \tag{269}$$

[239] Indeed, this can be proven just as in our above solution to Exercise 2.4.1 **(a)**.

[240] since the options available for $f(1), f(2), \ldots, f(m-1)$ in our proof of (169) depend on the choice of $f(m)$

[241] Indeed, its inverse is the map

$$\{\text{surjections from } [m-1] \text{ to } [n]\} \to \{\text{red surjections } f : [m] \to [n] \text{ such that } f(m) = i\},$$
$$g \mapsto (\text{the extension of } g \text{ to } [m] \text{ that sends } m \text{ to } i).$$

It is straightforward to see that this is well-defined.

(by (162), applied to $m-1$ instead of m).

Now, forget that we fixed i. Hence, we have proved (269) for each $i \in [n]$. Thus, (268) becomes

$$\begin{aligned}
&(\#\text{ of red surjections } f : [m] \to [n]) \\
&= \sum_{i \in [n]} \underbrace{(\#\text{ of red surjections } f : [m] \to [n] \text{ such that } f(m) = i)}_{\substack{=\operatorname{sur}(m-1,n) \\ \text{(by (269))}}} \\
&= \sum_{i \in [n]} \operatorname{sur}(m-1,n) = \underbrace{|[n]|}_{=n} \cdot \operatorname{sur}(m-1,n) = n \cdot \operatorname{sur}(m-1,n).
\end{aligned}$$

This formally proves (168).]

[*Proof of (169):* If $f : [m] \to [n]$ is a green surjection, then $f(m)$ is some element of $[n]$. Thus, the sum rule yields

$$\begin{aligned}
&(\#\text{ of green surjections } f : [m] \to [n]) \\
&= \sum_{i \in [n]} (\#\text{ of green surjections } f : [m] \to [n] \text{ such that } f(m) = i). \qquad (270)
\end{aligned}$$

But let $i \in [n]$. Thus, $[n] \setminus \{i\}$ is an $(n-1)$-element set (since $[n]$ is an n-element set). Also, $[m-1]$ is an $(m-1)$-element set. Now, the map[242]

$$\begin{aligned}
&\{\text{green surjections } f : [m] \to [n] \text{ such that } f(m) = i\} \\
&\to \{\text{surjections from } [m-1] \text{ to } [n] \setminus \{i\}\}, \\
&f \mapsto f|^{[n]\setminus\{i\}}_{[m-1]}
\end{aligned}$$

is well-defined (because if $f : [m] \to [n]$ is a green surjection, then its restriction $f|_{[m-1]}$ has image $[n] \setminus \{i\}$, and thus can be regarded as a surjective map from $[m-1]$ to $[n] \setminus \{i\}$), and is a bijection[243]. Thus, the bijection principle yields

$$\begin{aligned}
&(\#\text{ of green surjections } f : [m] \to [n] \text{ such that } f(m) = i) \\
&= (\#\text{ of surjections from } [m-1] \text{ to } [n] \setminus \{i\}) \\
&= (\#\text{ of surjective maps from } [m-1] \text{ to } [n] \setminus \{i\}) \\
&= \operatorname{sur}(m-1, n-1) \qquad (271)
\end{aligned}$$

[242] Here, $f|^{[n]\setminus\{i\}}_{[m-1]}$ means the restriction $f|_{[m-1]}$, regarded as a map from $[m-1]$ to $[n] \setminus \{i\}$. (This is well-defined, because if $f : [m] \to [n]$ is a green surjection such that $f(m) = i$, then the image of $f|_{[m-1]}$ is $[n] \setminus \{i\}$.)

[243] Indeed, its inverse is the map

$$\begin{aligned}
\{\text{surjections from } [m-1] \text{ to } [n] \setminus \{i\}\} &\to \{\text{green surjections } f : [m] \to [n] \text{ such that } f(m) = i\}, \\
g &\mapsto (\text{the extension of } g \text{ to } [m] \text{ that sends } m \text{ to } i).
\end{aligned}$$

It is straightforward to see that this is well-defined.

(by Proposition 2.4.11, applied to $m-1$, $n-1$, $[m-1]$ and $[n] \setminus \{i\}$).

Now, forget that we fixed i. Hence, we have proved (271) for each $i \in [n]$. Thus, (270) becomes

$$\begin{aligned}
&(\#\text{ of green surjections } f : [m] \to [n]) \\
&= \sum_{i \in [n]} \underbrace{(\#\text{ of green surjections } f : [m] \to [n] \text{ such that } f(m) = i)}_{\substack{=\operatorname{sur}(m-1,n-1) \\ \text{(by (271))}}} \\
&= \sum_{i \in [n]} \operatorname{sur}(m-1,n-1) = \underbrace{|[n]|}_{=n} \cdot \operatorname{sur}(m-1,n-1) = n \cdot \operatorname{sur}(m-1,n-1).
\end{aligned}$$

This formally proves (169).]

Thus, Exercise 2.4.2 is solved. □

7.21. Solution to Exercise 2.4.3

In order to solve Exercise 2.4.3, we need to prove Corollary 2.4.15.

Proof of Corollary 2.4.15. **(a)** We shall prove Corollary 2.4.15 **(a)** by induction on n:

Induction base: Proposition 2.4.12 **(a)** (applied to $m = 0$) yields $\operatorname{sur}(0,0) = [0=0] = 1 = 0!$ (since $0! = 1$). In other words, Corollary 2.4.15 **(a)** holds for $n = 0$. This completes the induction base.

Induction step: Let k be a positive integer. Assume that Corollary 2.4.15 **(a)** holds for $n = k-1$. We must prove that Corollary 2.4.15 **(a)** holds for $n = k$.

We have assumed that Corollary 2.4.15 **(a)** holds for $n = k-1$. In other words, $\operatorname{sur}(k-1,k-1) = (k-1)!$.

We have $k-1 \in \mathbb{N}$ (since k is a positive integer) and $k-1 < k$. Hence, Proposition 2.4.12 **(f)** (applied to $m = k-1$ and $n = k$) yields $\operatorname{sur}(k-1,k) = 0$.

Now, Proposition 2.4.14 (applied to $m = k$ and $n = k$) yields

$$\operatorname{sur}(k,k) = k \cdot \left(\underbrace{\operatorname{sur}(k-1,k)}_{=0} + \underbrace{\operatorname{sur}(k-1,k-1)}_{=(k-1)!} \right) = k \cdot (k-1)! = (k-1)! \cdot k.$$

Comparing this with

$$k! = (k-1)! \cdot k \qquad \text{(by Proposition 1.3.2, applied to } n = k\text{)},$$

we obtain $\operatorname{sur}(k,k) = k!$. In other words, Corollary 2.4.15 **(a)** holds for $n = k$. This completes the induction step. Thus, Corollary 2.4.15 **(a)** is proven by induction.

(b) We shall prove Corollary 2.4.15 **(b)** by induction on m:

Induction base: It is easy to see that the integer $\operatorname{sur}(0,n)$ is a multiple of $n!$ for all $n \in \mathbb{N}$ [244]. In other words, Corollary 2.4.15 **(b)** holds for $m = 0$. This completes the induction base.

Induction step: Let k be a positive integer. Assume that Corollary 2.4.15 **(b)** holds for $m = k-1$. We must prove that Corollary 2.4.15 **(b)** holds for $m = k$. In other words, we must prove that the integer $\operatorname{sur}(k,n)$ is a multiple of $n!$ for all $n \in \mathbb{N}$.

So let $n \in \mathbb{N}$. We must prove that the integer $\operatorname{sur}(k,n)$ is a multiple of $n!$. If $n = 0$, then this is obvious[245]. Thus, for the rest of this proof, we WLOG assume that $n \neq 0$. Thus, n is a positive integer. Proposition 2.4.14 (applied to $m = k$) thus yields

$$\operatorname{sur}(k,n) = n \cdot (\operatorname{sur}(k-1,n) + \operatorname{sur}(k-1,n-1)).$$

Also, Proposition 1.3.2 yields $n! = (n-1)! \cdot n$.

But we have assumed that Corollary 2.4.15 **(b)** holds for $m = k-1$. Thus, Corollary 2.4.15 **(b)** (applied to $k-1$ instead of m) yields that the integer $\operatorname{sur}(k-1,n)$ is a multiple of $n!$. Hence, $\operatorname{sur}(k-1,n) = n! \cdot a$ for some integer a. Consider this a.

Likewise, Corollary 2.4.15 **(b)** (applied to $k-1$ and $n-1$ instead of m and n) yields that the integer $\operatorname{sur}(k-1,n-1)$ is a multiple of $(n-1)!$. Hence, we have $\operatorname{sur}(k-1,n-1) = (n-1)! \cdot b$ for some integer b. Consider this b.

Now,

$$\begin{aligned}\operatorname{sur}(k,n) &= n \cdot \left(\underbrace{\operatorname{sur}(k-1,n)}_{=n! \cdot a} + \underbrace{\operatorname{sur}(k-1,n-1)}_{=(n-1)! \cdot b} \right) = n \cdot (n! \cdot a + (n-1)! \cdot b) \\ &= n \cdot n! \cdot a + \underbrace{n \cdot (n-1)!}_{=(n-1)! \cdot n = n!} \cdot b = n \cdot n! \cdot a + n! \cdot b = n! \cdot (na + b).\end{aligned}$$

This shows that the integer $\operatorname{sur}(k,n)$ is a multiple of $n!$.

Forget that we fixed n. We thus have shown that the integer $\operatorname{sur}(k,n)$ is a multiple of $n!$ for all $n \in \mathbb{N}$. In other words, Corollary 2.4.15 **(b)** holds for $m = k$. This completes the induction step. Thus, Corollary 2.4.15 **(b)** is proven by induction. □

Thus, Exercise 2.4.3 is solved.

7.22. Solution to Exercise 2.4.4

In order to solve Exercise 2.4.4, we need to prove Theorem 2.4.17. Before we do so, let us state a simple corollary of the binomial formula:

[244] *Proof.* Let $n \in \mathbb{N}$. We need to prove that $\operatorname{sur}(0,n)$ is a multiple of $n!$. We have $\operatorname{sur}(0,n) = [n=0]$ (by Proposition 2.4.12 **(d)**, applied to $k = n$). Hence, if $n \neq 0$, then $\operatorname{sur}(0,n) = [n=0] = 0$ (since $n \neq 0$) is clearly a multiple of $n!$. Thus, our proof is complete if $n \neq 0$. Hence, for the rest of this proof, we WLOG assume that $n = 0$. Thus, $n! = 0! = 1$, so that every integer is a multiple of $n!$. Hence, in particular, $\operatorname{sur}(0,n)$ is a multiple of $0!$. Qed.

[245] *Proof.* Assume that $n = 0$. Thus, $n! = 0! = 1$. Hence, every integer is a multiple of $n!$. Thus, in particular, $\operatorname{sur}(k,n)$ is a multiple of $n!$.

Corollary 7.22.1. Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Then,

$$(x+1)^n - x^n = \sum_{j=0}^{n-1} \binom{n}{j} x^j.$$

Proof of Corollary 7.22.1. Theorem 1.3.24 (applied to $y = 1$) yields

$$\begin{aligned}
(x+1)^n &= \sum_{k=0}^{n} \binom{n}{k} x^k \underbrace{1^{n-k}}_{=1} = \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{j=0}^{n} \binom{n}{j} x^j \\
&\qquad \text{(here, we have renamed the summation index } k \text{ as } j\text{)} \\
&= \sum_{j=0}^{n-1} \binom{n}{j} x^j + \underbrace{\binom{n}{n}}_{\substack{=1 \\ \text{(by Exercise 1.3.2)}}} x^n \\
&\qquad \text{(here, we have split off the addend for } j = n \text{ from the sum)} \\
&= \sum_{j=0}^{n-1} \binom{n}{j} x^j + x^n.
\end{aligned}$$

Subtracting x^n from this equality, we find $(x+1)^n - x^n = \sum_{j=0}^{n-1} \binom{n}{j} x^j$. This proves Corollary 7.22.1. □

Proof of Theorem 2.4.17. We shall prove Theorem 2.4.17 by strong induction over m:

Induction step: Let $q \in \mathbb{N}$. Assume that Theorem 2.4.17 holds for all $m < q$. We must now prove that Theorem 2.4.17 holds for $m = q$.

We have assumed that Theorem 2.4.17 holds for all $m < q$. In other words, we have

$$\operatorname{sur}(m,n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^m \tag{272}$$

for every $m \in \mathbb{N}$ and $n \in \mathbb{N}$ satisfying $m < q$.

Now, let $n \in \mathbb{N}$. We are going to prove that

$$\operatorname{sur}(q,n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q. \tag{273}$$

[*Proof of (273):* If $q = 0$, then (273) is easy to check[246]. Hence, for the rest of this proof, we WLOG assume that $q \neq 0$. Hence, $q \in \{1, 2, 3, \ldots\}$ (since $q \in \mathbb{N}$), so that $q > 0$. Since $q \neq 0$, we have $[q = 0] = 0$.

[246] *Proof.* Assume that $q = 0$. Thus, $\operatorname{sur}(q,n) = \operatorname{sur}(0,n) = [n = 0]$ (by Proposition 2.4.12 **(d)**,

If $n = 0$, then (273) is also easy to check[247]. Hence, for the rest of this proof, we WLOG assume that $n \neq 0$. Hence, $n \in \{1, 2, 3, \ldots\}$ (since $n \in \mathbb{N}$), so that $n > 0$. Hence, $n - 1 \in \mathbb{N}$. Therefore, for every $m \in \mathbb{N}$ satisfying $m < q$, we have

$$\operatorname{sur}(m, n-1) = \sum_{i=0}^{n-1} (-1)^{(n-1)-i} \binom{n-1}{i} i^m \tag{274}$$

(by (272) (applied to $n-1$ instead of n)).

Applying Proposition 2.4.13 to $m = q$, we find

$$\operatorname{sur}(q, n) = \sum_{j=1}^{q} \binom{q}{j} \cdot \operatorname{sur}(q-j, n-1) = \sum_{j=0}^{q-1} \binom{q}{j} \cdot \operatorname{sur}(j, n-1).$$

---

applied to $k = n$). Comparing this with

$$\begin{aligned}
\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q &= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \underbrace{i^0}_{=1} \qquad \text{(since } q = 0\text{)} \\
&= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} = \sum_{k=0}^{n} (-1)^{n-k} \underbrace{\binom{n}{k}}_{=\binom{n}{n-k}} \\
&\qquad \text{(by Theorem 1.3.11)} \\
&\qquad \text{(here, we have renamed the summation index } i \text{ as } k\text{)} \\
&= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{n-k} = \sum_{k=0}^{n} (-1)^{k} \binom{n}{k} \qquad \left(\begin{array}{c}\text{here, we have substituted } k \\ \text{for } n-k \text{ in the sum}\end{array}\right) \\
&= [n = 0] \qquad \text{(by Proposition 1.3.28)},
\end{aligned}$$

we obtain $\operatorname{sur}(q, n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q$. Thus, we have proven (273) under the assumption that $q = 0$.

[247] *Proof.* Assume that $n = 0$. Thus, $\operatorname{sur}(q, n) = \operatorname{sur}(q, 0) = [q = 0]$ (by Proposition 2.4.12 **(a)**, applied to $m = q$). Thus, $\operatorname{sur}(q, n) = [q = 0] = 0$. Comparing this with

$$\begin{aligned}
\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q &= \sum_{i=0}^{0} (-1)^{0-i} \binom{0}{i} i^q \qquad \text{(since } n = 0\text{)} \\
&= \underbrace{(-1)^{0-0}}_{=1} \underbrace{\binom{0}{0}}_{=1} 0^q = 0^q = 0 \qquad \text{(since } q > 0\text{)},
\end{aligned}$$

we obtain $\operatorname{sur}(q, n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q$. Thus, we have proven (273) under the assumption that $n = 0$.

Hence,

$$\operatorname{sur}(q,n) = \sum_{j=0}^{q-1} \binom{q}{j} \cdot \underbrace{\operatorname{sur}(j,n-1)}_{\substack{=\sum_{i=0}^{n-1}(-1)^{(n-1)-i}\binom{n-1}{i}i^j \\ \text{(by (274) (applied to } m=j\text{)} \\ \text{(since } j\leq q-1<q \text{ and } j\in\mathbb{N}\text{))}}}$$

$$= \sum_{j=0}^{q-1} \binom{q}{j} \cdot \sum_{i=0}^{n-1} (-1)^{(n-1)-i} \binom{n-1}{i} i^j = \underbrace{\sum_{j=0}^{q-1} \sum_{i=0}^{n-1}}_{=\sum_{i=0}^{n-1}\sum_{j=0}^{q-1}} \binom{q}{j} (-1)^{(n-1)-i} \binom{n-1}{i} i^j$$

$$= \sum_{i=0}^{n-1} \sum_{j=0}^{q-1} \binom{q}{j} (-1)^{(n-1)-i} \binom{n-1}{i} i^j$$

$$= \sum_{i=0}^{n-1} (-1)^{(n-1)-i} \binom{n-1}{i} \sum_{j=0}^{q-1} \binom{q}{j} i^j. \tag{275}$$

Recall that $n-1 \in \mathbb{N}$. Therefore, Proposition 1.3.6 (applied to $n-1$ and n instead of n and k) shows that $\binom{n-1}{n} = 0$ (since $n > n-1$).

Now, every $g \in \mathbb{Z}$ satisfies

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{g}{i} i^q = \sum_{i=1}^{n} (-1)^{n-i} \binom{g}{i} i^q + (-1)^{n-0} \binom{g}{0} \underbrace{0^q}_{\substack{=0 \\ \text{(since } q>0\text{)}}}$$

(here, we have split off the addend for $i = 0$ from the sum)

$$= \sum_{i=1}^{n} (-1)^{n-i} \binom{g}{i} i^q + \underbrace{(-1)^{n-0} \binom{g}{0} 0}_{=0}$$

$$= \sum_{i=1}^{n} (-1)^{n-i} \binom{g}{i} i^q. \tag{276}$$

Applying this to $g = n$, we obtain

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q = \sum_{i=1}^{n} (-1)^{n-i} \underbrace{\binom{n}{i}}_{=\binom{n-1}{i-1}+\binom{n-1}{i}} i^q$$

(by Theorem 1.3.8, applied to $k=i$)

$$= \sum_{i=1}^{n} (-1)^{n-i} \left(\binom{n-1}{i-1} + \binom{n-1}{i} \right) i^q$$

$$= \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^q + \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i} i^q. \tag{277}$$

But

$$\sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^q = \sum_{i=0}^{n-1} \underbrace{(-1)^{n-(i+1)}}_{=(-1)^{n-i-1}} \underbrace{\binom{n-1}{(i+1)-1}}_{=\binom{n-1}{i}} (i+1)^q$$

(here, we have substituted $i+1$ for i in the sum)

$$= \sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} (i+1)^q. \tag{278}$$

Also, (276) (applied to $g = n-1$) yields

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n-1}{i} i^q = \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i} i^q,$$

and thus we have

$$\sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i} i^q = \sum_{i=0}^{n} (-1)^{n-i} \binom{n-1}{i} i^q$$

$$= \sum_{i=0}^{n-1} \underbrace{(-1)^{n-i}}_{=-(-1)^{n-i-1}} \binom{n-1}{i} i^q + (-1)^{n-n} \underbrace{\binom{n-1}{n}}_{=0} n^q$$

(here, we have split off the addend for $i = n$ from the sum)

$$= \sum_{i=0}^{n-1} \left(-(-1)^{n-i-1} \right) \binom{n-1}{i} i^q + \underbrace{(-1)^{n-n} 0 n^q}_{=0}$$

$$= \sum_{i=0}^{n-1} \left(-(-1)^{n-i-1} \right) \binom{n-1}{i} i^q$$

$$= -\sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} i^q. \tag{279}$$

Now, (277) becomes

$$\begin{aligned}
&\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q \\
&= \underbrace{\sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^q}_{= \sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} (i+1)^q \text{ (by (278))}} + \underbrace{\sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i} i^q}_{= -\sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} i^q \text{ (by (279))}} \\
&= \sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} (i+1)^q + \left(-\sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} i^q \right) \\
&= \sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} (i+1)^q - \sum_{i=0}^{n-1} (-1)^{n-i-1} \binom{n-1}{i} i^q \\
&= \sum_{i=0}^{n-1} \underbrace{(-1)^{n-i-1}}_{=(-1)^{(n-1)-i}} \binom{n-1}{i} \underbrace{\left((i+1)^q - i^q \right)}_{= \sum_{j=0}^{q-1} \binom{q}{j} i^j \text{ (by Corollary 7.22.1, applied to } q \text{ and } i \text{ instead of } n \text{ and } x)} \\
&= \sum_{i=0}^{n-1} (-1)^{(n-1)-i} \binom{n-1}{i} \sum_{j=0}^{q-1} \binom{q}{j} i^j.
\end{aligned}$$

Comparing this with (275), we obtain

$$\operatorname{sur}(q,n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q.$$

This proves (273).]

Now, forget that we fixed n. We thus have proven that $\operatorname{sur}(q,n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^q$ for every $n \in \mathbb{N}$. In other words, Theorem 2.4.17 holds for $m = q$. This completes the induction step. Thus, Theorem 2.4.17 is proved. □

Thus, Exercise 2.4.4 is solved.[248]

[248] This solution has been taken from [17f-hw2s, Exercise 4].

7.23. Solution to Exercise 2.4.5

Solution to Exercise 2.4.5. **(a)** Theorem 2.4.17 yields

$$\begin{aligned}
&\operatorname{sur}(m,n) \\
&= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} i^m = (-1)^{n-0} \binom{n}{0} \underbrace{0^m}_{\substack{=0 \\ \text{(since } m \text{ is positive)}}} + \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} i^m \\
&\qquad \text{(here, we have split off the addend for } i=0 \text{ from the sum)} \\
&= \underbrace{(-1)^{n-0} \binom{n}{0} 0}_{=0} + \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} i^m = \sum_{i=1}^{n} (-1)^{n-i} \underbrace{\binom{n}{i}}_{\substack{= \frac{n}{i}\binom{n-1}{i-1} \\ \text{(by Proposition 1.3.36,} \\ \text{applied to } n \text{ and } i \\ \text{instead of } m \text{ and } n)}} \underbrace{i^m}_{\substack{= i i^{m-1} \\ \text{(since } m \text{ is positive)}}} \\
&= \sum_{i=1}^{n} (-1)^{n-i} \underbrace{\frac{n}{i}\binom{n-1}{i-1} i i^{m-1}}_{= n\binom{n-1}{i-1} i^{m-1}} = \sum_{i=1}^{n} (-1)^{n-i} n \binom{n-1}{i-1} i^{m-1} \\
&= n \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^{m-1}.
\end{aligned}$$

Comparing this with

$$\begin{aligned}
n \underbrace{\sum_{i=0}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^{m-1}}_{\substack{= (-1)^{n-0}\binom{n-1}{0-1} 0^{m-1} + \sum_{i=1}^{n} (-1)^{n-i}\binom{n-1}{i-1} i^{m-1} \\ \text{(here, we have split off the addend for } i=0 \text{ from the sum)}}} \\
= n \left((-1)^{n-0} \underbrace{\binom{n-1}{0-1}}_{\substack{=0 \\ \text{(by (43), since } 0-1 \notin \mathbb{N})}} 0^{m-1} + \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^{m-1} \right) \\
= n \left(\underbrace{(-1)^{n-0} 0 \cdot 0^{m-1}}_{=0} + \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^{m-1} \right) \\
= n \sum_{i=1}^{n} (-1)^{n-i} \binom{n-1}{i-1} i^{m-1},
\end{aligned}$$

we obtain

$$\operatorname{sur}(m,n) = n\sum_{i=0}^{n}(-1)^{n-i}\binom{n-1}{i-1}i^{m-1}.$$

This solves Exercise 2.4.5 **(a)**.

(b) The definition of the Stirling number $\left\{ {m \atop n} \right\}$ (in Remark 2.4.16) yields

$$\left\{ {m \atop n} \right\} = \operatorname{sur}(m,n)/n! = \frac{1}{n!}\underbrace{\operatorname{sur}(m,n)}_{\substack{=\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}i^m \\ \text{(by Theorem 2.4.17)}}} = \frac{1}{n!}\cdot\sum_{i=0}^{n}(-1)^{n-i}\underbrace{\binom{n}{i}}_{\substack{=\frac{n!}{i!\cdot(n-i)!} \\ \text{(by Theorem 1.3.9,} \\ \text{applied to } k=i\text{)}}}i^m$$

$$= \frac{1}{n!}\cdot\sum_{i=0}^{n}(-1)^{n-i}\frac{n!}{i!\cdot(n-i)!}i^m = \underbrace{\frac{1}{n!}\cdot n!}_{=1}\sum_{i=0}^{n}(-1)^{n-i}\frac{1}{i!\,(n-i)!}i^m$$

$$= \sum_{i=0}^{n}(-1)^{n-i}\frac{1}{i!\,(n-i)!}i^m = \sum_{i=0}^{n}(-1)^{n-i}\frac{i^m}{i!\,(n-i)!}.$$

This solves Exercise 2.4.5 **(b)**. [249] □

7.24. Solution to Exercise 2.5.1

Solution to Exercise 2.5.1. Fix $k \in \mathbb{N}$ and $m \in \mathbb{N}$. We must prove the equality (171) rigorously.

Our informal proof of this equality involved a sequence of three choices, each depending on the previous one. The easiest way to formalize such an argument is by reframing it as two applications of the sum rule (one corresponding to the choice of $i = |f([m])|$, and one corresponding to the choice of $f([m])$). Thus, we obtain the following proof:

[*Proof of (171):* If $f : [m] \to [k]$ is any map, then $|f([m])| \in \{0,1,\ldots,m\}$ [250]. Hence, the sum rule yields

$$\begin{aligned}&(\#\text{ of maps } f : [m] \to [k])\\ &= \sum_{i\in\{0,1,\ldots,m\}}(\#\text{ of maps } f : [m] \to [k] \text{ satisfying } |f([m])| = i).\end{aligned} \tag{280}$$

[249] This solution to Exercise 2.4.5 has been taken from [17f-hw3s, Exercise 2].

[250] *Proof.* Let $f : [m] \to [k]$. Then, $[m] = \{1,2,\ldots,m\}$ and thus $f([m]) = f(\{1,2,\ldots,m\}) = \{f(1), f(2), \ldots, f(m)\}$. But the set $\{f(1), f(2), \ldots, f(m)\}$ has at most m elements (since $f(1), f(2), \ldots, f(m)$ are m elements). In other words, $|\{f(1), f(2), \ldots, f(m)\}| \leq m$. In view of $f([m]) = \{f(1), f(2), \ldots, f(m)\}$, this rewrites as $|f([m])| \leq m$. Hence, $|f([m])| \in \{0,1,\ldots,m\}$ (since $|f([m])|$ is clearly a nonnegative integer).

Now, fix $i \in \{0,1,\ldots,m\}$. If $f : [m] \to [k]$ is any map satisfying $|f([m])| = i$, then $f([m])$ is an i-element subset of $[k]$ (since $f([m]) \subseteq [k]$ and $|f([m])| = i$). Thus, the sum rule yields

$$\begin{aligned}&(\#\text{ of maps } f : [m] \to [k] \text{ satisfying } |f([m])| = i) \\ &= \sum_{\substack{I \text{ is an } i\text{-element} \\ \text{subset of } [k]}} (\#\text{ of maps } f : [m] \to [k] \text{ satisfying } |f([m])| = i \text{ and } f([m]) = I)\,.\end{aligned} \tag{281}$$

Now, fix an i-element subset I of $[k]$. Then, $|I| = i$. Hence, each map $f : [m] \to [k]$ satisfying $f([m]) = I$ automatically satisfies $|f([m])| = i$ (since $f([m]) = I$ leads to $|f([m])| = |I| = i$). Hence, the condition "$|f([m])| = i$" in "(# of maps $f : [m] \to [k]$ satisfying $|f([m])| = i$ and $f([m]) = I$)" is redundant. Thus,

$$\begin{aligned}&(\#\text{ of maps } f : [m] \to [k] \text{ satisfying } |f([m])| = i \text{ and } f([m]) = I) \\ &= (\#\text{ of maps } f : [m] \to [k] \text{ satisfying } f([m]) = I) \\ &= (\#\text{ of surjective maps from } [m] \text{ to } I) \\ &\qquad \text{(by Exercise 2.4.1 } \textbf{(b)} \text{ (applied to } A = [m]\,,\ B = [k] \text{ and } C = I)) \\ &= \operatorname{sur}(m,i)\end{aligned} \tag{282}$$

(by Proposition 2.4.11, applied to $n = i$, $A = [m]$ and $B = I$).

Now, forget that we fixed I. We thus have proved (282) for each i-element subset I of $[k]$. Thus, (281) becomes

$$\begin{aligned}&(\#\text{ of maps } f : [m] \to [k] \text{ satisfying } |f([m])| = i) \\ &= \sum_{\substack{I \text{ is an } i\text{-element} \\ \text{subset of } [k]}} \underbrace{(\#\text{ of maps } f : [m] \to [k] \text{ satisfying } |f([m])| = i \text{ and } f([m]) = I)}_{\substack{=\operatorname{sur}(m,i) \\ \text{(by (282))}}} \\ &= \sum_{\substack{I \text{ is an } i\text{-element} \\ \text{subset of } [k]}} \operatorname{sur}(m,i) = \underbrace{(\#\text{ of } i\text{-element subsets of } [k])}_{\substack{=\binom{k}{i} \\ \text{(by Theorem 1.3.12,} \\ \text{applied to } k,\ i \text{ and } [k] \text{ instead of } n,\ k \text{ and } S)}} \cdot \operatorname{sur}(m,i) \\ &= \binom{k}{i} \cdot \operatorname{sur}(m,i)\,.\end{aligned} \tag{283}$$

Now, forget that we fixed i. We thus have proved (283) for each $i \in \{0,1,\ldots,m\}$.

Thus, (280) becomes

$$\begin{aligned}
&(\#\text{ of maps } f : [m] \to [k]) \\
&= \sum_{i \in \{0,1,\ldots,m\}} \underbrace{(\#\text{ of maps } f : [m] \to [k] \text{ satisfying } |f([m])| = i)}_{= \binom{k}{i} \cdot \operatorname{sur}(m,i) \text{ (by (283))}} \\
&= \underbrace{\sum_{i \in \{0,1,\ldots,m\}}}_{= \sum_{i=0}^{m}} \binom{k}{i} \cdot \operatorname{sur}(m,i) = \sum_{i=0}^{m} \binom{k}{i} \cdot \operatorname{sur}(m,i).
\end{aligned}$$

This proves (171).]

Thus, Exercise 2.5.1 is solved. □

7.25. Solution to Exercise 2.6.1

In order to solve Exercise 2.6.1, we need to formalize our proof of Theorem 1.3.37. Here is one way to do so:

First proof of Theorem 1.3.37 for $x \in \mathbb{N}$ (formal version). Let us first show the following:

Claim 1: We have

$$\binom{u}{n} = \sum_{k=0}^{v} \binom{v}{k} \binom{u-v}{n-k}$$

for any $u \in \mathbb{R}$ and $v \in \mathbb{N}$.

[*Proof of Claim 1:* We shall prove Claim 1 by induction on v.

Induction base: We have $\binom{u}{n} = \sum_{k=0}^{0} \binom{0}{k} \binom{u-0}{n-k}$ for any $u \in \mathbb{R}$ [251]. In other words, Claim 1 holds for $v = 0$. This completes the induction base.

Induction step: Let $w \in \mathbb{N}$. Assume that Claim 1 holds for $v = w$. We must prove that Claim 1 holds for $v = w + 1$.

[251] *Proof.* Let $u \in \mathbb{R}$. Then,

$$\sum_{k=0}^{0} \binom{0}{k} \binom{u-0}{n-k} = \underbrace{\binom{0}{0}}_{=1} \binom{u-0}{n-0} = \binom{u-0}{n-0} = \binom{u}{n}.$$

In other words, $\binom{u}{n} = \sum_{k=0}^{0} \binom{0}{k} \binom{u-0}{n-k}$, qed.

Let $u \in \mathbb{R}$. We have assumed that Claim 1 holds for $v = w$. Thus, we have

$$\begin{aligned}
\binom{u}{n} &= \sum_{k=0}^{w} \binom{w}{k} \underbrace{\binom{u-w}{n-k}}_{= \binom{u-w-1}{n-k-1} + \binom{u-w-1}{n-k}} \\
&\qquad \text{(by Theorem 1.3.8, applied to } u-w \text{ and } n-k \text{ instead of } n \text{ and } k\text{)} \\
&= \sum_{k=0}^{w} \binom{w}{k} \left(\binom{u-w-1}{n-k-1} + \binom{u-w-1}{n-k} \right) \\
&= \sum_{k=0}^{w} \left(\binom{w}{k} \binom{u-w-1}{n-k-1} + \binom{w}{k} \binom{u-w-1}{n-k} \right) \\
&= \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k-1} + \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k}. \qquad (284)
\end{aligned}$$

On the other hand, (43) (applied to w and -1 instead of n and k) yields $\binom{w}{-1} = 0$ (since $-1 \notin \mathbb{N}$). Furthermore, $w+1 > w$ and thus $\binom{w}{w+1} = 0$ (by Proposition 1.3.6, applied to w and $w+1$ instead of n and k).

But each $k \in \mathbb{N}$ satisfies

$$\begin{aligned}
\binom{w+1}{k} &= \binom{(w+1)-1}{k-1} + \binom{(w+1)-1}{k} \\
&\qquad \text{(by Theorem 1.3.8, applied to } w+1 \text{ instead of } n\text{)} \\
&= \binom{w}{k-1} + \binom{w}{k} \qquad (285)
\end{aligned}$$

(since $(w+1)-1 = w$). Hence,

$$\begin{aligned}
&\sum_{k=0}^{w+1} \underbrace{\binom{w+1}{k}}_{\substack{= \binom{w}{k-1} + \binom{w}{k} \\ \text{(by (285))}}} \underbrace{\binom{u-(w+1)}{n-k}}_{\substack{= \binom{u-w-1}{n-k} \\ \text{(since } u-(w+1)=u-w-1\text{)}}} \\
&= \sum_{k=0}^{w+1} \left(\binom{w}{k-1} + \binom{w}{k} \right) \binom{u-w-1}{n-k} \\
&= \sum_{k=0}^{w+1} \left(\binom{w}{k-1} \binom{u-w-1}{n-k} + \binom{w}{k} \binom{u-w-1}{n-k} \right) \\
&= \sum_{k=0}^{w+1} \binom{w}{k-1} \binom{u-w-1}{n-k} + \sum_{k=0}^{w+1} \binom{w}{k} \binom{u-w-1}{n-k}. \qquad (286)
\end{aligned}$$

We intend to show that the right hand sides of the equalities (284) and (286) are equal. To that aim, we transform the sums on the right hand side of the latter. Let us begin with the first sum:

$$\begin{aligned}
&\sum_{k=0}^{w+1} \binom{w}{k-1} \binom{u-w-1}{n-k} \\
&= \underbrace{\binom{w}{0-1}}_{=\binom{w}{-1}=0} \binom{u-w-1}{n-0} + \sum_{k=1}^{w+1} \binom{w}{k-1} \binom{u-w-1}{n-k} \\
&\qquad \text{(here, we have split off the addend for } k=0 \text{ from the sum)} \\
&= \sum_{k=1}^{w+1} \binom{w}{k-1} \binom{u-w-1}{n-k} = \sum_{k=0}^{w} \underbrace{\binom{w}{(k+1)-1}}_{=\binom{w}{k} \text{ (since } (k+1)-1=k)} \underbrace{\binom{u-w-1}{n-(k+1)}}_{=\binom{u-w-1}{n-k-1} \text{ (since } n-(k+1)=n-k-1)} \\
&\qquad \text{(here, we have substituted } k+1 \text{ for } k \text{ in the sum)} \\
&= \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k-1}. \qquad (287)
\end{aligned}$$

Let us next transform the second sum:

$$\begin{aligned}
&\sum_{k=0}^{w+1} \binom{w}{k} \binom{u-w-1}{n-k} \\
&= \underbrace{\binom{w}{w+1}}_{=0} \binom{u-w-1}{n-(w+1)} + \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k} \\
&\qquad \text{(here, we have split off the addend for } k=w+1 \text{ from the sum)} \\
&= \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k}. \qquad (288)
\end{aligned}$$

Thus, (286) becomes

$$\begin{aligned}
&\sum_{k=0}^{w+1} \binom{w+1}{k} \binom{u-(w+1)}{n-k} \\
&= \underbrace{\sum_{k=0}^{w+1} \binom{w}{k-1} \binom{u-w-1}{n-k}}_{\substack{= \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k-1} \\ \text{(by (287))}}} + \underbrace{\sum_{k=0}^{w+1} \binom{w}{k} \binom{u-w-1}{n-k}}_{\substack{= \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k} \\ \text{(by (288))}}} \\
&= \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k-1} + \sum_{k=0}^{w} \binom{w}{k} \binom{u-w-1}{n-k}.
\end{aligned}$$

Comparing this with (284), we obtain

$$\binom{u}{n} = \sum_{k=0}^{w+1} \binom{w+1}{k} \binom{u-(w+1)}{n-k}.$$

Now, forget that we fixed u. We thus have proved that

$$\binom{u}{n} = \sum_{k=0}^{w+1} \binom{w+1}{k} \binom{u-(w+1)}{n-k} \qquad \text{for any } u \in \mathbb{R}.$$

In other words, Claim 1 holds for $v = w+1$. This completes the induction step. Thus, Claim 1 is proven by induction.]

Now, let $x \in \mathbb{N}$ and $y \in \mathbb{R}$. Applying Claim 1 to $u = x+y$ and $v = x$, we get

$$\binom{x+y}{n} = \sum_{k=0}^{x} \binom{x}{k} \binom{(x+y)-x}{n-k} = \sum_{k=0}^{x} \binom{x}{k} \binom{y}{n-k} \tag{289}$$

(since $(x+y)-x = y$).

Now, recall that $x \in \mathbb{N}$. Hence, every $k \in \mathbb{N}$ satisfying $k > x$ must satisfy

$$\binom{x}{k} = 0 \tag{290}$$

(by Proposition 1.3.6, applied to x instead of n) and thus $\underbrace{\binom{x}{k}}_{=0} \binom{y}{n-k} = 0$. Thus, in the infinite sum $\sum_{k \in \mathbb{N}} \binom{x}{k} \binom{y}{n-k}$, every addend with $k > x$ is 0. Hence, this infinite sum has only finitely many nonzero addends (namely, the addends with

$k \leq x$). Thus, it is well-defined. Moreover,

$$\sum_{k \in \mathbb{N}} \binom{x}{k} \binom{y}{n-k} = \underbrace{\sum_{\substack{k \in \mathbb{N}; \\ k \leq x}}}_{= \sum\limits_{k \in \{0,1,\ldots,x\}} = \sum\limits_{k=0}^{x}} \binom{x}{k} \binom{y}{n-k} + \sum_{\substack{k \in \mathbb{N}; \\ k > x}} \underbrace{\binom{x}{k}}_{\substack{=0 \\ \text{(by (290))}}} \binom{y}{n-k}$$

$$= \sum_{k=0}^{x} \binom{x}{k} \binom{y}{n-k} + \underbrace{\sum_{\substack{k \in \mathbb{N}; \\ k > x}} 0 \binom{y}{n-k}}_{=0} = \sum_{k=0}^{x} \binom{x}{k} \binom{y}{n-k}.$$

Comparing this with (289), we obtain

$$\binom{x+y}{n} = \sum_{k \in \mathbb{N}} \binom{x}{k} \binom{y}{n-k}. \tag{291}$$

On the other hand, $n \in \mathbb{N}$. If k is an integer satisfying $k > n$, then $n - k < 0$ and thus $n - k \notin \mathbb{N}$ and therefore

$$\binom{y}{n-k} = 0 \tag{292}$$

(by (43), applied to y and $n - k$ instead of n and k). Thus,

$$\sum_{k \in \mathbb{N}} \binom{x}{k} \binom{y}{n-k} = \underbrace{\sum_{\substack{k \in \mathbb{N}; \\ k \leq n}}}_{= \sum\limits_{k \in \{0,1,\ldots,n\}} = \sum\limits_{k=0}^{n}} \binom{x}{k} \binom{y}{n-k} + \sum_{\substack{k \in \mathbb{N}; \\ k > n}} \binom{x}{k} \underbrace{\binom{y}{n-k}}_{\substack{=0 \\ \text{(by (292))}}}$$

$$= \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k} + \underbrace{\sum_{\substack{k \in \mathbb{N}; \\ k > n}} \binom{x}{k} 0}_{=0} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}.$$

Hence, (291) becomes

$$\binom{x+y}{n} = \sum_{k \in \mathbb{N}} \binom{x}{k} \binom{y}{n-k} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}.$$

Thus, (172) is proved. Hence, (173) follows as well[252]. This proves Theorem 2.6.1 for $x \in \mathbb{N}$. □

Thus, Exercise 2.6.1 is solved.

[252] because we have seen in Remark 2.6.2 that the right hand sides of (172) and of (173) are equal

7.26. Solution to Exercise 2.6.2

In order to solve Exercise 2.6.2, we need to give an alternative proof of Corollary 2.6.3:

Alternative proof of Corollary 2.6.3. We have $y \in \mathbb{N}$. Hence, we can apply (172) to y, x and y instead of x, y and n (since we have proved (172) for $x \in \mathbb{N}$ already). We thus obtain

$$\binom{y+x}{y} = \sum_{k=0}^{y} \binom{y}{k}\binom{x}{y-k} = \sum_{k=0}^{y} \binom{y}{y-k} \underbrace{\binom{x}{y-(y-k)}}_{\substack{=\binom{x}{k} \\ (\text{since } y-(y-k)=k)}}$$

$$(\text{here, we have substituted } y-k \text{ for } k \text{ in the sum})$$

$$= \sum_{k=0}^{y} \underbrace{\binom{y}{y-k}\binom{x}{k}}_{=\binom{x}{k}\binom{y}{y-k}} = \sum_{k=0}^{y} \binom{x}{k}\binom{y}{y-k}.$$

But

$$\sum_{k=0}^{y} \binom{x}{k} \underbrace{\binom{y}{k}}_{\substack{=\binom{y}{y-k} \\ (\text{by Theorem 1.3.11,} \\ \text{applied to } n=y)}} = \sum_{k=0}^{y} \binom{x}{k}\binom{y}{y-k}.$$

Comparing these two equalities, we find

$$\sum_{k=0}^{y} \binom{x}{k}\binom{y}{k} = \binom{y+x}{y} = \binom{x+y}{y} \qquad (\text{since } y+x = x+y).$$

This proves Corollary 2.6.3 again. □

7.27. Solution to Exercise 2.6.3

In order to solve Exercise 2.6.3, we need to solve Exercise 2.1.1 **(a)** again using Theorem 1.3.37:

*Alternative solution to Exercise 2.1.1 **(a)** using Theorem 1.3.37.* The equality (172) (applied to n, -1 and m instead of x, y and n) yields

$$\binom{n+(-1)}{m} = \sum_{k=0}^{m} \binom{n}{k}\binom{-1}{m-k}. \tag{293}$$

But every $k \in \{0,1,\ldots,m\}$ satisfies $m-k \in \{0,1,\ldots,m\} \subseteq \mathbb{N}$ and thus

$$\binom{-1}{m-k} = (-1)^{m-k} \tag{294}$$

(by (47), applied to $m-k$ instead of k). Hence, (293) becomes

$$\begin{aligned}
\binom{n+(-1)}{m} &= \sum_{k=0}^{m} \binom{n}{k} \underbrace{\binom{-1}{m-k}}_{\substack{=(-1)^{m-k} \\ \text{(by (294))}}} = \sum_{k=0}^{m} \binom{n}{k} \underbrace{(-1)^{m-k}}_{\substack{=(-1)^{m+k} \\ \text{(since } m-k \equiv m+k \bmod 2\text{)}}} \\
&= \sum_{k=0}^{m} \binom{n}{k} \underbrace{(-1)^{m+k}}_{=(-1)^m (-1)^k} = \sum_{k=0}^{m} \underbrace{\binom{n}{k} (-1)^m (-1)^k}_{=(-1)^m (-1)^k \binom{n}{k}} \\
&= \sum_{k=0}^{m} (-1)^m (-1)^k \binom{n}{k} = (-1)^m \sum_{k=0}^{m} (-1)^k \binom{n}{k}.
\end{aligned}$$

In view of $n+(-1) = n-1$, this rewrites as

$$\binom{n-1}{m} = (-1)^m \sum_{k=0}^{m} (-1)^k \binom{n}{k}.$$

Multiplying both sides of this equality by $(-1)^m$, we find

$$(-1)^m \binom{n-1}{m} = \underbrace{(-1)^m (-1)^m}_{\substack{=(-1)^{m+m}=1 \\ \text{(since } m+m=2m \text{ is even)}}} \sum_{k=0}^{m} (-1)^k \binom{n}{k} = \sum_{k=0}^{m} (-1)^k \binom{n}{k}.$$

Thus, Exercise 2.1.1 **(a)** is solved again. □

7.28. Solution to Exercise 2.6.4

In order to solve Exercise 2.6.4, we must give an alternative proof of Theorem 1.3.29 using Proposition 2.6.13. Let us do this:

Alternative proof of Theorem 1.3.29. Forget that we fixed k. For each $x \in \mathbb{N}$, we have

$$\begin{aligned}
\binom{n+1}{x+1} &= \sum_{k=0}^{n} \binom{k}{x} \underbrace{\binom{n-k}{0}}_{\substack{=1 \\ \text{(by (44), applied to } n-k \\ \text{instead of } n\text{)}}} \qquad \text{(by Proposition 2.6.13, applied to } y=0\text{)} \\
&= \sum_{k=0}^{n} \binom{k}{x} = \binom{0}{x} + \binom{1}{x} + \binom{2}{x} + \cdots + \binom{n}{x}
\end{aligned}$$

and thus

$$\binom{0}{x}+\binom{1}{x}+\binom{2}{x}+\cdots+\binom{n}{x}=\binom{n+1}{x+1}.$$

Renaming x as k in this statement, we obtain the following: For each $k \in \mathbb{N}$, we have

$$\binom{0}{k}+\binom{1}{k}+\binom{2}{k}+\cdots+\binom{n}{k}=\binom{n+1}{k+1}.$$

Thus, Theorem 1.3.29 is proved again. □

7.29. Reference to solution to Exercise 2.6.5

Exercise 2.6.5 appears (with solution) in [Grinbe15, Proposition 3.32 **(d)**]. (To be more precise, [Grinbe15, Proposition 3.32 **(d)**] is only the particular case of Exercise 2.6.5 when $x, y \in \mathbb{Z}$; but the general case can be proved by the exact same argument.)

7.30. Solution to Exercise 2.6.6

Solution to Exercise 2.6.6. We are in one of the following two cases:

Case 1: We have $x \leq n$.

Case 2: We have $x > n$.

Let us first consider Case 1. In this case, we have $x \leq n$. Hence, $n - x \geq 0$, so that $n - x \in \mathbb{N}$ (since $n \in \mathbb{N}$ and $x \in \mathbb{N}$). Now, $y - x - 1 = (-x - 1) + y$. Hence,

$$\begin{aligned}\binom{y-x-1}{n-x} &= \binom{(-x-1)+y}{n-x} \\ &= \sum_{k=0}^{n-x}\binom{-x-1}{k}\binom{y}{n-x-k} \end{aligned} \tag{295}$$

(by (172), applied to $-x-1$ and $n-x$ instead of x and n). Now, we claim the following:

Claim 1: We have $\dbinom{-x-1}{k} = (-1)^k \dbinom{x+k}{x}$ for each $k \in \mathbb{N}$.

[*Proof of Claim 1:* Let $k \in \mathbb{N}$. Applying upper negation (Proposition 1.3.7) to $x+1$ instead of n, we obtain

$$\binom{-(x+1)}{k} = (-1)^k \binom{x+1+k-1}{k} = (-1)^k \binom{x+k}{k}$$

(since $x+1+k-1 = x+k$). In view of $-(x+1) = -x-1$, we can rewrite this as

$$\binom{-x-1}{k} = (-1)^k \binom{x+k}{k}. \tag{296}$$

However, $x+k \in \mathbb{N}$ (since $x \in \mathbb{N}$ and $k \in \mathbb{N}$). Hence, Theorem 1.3.11 (applied to $x+k$ instead of n) yields $\binom{x+k}{k} = \binom{x+k}{(x+k)-k} = \binom{x+k}{x}$ (since $(x+k)-k = x$). This allows us to rewrite (296) as

$$\binom{-x-1}{k} = (-1)^k \binom{x+k}{x}.$$

This proves Claim 1.]

Now, (295) becomes

$$\begin{aligned}
\binom{y-x-1}{n-x} &= \sum_{k=0}^{n-x} \underbrace{\binom{-x-1}{k}}_{\substack{=(-1)^k\binom{x+k}{x} \\ \text{(by Claim 1)}}} \binom{y}{n-x-k} = \sum_{k=0}^{n-x} (-1)^k \binom{x+k}{x} \binom{y}{n-x-k} \\
&= \sum_{k=x}^{n} (-1)^{k-x} \underbrace{\binom{x+(k-x)}{x}}_{\substack{=\binom{k}{x} \\ \text{(since } x+(k-x)=k\text{)}}} \underbrace{\binom{y}{n-x-(k-x)}}_{\substack{=\binom{y}{n-k} \\ \text{(since } n-x-(k-x)=n-k\text{)}}} \\
&\qquad \left(\text{here, we have substituted } k-x \text{ for } k \text{ in the sum}\right) \\
&= \sum_{k=x}^{n} (-1)^{k-x} \binom{k}{x} \binom{y}{n-k}. \qquad (297)
\end{aligned}$$

However, for each $k \in \{0,1,\ldots,x-1\}$, we have $x > k$ (since $k \in \{0,1,\ldots,x-1\}$ entails $k \leq x-1 < x$) and therefore

$$\binom{k}{x} = 0 \qquad (298)$$

(by Proposition 1.3.6, applied to k and x instead of n and k).

From $x \in \mathbb{N}$, we obtain $x \geq 0$. Therefore, $0 \leq x \leq n$. Thus, we can split the sum

$\sum\limits_{k=0}^{n}(-1)^{k-x}\dbinom{k}{x}\dbinom{y}{n-k}$ up as follows:

$$\begin{aligned}
&\sum_{k=0}^{n}(-1)^{k-x}\binom{k}{x}\binom{y}{n-k}\\
&=\sum_{k=0}^{x-1}(-1)^{k-x}\underbrace{\binom{k}{x}}_{\substack{=0\\ \text{(by (298))}}}\binom{y}{n-k}+\sum_{k=x}^{n}(-1)^{k-x}\binom{k}{x}\binom{y}{n-k}\\
&=\underbrace{\sum_{k=0}^{x-1}(-1)^{k-x}0\binom{y}{n-k}}_{=0}+\sum_{k=x}^{n}(-1)^{k-x}\binom{k}{x}\binom{y}{n-k}\\
&=\sum_{k=x}^{n}(-1)^{k-x}\binom{k}{x}\binom{y}{n-k}.
\end{aligned}$$

Comparing this with (297), we obtain $\dbinom{y-x-1}{n-x}=\sum\limits_{k=0}^{n}(-1)^{k-x}\dbinom{k}{x}\dbinom{y}{n-k}$. Thus, Exercise 2.6.6 is solved in Case 1.

Let us now consider Case 2. In this case, we have $x>n$. In other words, $n<x$. Thus, $n-x<0$, so that $n-x\notin\mathbb{N}$. Hence, (43) (applied to $y-x-1$ and $n-x$ instead of n and k) yields

$$\binom{y-x-1}{n-x}=0. \tag{299}$$

On the other hand, for each $k\in\{0,1,\ldots,n\}$, we have $x>k$ (since $k\in\{0,1,\ldots,n\}$ entails $k\leq n<x$) and therefore

$$\binom{k}{x}=0 \tag{300}$$

(by Proposition 1.3.6, applied to k and x instead of n and k). Hence,

$$\sum_{k=0}^{n}(-1)^{k-x}\underbrace{\binom{k}{x}}_{\substack{=0\\ \text{(by (300))}}}\binom{y}{n-k}=\sum_{k=0}^{n}(-1)^{k-x}0\binom{y}{n-k}=0.$$

Comparing this with (299), we obtain $\dbinom{y-x-1}{n-x}=\sum\limits_{k=0}^{n}(-1)^{k-x}\dbinom{k}{x}\dbinom{y}{n-k}$. Thus, Exercise 2.6.6 is solved in Case 2.

We have now solved Exercise 2.6.6 in both Cases 1 and 2. This completes the solution of this exercise. □

We remark that the most important particular case of Exercise 2.6.6 (namely, the case when $x\leq n$) appears (with solution) in [Grinbe15, Proposition 3.32 **(e)**]. (To be more precise, [Grinbe15, Proposition 3.32 **(e)**] is only the particular case of Exercise

2.6.6 when $x \leq n$ and $y \in \mathbb{Z}$; however, the condition $y \in \mathbb{Z}$ is not used anywhere in the solution of [Grinbe15, Proposition 3.32 **(e)**].) The remaining case (viz., the case when $x > n$) can easily be dealt with by observing that both sides are 0 in this case. However, this is more or less exactly the solution we gave above.

7.31. Reference to solution to Exercise 2.6.7

Exercise 2.6.7 appears (with solution) in [Grinbe15, Proposition 3.37] (with x renamed as m). (To be more precise, [Grinbe15, Proposition 3.37] is only the particular case of Exercise 2.6.7 when $x \in \mathbb{Q}$; but the general case can be proved by the exact same argument.)

7.32. Solution to Exercise 2.6.8

Solution to Exercise 2.6.8. We shall first solve the exercise through a computation. In order to keep the computation short, we shall omit the justifications of some of its steps; these justifications will instead be provided after the computation.

Here is the computation:

$$\sum_{i=0}^{\min\{a,b\}} \binom{x+y+i}{i}\binom{x}{a-i}\binom{y}{b-i}$$

$$= \sum_{i=0}^{b} \underbrace{\binom{x+y+i}{i}}_{=\sum_{j\in\mathbb{N}}\binom{y+a}{j}\binom{x-a+i}{i-j}} \binom{x}{a-i}\binom{y}{b-i}$$

(by Chu–Vandermonde; see Justification 2 below for the details)

(see Justification 1 below for why this equality holds)

$$= \sum_{i=0}^{b} \left(\sum_{j\in\mathbb{N}} \binom{y+a}{j}\binom{x-a+i}{i-j}\right)\binom{x}{a-i}\binom{y}{b-i}$$

$$= \sum_{i=0}^{b} \sum_{j\in\mathbb{N}} \binom{y+a}{j} \underbrace{\binom{x-a+i}{i-j}\binom{x}{a-i}}_{=\binom{x}{a-j}\binom{a-j}{i-j}} \binom{y}{b-i}$$

(by Proposition 2.2.4; see Justification 3 below for the details)

$$= \sum_{i=0}^{b} \underbrace{\sum_{j\in\mathbb{N}} \binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i}}_{=\sum_{j=0}^{a}\binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i}}$$

(see Justification 4 below for why this equality holds)

$$= \underbrace{\sum_{i=0}^{b}\sum_{j=0}^{a}}_{=\sum_{j=0}^{a}\sum_{i=0}^{b}} \binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i}$$

$$= \sum_{j=0}^{a}\sum_{i=0}^{b} \binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i}$$

$$= \sum_{j=0}^{a} \binom{y+a}{j}\binom{x}{a-j} \underbrace{\sum_{i=0}^{b}\binom{a-j}{i-j}\binom{y}{b-i}}_{=\binom{a-j+y}{b-j}}$$

(by Chu–Vandermonde; see Justification 5 below for the details)

$$= \sum_{j=0}^{a} \binom{y+a}{j} \underbrace{\binom{x}{a-j}\binom{a-j+y}{b-j}}_{=\binom{a-j+y}{b-j}\binom{x}{a-j}} = \sum_{j=0}^{a} \underbrace{\binom{y+a}{j}\binom{a-j+y}{b-j}}_{=\binom{y+a}{b}\binom{b}{j}} \binom{x}{a-j}$$

(by Proposition 1.3.35; see Justification 6 below for the details)

$$= \sum_{j=0}^{a} \binom{y+a}{b}\binom{b}{j}\binom{x}{a-j} = \binom{y+a}{b} \underbrace{\sum_{j=0}^{a} \binom{b}{j}\binom{x}{a-j}}_{=\binom{x+b}{a}}$$

(by Chu–Vandermonde; see Justification 7 below for the details)

$$= \binom{y+a}{b}\binom{x+b}{a} = \binom{x+b}{a}\binom{y+a}{b}.$$

Here are the promised **justifications**:

1. **Justification 1:** We need to justify the equality

$$\sum_{i=0}^{\min\{a,b\}} \binom{x+y+i}{i}\binom{x}{a-i}\binom{y}{b-i} = \sum_{i=0}^{b} \binom{x+y+i}{i}\binom{x}{a-i}\binom{y}{b-i}. \tag{301}$$

   In order to do so, we WLOG assume that $\min\{a,b\} \neq b$ (because (301) is clearly true if $\min\{a,b\} = b$). Hence, we must have $\min\{a,b\} = a$ (since the number $\min\{a,b\}$ necessarily equals one of a and b). Therefore, $a = \min\{a,b\} \leq b$. Thus, $0 \leq a \leq b$. Hence, the sum on the right hand side of

(301) can be split up as follows:

$$\begin{aligned}
&\sum_{i=0}^{b} \binom{x+y+i}{i} \binom{x}{a-i} \binom{y}{b-i} \\
&= \underbrace{\sum_{i=0}^{a}}_{\substack{= \sum_{i=0}^{\min\{a,b\}} \\ \text{(since } a=\min\{a,b\}\text{)}}} \binom{x+y+i}{i} \binom{x}{a-i} \binom{y}{b-i} \\
&\quad + \sum_{i=a+1}^{b} \binom{x+y+i}{i} \underbrace{\binom{x}{a-i}}_{\substack{=0 \\ \text{(since } i \geq a+1 > a\text{,} \\ \text{thus } a-i<0\text{, hence } a-i \notin \mathbb{N}\text{,} \\ \text{and therefore } \binom{x}{a-i}=0 \\ \text{(by (43), applied to } n=x \text{ and } k=a-i\text{))}}} \binom{y}{b-i} \\
&= \sum_{i=0}^{\min\{a,b\}} \binom{x+y+i}{i} \binom{x}{a-i} \binom{y}{b-i} + \underbrace{\sum_{i=a+1}^{b} \binom{x+y+i}{i} 0 \binom{y}{b-i}}_{=0} \\
&= \sum_{i=0}^{\min\{a,b\}} \binom{x+y+i}{i} \binom{x}{a-i} \binom{y}{b-i}.
\end{aligned}$$

This proves (301).

2. **Justification 2:** We need to prove the equality

$$\binom{x+y+i}{i} = \sum_{j \in \mathbb{N}} \binom{y+a}{j} \binom{x-a+i}{i-j} \tag{302}$$

for each $i \in \{0,1,\ldots,b\}$.

To do so, we fix $i \in \{0,1,\ldots,b\}$. Then, $i \in \mathbb{N}$. Hence, (173) (applied to $y+a$,

$x-a+i$ and i instead of x, y and n) yields[253]

$$\begin{aligned}
&\binom{(y+a)+(x-a+i)}{i} \\
&= \underbrace{\sum_{k}}_{=\sum_{k\in\mathbb{Z}}} \binom{y+a}{k}\binom{x-a+i}{i-k} = \sum_{k\in\mathbb{Z}} \binom{y+a}{k}\binom{x-a+i}{i-k} \\
&= \underbrace{\sum_{\substack{k\in\mathbb{Z};\\ k\in\mathbb{N}}}}_{=\sum_{k\in\mathbb{N}}} \binom{y+a}{k}\binom{x-a+i}{i-k} + \sum_{\substack{k\in\mathbb{Z};\\ k\notin\mathbb{N}}} \underbrace{\binom{y+a}{k}}_{\substack{=0 \\ \text{(by (43) (applied to } n=y+a\text{)} \\ \text{(since } k\notin\mathbb{N}\text{))}}} \binom{x-a+i}{i-k} \\
&\qquad\qquad \left(\begin{array}{c}\text{since each } k\in\mathbb{Z} \text{ satisfies} \\ \text{either } k\in\mathbb{N} \text{ or } k\notin\mathbb{N} \text{ (but not both)}\end{array}\right) \\
&= \sum_{k\in\mathbb{N}} \binom{y+a}{k}\binom{x-a+i}{i-k} + \underbrace{\sum_{\substack{k\in\mathbb{Z};\\ k\notin\mathbb{N}}} 0\binom{x-a+i}{i-k}}_{=0} \\
&= \sum_{k\in\mathbb{N}} \binom{y+a}{k}\binom{x-a+i}{i-k} = \sum_{j\in\mathbb{N}} \binom{y+a}{j}\binom{x-a+i}{i-j}
\end{aligned}$$

(here, we have renamed the summation index k as j). In view of $(y+a)+(x-a+i) = x+y+i$, we can rewrite this as

$$\binom{x+y+i}{i} = \sum_{j\in\mathbb{N}} \binom{y+a}{j}\binom{x-a+i}{i-j}.$$

Thus, (302) is proven.

3. **Justification 3:** We need to prove the equality

$$\binom{x-a+i}{i-j}\binom{x}{a-i} = \binom{x}{a-j}\binom{a-j}{i-j} \tag{303}$$

for any $i \in \{0,1,\ldots,b\}$ and any $j \in \mathbb{N}$.

To prove this equality, we fix some $i \in \{0,1,\ldots,b\}$ and $j \in \mathbb{N}$. Then, Propo-

[253] The summation sign "$\sum_k$" here is shorthand for "$\sum_{k\in\mathbb{Z}}$".

sition 2.2.4 (applied to x, $a-j$ and $i-j$ instead of n, a and b) yields

$$\begin{aligned}\binom{x}{a-j}\binom{a-j}{i-j} &= \binom{x}{(a-j)-(i-j)}\binom{x-(a-j)+(i-j)}{i-j} \\ &= \binom{x}{a-i}\binom{x-a+i}{i-j} \\ &\qquad \left(\begin{array}{c}\text{since } (a-j)-(i-j)=a-i \\ \text{and } x-(a-j)+(i-j)=x-a+i\end{array}\right) \\ &= \binom{x-a+i}{i-j}\binom{x}{a-i}.\end{aligned}$$

This proves (303).

4. **Justification 4:** We need to explain why the equality

$$\begin{aligned}&\sum_{j\in\mathbb{N}}\binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i} \\ &= \sum_{j=0}^{a}\binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i}\end{aligned} \tag{304}$$

holds for each $i \in \{0,1,\ldots,b\}$.

For this purpose, we fix $i \in \{0,1,\ldots,b\}$. Then, each $j \in \mathbb{N}$ satisfies either $j \leq a$ or $j > a$ (but not both at the same time). Hence, we can split the sum

on the left hand side of (304) as follows:

$$\begin{aligned}
&\sum_{j\in\mathbb{N}} \binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i} \\
&= \underbrace{\sum_{\substack{j\in\mathbb{N};\\ j\leq a}}}_{\substack{=\sum_{j=0}^{a} \\ \text{(since } a\in\mathbb{N}\text{)}}} \binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i} \\
&\qquad + \sum_{\substack{j\in\mathbb{N};\\ j>a}} \binom{y+a}{j} \underbrace{\binom{x}{a-j}}_{\substack{=0 \\ \text{(since } j>a\text{,} \\ \text{thus } a-j<0\text{, hence } a-j\notin\mathbb{N}\text{,} \\ \text{and therefore } \binom{x}{a-j}=0 \\ \text{(by (43), applied to } n=x \text{ and } k=a-j\text{))}}} \binom{a-j}{i-j}\binom{y}{b-i} \\
&= \sum_{j=0}^{a} \binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i} \\
&\qquad + \underbrace{\sum_{\substack{j\in\mathbb{N};\\ j>a}} \binom{y+a}{j} 0 \binom{a-j}{i-j}\binom{y}{b-i}}_{=0} \\
&= \sum_{j=0}^{a} \binom{y+a}{j}\binom{x}{a-j}\binom{a-j}{i-j}\binom{y}{b-i}.
\end{aligned}$$

This proves (304).

5. **Justification 5:** We need to prove the equality

$$\sum_{i=0}^{b} \binom{a-j}{i-j}\binom{y}{b-i} = \binom{a-j+y}{b-j} \tag{305}$$

for each $j \in \{0,1,\ldots,a\}$.

To do so, we fix $j \in \{0,1,\ldots,a\}$. We must prove the equality (305). We are in one of the following two cases:

Case 1: We have $j \leq b$.

Case 2: We have $j > b$.

Let us first consider Case 1. In this case, we have $j \leq b$. Thus, $b-j \geq 0$, so that $b-j \in \mathbb{N}$. Hence, (172) (applied to $a-j$ and $b-j$ instead of x and n)

yields

$$\begin{aligned}\binom{a-j+y}{b-j} &= \sum_{k=0}^{b-j}\binom{a-j}{k}\binom{y}{b-j-k} \\ &= \sum_{i=j}^{b}\binom{a-j}{i-j}\underbrace{\binom{y}{b-j-(i-j)}}_{\substack{=\binom{y}{b-i} \\ \text{(since } b-j-(i-j)=b-i\text{)}}} \\ &\qquad \left(\text{here, we have substituted } i-j \text{ for } k \text{ in the sum}\right) \\ &= \sum_{i=j}^{b}\binom{a-j}{i-j}\binom{y}{b-i}. \end{aligned} \tag{306}$$

On the other hand, $0 \leq j \leq b$. Thus, we can subdivide the sum on the left hand side of (305) as follows:

$$\begin{aligned}&\sum_{i=0}^{b}\binom{a-j}{i-j}\binom{y}{b-i} \\ &= \sum_{i=0}^{j-1}\underbrace{\binom{a-j}{i-j}}_{\substack{=0 \\ \text{(since } i\leq j-1<j\text{,} \\ \text{thus } i-j<0\text{, hence } i-j\notin\mathbb{N}\text{,} \\ \text{and therefore } \binom{a-j}{i-j}=0 \\ \text{(by (43), applied to } n=a-j \text{ and } k=i-j\text{))}}}\binom{y}{b-i} + \sum_{i=j}^{b}\binom{a-j}{i-j}\binom{y}{b-i} \\ &= \underbrace{\sum_{i=0}^{j-1}0\binom{y}{b-i}}_{=0} + \sum_{i=j}^{b}\binom{a-j}{i-j}\binom{y}{b-i} \\ &= \sum_{i=j}^{b}\binom{a-j}{i-j}\binom{y}{b-i} = \binom{a-j+y}{b-j} \qquad \text{(by (306))}\,. \end{aligned}$$

Thus, (305) is proved in Case 1.

Let us now consider Case 2. In this case, we have $j > b$. In other words, $b < j$. Therefore, $b-j<0$, so that $b-j \notin \mathbb{N}$. Therefore, $\binom{a-j+y}{b-j} = 0$ (by (43),

applied to $n = a - j + y$ and $k = b - j$). Comparing this with

$$\sum_{i=0}^{b} \underbrace{\binom{a-j}{i-j}}_{\substack{=0 \\ \text{(since } i \leq b < j\text{,} \\ \text{thus } i-j<0\text{, hence } i-j \notin \mathbb{N}\text{,} \\ \text{and therefore } \binom{a-j}{i-j}=0 \\ \text{(by (43), applied to } n=a-j \text{ and } k=i-j\text{))}} \binom{y}{b-i} = \sum_{i=0}^{b} 0 \binom{y}{b-i} = 0,$$

we obtain $\sum_{i=0}^{b} \binom{a-j}{i-j}\binom{y}{b-i} = \binom{a-j+y}{b-j}$. Thus, (305) is proved in Case 2.

We have now proved (305) in both Cases 1 and 2. Thus, the proof of (305) is complete.

6. **Justification 6:** We need to verify the equality

$$\binom{y+a}{j}\binom{a-j+y}{b-j} = \binom{y+a}{b}\binom{b}{j} \tag{307}$$

for each $j \in \{0, 1, \ldots, a\}$.

To do so, we fix $j \in \{0, 1, \ldots, a\}$. Then, Proposition 1.3.35 (applied to $y + a$, b and j instead of n, a and b) yields

$$\binom{y+a}{b}\binom{b}{j} = \binom{y+a}{j}\binom{y+a-j}{b-j} = \binom{y+a}{j}\binom{a-j+y}{b-j}$$

(since $y + a - j = a - j + y$). This proves (307).

7. **Justification 7:** We need to prove that

$$\sum_{j=0}^{a} \binom{b}{j}\binom{x}{a-j} = \binom{x+b}{a}. \tag{308}$$

To do so, we apply (172) to b, x and a instead of x, y and n. We thus obtain

$$\binom{b+x}{a} = \sum_{k=0}^{a} \binom{b}{k}\binom{x}{a-k} = \sum_{j=0}^{a} \binom{b}{j}\binom{x}{a-j}$$

(here, we have renamed the summation index k as j). Thus,

$$\sum_{j=0}^{a} \binom{b}{j}\binom{x}{a-j} = \binom{b+x}{a} = \binom{x+b}{a} \qquad (\text{since } b + x = x + b)\,.$$

This proves (308).

We have now fully justified our above computation. The computation shows that

$$\sum_{i=0}^{\min\{a,b\}} \binom{x+y+i}{i} \binom{x}{a-i} \binom{y}{b-i} = \binom{x+b}{a} \binom{y+a}{b};$$

thus, Exercise 2.6.8 is solved. (The above solution comes from [Gould72, §3].) □

7.33. Solution to Exercise 2.6.9

Solution to Exercise 2.6.9. Let $u, v \in \mathbb{R}$. We must prove that $F_{x,n}(u,v) = F_{x,n}(v,u)$.

We shall first prove that

$$F_{x,n}(u,v) = \sum_{k=0}^{n} \binom{u}{k} \binom{v}{k} \binom{x+u+v-k}{n-k}. \tag{309}$$

The proof of this identity will be computational. For the sake of brevity, we will omit the justifications of some steps of this computation; these justifications will instead be provided after the computation.

Here is the computation:

$$
\begin{aligned}
&F_{x,n}\left(u,v\right) \\
&= \sum_{i=0}^{n} \binom{x+u}{n-i} \underbrace{\binom{u+i}{i}}_{= \sum_{b=0}^{i} \binom{u}{b}\binom{i}{b}} \binom{v}{i} \qquad \text{(by the definition of } F_{x,n}\left(u,v\right)\text{)} \\
&\qquad \text{(by an application of Corollary 2.6.3;} \\
&\qquad \text{see Justification 1 below for the details)} \\
&= \sum_{i=0}^{n} \underbrace{\binom{x+u}{n-i} \left(\sum_{b=0}^{i} \binom{u}{b}\binom{i}{b} \right) \binom{v}{i}}_{= \sum_{b=0}^{i} \binom{x+u}{n-i}\binom{u}{b}\binom{i}{b}\binom{v}{i}} \\
&= \underbrace{\sum_{i=0}^{n} \sum_{b=0}^{i}}_{= \sum_{b=0}^{n} \sum_{i=b}^{n}} \binom{x+u}{n-i}\binom{u}{b} \underbrace{\binom{i}{b}\binom{v}{i}}_{= \binom{v}{i}\binom{i}{b} = \binom{v}{b}\binom{v-b}{i-b}} \\
&\qquad \text{(see Justification 2 below for why this equality holds)} \\
&\qquad \text{(by Proposition 1.3.35, applied to } v \text{ and } i \text{ instead of } n \text{ and } a\text{)} \\
&= \sum_{b=0}^{n} \underbrace{\sum_{i=b}^{n} \binom{x+u}{n-i}\binom{u}{b}\binom{v}{b}\binom{v-b}{i-b}}_{= \binom{u}{b}\binom{v}{b} \sum_{i=b}^{n} \binom{x+u}{n-i}\binom{v-b}{i-b}} \\
&= \sum_{b=0}^{n} \binom{u}{b}\binom{v}{b} \underbrace{\sum_{i=b}^{n} \binom{x+u}{n-i}\binom{v-b}{i-b}}_{= \binom{x+u+v-b}{n-b}} \\
&\qquad \text{(by Chu–Vandermonde;} \\
&\qquad \text{see Justification 3 below for the details)} \\
&= \sum_{b=0}^{n} \binom{u}{b}\binom{v}{b}\binom{x+u+v-b}{n-b} = \sum_{k=0}^{n} \binom{u}{k}\binom{v}{k}\binom{x+u+v-k}{n-k}
\end{aligned}
$$

(here, we have renamed the summation index b as k).

Here are the promised **justifications**:

1. **Justification 1:** We need to justify the equality

$$\binom{u+i}{i} = \sum_{b=0}^{i} \binom{u}{b}\binom{i}{b} \tag{310}$$

for each $i \in \{0,1,\ldots,n\}$.

In order to do so, we fix an $i \in \{0,1,\ldots,n\}$. Then, Corollary 2.6.3 (applied to u and i instead of x and y) yields

$$\sum_{k=0}^{i} \binom{u}{k}\binom{i}{k} = \binom{u+i}{i}.$$

Thus,

$$\binom{u+i}{i} = \sum_{k=0}^{i} \binom{u}{k}\binom{i}{k} = \sum_{b=0}^{i} \binom{u}{b}\binom{i}{b}$$

(here, we have renamed the summation index k as b). This proves (310).

2. **Justification 2:** We need to prove the following equality of summation signs:

$$\sum_{i=0}^{n} \sum_{b=0}^{i} = \sum_{b=0}^{n} \sum_{i=b}^{n}. \tag{311}$$

To do so, we transform the left hand side as follows:

$$\underbrace{\sum_{i=0}^{n}}_{= \sum\limits_{i\in\{0,1,\ldots,n\}}} \underbrace{\sum_{b=0}^{i}}_{= \sum\limits_{b\in\{0,1,\ldots,i\}} = \sum\limits_{\substack{b\in\{0,1,\ldots,n\};\\ b\leq i}}}$$

(since the numbers $b\in\{0,1,\ldots,i\}$ are precisely the numbers $b\in\{0,1,\ldots,n\}$ that satisfy $b\leq i$ (because $i\leq n$))

$$= \sum_{i\in\{0,1,\ldots,n\}} \sum_{\substack{b\in\{0,1,\ldots,n\};\\ b\leq i}}$$

$$= \underbrace{\sum_{b\in\{0,1,\ldots,n\}}}_{= \sum\limits_{b=0}^{n}} \underbrace{\sum_{\substack{i\in\{0,1,\ldots,n\};\\ b\leq i}}}_{= \sum\limits_{\substack{i\in\{0,1,\ldots,n\};\\ i\geq b}}}$$

(since the condition "$b\leq i$" is equivalent to "$i\geq b$")

(here, we have interchanged the two summation signs using Theorem 1.6.6)

$$= \sum_{b=0}^{n} \underbrace{\sum_{\substack{i\in\{0,1,\ldots,n\};\\ i\geq b}}}_{= \sum\limits_{i\in\{b,b+1,\ldots,n\}}} = \sum_{b=0}^{n} \underbrace{\sum_{i\in\{b,b+1,\ldots,n\}}}_{= \sum\limits_{i=b}^{n}} = \sum_{b=0}^{n} \sum_{i=b}^{n}.$$

(since the numbers $i\in\{0,1,\ldots,n\}$ that satisfy $i\geq b$ are precisely the numbers $i\in\{b,b+1,\ldots,n\}$ (because $b\geq 0$))

Thus, (311) is proved.

(We note that (311) is an analogue of Corollary 1.6.9 in which the sums start at 0 instead of 1. This yields another easy way to prove (311).)

3. **Justification 3:** We need to prove the equality

$$\sum_{i=b}^{n} \binom{x+u}{n-i} \binom{v-b}{i-b} = \binom{x+u+v-b}{n-b} \tag{312}$$

for each $b \in \{0,1,\ldots,n\}$.

To prove this equality, we fix some $b \in \{0,1,\ldots,n\}$. Then, $b \leq n$, so that $n-b \geq 0$. Therefore, $n-b \in \mathbb{N}$. Hence, the Chu–Vandermonde identity (172) (applied to $x+u$, $v-b$ and $n-b$ instead of x, y and n) yields

$$\begin{aligned}
\binom{x+u+v-b}{n-b} &= \sum_{k=0}^{n-b} \binom{x+u}{k} \binom{v-b}{n-b-k} \\
&= \underbrace{\sum_{i=n-(n-b)}^{n}}_{\substack{=\sum_{i=b}^{n} \\ \text{(since } n-(n-b)=b\text{)}}} \binom{x+u}{n-i} \underbrace{\binom{v-b}{n-b-(n-i)}}_{\substack{=\binom{v-b}{i-b} \\ \text{(since } n-b-(n-i)=i-b\text{)}}} \\
&\qquad \text{(here, we have substituted } n-i \text{ for } k \text{ in the sum)} \\
&= \sum_{i=b}^{n} \binom{x+u}{n-i} \binom{v-b}{i-b}.
\end{aligned}$$

Thus, (312) is proven.

We have now fully justified our above computation. The computation proves the equality (309). The same argument (with the roles of u and v interchanged) shows that

$$F_{x,n}(v,u) = \sum_{k=0}^{n} \binom{v}{k} \binom{u}{k} \binom{x+v+u-k}{n-k}. \tag{313}$$

However, the right hand sides of the equalities (309) and (313) are equal, since

$$\sum_{k=0}^{n} \underbrace{\binom{u}{k}\binom{v}{k}}_{=\binom{v}{k}\binom{u}{k}} \underbrace{\binom{x+u+v-k}{n-k}}_{\substack{=\binom{x+v+u-k}{n-k} \\ \text{(since } u+v=v+u\text{)}}} = \sum_{k=0}^{n} \binom{v}{k} \binom{u}{k} \binom{x+v+u-k}{n-k}.$$

Therefore, the left hand sides of the equalities (309) and (313) must also be equal. In other words, we have $F_{x,n}(u,v) = F_{x,n}(v,u)$. This solves Exercise 2.6.9. □

Exercise 2.6.9 is a generalized and slightly rewritten version of American Mathematical Monthly problem #12016 (by Hideyuki Ohtsuka and Roberto Tauraso). (In the original problem, the sum in the definition of $F_{x,n}(u,v)$ had upper limit v instead of n; this necessitates requiring that $u, v \in \mathbb{N}$.)

7.34. Solution to Exercise 2.8.1

Exercise 2.8.1 appears (with solution) in [Grinbe15, §7.30]. More precisely:

- Exercise 2.8.1 **(a)** is [Grinbe15, Lemma 7.49] (with n and x renamed as m and n).
- Exercise 2.8.1 **(b)** follows from [Grinbe15, Exercise 3.22]. (Namely, rename n as m in [Grinbe15, Exercise 3.22], and substitute n for X in the resulting equality between polynomials; then, you obtain precisely the claim of Exercise 2.8.1 **(b)**.)
- Exercise 2.8.1 **(c)** is [Grinbe15, Corollary 7.53].

To keep these notes self-contained, let us nevertheless give a solution to Exercise 2.8.1 here (this is essentially the first solution given in [Grinbe15, §7.30]):

Solution to Exercise 2.8.1 (sketched). **(a)** Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$.

Let us work with polynomials in one variable X, with real coefficients. Lemma 2.8.1 (applied to $p = n$) yields

$$(1+X)^n = \sum_{i \in \mathbb{N}} \binom{n}{i} X^i \tag{314}$$

(here, we are using the letter i for the summation index that was called m in Lemma 2.8.1, because the letter m is already being used for another number in our current setting).

Substituting $-X$ for X in the equality (314), we obtain

$$\begin{aligned}(1+(-X))^n &= \sum_{i \in \mathbb{N}} \binom{n}{i} \underbrace{(-X)^i}_{=(-1)^i X^i} = \sum_{i \in \mathbb{N}} \binom{n}{i} (-1)^i X^i \\ &= \sum_{i \in \mathbb{N}} (-1)^i \binom{n}{i} X^i = \sum_{j \in \mathbb{N}} (-1)^j \binom{n}{j} X^j\end{aligned}$$

(here, we have renamed the summation index i as j). In view of $1+(-X) = 1-X$, this can be rewritten as

$$(1-X)^n = \sum_{j \in \mathbb{N}} (-1)^j \binom{n}{j} X^j. \tag{315}$$

Substituting X^2 for X on both sides of this equality, we find

$$\left(1-X^2\right)^n = \sum_{j\in\mathbb{N}} (-1)^j \binom{n}{j} \underbrace{\left(X^2\right)^j}_{=X^{2j}} = \sum_{j\in\mathbb{N}} (-1)^j \binom{n}{j} X^{2j}.$$

Define a polynomial P by $P = \left(1-X^2\right)^n$. Thus,

$$P = \left(1-X^2\right)^n = \sum_{j\in\mathbb{N}} (-1)^j \binom{n}{j} X^{2j} = \sum_{\substack{i\in\mathbb{N};\\ i \text{ is even}}} (-1)^{i/2} \binom{n}{i/2} X^i$$

(here, we have substituted i for $2j$ in the sum). Hence,

$$\begin{aligned} &(\text{the } m\text{-th coefficient of } P) \\ &= \begin{cases} (-1)^{m/2} \binom{n}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases}. \end{aligned} \tag{316}$$

On the other hand, we have

$$P = \left(\underbrace{1-X^2}_{=(1-X)(1+X)} \right)^n = \left((1-X)(1+X)\right)^n$$

$$= \underbrace{(1-X)^n}_{\substack{=\sum_{j\in\mathbb{N}} (-1)^j \binom{n}{j} X^j \\ \text{(by (315))}}} \cdot \underbrace{(1+X)^n}_{\substack{=\sum_{i\in\mathbb{N}} \binom{n}{i} X^i \\ \text{(by (314))}}}$$

$$= \left(\sum_{j\in\mathbb{N}} (-1)^j \binom{n}{j} X^j \right) \cdot \left(\sum_{i\in\mathbb{N}} \binom{n}{i} X^i \right)$$

$$= \sum_{j\in\mathbb{N}} \underbrace{(-1)^j \binom{n}{j} X^j \sum_{i\in\mathbb{N}} \binom{n}{i} X^i}_{=\sum_{i\in\mathbb{N}} (-1)^j \binom{n}{j} X^j \binom{n}{i} X^i} = \sum_{j\in\mathbb{N}} \sum_{i\in\mathbb{N}} (-1)^j \underbrace{\binom{n}{j} X^j \binom{n}{i} X^i}_{=\binom{n}{j}\binom{n}{i} X^{j+i}}$$

$$= \sum_{j\in\mathbb{N}} \sum_{i\in\mathbb{N}} (-1)^j \binom{n}{j} \binom{n}{i} X^{j+i} = \sum_{(j,i)\in\mathbb{N}^2} (-1)^j \binom{n}{j} \binom{n}{i} X^{j+i}$$

$$\left(\begin{array}{c} \text{by the first equality sign in Theorem 1.6.11,} \\ \text{since only finitely many } (j,i) \in \mathbb{N}^2 \text{ satisfy } (-1)^j \binom{n}{j} \binom{n}{i} X^{j+i} \neq 0 \end{array} \right)$$

$$= \sum_{k\in\mathbb{N}} \sum_{\substack{(j,i)\in\mathbb{N}^2; \\ j+i=k}} (-1)^j \binom{n}{j} \binom{n}{i} \underbrace{X^{j+i}}_{\substack{=X^k \\ \text{(since } j+i=k\text{)}}}$$

(here, we have used the analogue of (37) for infinite sums)

$$= \sum_{k\in\mathbb{N}} \sum_{\substack{(j,i)\in\mathbb{N}^2; \\ j+i=k}} (-1)^j \binom{n}{j} \binom{n}{i} X^k = \sum_{k\in\mathbb{N}} \left(\sum_{\substack{(j,i)\in\mathbb{N}^2; \\ j+i=k}} (-1)^j \binom{n}{j} \binom{n}{i} \right) X^k.$$

Hence,

$$(\text{the } m\text{-th coefficient of } P) = \sum_{\substack{(j,i)\in\mathbb{N}^2; \\ j+i=m}} (-1)^j \binom{n}{j} \binom{n}{i} = \sum_{k=0}^{m} (-1)^k \binom{n}{k} \binom{n}{m-k}$$

(here, we have substituted $(k, m-k)$ for (j,i) in the sum, since the map

$$\begin{aligned} \{0,1,\ldots,m\} &\to \left\{ (j,i) \in \mathbb{N}^2 \mid j+i=m \right\}, \\ k &\mapsto (k, m-k) \end{aligned}$$

is a bijection[254]).

Comparing this with (316), we find

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} \binom{n}{m-k} = \begin{cases} (-1)^{m/2} \binom{n}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases}.$$

This solves Exercise 2.8.1 **(a)**.

(b) This is a matter of applying Corollary 2.6.10. Indeed, let us fix $m \in \mathbb{N}$. Define two polynomials P and Q (in one variable X, with real coefficients) by

$$P = \sum_{k=0}^{m} (-1)^k \binom{X}{k} \binom{X}{m-k} \tag{317}$$

and

$$Q = \begin{cases} (-1)^{m/2} \binom{X}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases}. \tag{318}$$

(Both P and Q are indeed polynomials, since m is fixed!)

Now, recall Proposition 2.6.12. This proposition says that if we substitute a real number $n \in \mathbb{R}$ into the polynomial $\binom{X}{k}$ (for some given $k \in \mathbb{R}$), then we obtain the number $\binom{n}{k}$. Renaming the number n as x in this statement, we obtain the following: If we substitute a real number $x \in \mathbb{R}$ into the polynomial $\binom{X}{k}$ (for some given $k \in \mathbb{R}$), then we obtain the number $\binom{x}{k}$.

Hence, for each $x \in \mathbb{R}$, we have

$$P(x) = \sum_{k=0}^{m} (-1)^k \binom{x}{k} \binom{x}{m-k} \tag{319}$$

(indeed, this follows by substituting x on both sides of (317)) and

$$Q(x) = \begin{cases} (-1)^{m/2} \binom{x}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases} \tag{320}$$

[254] In informal terms, this is just saying that each pair $(j,i) \in \mathbb{N}^2$ of nonnegative integers satisfying $j+i=m$ has the form $(k, m-k)$ for a unique $k \in \{0,1,\ldots,m\}$ (namely, for $k=j$), and conversely, any pair of the latter form is a pair $(j,i) \in \mathbb{N}^2$ of nonnegative integers satisfying $j+i=m$.

(likewise). Hence, for each $x \in \mathbb{N}$, we have

$$\begin{aligned} P(x) &= \sum_{k=0}^{m} (-1)^k \binom{x}{k} \binom{x}{m-k} \qquad \text{(by (319))} \\ &= \begin{cases} (-1)^{m/2} \binom{x}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases} \qquad \text{(by Exercise 2.8.1 \textbf{(a)}, applied to } n = x) \\ &= Q(x) \qquad \text{(by (320))}. \end{aligned}$$

Therefore, Corollary 2.6.10 yields $P = Q$. Thus, $P(x) = Q(x)$ for all $x \in \mathbb{R}$. In view of (319) and (320), we can rewrite this as follows:

$$\sum_{k=0}^{m} (-1)^k \binom{x}{k} \binom{x}{m-k} = \begin{cases} (-1)^{m/2} \binom{x}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases} \qquad \text{for all } x \in \mathbb{R}.$$

Renaming the variable x as n in this result, we obtain the following:

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} \binom{n}{m-k} = \begin{cases} (-1)^{m/2} \binom{n}{m/2}, & \text{if } m \text{ is even;} \\ 0, & \text{if } m \text{ is odd} \end{cases} \qquad \text{for all } n \in \mathbb{R}.$$

In other words, the claim of Exercise 2.8.1 **(a)** holds for all $n \in \mathbb{R}$ (rather than only for $n \in \mathbb{N}$). This solves Exercise 2.8.1 **(b)**.

(c) Let $n \in \mathbb{N}$. Then,

$$\begin{aligned} &\sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k}^2}_{= \binom{n}{k}\binom{n}{k}} \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \underbrace{\binom{n}{k}}_{= \binom{n}{n-k}} \\ &\qquad \text{(by Theorem 1.3.11)} \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{n}{n-k} = \begin{cases} (-1)^{n/2} \binom{n}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \end{aligned}$$

(by Exercise 2.8.1 **(a)**, applied to $m = n$). This solves Exercise 2.8.1 **(c)**. □

7.35. Solution to Exercise 2.8.2

Exercise 2.8.2 is Gazeta Matematica problem #400, proposed by Mihal Prunescu. Here is a solution using Exercise 2.8.1 **(c)**:

Solution to Exercise 2.8.2. First, we shall show that

$$2^m = \sum_{i=0}^{n} \binom{m}{i} \tag{321}$$

for each $m \in \{0, 1, \ldots, n\}$.

[*Proof of (321):* Let $m \in \{0, 1, \ldots, n\}$. Each $k \in \{m+1, m+2, \ldots, n\}$ satisfies $k \geq m+1 > m$ and therefore

$$\binom{m}{k} = 0 \tag{322}$$

(by Proposition 1.3.6, applied to m instead of n).

However, from $m \in \{0, 1, \ldots, n\}$, we obtain $0 \leq m \leq n$. Hence, we can split the sum $\sum_{k=0}^{n} \binom{m}{k}$ as follows:

$$\sum_{k=0}^{n} \binom{m}{k} = \underbrace{\sum_{k=0}^{m} \binom{m}{k}}_{\substack{=2^m \\ \text{(by Corollary 1.3.27,} \\ \text{applied to } m \text{ instead of } n\text{)}}} + \sum_{k=m+1}^{n} \underbrace{\binom{m}{k}}_{\substack{=0 \\ \text{(by (322))}}} = 2^m + \underbrace{\sum_{k=m+1}^{n} 0}_{=0} = 2^m.$$

Therefore,

$$2^m = \sum_{k=0}^{n} \binom{m}{k} = \sum_{i=0}^{n} \binom{m}{i} \qquad \left(\begin{array}{c} \text{here, we renamed the} \\ \text{summation index } k \text{ as } i \end{array} \right).$$

This proves (321).]

Now, we have

$$\begin{aligned}
&\sum_{k=0}^{n} \underbrace{(-2)^k}_{=(-1)^k 2^k} \binom{n}{k}\binom{2n-k}{n-k} \\
&= \sum_{k=0}^{n} (-1)^k \underbrace{2^k}_{\substack{=\sum_{i=0}^{n}\binom{k}{i} \\ \text{(by (321),} \\ \text{applied to } m=k)}} \binom{n}{k}\binom{2n-k}{n-k} \\
&= \sum_{k=0}^{n} \underbrace{(-1)^k \left(\sum_{i=0}^{n}\binom{k}{i}\right)\binom{n}{k}\binom{2n-k}{n-k}}_{=\sum_{i=0}^{n}(-1)^k\binom{k}{i}\binom{n}{k}\binom{2n-k}{n-k}} \\
&= \underbrace{\sum_{k=0}^{n}\sum_{i=0}^{n}}_{=\sum_{i=0}^{n}\sum_{k=0}^{n}} (-1)^k \underbrace{\binom{k}{i}\binom{n}{k}}_{=\binom{n}{k}\binom{k}{i}} \binom{2n-k}{n-k} \\
&= \sum_{i=0}^{n}\sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k}\binom{k}{i}}_{=\binom{n}{i}\binom{n-i}{k-i}} \binom{2n-k}{n-k} \\
&\qquad \left(\begin{array}{c}\text{by Proposition 1.3.35,} \\ \text{applied to } a=k \text{ and } b=i\end{array}\right) \\
&= \sum_{i=0}^{n} \underbrace{\sum_{k=0}^{n} (-1)^k \binom{n}{i}\binom{n-i}{k-i}\binom{2n-k}{n-k}}_{=\binom{n}{i}\sum_{k=0}^{n}(-1)^k\binom{n-i}{k-i}\binom{2n-k}{n-k}} \\
&= \sum_{i=0}^{n} \binom{n}{i} \sum_{k=0}^{n} (-1)^k \binom{n-i}{k-i}\binom{2n-k}{n-k}. \qquad (323)
\end{aligned}$$

Now, we shall show that

$$\sum_{k=0}^{n} (-1)^k \binom{n-i}{k-i}\binom{2n-k}{n-k} = (-1)^i \binom{n}{i} \qquad (324)$$

for each $i \in \{0,1,\ldots,n\}$.

[*Proof of (324):* Let $i \in \{0,1,\ldots,n\}$. Thus, $0 \leq i \leq n$. From $i \leq n$, we obtain $n-i \geq 0$, thus $n-i \in \mathbb{N}$.

For each $k \in \mathbb{Z}$, we have

$$\begin{aligned}
\binom{2n-k}{n-k} &= \binom{-(k-2n)}{n-k} \qquad (\text{since } 2n-k = -(k-2n)) \\
&= (-1)^{n-k} \binom{(k-2n)+(n-k)-1}{n-k} \qquad \left(\begin{array}{c} \text{by Proposition 1.3.7,} \\ \text{applied to } k-2n \text{ and } n-k \\ \text{instead of } n \text{ and } k \end{array} \right) \\
&= (-1)^{n-k} \binom{-n-1}{n-k} \qquad (325)
\end{aligned}$$

(since $(k-2n)+(n-k)-1 = -n-1$). Hence,

$$\begin{aligned}
&\sum_{k=0}^{n} (-1)^k \binom{n-i}{k-i} \underbrace{\binom{2n-k}{n-k}}_{\substack{=(-1)^{n-k}\binom{-n-1}{n-k} \\ \text{(by (325))}}} \\
&= \sum_{k=0}^{n} (-1)^k \binom{n-i}{k-i} (-1)^{n-k} \binom{-n-1}{n-k} \\
&= \sum_{k=0}^{n} \underbrace{(-1)^k (-1)^{n-k}}_{\substack{=(-1)^{k+(n-k)}=(-1)^n \\ \text{(since } k+(n-k)=n\text{)}}} \binom{n-i}{k-i} \binom{-n-1}{n-k} \\
&= \sum_{k=0}^{n} (-1)^n \binom{n-i}{k-i} \binom{-n-1}{n-k}. \qquad (326)
\end{aligned}$$

However, each $k \in \{0, 1, \ldots, i-1\}$ satisfies $k \leq i-1 < i$ and thus $k-i < 0$, so that $k-i \notin \mathbb{N}$ and therefore

$$\binom{n-i}{k-i} = 0 \qquad (327)$$

(by (43), applied to $n-i$ and $k-i$ instead of n and k). Now, (326) becomes

$$\begin{aligned}
&\sum_{k=0}^{n} (-1)^k \binom{n-i}{k-i} \binom{2n-k}{n-k} \\
&= \sum_{k=0}^{n} (-1)^n \binom{n-i}{k-i} \binom{-n-1}{n-k} \\
&= \sum_{k=0}^{i-1} (-1)^n \underbrace{\binom{n-i}{k-i}}_{\substack{=0 \\ \text{(by (327))}}} \binom{-n-1}{n-k} + \sum_{k=i}^{n} (-1)^n \binom{n-i}{k-i} \binom{-n-1}{n-k} \\
&\qquad \text{(here, we have split the sum, because } 0 \leq i \leq n\text{)} \\
&= \underbrace{\sum_{k=0}^{i-1} (-1)^n 0 \binom{-n-1}{n-k}}_{=0} + \sum_{k=i}^{n} (-1)^n \binom{n-i}{k-i} \binom{-n-1}{n-k} \\
&= \sum_{k=i}^{n} (-1)^n \binom{n-i}{k-i} \binom{-n-1}{n-k} \\
&= \sum_{k=0}^{n-i} (-1)^n \underbrace{\binom{n-i}{(k+i)-i}}_{\substack{= \binom{n-i}{k} \\ \text{(since } (k+i)-i=k\text{)}}} \underbrace{\binom{-n-1}{n-(k+i)}}_{\substack{= \binom{-n-1}{(n-i)-k} \\ \text{(since } n-(k+i)=(n-i)-k\text{)}}} \qquad \left(\begin{array}{c}\text{here, we have substituted } k+i \\ \text{for } k \text{ in the sum}\end{array}\right) \\
&= \sum_{k=0}^{n-i} (-1)^n \binom{n-i}{k} \binom{-n-1}{(n-i)-k} \\
&= (-1)^n \sum_{k=0}^{n-i} \binom{n-i}{k} \binom{-n-1}{(n-i)-k}. \qquad (328)
\end{aligned}$$

Now, recall that $n-i \in \mathbb{N}$. Thus, the Chu–Vandermonde identity (172) (applied to $n-i$, $n-i$ and $-n-1$ instead of n, x and y) yields

$$\binom{(n-i)+(-n-1)}{n-i} = \sum_{k=0}^{n-i} \binom{n-i}{k} \binom{-n-1}{(n-i)-k}.$$

Therefore,

$$\begin{aligned}
&\sum_{k=0}^{n-i} \binom{n-i}{k} \binom{-n-1}{(n-i)-k} \\
&= \binom{(n-i)+(-n-1)}{n-i} \\
&= \binom{-(i+1)}{n-i} \qquad (\text{since } (n-i)+(-n-1) = -(i+1)) \\
&= (-1)^{n-i} \binom{(i+1)+(n-i)-1}{n-i} \qquad \left(\begin{array}{c} \text{by Proposition 1.3.7,} \\ \text{applied to } i+1 \text{ and } n-i \\ \text{instead of } n \text{ and } k \end{array} \right) \\
&= (-1)^{n-i} \underbrace{\binom{n}{n-i}}_{= \binom{n}{n-(n-i)}} \qquad (\text{since } (i+1)+(n-i)-1 = n) \\
&\qquad \begin{array}{c} \\ \\ \\ \text{(by Theorem 1.3.11,} \\ \text{applied to } k=n-i\text{)} \end{array} \\
&= (-1)^{n-i} \binom{n}{n-(n-i)} = (-1)^{n-i} \binom{n}{i} \qquad (\text{since } n-(n-i) = i).
\end{aligned}$$

Hence, we can rewrite (328) as

$$\sum_{k=0}^{n} (-1)^k \binom{n-i}{k-i} \binom{2n-k}{n-k} = \underbrace{(-1)^n (-1)^{n-i}}_{\substack{= (-1)^{n+(n-i)} = (-1)^i \\ (\text{since } n+(n-i) = 2n-i \equiv i \bmod 2)}} \qquad \binom{n}{i} = (-1)^i \binom{n}{i}.$$

This proves (324).]

Now, (323) becomes

$$\begin{aligned}
&\sum_{k=0}^{n} (-2)^k \binom{n}{k} \binom{2n-k}{n-k} \\
&= \sum_{i=0}^{n} \binom{n}{i} \underbrace{\sum_{k=0}^{n} (-1)^k \binom{n-i}{k-i} \binom{2n-k}{n-k}}_{=(-1)^i \binom{n}{i} \text{ (by (324))}} = \sum_{i=0}^{n} \underbrace{\binom{n}{i} (-1)^i \binom{n}{i}}_{=(-1)^i \binom{n}{i}^2} \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i}^2 \\
&= \sum_{k=0}^{n} (-1)^k \binom{n}{k}^2 \qquad \text{(here, we have renamed the summation index } i \text{ as } k\text{)} \\
&= \begin{cases} (-1)^{n/2} \binom{n}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \qquad \text{(by Exercise 2.8.1 \textbf{(c)})}.
\end{aligned}$$

This solves Exercise 2.8.2. □

7.36. Reference to solution to Exercise 2.9.1

Proposition 2.9.12 appears (with proof) in [18f-hw3s, Proposition 6.4] (with S and T renamed as G and S).

7.37. Solution to Exercise 2.9.2

Before we solve Exercise 2.9.2, let us recall two fundamental facts from elementary set theory (often called de Morgan's laws):

Proposition 7.37.1. Let U, X and Y be three sets. Then:
(a) We have $U \setminus (X \cup Y) = (U \setminus X) \cap (U \setminus Y)$.
(b) We have $U \setminus (X \cap Y) = (U \setminus X) \cup (U \setminus Y)$.

We will not prove Proposition 7.37.1, as it is the domain of introductory textbooks on proofs and sets; suffice to say that both parts of the proposition can be proved in straightforward ways using basic logic and the fact that two sets P and Q satisfy $P = Q$ if and only if $(P \subseteq Q$ and $Q \subseteq P)$.

We will use the following generalization of Proposition 7.37.1 to multiple sets:

Proposition 7.37.2. Let k be a positive integer. Let U be a set. Let $P_1, P_2, \ldots, P_k$ be any k sets. Then:

(a) We have

$$U \setminus (P_1 \cup P_2 \cup \cdots \cup P_k) = (U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_k).$$

(b) We have

$$U \setminus (P_1 \cap P_2 \cap \cdots \cap P_k) = (U \setminus P_1) \cup (U \setminus P_2) \cup \cdots \cup (U \setminus P_k).$$

Proof of Proposition 7.37.2. **(a)** We shall prove Proposition 7.37.2 **(a)** by induction on k:

Induction base: It is easy to see that Proposition 7.37.2 **(a)** holds for $k = 1$ [255]. This completes the induction base.

Induction step: Let m be a positive integer. Assume that Proposition 7.37.2 **(a)** holds for $k = m$. We must prove that Proposition 7.37.2 **(a)** holds for $k = m + 1$.

Let U be a set. Let $P_1, P_2, \ldots, P_{m+1}$ be any $m + 1$ sets. We have assumed that Proposition 7.37.2 **(a)** holds for $k = m$. Thus, Proposition 7.37.2 **(a)** (applied to $k = m$) yields

$$U \setminus (P_1 \cup P_2 \cup \cdots \cup P_m) = (U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_m).$$

Now,

$$\begin{aligned}
&U \setminus \underbrace{(P_1 \cup P_2 \cup \cdots \cup P_{m+1})}_{=(P_1 \cup P_2 \cup \cdots \cup P_m) \cup P_{m+1}} \\
&= U \setminus ((P_1 \cup P_2 \cup \cdots \cup P_m) \cup P_{m+1}) \\
&= \underbrace{(U \setminus (P_1 \cup P_2 \cup \cdots \cup P_m))}_{=(U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_m)} \cap (U \setminus P_{m+1}) \\
&\qquad \text{(by Proposition 7.37.1 \textbf{(a)}, applied to } X = P_1 \cup P_2 \cup \cdots \cup P_m \text{ and } Y = P_{m+1}) \\
&= ((U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_m)) \cap (U \setminus P_{m+1}) \\
&= (U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_{m+1}).
\end{aligned}$$

Now, forget that we fixed U and $P_1, P_2, \ldots, P_{m+1}$. We thus have shown that if U is a set, and if $P_1, P_2, \ldots, P_{m+1}$ are any $m + 1$ sets, then

$$U \setminus (P_1 \cup P_2 \cup \cdots \cup P_{m+1}) = (U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_{m+1}).$$

In other words, Proposition 7.37.2 **(a)** holds for $k = m + 1$. This completes the induction step. Hence, Proposition 7.37.2 **(a)** is proved by induction.

[255] *Proof.* If U is a set, and if $P_1, P_2, \ldots, P_1$ are any 1 sets, then

$$U \setminus \underbrace{(P_1 \cup P_2 \cup \cdots \cup P_1)}_{=P_1} = U \setminus P_1 = (U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_1)$$

(since $(U \setminus P_1) \cap (U \setminus P_2) \cap \cdots \cap (U \setminus P_1) = U \setminus P_1$). In other words, Proposition 7.37.2 **(a)** holds for $k = 1$.

(b) In order to obtain a proof of Proposition 7.37.2 **(b)**, it suffices to make some simple modifications to our above proof of Proposition 7.37.2 **(a)** (namely: replace all "$\cup$" signs by "$\cap$" signs and vice versa, and replace the reference to Proposition 7.37.1 **(a)** by a reference to Proposition 7.37.1 **(b)**). $\square$

Now, let us solve Exercise 2.9.2:

Solution to Exercise 2.9.2. Let U be the set $A_1 \cup A_2 \cup \cdots \cup A_n$. Thus, U is the union of the n finite sets $A_1, A_2, \ldots, A_n$, and thus itself a finite set. Moreover, all the n sets $A_1, A_2, \ldots, A_n$ clearly are subsets of their union $A_1 \cup A_2 \cup \cdots \cup A_n$. In other words, all the n sets $A_1, A_2, \ldots, A_n$ are subsets of U (since $U = A_1 \cup A_2 \cup \cdots \cup A_n$).

For each $i \in \{1, 2, \ldots, n\}$, we define a set B_i by $B_i = U \setminus A_i$. Thus, for each $i \in \{1, 2, \ldots, n\}$, the set B_i is a subset of the set U (since $B_i = U \setminus A_i$), and thus is finite (since U is finite). Hence, Theorem 2.9.1 (applied to B_i instead of A_i) yields

$$\begin{aligned} &\left|B_1 \cup B_2 \cup \cdots \cup B_n\right| \\ &= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_m}\right|. \end{aligned} \tag{329}$$

On the other hand, Theorem 2.9.1 (applied to U instead of A_i) yields

$$\begin{aligned} \left|\underbrace{U \cup U \cup \cdots \cup U}_{n \text{ times}}\right| &= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left|\underbrace{\underbrace{U \cap U \cap \cdots \cap U}_{m \text{ times}}}_{\substack{=U \\ (\text{since } m \geq 1)}}\right| \\ &= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} |U|. \end{aligned}$$

In view of

$$\underbrace{U \cup U \cup \cdots \cup U}_{n \text{ times}} = U \qquad (\text{since } n \text{ is positive}),$$

this rewrites as

$$|U| = \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} |U|. \tag{330}$$

However, we have the following two statements:

Statement 1: We have

$$\left|B_1 \cup B_2 \cup \cdots \cup B_n\right| = |U| - \left|A_1 \cap A_2 \cap \cdots \cap A_n\right|.$$

Statement 2: Let $m \in \{1,2,\ldots,n\}$. Let $(i_1, i_2, \ldots, i_m) \in [n]^m$. Then,

$$\left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_m}\right| = |U| - \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|.$$

[*Proof of Statement 1:* Recall that all the n sets $A_1, A_2, \ldots, A_n$ are subsets of U. Thus, in particular, A_1 is a subset of U. In other words, $A_1 \subseteq U$. Hence, $A_1 \cap A_2 \cap \cdots \cap A_n$ is a subset of U as well (since $A_1 \cap A_2 \cap \cdots \cap A_n \subseteq A_1 \subseteq U$). Hence, Theorem 1.4.7 **(a)** (applied to U and $A_1 \cap A_2 \cap \cdots \cap A_n$ instead of A and B) yields

$$|U \setminus (A_1 \cap A_2 \cap \cdots \cap A_n)| = |U| - |A_1 \cap A_2 \cap \cdots \cap A_n|. \tag{331}$$

But each $i \in \{1,2,\ldots,n\}$ satisfies $B_i = U \setminus A_i$ (by the definition of B_i). Hence,

$$(B_1, B_2, \ldots, B_n) = (U \setminus A_1, U \setminus A_2, \ldots, U \setminus A_n).$$

Thus,

$$B_1 \cup B_2 \cup \cdots \cup B_n = (U \setminus A_1) \cup (U \setminus A_2) \cup \cdots \cup (U \setminus A_n).$$

But Proposition 7.37.2 **(b)** (applied to $k = n$ and $P_j = A_j$) yields

$$U \setminus (A_1 \cap A_2 \cap \cdots \cap A_n) = (U \setminus A_1) \cup (U \setminus A_2) \cup \cdots \cup (U \setminus A_n).$$

Comparing these two equalities, we obtain

$$U \setminus (A_1 \cap A_2 \cap \cdots \cap A_n) = B_1 \cup B_2 \cup \cdots \cup B_n.$$

In light of this equality, we can rewrite (331) as

$$|B_1 \cup B_2 \cup \cdots \cup B_n| = |U| - |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

This proves Statement 1.]

[*Proof of Statement 2:* We have $(i_1, i_2, \ldots, i_m) \in [n]^m$. Thus, $i_1, i_2, \ldots, i_m$ are elements of $[n] = \{1,2,\ldots,n\}$.

Recall that all the n sets $A_1, A_2, \ldots, A_n$ are subsets of U. Hence, in particular, the sets $A_{i_1}, A_{i_2}, \ldots, A_{i_m}$ are subsets of U (since $i_1, i_2, \ldots, i_m$ are elements of $\{1,2,\ldots,n\}$). Thus, their union $A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}$ is a subset of U as well (since a union of subsets of U is always a subset of U). Hence, Theorem 1.4.7 **(a)** (applied to U and $A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}$ instead of A and B) yields

$$\left|U \setminus \left(A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right)\right| = |U| - \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|. \tag{332}$$

But each $j \in \{1,2,\ldots,m\}$ satisfies $B_{i_j} = U \setminus A_{i_j}$ (by the definition of B_{i_j}). Hence,

$$\left(B_{i_1}, B_{i_2}, \ldots, B_{i_m}\right) = \left(U \setminus A_{i_1}, U \setminus A_{i_2}, \ldots, U \setminus A_{i_m}\right).$$

Thus,

$$B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_m} = \left(U \setminus A_{i_1}\right) \cap \left(U \setminus A_{i_2}\right) \cap \cdots \cap \left(U \setminus A_{i_m}\right).$$

But Proposition 7.37.2 **(a)** (applied to $k = m$ and $P_j = A_{i_j}$) yields

$$U \setminus \left(A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right) = \left(U \setminus A_{i_1}\right) \cap \left(U \setminus A_{i_2}\right) \cap \cdots \cap \left(U \setminus A_{i_m}\right).$$

Comparing these two equalities, we obtain

$$U \setminus \left(A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right) = B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_m}.$$

In light of this equality, we can rewrite (332) as

$$\left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_m}\right| = |U| - \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|.$$

This proves Statement 2.]

Now, (329) becomes

$$\begin{aligned}
&\left|B_1 \cup B_2 \cup \cdots \cup B_n\right| \\
&= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \underbrace{\left|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_m}\right|}_{\substack{=|U|-\left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right| \\ \text{(by Statement 2)}}} \\
&= \sum_{m=1}^{n} (-1)^{m-1} \underbrace{\sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \left(|U| - \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|\right)}_{= \sum\limits_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} |U| - \sum\limits_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|} \\
&= \sum_{m=1}^{n} \underbrace{(-1)^{m-1} \left(\sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} |U| - \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right| \right)}_{= (-1)^{m-1} \sum\limits_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} |U| - (-1)^{m-1} \sum\limits_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|} \\
&= \sum_{m=1}^{n} \left((-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} |U| - (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right| \right) \\
&= \underbrace{\sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} |U|}_{\substack{=|U| \\ \text{(by (330))}}} - \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right| \\
&= |U| - \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1<i_2<\cdots<i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right|. \qquad (333)
\end{aligned}$$

Now, Statement 1 yields

$$|B_1 \cup B_2 \cup \cdots \cup B_n| = |U| - |A_1 \cap A_2 \cap \cdots \cap A_n| .$$

Solving this equality for $|A_1 \cap A_2 \cap \cdots \cap A_n|$, we find

$$\begin{aligned}
&|A_1 \cap A_2 \cap \cdots \cap A_n| \\
&= |U| - \underbrace{|B_1 \cup B_2 \cup \cdots \cup B_n|}_{= |U| - \sum\limits_{m=1}^{n} (-1)^{m-1} \sum\limits_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right| \text{ (by (333))}} \\
&= |U| - \left(|U| - \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right| \right) \\
&= \sum_{m=1}^{n} (-1)^{m-1} \sum_{\substack{(i_1,i_2,\ldots,i_m) \in [n]^m; \\ i_1 < i_2 < \cdots < i_m}} \left|A_{i_1} \cup A_{i_2} \cup \cdots \cup A_{i_m}\right| .
\end{aligned}$$

This solves Exercise 2.9.2. □

7.38. Solution to Exercise 2.9.3

Solution to Exercise 2.9.3. Here are the statements that were left unproved in our (sketched) proof of Proposition 2.9.14:[256]

> *Statement 1:* Let $\sigma \in S_X$ be a permutation satisfying ($\sigma(i) = i$ for each $i \in I$). Then, we can define a map $\widetilde{\sigma} : X \setminus I \to X \setminus I$ by setting
>
> $$\widetilde{\sigma}(p) = \sigma(p) \qquad \text{for each } p \in X \setminus I.$$
>
> *Statement 2:* Let $\sigma \in S_X$ be a permutation satisfying ($\sigma(i) = i$ for each $i \in I$). Then, the map $\widetilde{\sigma} : X \setminus I \to X \setminus I$ defined in Statement 1 is a permutation of $X \setminus I$ (and thus belongs to $S_{X \setminus I}$).
>
> *Statement 3:* Let τ be a permutation of $X \setminus I$. Then, we can define a map $\widehat{\tau} : X \to X$ by setting
>
> $$\widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{for each } p \in X.$$

[256] Statement 2 shows that the map A is well-defined. Statement 4 shows that the map B is well-defined. Statement 5 and Statement 6 (when combined) show that the maps A and B are mutually inverse.

Statement 4: Let τ be a permutation of $X \setminus I$. Then, the map $\widehat{\tau} : X \to X$ defined in Statement 3 is a permutation in S_X satisfying ($\widehat{\tau}(i) = i$ for each $i \in I$) (and thus belongs to $\{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}$).

Statement 5: The maps A and B satisfy $A \circ B = \mathrm{id}$.

Statement 6: The maps A and B satisfy $B \circ A = \mathrm{id}$.

Let us now prove these statements:

[*Proof of Statement 1:* We have $\sigma(p) \in X \setminus I$ for each $p \in X \setminus I$ [257]. Hence, we can define a map $\widetilde{\sigma} : X \setminus I \to X \setminus I$ by setting

$$\widetilde{\sigma}(p) = \sigma(p) \qquad \text{for each } p \in X \setminus I.$$

This proves Statement 1.]

[*Proof of Statement 2:* The map σ is a permutation of X (since $\sigma \in S_X$), thus a bijection from X to X. Hence, σ is bijective, thus injective and surjective.

We must prove that $\widetilde{\sigma}$ is a permutation of $X \setminus I$. In other words, we must prove that $\widetilde{\sigma}$ is a bijection from $X \setminus I$ to $X \setminus I$.

It is easy to see that the map $\widetilde{\sigma}$ is injective[258] and surjective[259]. Hence, $\widetilde{\sigma}$ is bijective. In other words, $\widetilde{\sigma}$ is a bijection from X to X. Hence, $\widetilde{\sigma}$ is a permutation of $X \setminus I$. In other words, $\widetilde{\sigma}$ belongs to $S_{X \setminus I}$. This proves Statement 2.]

[*Proof of Statement 3:* Let $p \in X$. We claim that $\begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \in X$.

[257] *Proof.* Let $p \in X \setminus I$. We must prove that $\sigma(p) \in X \setminus I$.

Assume the contrary. Thus, $\sigma(p) \notin X \setminus I$. Combining $\sigma(p) \in X$ with $\sigma(p) \notin X \setminus I$, we obtain $\sigma(p) \in X \setminus (X \setminus I) \subseteq I$.

Now, recall that ($\sigma(i) = i$ for each $i \in I$). Applying this to $i = \sigma(p)$, we obtain $\sigma(\sigma(p)) = \sigma(p)$.

But the map σ is a permutation of X (since $\sigma \in S_X$), thus a bijection from X to X. Hence, σ is bijective, thus injective. In other words, if u and v are two elements of X such that $\sigma(u) = \sigma(v)$, then $u = v$. Applying this to $u = \sigma(p)$ and $v = p$, we find $\sigma(p) = p$ (since $\sigma(\sigma(p)) = \sigma(p)$). Hence, $\sigma(p) = p \in X \setminus I$, so that $\sigma(p) \notin I$. This contradicts $\sigma(p) \in I$. This contradiction shows that our assumption was wrong. Hence, $\sigma(p) \in X \setminus I$ is proved.

[258] *Proof.* Let u and v be two elements of $X \setminus I$ such that $\widetilde{\sigma}(u) = \widetilde{\sigma}(v)$. We shall show that $u = v$.

The definition of $\widetilde{\sigma}$ yields $\widetilde{\sigma}(u) = \sigma(u)$ and $\widetilde{\sigma}(v) = \sigma(v)$. Hence, $\sigma(u) = \widetilde{\sigma}(u) = \widetilde{\sigma}(v) = \sigma(v)$. Since σ is injective, we can thus conclude that $u = v$.

Now, forget that we fixed u and v. We thus have proved that if u and v are two elements of $X \setminus I$ such that $\widetilde{\sigma}(u) = \widetilde{\sigma}(v)$, then $u = v$. In other words, the map $\widetilde{\sigma}$ is injective.

[259] *Proof.* Let $p \in X \setminus I$. We shall prove that there exists some $x \in X \setminus I$ such that $p = \widetilde{\sigma}(x)$.

Recall that the map σ is injective. Thus, there exists some $q \in X$ such that $p = \sigma(q)$. Consider this q. Thus, $\sigma(q) = p \notin I$ (since $p \in X \setminus I$).

If we had $q \in I$, then we would have $\sigma(q) = q$ (by the assumption "$\sigma(i) = i$ for each $i \in I$", applied to $i = q$), which would entail $\sigma(q) = q \in I$; but this would contradict $\sigma(q) \notin I$. This, we cannot have $q \in I$. Hence, we have $q \notin I$. Combining $q \in X$ with $q \notin I$, we obtain $q \in X \setminus I$. Hence, $\widetilde{\sigma}(q)$ is well-defined. Moreover, the definition of $\widetilde{\sigma}$ yields $\widetilde{\sigma}(q) = \sigma(q) = p$. In other words, $p = \widetilde{\sigma}(q)$. Hence, there exists some $x \in X \setminus I$ such that $p = \widetilde{\sigma}(x)$ (namely, $x = q$).

Forget that we fixed p. We thus have proved that for each $p \in X \setminus I$, there exists some $x \in X \setminus I$ such that $p = \widetilde{\sigma}(x)$. In other words, $\widetilde{\sigma}$ is surjective.

Indeed, if $p \in I$, then this follows from

$$\begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} = p \qquad (\text{since } p \in I)$$
$$\in X.$$

Hence, for the rest of this proof, we WLOG assume that $p \notin I$. Hence, $p \in X \setminus I$ (since $p \in X$ and $p \notin I$), so that $\tau(p)$ is well-defined (since τ is a permutation of $X \setminus I$). Moreover,

$$\begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} = \tau(p) \in X \setminus I \qquad (\text{since } \tau \text{ is a permutation of } X \setminus I)$$
$$\subseteq X.$$

Thus, $\begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \in X$ is proved.

Now, forget that we fixed p. We thus have shown that $\begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \in X$ for each $p \in X$. Hence, we can define a map $\widehat{\tau} : X \to X$ by setting

$$\widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{for each } p \in X.$$

This proves Statement 3.]

[*Proof of Statement 4:* We shall first prove that $\widehat{\tau}$ is a permutation of X.

There are two ways to prove this. One way to do so is by showing that $\widehat{\tau}$ is both surjective and injective. This is straightforward but boring. A slicker approach is by constructing its inverse map. Let us do the latter.

The map τ is a permutation of $X \setminus I$, thus a bijection from $X \setminus I$ to $X \setminus I$. Hence, its inverse τ^{-1} is well-defined, and is also a bijection from $X \setminus I$ to $X \setminus I$. In other words, τ^{-1} is also a permutation of $X \setminus I$. Thus, Statement 4 (applied to τ^{-1} instead of τ) shows that we can define a map $\widehat{\tau^{-1}} : X \to X$ by setting

$$\widehat{\tau^{-1}}(p) = \begin{cases} \tau^{-1}(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{for each } p \in X.$$

Consider this map $\widehat{\tau^{-1}}$. Note that $\tau \circ \tau^{-1} = \mathrm{id}$ and $\tau^{-1} \circ \tau = \mathrm{id}$. We shall now prove that $\widehat{\tau} \circ \widehat{\tau^{-1}} = \mathrm{id}$ and $\widehat{\tau^{-1}} \circ \widehat{\tau} = \mathrm{id}$.

[*Proof of* $\widehat{\tau} \circ \widehat{\tau^{-1}} = \mathrm{id}$*:* Let $q \in X$. We shall show that $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = q$.

Indeed, we are in one of the following two cases:

Case 1: We have $q \in I$.

Case 2: We have $q \notin I$.

Let us first consider Case 1. In this case, we have $q \in I$. Now, the definition of $\widehat{\tau^{-1}}$ yields $\widehat{\tau^{-1}}(q) = \begin{cases} \tau^{-1}(q), & \text{if } q \notin I; \\ q, & \text{if } q \in I \end{cases} = q$ (since $q \in I$). Applying the map $\widehat{\tau}$ to both sides of this equality, we find

$$\widehat{\tau}\left(\underbrace{\widehat{\tau^{-1}}(q)}_{=q}\right) = \widehat{\tau}(q) = \begin{cases} \tau(q), & \text{if } q \notin I; \\ q, & \text{if } q \in I \end{cases} \qquad \text{(by the definition of } \widehat{\tau}\text{)}$$
$$= q \qquad (\text{since } q \in I).$$

Hence, $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = \widehat{\tau}\left(\widehat{\tau^{-1}}(q)\right) = q$. Thus, $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = q$ is proven in Case 1.

Let us next consider Case 2. In this case, we have $q \notin I$. Combining $q \in X$ with $q \notin I$, we find $q \in X \setminus I$. Hence, $\tau^{-1}(q)$ is well-defined (since τ^{-1} is a map from from $X \setminus I$ to $X \setminus I$) and satisfies $\tau^{-1}(q) \in X \setminus I$ (for the same reason). From $\tau^{-1}(q) \in X \setminus I$, we obtain $\tau^{-1}(q) \in X$ and $\tau^{-1}(q) \notin I$.

The definition of $\widehat{\tau^{-1}}$ yields $\widehat{\tau^{-1}}(q) = \begin{cases} \tau^{-1}(q), & \text{if } q \notin I; \\ q, & \text{if } q \in I \end{cases} = \tau^{-1}(q)$ (since $q \notin I$). Applying the map $\widehat{\tau}$ to both sides of this equality, we find

$$\widehat{\tau}\left(\underbrace{\widehat{\tau^{-1}}(q)}_{=q}\right) = \widehat{\tau}\left(\tau^{-1}(q)\right)$$
$$= \begin{cases} \tau\left(\tau^{-1}(q)\right), & \text{if } \tau^{-1}(q) \notin I; \\ \tau^{-1}(q), & \text{if } \tau^{-1}(q) \in I \end{cases} \qquad \text{(by the definition of } \widehat{\tau}\text{)}$$
$$= \tau\left(\tau^{-1}(q)\right) \qquad \left(\text{since } \tau^{-1}(q) \notin I\right)$$
$$= q.$$

Hence, $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = \widehat{\tau}\left(\widehat{\tau^{-1}}(q)\right) = q$. Thus, $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = q$ is proven in Case 2.

We have now proved $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = q$ in each of the two Cases 1 and 2. Thus, $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = q$ always holds. Hence, $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = q = \mathrm{id}(q)$.

Now, forget that we fixed q. We thus know that $\left(\widehat{\tau} \circ \widehat{\tau^{-1}}\right)(q) = \mathrm{id}(q)$ for each $q \in X$. In other words, $\widehat{\tau} \circ \widehat{\tau^{-1}} = \mathrm{id}$. The same argument (but with the roles of τ and τ^{-1} interchanged[260]) shows that $\widehat{\tau^{-1}} \circ \widehat{\tau} = \mathrm{id}$. Combining these two equalities, we conclude that the maps $\widehat{\tau}$ and $\widehat{\tau^{-1}}$ are mutually inverse. Hence, the map $\widehat{\tau}$ is

[260]This means that the roles of $\widehat{\tau}$ and $\widehat{\tau^{-1}}$ also get interchanged.

invertible. In other words, $\widehat{\tau}$ is a bijection from X to X. In other words, $\widehat{\tau}$ is a permutation of X. In other words, $\widehat{\tau} \in S_X$.

For each $i \in I$, we have

$$\begin{aligned}\widehat{\tau}(i) &= \begin{cases} \tau(i), & \text{if } i \notin I; \\ i, & \text{if } i \in I \end{cases} \qquad \text{(by the definition of } \widehat{\tau}\text{)} \\ &= i \qquad (\text{since } i \in I).\end{aligned}$$

Thus, we have shown that ($\widehat{\tau}(i) = i$ for each $i \in I$). Hence, $\widehat{\tau}$ is an element of S_X that satisfies ($\widehat{\tau}(i) = i$ for each $i \in I$).

In other words, $\widehat{\tau}$ belongs to $\{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}$. This proves Statement 4.]

[*Proof of Statement 5:* Let $\tau \in S_{X \setminus I}$. We shall show that $(A \circ B)(\tau) = \tau$.

Indeed, let $p \in X \setminus I$. Thus, $p \in X$ and $p \notin I$. Now, $B(\tau) = \widehat{\tau}$ (by the definition of B). Also,

$$(A \circ B)(\tau) = A(B(\tau)) = \widetilde{B(\tau)} \qquad \text{(by the definition of } A\text{)}.$$

Applying both sides of this equality to p, we obtain

$$\begin{aligned}((A \circ B)(\tau))(p) &= \left(\widetilde{B(\tau)}\right)(p) = \underbrace{(B(\tau))}_{=\widehat{\tau}}(p) \qquad \left(\text{by the definition of } \widetilde{B(\tau)}\right) \\ &= \widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{(by the definition of } \widehat{\tau}\text{)} \\ &= \tau(p) \qquad (\text{since } p \notin I).\end{aligned}$$

Forget that we fixed p. We thus have shown that $((A \circ B)(\tau))(p) = \tau(p)$ for each $p \in X \setminus I$. In other words, $(A \circ B)(\tau) = \tau = \mathrm{id}(\tau)$.

Forget that we fixed τ. We thus have shown that $(A \circ B)(\tau) = \mathrm{id}(\tau)$ for each $\tau \in S_{X \setminus I}$. In other words, $A \circ B = \mathrm{id}$. This proves Statement 5.]

[*Proof of Statement 6:* Let $\gamma \in \{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}$. We shall show that $(B \circ A)(\gamma) = \gamma$.

We have $\gamma \in \{\sigma \in S_X \mid \sigma(i) = i \text{ for each } i \in I\}$. In other words, γ is a $\sigma \in S_X$ such that ($\sigma(i) = i$ for each $i \in I$). In other words, γ is an element of S_X and satisfies

$$(\gamma(i) = i \text{ for each } i \in I). \tag{334}$$

Thus, γ is a permutation of X (since $\gamma \in S_X$).

Now, let $p \in X$. We shall show that $((B \circ A)(\gamma))(p) = \gamma(p)$.

We have $A(\gamma) = \widetilde{\gamma}$ (by the definition of A). Furthermore,

$$(B \circ A)(\gamma) = B(A(\gamma)) = \widehat{A(\gamma)}.$$

Applying both sides of this equality to p, we obtain

$$\begin{aligned}\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) &= \left(\widehat{A\left(\gamma\right)}\right)\left(p\right) \\ &= \begin{cases} \left(A\left(\gamma\right)\right)\left(p\right), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases}\end{aligned} \tag{335}$$

(by the definition of $\widehat{A\left(\gamma\right)}$).

Now, we are in one of the following two cases:

Case 1: We have $p \in I$.

Case 2: We have $p \notin I$.

Let us first consider Case 1. In this case, we have $p \in I$. Thus, $\gamma\left(p\right) = p$ (by (334), applied to $i = p$). But (335) becomes

$$\begin{aligned}\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) &= \begin{cases} \left(A\left(\gamma\right)\right)\left(p\right), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} = p \qquad \left(\text{since } p \in I\right) \\ &= \gamma\left(p\right) \qquad \left(\text{since } \gamma\left(p\right) = p\right).\end{aligned}$$

Hence, $\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) = \gamma\left(p\right)$ is proved in Case 1.

Let us now consider Case 2. In this case, we have $p \notin I$. Thus, $p \in X \setminus I$ (since $p \in X$ and $p \notin I$). Now, (335) becomes

$$\begin{aligned}\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) &= \begin{cases} \left(A\left(\gamma\right)\right)\left(p\right), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} = \underbrace{\left(A\left(\gamma\right)\right)}_{=\widetilde{\gamma}}\left(p\right) \qquad \left(\text{since } p \notin I\right) \\ &= \widetilde{\gamma}\left(p\right) = \gamma\left(p\right) \qquad \left(\text{by the definition of } \widetilde{\gamma}\right).\end{aligned}$$

Hence, $\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) = \gamma\left(p\right)$ is proved in Case 2.

We have now proved $\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) = \gamma\left(p\right)$ in each of the two Cases 1 and 2. Thus, $\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) = \gamma\left(p\right)$ always holds.

Forget that we fixed p. We thus have proved that $\left(\left(B \circ A\right)\left(\gamma\right)\right)\left(p\right) = \gamma\left(p\right)$ for each $p \in X$. In other words, $\left(B \circ A\right)\left(\gamma\right) = \gamma = \mathrm{id}\left(\gamma\right)$.

Forget that we fixed γ. We thus have proved that $\left(B \circ A\right)\left(\gamma\right) = \mathrm{id}\left(\gamma\right)$ for each $\gamma \in \left\{\sigma \in S_X \mid \sigma\left(i\right) = i \text{ for each } i \in I\right\}$. In other words, $B \circ A = \mathrm{id}$. This proves Statement 6.]

We have now proved all six Statements 1, 2, 3, 4, 5 and 6. This fills all the gaps in our proof of Proposition 2.9.14. Thus, Exercise 2.9.3 is solved. □

7.39. Solution to Exercise 2.9.4

In order to solve Exercise 2.9.4, we have to prove parts **(a)**, **(b)** and **(c)** of Theorem 1.7.9. In doing so, we can use part **(d)** of this theorem, since it has already been proven.

*Proof of Theorem 1.7.9 **(b)**.* Let n be an integer such that $n \geq 1$. Thus, n is a positive integer, so that $n \in \mathbb{N}$ and $n-1 \in \mathbb{N}$. Hence, Theorem 1.7.9 **(d)** (applied to $n-1$ instead of n) yields

$$D_{n-1} = \sum_{k=0}^{n-1} (-1)^k \frac{(n-1)!}{k!}. \tag{336}$$

Also, Theorem 1.7.9 **(d)** yields

$$D_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = (-1)^n \underbrace{\frac{n!}{n!}}_{=1} + \sum_{k=0}^{n-1} (-1)^k \underbrace{\frac{n!}{k!}}_{\substack{=\frac{(n-1)!\cdot n}{k!} \\ \text{(since Proposition 1.3.2} \\ \text{yields } n! = (n-1)!\cdot n)}}$$

(here, we have split off the addend for $k = n$ from the sum)

$$= (-1)^n + \sum_{k=0}^{n-1} \underbrace{(-1)^k \frac{(n-1)!\cdot n}{k!}}_{=n(-1)^k \frac{(n-1)!}{k!}} = (-1)^n + \underbrace{\sum_{k=0}^{n-1} n\,(-1)^k \frac{(n-1)!}{k!}}_{=n\sum_{k=0}^{n-1}(-1)^k \frac{(n-1)!}{k!}}$$

$$= (-1)^n + n \underbrace{\sum_{k=0}^{n-1} (-1)^k \frac{(n-1)!}{k!}}_{\substack{=D_{n-1} \\ \text{(by (336))}}} = (-1)^n + nD_{n-1} = nD_{n-1} + (-1)^n.$$

This proves Theorem 1.7.9 **(b)**. □

Now that we have proved Theorem 1.7.9 **(b)**, we shall derive Theorem 1.7.9 **(a)** from it. In doing so, we shall use the following simple lemma ([19f-hw1s, Exercise 5]):

Lemma 7.39.1. Let $(u_0, u_1, u_2, \ldots)$ be a sequence of real numbers such that every integer $n \geq 1$ satisfies

$$u_n = nu_{n-1} + (-1)^n. \tag{337}$$

Then, $u_n = (n-1)(u_{n-1} + u_{n-2})$ for each integer $n \geq 2$.

Proof of Lemma 7.39.1. Let $n \geq 2$ be an integer. Thus, $n-1 \geq 2-1 = 1$. Hence, (337) (applied to $n-1$ instead of n) yields

$$u_{n-1} = (n-1)\underbrace{u_{(n-1)-1}}_{=u_{n-2}} + \underbrace{(-1)^{n-1}}_{=-(-1)^n} = (n-1)\,u_{n-2} + \left(-(-1)^n\right)$$
$$= (n-1)\,u_{n-2} - (-1)^n.$$

Thus,

$$u_{n-1} + (-1)^n = (n-1)\, u_{n-2}. \tag{338}$$

But $n \geq 2 \geq 1$. Hence, (337) yields

$$\begin{aligned} u_n &= \underbrace{n}_{=(n-1)+1} u_{n-1} + (-1)^n = \underbrace{((n-1)+1)\, u_{n-1}}_{=(n-1)u_{n-1}+u_{n-1}} + (-1)^n \\ &= (n-1)\, u_{n-1} + \underbrace{u_{n-1} + (-1)^n}_{\substack{=(n-1)u_{n-2} \\ \text{(by (338))}}} = (n-1)\, u_{n-1} + (n-1)\, u_{n-2} \\ &= (n-1)\left(u_{n-1} + u_{n-2}\right). \end{aligned}$$

This proves Lemma 7.39.1. □

*Proof of Theorem 1.7.9 **(a)**.* Theorem 1.7.9 **(b)** shows that every integer $n \geq 1$ satisfies $D_n = nD_{n-1} + (-1)^n$. Hence, Lemma 7.39.1 (applied to $u_j = D_j$) shows that $D_n = (n-1)\left(D_{n-1} + D_{n-2}\right)$ for each integer $n \geq 2$. This proves Theorem 1.7.9 **(a)**. □

It remains to prove Theorem 1.7.9 **(c)**. There are several ways to do this. In particular, there is a rather simple double-counting argument, which uses the following concept:

Definition 7.39.2. Let X be a set. Let $f : X \to X$ be any map. Then, $\operatorname{Fix} f$ shall denote the set of all fixed points of f.

We will need a fact similar to Proposition 2.9.14:

Proposition 7.39.3. Let X be a set. Let I be a subset of X. Then, there is a bijection

$$\text{from } \{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\} \text{ to } \{\text{derangements of } X \setminus I\}.$$

Proof of Proposition 7.39.3. Let us first give a sketch of the proof (similarly to the proof of Proposition 2.9.14 we sketched), and then fill in the details (similarly to the solution of Exercise 2.9.3):

To each permutation $\sigma \in S_X$ satisfying $\operatorname{Fix}\sigma = I$, we can assign a derangement $\widetilde{\sigma}$ of $X \setminus I$ by letting

$$\widetilde{\sigma}(p) = \sigma(p) \qquad \text{for each } p \in X \setminus I.$$

[261] This defines a map

$$\begin{aligned} A : \{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\} &\to \{\text{derangements of } X \setminus I\}, \\ \sigma &\mapsto \widetilde{\sigma}. \end{aligned}$$

[261] Why is this map $\widetilde{\sigma}$ well-defined, and why is it really a derangement of $X \setminus I$? This will follow from Statement 1′ and Statement 2′ further below.

Conversely, to each derangement τ of $X \setminus I$, we can assign a permutation $\widehat{\tau} \in S_X$ satisfying $\operatorname{Fix} \widehat{\tau} = I$ by setting

$$\widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{for each } p \in X.$$

[262] This defines a map

$$B : \{\text{derangements of } X \setminus I\} \to \{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\}, \\ \tau \mapsto \widehat{\tau}.$$

The maps A and B are well-defined and mutually inverse[263]. Hence, they are bijections. Thus, there is a bijection from the set $\{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\}$ to the set $\{\text{derangements of } X \setminus I\}$ (namely, A). This proves Proposition 7.39.3, once the details are filled in.

Let us now fill in the details. Here are the statements that were left unproved in our above proof:[264]

> *Statement 1′:* Let $\sigma \in S_X$ be a permutation satisfying $\operatorname{Fix}\sigma = I$. Then, we can define a map $\widetilde{\sigma} : X \setminus I \to X \setminus I$ by setting
>
> $$\widetilde{\sigma}(p) = \sigma(p) \qquad \text{for each } p \in X \setminus I.$$
>
> *Statement 2′:* Let $\sigma \in S_X$ be a permutation satisfying $\operatorname{Fix}\sigma = I$. Then, the map $\widetilde{\sigma} : X \setminus I \to X \setminus I$ defined in Statement 1′ is a derangement of $X \setminus I$ (and thus belongs to $\{\text{derangements of } X \setminus I\}$).
>
> *Statement 3′:* Let τ be a derangement of $X \setminus I$. Then, we can define a map $\widehat{\tau} : X \to X$ by setting
>
> $$\widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{for each } p \in X.$$
>
> *Statement 4′:* Let τ be a derangement of $X \setminus I$. Then, the map $\widehat{\tau} : X \to X$ defined in Statement 3′ is a permutation in S_X satisfying $\operatorname{Fix}\widehat{\tau} = I$ (and thus belongs to $\{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\}$).
>
> *Statement 5′:* The maps A and B satisfy $A \circ B = \mathrm{id}$.
>
> *Statement 6′:* The maps A and B satisfy $B \circ A = \mathrm{id}$.

[262] Again, this will be proved below.

[263] Again, this will be proved below.

[264] Statement 2′ shows that the map A is well-defined. Statement 4′ shows that the map B is well-defined. Statement 5′ and Statement 6′ (when combined) show that the maps A and B are mutually inverse.

Let us now prove these statements:

[*Proof of Statement 1′:* Let $i \in I$. Then, $i \in I = \operatorname{Fix}\sigma$ (since $\operatorname{Fix}\sigma = I$). This means that i is a fixed point of σ (since $\operatorname{Fix}\sigma$ was defined as the set of all fixed points of σ). In other words, $\sigma(i) = i$ (by the definition of "fixed point").

Forget that we fixed i. We thus have shown that $\sigma(i) = i$ for each $i \in I$. Thus, Statement 1 from our above solution to Exercise 2.9.3 shows that we can define a map $\widetilde{\sigma} : X \setminus I \to X \setminus I$ by setting

$$\widetilde{\sigma}(p) = \sigma(p) \qquad \text{for each } p \in X \setminus I.$$

This proves Statement 1′.]

[*Proof of Statement 2′:* The map σ is a permutation of X (since $\sigma \in S_X$), thus a bijection from X to X. Moreover, we have $\sigma(i) = i$ for each $i \in I$. (Indeed, this can be proven just as in our proof of Statement 1′ above.) Thus, Statement 2 from our above solution to Exercise 2.9.3 shows that $\widetilde{\sigma}$ is a permutation of $X \setminus I$. Moreover, this permutation $\widetilde{\sigma}$ has no fixed points[265]; in other words, $\widetilde{\sigma}$ is a derangement of $X \setminus I$ (by the definition of "derangement"). In other words, $\widetilde{\sigma}$ belongs to $\{\text{derangements of } X \setminus I\}$. This proves Statement 2′.]

[*Proof of Statement 3′:* The map τ is a derangement of $X \setminus I$, and thus is a permutation of $X \setminus I$ (since any derangement is a permutation). Hence, Statement 3 from our above solution to Exercise 2.9.3 shows that we can define a map $\widehat{\tau} : X \to X$ by setting

$$\widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} \qquad \text{for each } p \in X.$$

This proves Statement 3′.]

[*Proof of Statement 4′:* The map τ is a derangement of $X \setminus I$, and thus is a permutation of $X \setminus I$ (since any derangement is a permutation). Hence, Statement 4 from our above solution to Exercise 2.9.3 shows that the map $\widehat{\tau} : X \to X$ is a permutation in S_X satisfying ($\widehat{\tau}(i) = i$ for each $i \in I$). Now, we shall show that $\operatorname{Fix}\widehat{\tau} = I$.

Indeed, $I \subseteq \operatorname{Fix}\widehat{\tau}$ [266] and $\operatorname{Fix}\widehat{\tau} \subseteq I$ [267]. Combining these two facts, we obtain $\operatorname{Fix}\widehat{\tau} = I$. Thus, we have showed that $\widehat{\tau}$ is an element of S_X that satisfies $\operatorname{Fix}\widehat{\tau} = I$.

[265] *Proof.* Let z be a fixed point of $\widetilde{\sigma}$. Thus, z is an element of $X \setminus I$ satisfying $\widetilde{\sigma}(z) = z$ (by the definition of "fixed point"). But the definition of $\widetilde{\sigma}$ yields $\widetilde{\sigma}(z) = \sigma(z)$, so that $\sigma(z) = \widetilde{\sigma}(z) = z$. In other words, z is a fixed point of σ. In other words, $z \in \operatorname{Fix}\sigma$ (by the definition of $\operatorname{Fix}\sigma$). Hence, $z \in \operatorname{Fix}\sigma = I$. But recall that $z \in X \setminus I$, so that $z \in X$ and $z \notin I$. Now, $z \in I$ contradicts $z \notin I$.

Forget that we fixed z. We thus have obtained a contradiction for each fixed point z of $\widetilde{\sigma}$. Hence, there exist no fixed points of $\widetilde{\sigma}$. In other words, $\widetilde{\sigma}$ has no fixed points.

[266] *Proof.* Let $i \in I$. The definition of $\widehat{\tau}$ yields $\widehat{\tau}(i) = \begin{cases} \tau(i), & \text{if } i \notin I; \\ i, & \text{if } i \in I \end{cases} = i$ (since $i \in I$). In other words, i is a fixed point of $\widehat{\tau}$. In other words, $i \in \operatorname{Fix}\widehat{\tau}$ (by the definition of $\operatorname{Fix}\widehat{\tau}$).

Forget that we fixed i. We thus have showed that $i \in \operatorname{Fix}\widehat{\tau}$ for each $i \in I$. In other words, $I \subseteq \operatorname{Fix}\widehat{\tau}$.

[267] *Proof.* Let $p \in \operatorname{Fix}\widehat{\tau}$. Thus, p is a fixed point of $\widehat{\tau}$ (by the definition of $\operatorname{Fix}\widehat{\tau}$). In other words, p is an element of X satisfying $\widehat{\tau}(p) = p$.

We want to prove that $p \in I$. Indeed, assume the contrary. Thus, $p \notin I$. Combining $p \in X$

In other words, $\widehat{\tau}$ belongs to $\{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\}$. This proves Statement 4′.]

[*Proof of Statement 5′:* The proof of Statement 5′ is entirely analogous to the proof of Statement 5 in our above solution to Exercise 2.9.3 (since any derangement of $X \setminus I$ is a permutation of $X \setminus I$).]

[*Proof of Statement 6′:* The proof of Statement 6′ is entirely analogous to the proof of Statement 6 in our above solution to Exercise 2.9.3.]

We have now proved all six Statements 1′, 2′, 3′, 4′, 5′ and 6′. This fills all the gaps in our above argument. Hence, Proposition 7.39.3 is completely proved. □

We can draw the following conclusion from Proposition 7.39.3 (analogous to Corollary 2.9.16):

Corollary 7.39.4. Let $n \in \mathbb{N}$. Let X be an n-element set. Let I be a subset of X. Then,

$$|\{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\}| = D_{n-|I|}.$$

Proof of Corollary 7.39.4. The set $X \setminus I$ is finite and satisfies $|X \setminus I| = n - |I|$. (This can be proved in the same way as in our above proof of Corollary 2.9.16.)

Proposition 7.39.3 shows that there is a bijection

$$\text{from } \{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\} \text{ to } \{\text{derangements of } X \setminus I\}.$$

Hence, the bijection principle yields

$$\begin{aligned} |\{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\}| &= |\{\text{derangements of } X \setminus I\}| \\ &= (\#\text{ of derangements of } X \setminus I). \end{aligned}$$

But $X \setminus I$ is an $(n - |I|)$-element set (since $|X \setminus I| = n - |I|$), and we have $n - |I| = |X \setminus I| \in \mathbb{N}$. Hence, Lemma 1.7.6 (applied to $X \setminus I$ and $n - |I|$ instead of X and n) shows that

$$(\#\text{ of derangements of } X \setminus I) = (\#\text{ of derangements of } [n - |I|]) = D_{n-|I|}$$

(since $D_{n-|I|}$ is defined as the # of derangements of $[n - |I|]$). Thus,

$$|\{\sigma \in S_X \mid \operatorname{Fix}\sigma = I\}| = (\#\text{ of derangements of } X \setminus I) = D_{n-|I|}.$$

This proves Corollary 7.39.4. □

with $p \notin I$, we obtain $p \in X \setminus I$. Now, the definition of $\widehat{\tau}$ yields

$$\widehat{\tau}(p) = \begin{cases} \tau(p), & \text{if } p \notin I; \\ p, & \text{if } p \in I \end{cases} = \tau(p) \qquad (\text{since } p \notin I),$$

so that $\tau(p) = \widehat{\tau}(p) = p$. In other words, p is a fixed point of τ. But the permutation τ is a derangement, and thus has no fixed points (by the definition of "derangement"). Hence, p cannot be a fixed point of τ. This contradicts the fact that p is a fixed point of τ. This contradiction shows that our assumption was false. Hence, $p \in I$ is proven.

Now, forget that we fixed p. We thus have proved that $p \in I$ for each $p \in \operatorname{Fix}\widehat{\tau}$. In other words, $\operatorname{Fix}\widehat{\tau} \subseteq I$.

We can now prove Theorem 1.7.9 **(c)** at last:

Proof of Theorem 1.7.9 (c). Let $n \in \mathbb{N}$. Then, $\operatorname{Fix}\sigma$ is a subset of $[n]$ for each permutation $\sigma \in S_{[n]}$ (by the definition of $\operatorname{Fix}\sigma$). Hence, the sum rule (Theorem 1.2.5) yields

$$\left|S_{[n]}\right| = \sum_{I \text{ is a subset of } [n]} \left(\#\text{ of } \sigma \in S_{[n]} \text{ satisfying } \operatorname{Fix}\sigma = I\right).$$

Comparing this with

$$\begin{aligned}\left|S_{[n]}\right| &= \underbrace{|[n]|}_{=n}! \qquad \text{(by (220), applied to } X = [n]) \\ &= n!,\end{aligned}$$

we obtain

$$\begin{aligned} n! &= \sum_{I \text{ is a subset of } [n]} \underbrace{\left(\#\text{ of } \sigma \in S_{[n]} \text{ satisfying } \operatorname{Fix}\sigma = I\right)}_{\substack{=\left|\left\{\sigma \in S_{[n]} \mid \operatorname{Fix}\sigma = I\right\}\right| \\ =D_{n-|I|} \\ \text{(by Corollary 7.39.4, applied to } X=[n])}} \\ &= \sum_{I \text{ is a subset of } [n]} D_{n-|I|}. \end{aligned} \tag{339}$$

Now, let us note that each subset I of $[n]$ satisfies $|I| \in \{0, 1, \ldots, n\}$ (since Theorem 1.4.7 **(b)** yields $|I| \leq |[n]| = n$). Hence, we can split the sum $\sum_{I \text{ is a subset of } [n]} D_{n-|I|}$ according to the value of $|I|$, obtaining the following:

$$\begin{aligned} \sum_{I \text{ is a subset of } [n]} D_{n-|I|} &= \sum_{k \in \{0,1,\ldots,n\}} \sum_{\substack{I \text{ is a subset of } [n]; \\ |I|=k}} \underbrace{D_{n-|I|}}_{\substack{=D_{n-k} \\ \text{(since } |I|=k)}} \\ &= \underbrace{\sum_{k \in \{0,1,\ldots,n\}}}_{=\sum_{k=0}^{n}} \underbrace{\sum_{\substack{I \text{ is a subset of } [n]; \\ |I|=k}} D_{n-k}}_{=(\#\text{ of subsets } I \text{ of } [n] \text{ satisfying } |I|=k) D_{n-k}} \\ &= \sum_{k=0}^{n} \underbrace{\left(\#\text{ of subsets } I \text{ of } [n] \text{ satisfying } |I| = k\right)}_{\substack{=(\#\text{ of } k\text{-element subsets of } [n]) \\ =\binom{n}{k} \\ \text{(by Theorem 1.3.12, applied to } S=[n])}} D_{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k} D_{n-k}. \end{aligned}$$

Thus, (339) becomes

$$n! = \sum_{I \text{ is a subset of } [n]} D_{n-|I|} = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}.$$

This proves Theorem 1.7.9 **(c).** □

We have now proved parts **(a)**, **(b)** and **(c)** of Theorem 1.7.9. This solves Exercise 2.9.4.

7.40. Reference to solution to Exercise 2.9.5

Exercise 2.9.5 is [19s, Exercise 2.14.4].

7.41. Reference to solution to Exercise 2.9.6

Exercise 2.9.6 is [19s, Exercise 2.14.5].

7.42. Reference to solution to Exercise 2.9.7

Exercise 2.9.7 asks us to prove Lemma 2.9.21.

Lemma 2.9.21 appears (with a sketch of a proof) in [Galvin17, Lemma 16.2]. Alternatively, it can be proved by induction on n, similarly to how Theorem 1.4.1 was proved in our solution of Exercise 1.4.1. (Actually, if we apply Lemma 2.9.21 **(a)** to $a_i = 1$, then we obtain $(\#\text{ of subsets of } [n]) = 2^n$, which is exactly what Theorem 1.4.1 says for $S = [n]$.)

Alternatively, Lemma 2.9.21 can be easily obtained from the following identity:

Lemma 7.42.1. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be n numbers. Let $b_1, b_2, \ldots, b_n$ be n further numbers. Then,

$$\prod_{i=1}^{n} (a_i + b_i) = \sum_{I \subseteq [n]} \left(\prod_{i \in I} a_i \right) \left(\prod_{i \in [n] \setminus I} b_i \right).$$

Lemma 7.42.1 appears (with detailed proof) in [Grinbe15, Exercise 6.1 **(a)**]. Now, Lemma 2.9.21 can easily be derived from it:

Proof of Lemma 2.9.21. **(a)** Lemma 7.42.1 (applied to $b_i = 1$) yields

$$\prod_{i=1}^{n} (a_i + 1) = \sum_{I \subseteq [n]} \left(\prod_{i \in I} a_i \right) \underbrace{\left(\prod_{i \in [n] \setminus I} 1 \right)}_{=1} = \sum_{I \subseteq [n]} \prod_{i \in I} a_i.$$

Hence,

$$\sum_{I\subseteq[n]}\prod_{i\in I}a_i=\prod_{i=1}^{n}\underbrace{\left(a_i+1\right)}_{=1+a_i}=\prod_{i=1}^{n}\left(1+a_i\right)=\left(1+a_1\right)\left(1+a_2\right)\cdots\left(1+a_n\right).$$

This proves Lemma 2.9.21 **(a)**.

(b) Lemma 2.9.21 **(a)** (applied to $-a_i$ instead of a_i) yields

$$\begin{aligned}\sum_{I\subseteq[n]}\prod_{i\in I}\left(-a_i\right)&=\left(1+\left(-a_1\right)\right)\left(1+\left(-a_2\right)\right)\cdots\left(1+\left(-a_n\right)\right)\\&=\left(1-a_1\right)\left(1-a_2\right)\cdots\left(1-a_n\right)\end{aligned}$$

(since $1+\left(-a_i\right)=1-a_i$ for each $i\in[n]$). Comparing this with

$$\sum_{I\subseteq[n]}\underbrace{\prod_{i\in I}\left(-a_i\right)}_{=\left(-1\right)^{|I|}\prod_{i\in I}a_i}=\sum_{I\subseteq[n]}\left(-1\right)^{|I|}\prod_{i\in I}a_i,$$

we obtain

$$\sum_{I\subseteq[n]}\left(-1\right)^{|I|}\prod_{i\in I}a_i=\left(1-a_1\right)\left(1-a_2\right)\cdots\left(1-a_n\right).$$

This proves Lemma 2.9.21 **(b)**. □

7.43. Solution to Exercise 2.9.8

In order to solve Exercise 2.9.8, we need to prove Lemma 2.9.25. First, we will show an auxiliary fact:

Lemma 7.43.1. Any two distinct primes are coprime.

Proof of Lemma 7.43.1. Let p and q be two distinct primes. We must prove that p and q are coprime. In other words, we must prove that $\gcd\left(p,q\right)=1$ (since this is what it means for p and q to be coprime).

Assume the contrary. Thus, $\gcd\left(p,q\right)\neq1$.

The definition of $\gcd\left(p,q\right)$ shows that $\gcd\left(p,q\right)$ is the greatest positive integer that divides both p and q. Thus, $\gcd\left(p,q\right)$ is a positive integer and divides both p and q. In particular, $\gcd\left(p,q\right)$ is a positive divisor of p (since $\gcd\left(p,q\right)$ is positive and divides p).

But p is prime. In other words, p is an integer greater than 1 and having the property that the only positive divisors of p are 1 and p. In particular, the only positive divisors of p are 1 and p. Hence, $\gcd\left(p,q\right)$ must be either 1 or p (since $\gcd\left(p,q\right)$ is a positive divisor of p). Since $\gcd\left(p,q\right)$ cannot be 1 (because $\gcd\left(p,q\right)\neq1$), we thus conclude that $\gcd\left(p,q\right)=p$.

Similarly, we obtain $\gcd\left(p,q\right)=q$ (since $\gcd\left(p,q\right)$ divides not only p but also q).

Comparing $\gcd(p,q) = p$ with $\gcd(p,q) = q$, we obtain $p = q$. This contradicts the fact that p and q are distinct. This contradiction shows that our assumption was false. Hence, $\gcd(p,q) = 1$ is proved. In other words, p and q are coprime. This proves Lemma 7.43.1. □

We can now prove Lemma 2.9.25:

Proof of Lemma 2.9.25. The k numbers $b_1, b_2, \ldots, b_k$ are primes, and thus are positive integers.

Lemma 7.43.1 shows that any two distinct primes are coprime. Hence, any k distinct primes are mutually coprime. Thus, the k positive integers $b_1, b_2, \ldots, b_k$ are mutually coprime (since they are k distinct primes). Thus, Lemma 2.9.24 shows that $b_1 b_2 \cdots b_k \mid c$. This proves Lemma 2.9.25. □

Thus, Exercise 2.9.8 is solved.

7.44. Solution to Exercise 2.9.9

In order to solve Exercise 2.9.9, we must prove Lemma 2.9.26.

Proof of Lemma 2.9.26. We must prove the equivalence (230). We shall do this by separately proving the "$\Longrightarrow$" and "$\Longleftarrow$" implications of this equivalence:

Proof of the "$\Longrightarrow$" implication of (230): Assume that p_j divides m for each $j \in I$. We must show that $\prod_{i \in I} p_i$ divides m.

Let $h_1, h_2, \ldots, h_k$ be all elements of I, listed in some order (with no repetitions). Thus, $I = \{h_1, h_2, \ldots, h_k\}$ and $\prod_{i \in I} p_i = p_{h_1} p_{h_2} \cdots p_{h_k}$.

The primes $p_{h_1}, p_{h_2}, \ldots, p_{h_k}$ are distinct[268].

Let $i \in \{1, 2, \ldots, k\}$. Hence, $h_i \in \{h_1, h_2, \ldots, h_k\} = I$. But p_j divides m for each $j \in I$ (by our assumption). Applying this to $j = h_i$, we obtain that p_{h_i} divides m (since $h_i \in I$). In other words, $p_{h_i} \mid m$.

Forget that we fixed i. We thus have showed that $p_{h_i} \mid m$ for each $i \in \{1, 2, \ldots, k\}$. Hence, Lemma 2.9.25 (applied to $b_i = p_{h_i}$) shows that $p_{h_1} p_{h_2} \cdots p_{h_k} \mid m$ (since $p_{h_1}, p_{h_2}, \ldots, p_{h_k}$ are k distinct primes). In view of $\prod_{i \in I} p_i = p_{h_1} p_{h_2} \cdots p_{h_k}$, this rewrites as $\prod_{i \in I} p_i \mid m$. In other words, $\prod_{i \in I} p_i$ divides m.

We thus have shown that if p_j divides m for each $j \in I$, then $\prod_{i \in I} p_i$ divides m. In other words, we have proved the "$\Longrightarrow$" implication of (230).

[268] *Proof.* Let u and v be two elements of $[k]$ such that $u \neq v$. We shall show that $p_{h_u} \neq p_{h_v}$.

The elements $h_1, h_2, \ldots, h_k$ are distinct (since they are all elements of I, listed **with no repetitions**). Hence, from $u \neq v$, we obtain $h_u \neq h_v$. Therefore, $p_{h_u} \neq p_{h_v}$, since all the primes p_i (for different $i \in I$) are distinct.

Forget that we fixed u and v. We thus have shown that if u and v are two elements of $[k]$ such that $u \neq v$, then $p_{h_u} \neq p_{h_v}$. In other words, the primes $p_{h_1}, p_{h_2}, \ldots, p_{h_k}$ are distinct.

Proof of the "$\Longleftarrow$" implication of (230): Assume that $\prod_{i \in I} p_i$ divides m. We must show that p_j divides m for each $j \in I$.

Fix $j \in I$. Then, we can split off the factor for $i = j$ from the product $\prod_{i \in I} p_i$. We thus obtain

$$\prod_{i \in I} p_i = p_j \cdot \underbrace{\prod_{i \in I \setminus \{j\}} p_i}_{\text{an integer}}.$$

Hence, $p_j \mid \prod_{i \in I} p_i$. But $\prod_{i \in I} p_i \mid m$ (since $\prod_{i \in I} p_i$ divides m). Combining the preceding two sentences, we conclude that $p_j \mid \prod_{i \in I} p_i \mid m$, thus $p_j \mid m$ [269]. In other words, p_j divides m.

Forget that we fixed j. We thus have proved that p_j divides m for each $j \in I$.

We thus have shown that if $\prod_{i \in I} p_i$ divides m, then p_j divides m for each $j \in I$. In other words, we have proved the "$\Longleftarrow$" implication of (230).

We now have proved both "$\Longrightarrow$" and "$\Longleftarrow$" implications of (230). Thus, (230) holds, and therefore Lemma 2.9.26 is proved. □

This solves Exercise 2.9.9.

7.45. Solution to Exercise 2.9.10

In order to solve Exercise 2.9.10, we must prove Lemma 2.9.27. First, we recall a very elementary fact ([19s, Proposition 2.13.8]):

Proposition 7.45.1. Let $n > 1$ be an integer. Then, there exists at least one prime p such that $p \mid n$.

Proof of Lemma 2.9.27. We must prove the equivalence

$$\begin{aligned} &(m \text{ is coprime to } u) \\ &\Longleftrightarrow \ ((p_i \text{ does not divide } m) \text{ for each } i \in [n]). \end{aligned} \tag{340}$$

We shall do this by separately proving the "$\Longrightarrow$" and "$\Longleftarrow$" implications of this equivalence:

Proof of the "$\Longrightarrow$" implication of (340): Assume that m is coprime to u. We must show that $(p_i$ does not divide $m)$ for each $i \in [n]$.

Fix $i \in [n]$. We shall show that p_i does not divide m.

Indeed, assume the contrary. Thus, p_i divides m. But p_i is a prime that divides u (since all of $p_1, p_2, \ldots, p_n$ are primes that divide u); thus, p_i divides u. Hence, the positive integer p_i divides both m and u. Since p_i is a prime, we have $p_i > 1$.

[269] Here we are using the *transitivity of divisibility* (i.e., the fact that if a, b and c are three integers satisfying $a \mid b$ and $b \mid c$, then $a \mid c$). This is [19s, Proposition 2.2.4 **(b)**] (and is easy to prove).

We have assumed that m is coprime to u. In other words, $\gcd(m,u) = 1$ (by the definition of "coprime"). But $\gcd(m,u)$ is defined to be the greatest positive integer that divides both m and u. Therefore, if r is any positive integer that divides both m and u, then $r \leq \gcd(m,u)$. Applying this to $r = p_i$, we obtain $p_i \leq \gcd(m,u)$ (since p_i is a positive integer that divides both m and u). Thus, $p_i \leq \gcd(m,u) = 1$. This contradicts $p_i > 1$.

This contradiction shows that our assumption was wrong. Hence, p_i does not divide m.

Forget that we fixed i. We thus have proved that (p_i does not divide m) for each $i \in [n]$.

We thus have shown that if m is coprime to u, then (p_i does not divide m) for each $i \in [n]$. In other words, we have proved the "$\Longrightarrow$" implication of (340).

Proof of the "$\Longleftarrow$" implication of (340): Assume that (p_i does not divide m) for each $i \in [n]$. We must show that m is coprime to u. In other words, we must show that $\gcd(m,u) = 1$ (because this is what it means for m to be coprime to u).

Indeed, assume the contrary. Thus, $\gcd(m,u) \neq 1$. But $\gcd(m,u)$ is the greatest positive integer that divides both m and u (by the definition of $\gcd(m,u)$). Hence, $\gcd(m,u)$ is a positive integer. Therefore, from $\gcd(m,u) \neq 1$, we obtain $\gcd(m,u) > 1$. Hence, Proposition 7.45.1 (applied to $\gcd(m,u)$ instead of n) yields that there exists at least one prime p such that $p \mid \gcd(m,u)$. Consider this p.

Recall that $\gcd(m,u)$ divides both m and u. In other words, $\gcd(m,u) \mid m$ and $\gcd(m,u) \mid u$.

We have $p \mid \gcd(m,u)$ and $\gcd(m,u) \mid m$. Combining these two divisibilities, we find $p \mid \gcd(m,u) \mid m$, thus $p \mid m$ [270]. Likewise, combining $p \mid \gcd(m,u)$ with $\gcd(m,u) \mid u$, we find $p \mid \gcd(m,u) \mid u$, so that $p \mid u$ [271]. Thus, p is a prime that divides u (since p is a prime). Hence, p must be one of the n primes $p_1, p_2, \ldots, p_n$ (since these n primes $p_1, p_2, \ldots, p_n$ are precisely the distinct primes that divide u). In other words, $p = p_j$ for some $j \in [n]$. Consider this j.

Recall that we assumed that (p_i does not divide m) for each $i \in [n]$. Applying this to $i = j$, we conclude that p_j does not divide m. In other words, p does not divide m (since $p = p_j$). But this contradicts $p \mid m$. This contradiction shows that our assumption was false. Hence, we have proved that $\gcd(m,u) = 1$. In other words, m is coprime to u.

We thus have shown that if (p_i does not divide m) for each $i \in [n]$, then m is coprime to u. In other words, we have proved the "$\Longleftarrow$" implication of (340).

We now have proved both "$\Longrightarrow$" and "$\Longleftarrow$" implications of (340). Thus, (340) holds, and therefore Lemma 2.9.27 is proved. □

This solves Exercise 2.9.10.

[270] Here we are using the *transitivity of divisibility* (i.e., the fact that if a, b and c are three integers satisfying $a \mid b$ and $b \mid c$, then $a \mid c$). This is [19s, Proposition 2.2.4 **(b)**] (and is easy to prove).

[271] again, by the transitivity of divisibility

7.46. Solution to Exercise 2.9.11

Solution to Exercise 2.9.11. We proceed similarly to the second proof of Proposition 2.9.10.

We are in one of the following two cases:

Case 1: We have $S \subseteq T$.

Case 2: We don't have $S \subseteq T$.

Let us first consider Case 1. In this case, we have $S \subseteq T$. Hence, every subset I of S satisfies

$$(-1)^{|I \setminus T|} = 1. \tag{341}$$

[*Proof of (341):* Let I be a subset of S. Thus, $I \subseteq S \subseteq T$, so that $I \setminus T = \varnothing$. Thus, $|I \setminus T| = |\varnothing| = 0$. Hence, $(-1)^{|I \setminus T|} = (-1)^0 = 1$. This proves (341).]

On the other hand, S is a $|S|$-element set. Hence, Theorem 1.4.1 (applied to $n = |S|$) yields (# of subsets of S) $= 2^{|S|}$.

Now,

$$\begin{aligned}\sum_{I \subseteq S} \underbrace{(-1)^{|I \setminus T|}}_{\substack{=1 \\ \text{(by (341))}}} &= \sum_{I \subseteq S} 1 = (\text{\# of subsets } I \text{ of } S) \cdot 1 \\ &= (\text{\# of subsets } I \text{ of } S) = (\text{\# of subsets of } S) = 2^{|S|}.\end{aligned}$$

Comparing this with

$$\begin{cases} 2^{|S|}, & \text{if } S \subseteq T; \\ 0, & \text{otherwise} \end{cases} = 2^{|S|} \qquad (\text{since } S \subseteq T),$$

we obtain

$$\sum_{I \subseteq S} (-1)^{|I \setminus T|} = \begin{cases} 2^{|S|}, & \text{if } S \subseteq T; \\ 0, & \text{otherwise} \end{cases}.$$

Thus, Exercise 2.9.11 is solved in Case 1.

Let us now consider Case 2. In this case, we don't have $S \subseteq T$. Hence, there exists some $g \in S$ such that $g \notin T$. Consider this g. (We can have many choices for g, but we just pick one.) Note that the sets $\{g\}$ and T are disjoint (since $g \notin T$). Hence, $\{g\} \setminus T = \{g\}$.

Each subset I of S must satisfy either $g \in I$ or $g \notin I$ (but not both at the same time). Hence, we can split the sum $\sum_{I \subseteq S} (-1)^{|I \setminus T|}$ as follows:

$$\sum_{I \subseteq S} (-1)^{|I \setminus T|} = \sum_{\substack{I \subseteq S; \\ g \in I}} (-1)^{|I \setminus T|} + \sum_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I \setminus T|}. \tag{342}$$

The map[272]

$$\{I \subseteq S \mid g \notin I\} \to \{I \subseteq S \mid g \in I\}, \\ J \mapsto J \cup \{g\}$$

is a bijection. (This can be proved in the exact same way as it was proved during our second proof of Proposition 2.9.10.)

Moreover, every subset J of S satisfying $g \notin J$ must satisfy

$$(-1)^{|(J \cup \{g\}) \setminus T|} = -(-1)^{|J \setminus T|}. \tag{343}$$

[*Proof of (343):* Let J be a subset of S satisfying $g \notin J$. Then, we cannot have $g \in J \setminus T$ (since $g \in J \setminus T$ would imply $g \in J \setminus T \subseteq J$, which would contradict $g \notin J$). Thus, we must have $g \notin J \setminus T$. But any three sets X, Y and Z satisfy $(X \cup Y) \setminus Z = (X \setminus Z) \cup (Y \setminus Z)$. Applying this to $X = J$, $Y = \{g\}$ and $Z = T$, we find

$$(J \cup \{g\}) \setminus T = (J \setminus T) \cup \underbrace{(\{g\} \setminus T)}_{=\{g\}} = (J \setminus T) \cup \{g\}.$$

Hence, $|(J \cup \{g\}) \setminus T| = |(J \setminus T) \cup \{g\}| = |J \setminus T| + 1$ (since $g \notin J \setminus T$). Thus, $(-1)^{|(J \cup \{g\}) \setminus T|} = (-1)^{|J \setminus T|+1} = -(-1)^{|J \setminus T|}$. This proves (343).]

Now, we can substitute $J \cup \{g\}$ for I in the sum $\sum\limits_{\substack{I \subseteq S; \\ g \in I}} (-1)^{|I \setminus T|}$ (since the map $\{I \subseteq S \mid g \notin I\} \to \{I \subseteq S \mid g \in I\}$, $J \mapsto J \cup \{g\}$ is a bijection). We thus obtain

$$\sum_{\substack{I \subseteq S; \\ g \in I}} (-1)^{|I \setminus T|} = \sum_{\substack{J \subseteq S; \\ g \notin J}} \underbrace{(-1)^{|(J \cup \{g\}) \setminus T|}}_{\substack{=-(-1)^{|J \setminus T|} \\ \text{(by (343))}}} = \sum_{\substack{J \subseteq S; \\ g \notin J}} \left(-(-1)^{|J \setminus T|}\right) = -\sum_{\substack{J \subseteq S; \\ g \notin J}} (-1)^{|J \setminus T|}$$

$$= -\sum_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I \setminus T|} \tag{344}$$

(here, we have renamed the summation index J as I).

Now, (342) becomes

$$\sum_{I \subseteq S} (-1)^{|I \setminus T|} = \underbrace{\sum_{\substack{I \subseteq S; \\ g \in I}} (-1)^{|I \setminus T|}}_{\substack{=-\sum\limits_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I \setminus T|} \\ \text{(by (344))}}} + \sum_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I \setminus T|} = -\sum_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I \setminus T|} + \sum_{\substack{I \subseteq S; \\ g \notin I}} (-1)^{|I \setminus T|} = 0.$$

[272] The notation "$\{I \subseteq S \mid g \notin I\}$" means "the set of all subsets I of S satisfying $g \notin I$". Similarly, the notation "$\{I \subseteq S \mid g \in I\}$" means "the set of all subsets I of S satisfying $g \in I$".

Comparing this with

$$\begin{cases} 2^{|S|}, & \text{if } S \subseteq T; \\ 0, & \text{otherwise} \end{cases} = 0 \qquad (\text{since we don't have } S \subseteq T),$$

we obtain

$$\sum_{I \subseteq S} (-1)^{|I \setminus T|} = \begin{cases} 2^{|S|}, & \text{if } S \subseteq T; \\ 0, & \text{otherwise} \end{cases}.$$

Thus, Exercise 2.9.11 is solved in Case 2.

Thus, Exercise 2.9.11 is solved (since we have solved it in both Cases 1 and 2). □

7.47. Reference to solution to Exercise 2.9.12

Exercise 2.9.12 is [19f-mt2s, Exercise 2].

7.48. Solution to Exercise 2.10.1

Solution to Exercise 2.10.1. **(a)** Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. We must prove that

$$\binom{n-1}{n-k} = \begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases}. \tag{345}$$

We are in one of the following two cases:

Case 1: We have $n = 0$.

Case 2: We have $n \neq 0$.

Let us first consider Case 1. In this case, we have $n = 0$. We are in one of the following two subcases:

Subcase 1.1: We have $k = 0$.

Subcase 1.2: We have $k \neq 0$.

Let us first consider Subcase 1.1. In this subcase, we have $k = 0$. From $n = 0$ and $k = 0$, we obtain $\dbinom{n-1}{n-k} = \dbinom{0-1}{0-0} = \dbinom{-1}{0} = 1$ (by (44)). Comparing this with

$$\begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases} = [k=0] \qquad (\text{since } n = 0)$$
$$= 1 \qquad (\text{since } k = 0),$$

we find $\dbinom{n-1}{n-k} = \begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases}$. Thus, (345) is proved in Subcase 1.1.

Let us next consider Subcase 1.2. In this subcase, we have $k \neq 0$. Hence, $k > 0$ (since $k \in \mathbb{N}$), so that $-k < 0$ and therefore $-k \notin \mathbb{N}$. Thus, $\underbrace{n}_{=0} - k = 0 - k = -k \notin \mathbb{N}$. Therefore, (43) (applied to $n-1$ and $n-k$ instead of n and k) yields $\binom{n-1}{n-k} = 0$. Comparing this with

$$\begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases} = [k=0] \qquad (\text{since } n = 0)$$
$$= 0 \qquad (\text{since } k \neq 0),$$

we find $\binom{n-1}{n-k} = \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases}$. Thus, (345) is proved in Subcase 1.2.

We have now proved (345) in each of the two Subcases 1.1 and 1.2. Hence, (345) is proved in Case 1 (since Subcases 1.1 and 1.2 cover Case 1).

Let us next consider Case 2. In this case, we have $n \neq 0$. Hence, n is a positive integer (since $n \in \mathbb{N}$). Thus, $n \geq 1$, so that $n-1 \in \mathbb{N}$. Therefore, Theorem 1.3.11 (applied to $n-1$ and $n-k$ instead of n and k) yields

$$\binom{n-1}{n-k} = \binom{n-1}{(n-1)-(n-k)} = \binom{n-1}{k-1} \qquad (\text{since } (n-1)-(n-k) = k-1).$$

Comparing this with

$$\begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases} = \binom{n-1}{k-1} \qquad (\text{since } n > 0 \text{ (because } n \geq 1)),$$

we obtain $\binom{n-1}{n-k} = \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases}$. Thus, (345) is proved in Case 2.

We have now proved (345) in each of the two Cases 1 and 2. Hence, (345) always holds.

Thus, we have proved (345). This solves Exercise 2.10.1 **(a)**.

(b) We must prove that Theorem 2.10.1 holds for $n = 0$.

So let $n \in \mathbb{N}$ and $k \in \mathbb{N}$, and assume that $n = 0$. We must prove the claim of Theorem 2.10.1.

We shall first prove (239). We are in one of the following two cases:

Case 1: We have $k = 0$.

Case 2: We have $k \neq 0$.

Let us first consider Case 1. In this case, we have $k = 0$. Hence,

$$\begin{aligned}
&\Big(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\Big) \\
&= \left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \mathbb{P}^0 \text{ satisfying } \underbrace{x_1 + x_2 + \cdots + x_0}_{=(\text{empty sum})=0} = \underbrace{n}_{=0}\right) \\
&= \Big(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \mathbb{P}^0 \text{ satisfying } 0 = 0\Big) \\
&= \Big(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \mathbb{P}^0\Big) \\
&\qquad\qquad \Big(\text{since every } (x_1, x_2, \ldots, x_0) \in \mathbb{P}^0 \text{ satisfies } 0 = 0\Big) \\
&= 1
\end{aligned}$$

(because there exists exactly one 0-tuple $(x_1, x_2, \ldots, x_0) \in \mathbb{P}^0$: namely, the empty list $()$). Comparing this with

$$\begin{aligned}
\binom{n-1}{n-k} &= \binom{0-1}{0-0} \qquad (\text{since } n = 0 \text{ and } k = 0) \\
&= \binom{0-1}{0} = 1 \qquad (\text{by (44)}),
\end{aligned}$$

we obtain

$$\Big(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\Big) = \binom{n-1}{n-k}.$$

Hence, (239) is proved in Case 1.

Let us next consider Case 2. In this case, we have $k \neq 0$. Hence, $k > 0$ (since $k \in \mathbb{N}$), so that $n - \underbrace{k}_{>0} < n = 0$ and therefore $n - k \notin \mathbb{N}$. Thus, (43) (applied to $n-1$ and $n-k$ instead of n and k) yields $\dbinom{n-1}{n-k} = 0$.

We have $k > 0$. Thus, $x_1 + x_2 + \cdots + x_k \neq n$ for each $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$ [273]. In other words, there exists no $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$. Thus,

$$\Big(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\Big) = 0.$$

[273] *Proof.* Let $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$. Thus, $x_1, x_2, \ldots, x_k$ are elements of $\mathbb{P}$; in other words, $x_1, x_2, \ldots x_k$ are positive integers (since $\mathbb{P}$ is the set of all positive integers). Thus, $x_1 + x_2 + \cdots + x_k$ is a sum of k positive integers. Thus, $x_1 + x_2 + \cdots + x_k$ is a positive integer itself (since any sum of k positive integers is a positive integer (because $k \neq 0$)). Hence, $x_1 + x_2 + \cdots + x_k > 0$, so that $x_1 + x_2 + \cdots + x_k \neq 0$. In other words, $x_1 + x_2 + \cdots + x_k \neq n$ (since $n = 0$). Qed.

Comparing this with $\binom{n-1}{n-k} = 0$, we obtain

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) = \binom{n-1}{n-k}.$$

Hence, (239) is proved in Case 2.

Hence, we have proved (239) in each of the two Cases 1 and 2. Thus, (239) always holds.

Now, (239) yields

$$\begin{aligned}&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\ &= \binom{n-1}{n-k} = \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ [k = 0], & \text{if } n = 0 \end{cases} \qquad \text{(by Exercise 2.10.1 \textbf{(a)})}.\end{aligned}$$

Thus, we have proved Theorem 2.10.1 under the assumption that $n = 0$. So we know that Theorem 2.10.1 holds for $n = 0$. This completes the solution to Exercise 2.10.1 **(b)**.

(c) We must prove that Theorem 2.10.1 holds for $k = 0$.

So let $n \in \mathbb{N}$ and $k \in \mathbb{N}$, and assume that $k = 0$. We must prove the claim of Theorem 2.10.1.

If $n = 0$, then this follows from Exercise 2.10.1 **(b)** (which was solved above). Hence, for the rest of this proof, we WLOG assume that $n \neq 0$. Hence, $n \geq 1$ (since $n \in \mathbb{N}$), so that $n - 1 \geq 0$ and thus $n - 1 \in \mathbb{N}$. Moreover, $n - \underbrace{k}_{=0} = n > n - 1$. Hence, Proposition 1.3.6 (applied to $n - 1$ and $n - k$ instead of n and k) yields $\binom{n-1}{n-k} = 0$.

Also, we have $x_1 + x_2 + \cdots + x_k \neq n$ for each $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$ [274]. In other words, there exists no $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$. Thus,

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) = 0.$$

Comparing this with $\binom{n-1}{n-k} = 0$, we obtain

$$\begin{aligned}&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\ &= \binom{n-1}{n-k} = \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ [k = 0], & \text{if } n = 0 \end{cases} \qquad \text{(by Exercise 2.10.1 \textbf{(a)})}.\end{aligned}$$

[274] *Proof.* Let $(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k$. From $k = 0$, we obtain $x_1 + x_2 + \cdots + x_k = x_1 + x_2 + \cdots + x_0 =$ (empty sum) $= 0 \neq n$ (since $n \neq 0$). Qed.

Thus, we have proved Theorem 2.10.1 under the assumption that $k = 0$. So we know that Theorem 2.10.1 holds for $k = 0$. This completes the solution to Exercise 2.10.1 **(c)**. □

7.49. Solution to Exercise 2.10.2

In order to solve Exercise 2.10.2, we need to give an alternative proof of Theorem 2.10.1.

Second proof of Theorem 2.10.1. Forget that we fixed n and k.

First, we shall prove (239) by induction on k.

Induction base: We know (from Exercise 2.10.1 **(c)**) that Theorem 2.10.1 holds for $k = 0$. Hence, in particular, (239) holds for $k = 0$. This completes the induction base.

Induction step: Let q be a positive integer. Assume (as the induction hypothesis) that (239) holds for $k = q - 1$. We must show that (239) holds for $k = q$.

We have assumed that (239) holds for $k = q - 1$. In other words, we have

$$\begin{aligned}&\left(\#\text{ of } \left(x_1, x_2, \ldots, x_{q-1}\right) \in \mathbb{P}^{q-1} \text{ satisfying } x_1 + x_2 + \cdots + x_{q-1} = n\right)\\ &= \binom{n-1}{n-(q-1)}\end{aligned} \tag{346}$$

for each $n \in \mathbb{N}$.

Now, let $n \in \mathbb{N}$. We shall compute the # of $\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q$ satisfying $x_1 + x_2 + \cdots + x_q = n$.

First, we notice that if $\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q$ satisfies $x_1 + x_2 + \cdots + x_q = n$, then $x_q \in [n]$ [275]. Hence, the sum rule (Theorem 1.2.5) yields

$$\begin{aligned}&\left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right)\\ &= \sum_{p \in [n]} \left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right).\end{aligned}$$

Now, let $p \in [n]$. Then, p is a positive integer, so that $p \in \mathbb{P}$. Moreover, from $p \in [n] = \{1, 2, \ldots, n\}$, we obtain $p \leq n$, so that $n - p \in \mathbb{N}$. Hence, (346) (applied

[275] *Proof.* Let $\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q$ be such that $x_1 + x_2 + \cdots + x_q = n$. We must prove that $x_q \in [n]$.

We have $x_1, x_2, \ldots, x_q \in \mathbb{P}$ (since $\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q$). In other words, $x_1, x_2, \ldots, x_q$ are positive integers (since $\mathbb{P}$ is the set of all positive integers). Thus, in particular, x_q is a positive integer. Moreover, $x_1 + x_2 + \cdots + x_{q-1}$ is a sum of positive integers (since $x_1, x_2, \ldots, x_q$ are positive integers), and thus nonnegative. Hence, $x_1 + x_2 + \cdots + x_{q-1} \geq 0$. Now,

$$n = x_1 + x_2 + \cdots + x_q = \underbrace{\left(x_1 + x_2 + \cdots + x_{q-1}\right)}_{\geq 0} + x_q \geq x_q.$$

In other words, $x_q \leq n$. Since x_q is a positive integer, we thus obtain $x_q \in \{1, 2, \ldots, n\} = [n]$. Qed.

to $n-p$ instead of n) yields

$$\begin{aligned}&\Big(\#\text{ of } \left(x_1, x_2, \ldots, x_{q-1}\right) \in \mathbb{P}^{q-1} \text{ satisfying } x_1 + x_2 + \cdots + x_{q-1} = n-p\Big)\\ &= \binom{(n-p)-1}{(n-p)-(q-1)}. \end{aligned} \tag{347}$$

If $\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q$ satisfies $x_1 + x_2 + \cdots + x_q = n$ and $x_q = p$, then $x_1 + x_2 + \cdots + x_{q-1} = n - p$ [276]. Hence, we can define a map

$$\begin{aligned}&\left\{\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \;\mid\; x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\}\\ &\to \left\{\left(x_1, x_2, \ldots, x_{q-1}\right) \in \mathbb{P}^{q-1} \;\mid\; x_1 + x_2 + \cdots + x_{q-1} = n-p\right\}\end{aligned}$$

that sends each q-tuple $\left(x_1, x_2, \ldots, x_q\right)$ to $\left(x_1, x_2, \ldots, x_{q-1}\right)$. Conversely, we can define a map

$$\begin{aligned}&\left\{\left(x_1, x_2, \ldots, x_{q-1}\right) \in \mathbb{P}^{q-1} \;\mid\; x_1 + x_2 + \cdots + x_{q-1} = n-p\right\}\\ &\to \left\{\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \;\mid\; x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\}\end{aligned}$$

that sends each $(q-1)$-tuple $\left(x_1, x_2, \ldots, x_{q-1}\right)$ to $\left(x_1, x_2, \ldots, x_{q-1}, p\right)$ (because if $\left(x_1, x_2, \ldots, x_{q-1}\right) \in \mathbb{P}^{q-1}$ satisfies $x_1 + x_2 + \cdots + x_{q-1} = n-p$, then the entries of the q-tuple $\left(x_1, x_2, \ldots, x_{q-1}, p\right)$ sum up to $\underbrace{x_1 + x_2 + \cdots + x_{q-1}}_{=n-p} + p = (n-p) + p = n$). These two maps are mutually inverse, and thus are bijections. Hence, the bijection principle yields

$$\begin{aligned}&\left|\left\{\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \;\mid\; x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\}\right|\\ &= \left|\left\{\left(x_1, x_2, \ldots, x_{q-1}\right) \in \mathbb{P}^{q-1} \;\mid\; x_1 + x_2 + \cdots + x_{q-1} = n-p\right\}\right|\\ &= \Big(\#\text{ of } \left(x_1, x_2, \ldots, x_{q-1}\right) \in \mathbb{P}^{q-1} \text{ satisfying } x_1 + x_2 + \cdots + x_{q-1} = n-p\Big)\\ &= \binom{(n-p)-1}{(n-p)-(q-1)} \qquad \text{(by (347))}. \end{aligned} \tag{348}$$

Forget that we fixed p. We thus have proved (348) for each $p \in [n]$. Now, we can

[276] because $n = x_1 + x_2 + \cdots + x_q = \left(x_1 + x_2 + \cdots + x_{q-1}\right) + \underbrace{x_q}_{=p} = \left(x_1 + x_2 + \cdots + x_{q-1}\right) + p$

continue our computation from before:

$$\begin{aligned}
&\left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) \\
&= \sum_{p \in [n]} \underbrace{\left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right)}_{= \left|\left\{\left(x_1, x_2, \ldots, x_q\right) \in \mathbb{P}^q \mid x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\}\right|} \\
&\qquad\qquad = \underbrace{\binom{(n-p)-1}{(n-p)-(q-1)}}_{\text{(by (348))}} \\
&= \underbrace{\sum_{p \in [n]}}_{= \sum_{p=1}^{n}} \binom{(n-p)-1}{(n-p)-(q-1)} = \sum_{p=1}^{n} \binom{(n-p)-1}{(n-p)-(q-1)} \\
&= \sum_{j=0}^{n-1} \binom{j-1}{j-(q-1)} \qquad (349)
\end{aligned}$$

(here, we have substituted j for $n-p$ in the sum).

But let $j \in \mathbb{Z}$. Then, Theorem 1.3.8 (applied to j and $j-(q-1)$ instead of n and k) yields

$$\binom{j}{j-(q-1)} = \binom{j-1}{j-(q-1)-1} + \binom{j-1}{j-(q-1)} = \binom{j-1}{j-q} + \binom{j-1}{j-(q-1)}$$

(since $j-(q-1)-1 = j-q$). Solving this equation for $\binom{j-1}{j-(q-1)}$, we obtain

$$\begin{aligned}
\binom{j-1}{j-(q-1)} &= \underbrace{\binom{j}{j-(q-1)}}_{= \binom{(j+1)-1}{((j+1)-1)-(q-1)}} - \binom{j-1}{j-q} \\
&\qquad\qquad \text{(since } j=(j+1)-1\text{)} \\
&= \binom{(j+1)-1}{((j+1)-1)-(q-1)} - \binom{j-1}{j-q} \\
&= \binom{(j+1)-1}{(j+1)-q} - \binom{j-1}{j-q} \qquad (350)
\end{aligned}$$

(since $((j+1)-1)-(q-1) = (j+1)-q$).

Forget that we fixed j. We thus have proved (350) for each $j \in \mathbb{Z}$.

Now, (349) becomes

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_q) \in \mathbb{P}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) \\
&= \sum_{j=0}^{n-1} \underbrace{\binom{j-1}{j-(q-1)}}_{\substack{= \binom{(j+1)-1}{(j+1)-q} - \binom{j-1}{j-q} \\ \text{(by (350))}}} \\
&= \sum_{j=0}^{n-1} \left(\binom{(j+1)-1}{(j+1)-q} - \binom{j-1}{j-q} \right) = \binom{((n-1)+1)-1}{((n-1)+1)-q} - \binom{0-1}{0-q} \\
&\qquad \left(\text{by Theorem 2.1.1, applied to } u = 0 \text{ and } v = n-1 \text{ and } a_j = \binom{j-1}{j-q} \right) \\
&= \binom{n-1}{n-q} - \binom{0-1}{-q} \qquad \left(\text{since } (n-1)+1 = n \text{ and } 0-q = -q\right).
\end{aligned}$$

But q is positive, and thus $-q$ is negative. Hence, $-q \notin \mathbb{N}$. Hence, (43) (applied to $0-1$ and $-q$ instead of n and k) yields $\binom{0-1}{-q} = 0$. Thus, we obtain

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_q) \in \mathbb{P}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) \\
&= \binom{n-1}{n-q} - \underbrace{\binom{0-1}{-q}}_{=0} = \binom{n-1}{n-q}.
\end{aligned}$$

Now, forget that we fixed n. We thus have proved that

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_q) \in \mathbb{P}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) = \binom{n-1}{n-q}$$

for each $n \in \mathbb{N}$. In other words, (239) holds for $k = q$. This completes the induction step.

Thus, we have proved (239) by induction. Now, for each $n \in \mathbb{N}$ and $k \in \mathbb{N}$, we have

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\
&= \binom{n-1}{n-k} \qquad \left(\text{by (239)}\right) \\
&= \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ [k=0], & \text{if } n = 0 \end{cases} \qquad \left(\text{by Exercise 2.10.1 } \textbf{(a)}\right).
\end{aligned}$$

This proves Theorem 2.10.1. □

7.50. Solution to Exercise 2.10.3

In order to solve Exercise 2.10.3, we need to give an alternative proof of Theorem 2.10.4.

Second proof of Theorem 2.10.4. Forget that we fixed n and k.

We shall prove Theorem 2.10.4 by induction on k.

Induction base: It is easy to see that Theorem 2.10.4 holds for $k = 0$ [277]. This completes the induction base.

Induction step: Let q be a positive integer. Assume (as the induction hypothesis) that Theorem 2.10.4 holds for $k = q - 1$. We must show that Theorem 2.10.4 holds for $k = q$.

[277] *Proof.* Assume that $k = 0$. Let $n \in \mathbb{Z}$ be arbitrary. Now,

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \{0,1\}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\
&= \left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \{0,1\}^0 \text{ satisfying } \underbrace{x_1 + x_2 + \cdots + x_0}_{=(\text{empty sum})=0} = n\right) \qquad (\text{since } k = 0) \\
&= \left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \{0,1\}^0 \text{ satisfying } 0 = n\right).
\end{aligned}$$

But the right hand side is easy to compute:

- If $n = 0$, then $\left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \{0,1\}^0 \text{ satisfying } 0 = n\right) = 1$ (because there is exactly one 0-tuple $(x_1, x_2, \ldots, x_0) \in \{0,1\}^0$ (namely, the empty list $()$), and clearly this 0-tuple satisfies $0 = n$ (since $n = 0$)).
- If $n \neq 0$, then $\left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \{0,1\}^0 \text{ satisfying } 0 = n\right) = 0$ (because there is no 0-tuple $(x_1, x_2, \ldots, x_0) \in \{0,1\}^0$ satisfying $0 = n$ (since $0 \neq n$)).

Combining these two observations, we conclude that

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \{0,1\}^0 \text{ satisfying } 0 = n\right) = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases}.$$

Comparing this with

$$\begin{aligned}
\binom{k}{n} &= \binom{0}{n} \qquad (\text{since } k = 0) \\
&= [n = 0] \qquad (\text{by Lemma 1.3.14, applied to } n \text{ instead of } k) \\
&= \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{otherwise} \end{cases} = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases},
\end{aligned}$$

we obtain

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \{0,1\}^0 \text{ satisfying } x_1 + x_2 + \cdots + x_0 = n\right) = \binom{k}{n}.$$

Hence,

$$\begin{aligned}
&\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \{0,1\}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\
&= \left(\#\text{ of } (x_1, x_2, \ldots, x_0) \in \{0,1\}^0 \text{ satisfying } 0 = n\right) = \binom{k}{n}.
\end{aligned}$$

In other words, Theorem 2.10.4 holds for our k and n. We have thus shown that Theorem 2.10.4 holds under the assumption that $k = 0$. Hence, Theorem 2.10.4 holds for $k = 0$.

We have assumed that Theorem 2.10.4 holds for $k = q-1$. In other words, we have

$$\begin{aligned}&\Big(\#\text{ of } (x_1, x_2, \ldots, x_{q-1}) \in \{0,1\}^{q-1} \text{ satisfying } x_1 + x_2 + \cdots + x_{q-1} = n\Big) \\ &= \binom{q-1}{n} \end{aligned} \tag{351}$$

for each $n \in \mathbb{Z}$.

Now, let $n \in \mathbb{Z}$. We shall compute the # of $(x_1, x_2, \ldots, x_q) \in \{0,1\}^q$ satisfying $x_1 + x_2 + \cdots + x_q = n$.

Clearly, if $(x_1, x_2, \ldots, x_q) \in \{0,1\}^q$ satisfies $x_1 + x_2 + \cdots + x_q = n$, then $x_q \in \{0,1\}$. Hence, the sum rule (Theorem 1.2.5) yields

$$\begin{aligned}&\left(\#\text{ of } (x_1, x_2, \ldots, x_q) \in \{0,1\}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) \\ &= \sum_{p \in \{0,1\}} \left(\#\text{ of } (x_1, x_2, \ldots, x_q) \in \{0,1\}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right).\end{aligned}$$

Now, let $p \in \{0,1\}$. Then, (351) (applied to $n-p$ instead of n) yields

$$\begin{aligned}&\Big(\#\text{ of } (x_1, x_2, \ldots, x_{q-1}) \in \{0,1\}^{q-1} \text{ satisfying } x_1 + x_2 + \cdots + x_{q-1} = n - p\Big) \\ &= \binom{q-1}{n-p}.\end{aligned} \tag{352}$$

If $(x_1, x_2, \ldots, x_q) \in \{0,1\}^q$ satisfies $x_1 + x_2 + \cdots + x_q = n$ and $x_q = p$, then $x_1 + x_2 + \cdots + x_{q-1} = n - p$ [278]. Hence, we can define a map

$$\begin{aligned}&\left\{(x_1, x_2, \ldots, x_q) \in \{0,1\}^q \;\mid\; x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\} \\ &\to \left\{(x_1, x_2, \ldots, x_{q-1}) \in \{0,1\}^{q-1} \;\mid\; x_1 + x_2 + \cdots + x_{q-1} = n - p\right\}\end{aligned}$$

that sends each q-tuple $(x_1, x_2, \ldots, x_q)$ to $(x_1, x_2, \ldots, x_{q-1})$. Conversely, we can define a map

$$\begin{aligned}&\left\{(x_1, x_2, \ldots, x_{q-1}) \in \{0,1\}^{q-1} \;\mid\; x_1 + x_2 + \cdots + x_{q-1} = n - p\right\} \\ &\to \left\{(x_1, x_2, \ldots, x_q) \in \{0,1\}^q \;\mid\; x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\}\end{aligned}$$

that sends each $(q-1)$-tuple $(x_1, x_2, \ldots, x_{q-1})$ to $(x_1, x_2, \ldots, x_{q-1}, p)$ (because if $(x_1, x_2, \ldots, x_{q-1}) \in \{0,1\}^{q-1}$ satisfies $x_1 + x_2 + \cdots + x_{q-1} = n - p$, then the entries of the q-tuple $(x_1, x_2, \ldots, x_{q-1}, p)$ sum up to $\underbrace{x_1 + x_2 + \cdots + x_{q-1}}_{=n-p} + p = (n-p) +$

[278] because $n = x_1 + x_2 + \cdots + x_q = \left(x_1 + x_2 + \cdots + x_{q-1}\right) + \underbrace{x_q}_{=p} = (x_1 + x_2 + \cdots + x_{q-1}) + p$

$p = n$). These two maps are mutually inverse, and thus are bijections. Hence, the bijection principle yields

$$\begin{aligned}
&\left|\left\{\left(x_1, x_2, \ldots, x_q\right) \in \{0,1\}^q \;\mid\; x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\}\right| \\
&= \left|\left\{\left(x_1, x_2, \ldots, x_{q-1}\right) \in \{0,1\}^{q-1} \;\mid\; x_1 + x_2 + \cdots + x_{q-1} = n - p\right\}\right| \\
&= \left(\#\text{ of } \left(x_1, x_2, \ldots, x_{q-1}\right) \in \{0,1\}^{q-1} \text{ satisfying } x_1 + x_2 + \cdots + x_{q-1} = n - p\right) \\
&= \binom{q-1}{n-p} \qquad \text{(by (352))}. \qquad (353)
\end{aligned}$$

Forget that we fixed p. We thus have proved (353) for each $p \in \{0,1\}$. Now, we can continue our computation from before:

$$\begin{aligned}
&\left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \{0,1\}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) \\
&= \sum_{p \in \{0,1\}} \underbrace{\left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \{0,1\}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right)}_{\substack{= \left|\left\{\left(x_1, x_2, \ldots, x_q\right) \in \{0,1\}^q \;\mid\; x_1 + x_2 + \cdots + x_q = n \text{ and } x_q = p\right\}\right| \\ = \binom{q-1}{n-p} \\ \text{(by (353))}}} \\
&= \sum_{p \in \{0,1\}} \binom{q-1}{n-p} = \binom{q-1}{n-0} + \binom{q-1}{n-1} = \binom{q-1}{n-1} + \binom{q-1}{n-0} \\
&= \binom{q-1}{n-1} + \binom{q-1}{n} \qquad (\text{since } n - 0 = n).
\end{aligned}$$

Comparing this with

$$\binom{q}{n} = \binom{q-1}{n-1} + \binom{q-1}{n} \qquad \left(\begin{array}{c}\text{by Theorem 1.3.8, applied to } q \text{ and } n \\ \text{instead of } n \text{ and } k\end{array}\right),$$

we obtain

$$\left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \{0,1\}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) = \binom{q}{n}.$$

Forget that we fixed n. We thus have proved

$$\left(\#\text{ of } \left(x_1, x_2, \ldots, x_q\right) \in \{0,1\}^q \text{ satisfying } x_1 + x_2 + \cdots + x_q = n\right) = \binom{q}{n}$$

for each $n \in \mathbb{Z}$. In other words, Theorem 2.10.4 holds for $k = q$. This completes the induction step. Thus, Theorem 2.10.4 is proved by induction. $\square$

7.51. Solution to Exercise 2.10.4

Solution to Exercise 2.10.4. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. We are in one of the following two cases:

Case 1: We have $k = 0$.

Case 2: We have $k \neq 0$.

Let us first consider Case 1. In this case, we have $k = 0$. We are in one of the following two subcases:

Subcase 1.1: We have $n = 0$.

Subcase 1.2: We have $n \neq 0$.

Let us first consider Subcase 1.1. In this subcase, we have $n = 0$. From $n = 0$ and $k = 0$, we obtain $\binom{n+k-1}{n} = \binom{0+0-1}{0} = 1$ (by (44)). Comparing this with

$$\begin{cases} \binom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases} = [n=0] \qquad (\text{since } k = 0)$$
$$= 1 \qquad (\text{since } n = 0),$$

we find $\binom{n+k-1}{n} = \begin{cases} \binom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases}$. Thus, Exercise 2.10.4 is proved in Subcase 1.1.

Let us next consider Subcase 1.2. In this subcase, we have $n \neq 0$. Hence, $n \geq 1$ (since $n \in \mathbb{N}$), so that $n - 1 \geq 0$ and thus $n - 1 \in \mathbb{N}$. Hence, Proposition 1.3.6 (applied to $n-1$ and n instead of n and k) yields $\binom{n-1}{n} = 0$ (since $n > n - 1$). Now, $n + \underbrace{k}_{=0} - 1 = n - 1$, so that $\binom{n+k-1}{n} = \binom{n-1}{n} = 0$. Comparing this with

$$\begin{cases} \binom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases} = [n=0] \qquad (\text{since } k = 0)$$
$$= 0 \qquad (\text{since } n \neq 0),$$

we find $\binom{n+k-1}{n} = \begin{cases} \binom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases}$. Thus, Exercise 2.10.4 is proved in Subcase 1.2.

We have now proved Exercise 2.10.4 in each of the two Subcases 1.1 and 1.2. Hence, Exercise 2.10.4 is proved in Case 1 (since Subcases 1.1 and 1.2 cover Case 1).

Let us next consider Case 2. In this case, we have $k \neq 0$. Hence, $k \geq 1$ (since $k \in \mathbb{N}$), so that $n + \underbrace{k}_{\geq 1} - 1 \geq n + 1 - 1 = n \geq 0$ (since $n \in \mathbb{N}$). Hence, $n + k - 1 \in \mathbb{N}$. Therefore, Theorem 1.3.11 (applied to $n + k - 1$ and n instead of n and k) yields

$$\binom{n+k-1}{n} = \binom{n+k-1}{(n+k-1)-n} = \binom{n+k-1}{k-1} \qquad (\text{since } (n+k-1)-n = k-1).$$

Comparing this with

$$\begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases} = \binom{n+k-1}{k-1} \qquad (\text{since } k > 0 \text{ (because } k \geq 1)),$$

we obtain $\dbinom{n+k-1}{n} = \begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ [n=0], & \text{if } k = 0 \end{cases}$. Thus, Exercise 2.10.4 is proved in Case 2.

We have now proved Exercise 2.10.4 in each of the two Cases 1 and 2. Hence, Exercise 2.10.4 always holds. □

7.52. Solution to Exercise 2.10.5

Our solution to Exercise 2.10.5 will use the following simple lemma:

Lemma 7.52.1. Let $n \in \mathbb{N}$. Let $(x_1, x_2, \ldots, x_k)$ be a composition of n. Then, $k \leq n$.

Proof of Lemma 7.52.1. We know that $(x_1, x_2, \ldots, x_k)$ is a composition of n. In other words, $(x_1, x_2, \ldots, x_k)$ is a tuple of positive integers whose sum is n (by Definition 2.10.2 **(c)**). Hence, $x_1, x_2, \ldots, x_k$ are positive integers whose sum is n. In other words, $x_1, x_2, \ldots, x_k$ are positive integers and satisfy $x_1 + x_2 + \cdots + x_k = n$.

For each $i \in \{1, 2, \ldots, k\}$, the number x_i is a positive integer (since $x_1, x_2, \ldots, x_k$ are positive integers) and thus satisfies $x_i \geq 1$ (since any positive integer is ≥ 1). Summing up these inequalities for all $i \in \{1, 2, \ldots, k\}$, we obtain $x_1 + x_2 + \cdots + x_k \geq \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} = k \cdot 1 = k$. In view of $x_1 + x_2 + \cdots + x_k = n$, this rewrites as $n \geq k$. In other words, $k \leq n$. This proves Lemma 7.52.1. □

Solution to Exercise 2.10.5. There are many ways to solve Exercise 2.10.5 **(a)**. One way is to use strong induction on n. Another is to construct a bijection

$$\{\{1,2\}\text{-compositions of } n\} \to \{\text{lacunar subsets of } [n-1]\}$$

(defined in the same way as the bijection C in our first proof of Theorem 2.10.1), and then use the bijection principle (and Proposition 1.4.9). Yet another is to find a bijection

$$\{\{1,2\}\text{-compositions of } n\} \to \{\text{domino tilings of } R_{n,2}\},$$

and then use the bijection principle (and Proposition 1.1.11). All these approaches can be easily adapted to yield Exercise 2.10.5 **(b)** as well.

We shall, however, use the conceptually simplest approach: We will first solve Exercise 2.10.5 **(b)** by deriving it from Theorem 2.10.4, and then solve Exercise 2.10.5 **(a)** by summing the result over all k. So let us start with the solution to Exercise 2.10.5 **(b)**:

(b) If $(u_1, u_2, \ldots, u_k)$ is a $\{1,2\}$-composition of n into k parts, then $(u_1 - 1, u_2 - 1, \ldots, u_k - 1)$ is a k-tuple $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n - k$ [279]. Hence, we can define a map

$$A : \{\{1,2\}\text{-compositions of } n \text{ into } k \text{ parts}\} \to \left\{(x_1, x_2, \ldots, x_k) \in \{0,1\}^k \mid x_1 + x_2 + \cdots + x_k = n - k\right\},$$
$$(u_1, u_2, \ldots, u_k) \mapsto (u_1 - 1, u_2 - 1, \ldots, u_k - 1).$$

Let us now construct a map in the opposite direction.

If $(p_1, p_2, \ldots, p_k) \in \left\{(x_1, x_2, \ldots, x_k) \in \{0,1\}^k \mid x_1 + x_2 + \cdots + x_k = n - k\right\}$, then $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is a $\{1,2\}$-composition of n into k parts[280]. Hence, we

[279] *Proof.* Let $(u_1, u_2, \ldots, u_k)$ be a $\{1,2\}$-composition of n into k parts. We must show that $(u_1 - 1, u_2 - 1, \ldots, u_k - 1)$ is a k-tuple $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n - k$.

We know that $(u_1, u_2, \ldots, u_k)$ is a $\{1,2\}$-composition of n into k parts. In other words, $(u_1, u_2, \ldots, u_k)$ is a composition $(x_1, x_2, \ldots, x_k)$ of n into k parts such that $x_1, x_2, \ldots, x_k \in \{1,2\}$ (by the definition of a "$\{1,2\}$-composition of n into k parts"). In other words, $(u_1, u_2, \ldots, u_k)$ is a composition of n into k parts and satisfies $u_1, u_2, \ldots, u_k \in \{1,2\}$. From $u_1, u_2, \ldots, u_k \in \{1,2\}$, we obtain $u_1 - 1, u_2 - 1, \ldots, u_k - 1 \in \{0,1\}$ (since $p - 1 \in \{0,1\}$ for each $p \in \{1,2\}$). In other words, $(u_1 - 1, u_2 - 1, \ldots, u_k - 1) \in \{0,1\}^k$. Moreover, $(u_1, u_2, \ldots, u_k)$ is a composition of n into k parts; in other words, $(u_1, u_2, \ldots, u_k)$ is a k-tuple of positive integers whose sum is n (by Definition 2.10.2 **(d)**). In other words, $(u_1, u_2, \ldots, u_k)$ is a k-tuple of positive integers and satisfies $u_1 + u_2 + \cdots + u_k = n$. Hence,

$$(u_1 - 1) + (u_2 - 1) + \cdots + (u_k - 1) = \underbrace{(u_1 + u_2 + \cdots + u_k)}_{=n} - \underbrace{\underbrace{(1 + 1 + \cdots + 1)}_{k \text{ times}}}_{=k} = n - k.$$

Thus, we have shown that $(u_1 - 1, u_2 - 1, \ldots, u_k - 1) \in \{0,1\}^k$ and $(u_1 - 1) + (u_2 - 1) + \cdots + (u_k - 1) = n - k$. In other words, $(u_1 - 1, u_2 - 1, \ldots, u_k - 1)$ is a k-tuple $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n - k$. Qed.

[280] *Proof.* Let $(p_1, p_2, \ldots, p_k) \in \left\{(x_1, x_2, \ldots, x_k) \in \{0,1\}^k \mid x_1 + x_2 + \cdots + x_k = n - k\right\}$. Thus, $(p_1, p_2, \ldots, p_k)$ is a k-tuple $(x_1, x_2, \ldots, x_k) \in \{0,1\}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n - k$. In other words, $(p_1, p_2, \ldots, p_k) \in \{0,1\}^k$ is a k-tuple satisfying $p_1 + p_2 + \cdots + p_k = n - k$. We must prove that $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is a $\{1,2\}$-composition of n into k parts.

We have $(p_1, p_2, \ldots, p_k) \in \{0,1\}^k$. In other words, $p_1, p_2, \ldots, p_k \in \{0,1\}$. Hence, $p_1 + 1, p_2 + 1, \ldots, p_k + 1 \in \{1,2\}$ (since $q + 1 \in \{1,2\}$ for each $q \in \{0,1\}$). Hence, $(p_1 + 1, p_2 + 1, \ldots, p_k + 1) \in \{1,2\}^k \subseteq \mathbb{P}^k$ (since $\{1,2\} \subseteq \mathbb{P}$). In other words, $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is a k-tuple of positive integers (since $\mathbb{P}$ is the set of all positive inte-

can define a map

$$\begin{aligned} B : \left\{(x_1, x_2, \ldots, x_k) \in \{0,1\}^k \mid x_1 + x_2 + \cdots + x_k = n - k\right\} \\ \to \{\{1,2\}\text{-compositions of } n \text{ into } k \text{ parts}\}, \\ (p_1, p_2, \ldots, p_k) \mapsto (p_1 + 1, p_2 + 1, \ldots, p_k + 1). \end{aligned}$$

Clearly, the maps A and B are mutually inverse (since the map A subtracts 1 from each entry of the k-tuple it is applied to, whereas the map B adds 1 to each entry of the k-tuple it is applied to). Thus, the map A is invertible, i.e., is a bijection. Hence, the bijection principle yields

$$\begin{aligned} &|\{\{1,2\}\text{-compositions of } n \text{ into } k \text{ parts}\}| \\ &= \left|\left\{(x_1, x_2, \ldots, x_k) \in \{0,1\}^k \mid x_1 + x_2 + \cdots + x_k = n - k\right\}\right| \\ &= \left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \{0,1\}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n - k\right) \\ &= \binom{k}{n-k} \qquad \text{(by Theorem 2.10.4, applied to } n-k \text{ instead of } n\text{)}. \end{aligned}$$

Hence,

$$\begin{aligned} &(\#\text{ of } \{1,2\}\text{-compositions of } n \text{ into } k \text{ parts}) \\ &= |\{\{1,2\}\text{-compositions of } n \text{ into } k \text{ parts}\}| \\ &= \binom{k}{n-k}. \end{aligned}$$

This solves Exercise 2.10.5 **(b)**.

(a) Recall that the *length* of a list is the number of entries of this list. Thus, the length of a list $(a_1, a_2, \ldots, a_p)$ is the integer p.

Let $k \in \mathbb{N}$. Comparing the definitions of "composition of n" and "composition of n into k parts", we see that a composition of n into k parts is the same thing as a composition of n that is a k-tuple. In other words, a composition of n into k parts is the same thing as a composition of n whose length is k.

---

gers). Moreover, the sum of the entries of the k-tuple $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is

$$(p_1+1)+(p_2+1)+\cdots+(p_k+1) = \underbrace{(p_1+p_2+\cdots+p_k)}_{=n-k} + \underbrace{\underbrace{(1+1+\cdots+1)}_{k \text{ times}}}_{=k} = (n-k)+k = n.$$

Hence, $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is a k-tuple of positive integers whose sum is n. In other words, $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is a composition of n into k parts. Therefore, $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is a composition $(x_1, x_2, \ldots, x_k)$ of n into k parts such that $x_1, x_2, \ldots, x_k \in \{1,2\}$ (since $p_1 + 1, p_2 + 1, \ldots, p_k + 1 \in \{1,2\}$). In other words, $(p_1 + 1, p_2 + 1, \ldots, p_k + 1)$ is a $\{1,2\}$-composition of n into k parts (by the definition of a "$\{1,2\}$-composition of n into k parts"). Qed.

Thus, comparing the definitions of "$\{1,2\}$-composition of n" and "$\{1,2\}$-composition of n into k parts", we conclude that a $\{1,2\}$-composition of n into k parts is the same thing as a $\{1,2\}$-composition of n whose length is k. Thus,

$$\begin{aligned}&(\#\text{ of }\{1,2\}\text{-compositions of } n \text{ into } k \text{ parts})\\ &= (\#\text{ of }\{1,2\}\text{-compositions of } n \text{ whose length is } k)\,.\end{aligned}$$

Hence,

$$\begin{aligned}&(\#\text{ of }\{1,2\}\text{-compositions of } n \text{ whose length is } k)\\ &= (\#\text{ of }\{1,2\}\text{-compositions of } n \text{ into } k \text{ parts})\\ &= \binom{k}{n-k} \qquad (354)\end{aligned}$$

(by Exercise 2.10.5 **(b)**).

Now, forget that we fixed k. We thus have proved (354) for each $k \in \mathbb{N}$.

If $\mathbf{s}$ is a $\{1,2\}$-composition of n, then the length of $\mathbf{s}$ is an element of $\{0,1,\ldots,n\}$ [281]. Hence, the sum rule (Theorem 1.2.5) yields

$$\begin{aligned}&(\#\text{ of }\{1,2\}\text{-compositions of } n)\\ &= \underbrace{\sum_{k\in\{0,1,\ldots,n\}}}_{=\sum_{k=0}^{n}} \underbrace{(\#\text{ of }\{1,2\}\text{-compositions of } n \text{ whose length is } k)}_{=\binom{k}{n-k} \text{ (by (354))}}\\ &= \sum_{k=0}^{n}\binom{k}{n-k} = \sum_{k=0}^{n}\underbrace{\binom{n-k}{n-(n-k)}}_{=\binom{n-k}{k} \text{ (since } n-(n-k)=k)}\\ &\qquad (\text{here, we have substituted } n-k \text{ for } k \text{ in the sum})\\ &= \sum_{k=0}^{n}\binom{n-k}{k}.\end{aligned}$$

[281] *Proof.* Let $\mathbf{s}$ be a $\{1,2\}$-composition of n. We must prove that the length of $\mathbf{s}$ is an element of $\{0,1,\ldots,n\}$.

We know that $\mathbf{s}$ is a $\{1,2\}$-composition of n. In other words, $\mathbf{s}$ is a composition $(x_1,x_2,\ldots,x_k)$ of n such that $x_1,x_2,\ldots,x_k \in \{1,2\}$ (by the definition of a "$\{1,2\}$-composition of n"). Hence, $\mathbf{s}$ has the form $\mathbf{s} = (x_1,x_2,\ldots,x_k)$, where $(x_1,x_2,\ldots,x_k)$ is a composition of n such that $x_1,x_2,\ldots,x_k \in \{1,2\}$. Consider this $(x_1,x_2,\ldots,x_k)$. From $\mathbf{s} = (x_1,x_2,\ldots,x_k)$, we conclude that the length of $\mathbf{s}$ is k.

Lemma 7.52.1 yields $k \leq n$. Hence, $k \in \{0,1,\ldots,n\}$ (since $k \in \mathbb{N}$). In other words, k is an element of $\{0,1,\ldots,n\}$. In other words, the length of $\mathbf{s}$ is an element of $\{0,1,\ldots,n\}$ (since the length of $\mathbf{s}$ is k). Qed.

But Proposition 1.3.32 yields

$$f_{n+1} = \sum_{k=0}^{n} \binom{n-k}{k}.$$

Comparing these two equalities, we obtain

$$(\#\text{ of } \{1,2\}\text{-compositions of } n) = f_{n+1}.$$

This solves Exercise 2.10.5 **(a)**. □

7.53. Solution to Exercise 2.10.6

For our solution to Exercise 2.10.6, we will need a minor generalization of (243):

Lemma 7.53.1. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then,

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) = \binom{n+k-1}{n}.$$

Proof of Lemma 7.53.1. If $n \in \mathbb{N}$, then this follows immediately from (243). Hence, for the rest of this proof, we WLOG assume that $n \notin \mathbb{N}$. Hence, (43) (applied to $n+k-1$ and n instead of n and k) yields $\binom{n+k-1}{n} = 0$.

But there exists no $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$ [282]. Hence,

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) = 0.$$

Comparing this with $\binom{n+k-1}{n} = 0$, we obtain

$$\left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) = \binom{n+k-1}{n}.$$

Thus, Lemma 7.53.1 is proved. □

[282] *Proof.* Let $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$. Hence, the k elements $x_1, x_2, \ldots, x_k$ are k elements of $\mathbb{N}$. Thus, the sum $x_1 + x_2 + \cdots + x_k$ of these k elements must also be an element of $\mathbb{N}$. In other words, $x_1 + x_2 + \cdots + x_k \in \mathbb{N}$. If we had $x_1 + x_2 + \cdots + x_k = n$, then this would entail that $n = x_1 + x_2 + \cdots + x_k \in \mathbb{N}$, which would contradict $n \notin \mathbb{N}$. Hence, we cannot have $x_1 + x_2 + \cdots + x_k = n$. In other words, we have $x_1 + x_2 + \cdots + x_k \neq n$.

Forget that we fixed $(x_1, x_2, \ldots, x_k)$. We thus have showed that each $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfies $x_1 + x_2 + \cdots + x_k \neq n$. In other words, there exists no $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$.

Solution to Exercise 2.10.6. Set

$$U = \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n \right\}. \tag{355}$$

Thus,

$$\begin{aligned} |U| &= \left| \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n \right\} \right| \\ &= \left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n \right) \\ &= \binom{n+k-1}{n} \qquad \text{(by Lemma 7.53.1)}. \end{aligned}$$

This shows that U is a finite set. Also, clearly, $U \subseteq \mathbb{N}^k$ (by the definition of U).

For each $i \in \{1, 2, \ldots, k\}$, we define a subset A_i of U by

$$A_i = \{ (x_1, x_2, \ldots, x_k) \in U \mid x_i \geq p \}. \tag{356}$$

Then, $A_1, A_2, \ldots, A_k$ are k subsets of U. Moreover, for any $(y_1, y_2, \ldots, y_k) \in U$ and any $i \in \{1, 2, \ldots, k\}$, we have the logical equivalence

$$((y_1, y_2, \ldots, y_k) \in A_i) \iff (y_i \geq p) \tag{357}$$

(by (356)).

Now, we claim the following:

Statement 1: We have

$$\begin{aligned} &U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k) \\ &= \left\{ (x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n \right\}. \end{aligned}$$

[*Proof of Statement 1:* It is easy to see that

$$\begin{aligned} &U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k) \\ &\subseteq \left\{ (x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n \right\}. \end{aligned} \tag{358}$$

[283] *Proof of (358):* Let $\mathbf{t} \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k)$. Thus, $\mathbf{t} \in U$ and $\mathbf{t} \notin A_1 \cup A_2 \cup \cdots \cup A_k$. From

$$\mathbf{t} \in U = \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n \right\},$$

we conclude that $\mathbf{t}$ can be written in the form $\mathbf{t} = (x_1, x_2, \ldots, x_k)$ for some $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$. Consider this $(x_1, x_2, \ldots, x_k)$, and denote it by $(y_1, y_2, \ldots, y_k)$. Thus, $(y_1, y_2, \ldots, y_k) \in \mathbb{N}^k$ satisfies $y_1 + y_2 + \cdots + y_k = n$ and $\mathbf{t} = (y_1, y_2, \ldots, y_k)$.

Let $i \in \{1, 2, \ldots, k\}$. If we had $\mathbf{t} \in A_i$, then we would have $\mathbf{t} \in A_i \subseteq A_1 \cup A_2 \cup \cdots \cup A_k$, which would contradict $\mathbf{t} \notin A_1 \cup A_2 \cup \cdots \cup A_k$. Hence, we do not have $\mathbf{t} \in A_i$. In other words, we do

It is also easy to see that

$$\left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\} \subseteq U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k). \tag{359}$$

284

not have $(y_1, y_2, \ldots, y_k) \in A_i$ (since $\mathbf{t} = (y_1, y_2, \ldots, y_k)$). Because of the equivalence (357), we can thus conclude that we do not have $y_i \geq p$. In other words, we have $y_i < p$. But $y_i \in \mathbb{N}$ (since $(y_1, y_2, \ldots, y_k) \in \mathbb{N}^k$). Hence, $y_i \in \{0, 1, \ldots, p-1\}$ (since $y_i \in \mathbb{N}$ and $y_i < p$).

Forget that we fixed i. We thus have proved that $y_i \in \{0, 1, \ldots, p-1\}$ for each $i \in \{1, 2, \ldots, k\}$. Therefore, $(y_1, y_2, \ldots, y_k) \in \{0, 1, \ldots, p-1\}^k$. Thus, $(y_1, y_2, \ldots, y_k)$ is an $(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$ (since $y_1 + y_2 + \cdots + y_k = n$). In other words,

$$(y_1, y_2, \ldots, y_k) \in \left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}.$$

In view of $\mathbf{t} = (y_1, y_2, \ldots, y_k)$, this rewrites as

$$\mathbf{t} \in \left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}.$$

Forget that we fixed $\mathbf{t}$. We thus have showed that

$$\mathbf{t} \in \left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}$$

for each $\mathbf{t} \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k)$. In other words,

$$U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k) \subseteq \left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}.$$

This proves (358).

[284] *Proof of (359):* Let $\mathbf{s} \in \left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}$. Thus, $\mathbf{s}$ can be written in the form $\mathbf{s} = (x_1, x_2, \ldots, x_k)$ for some $(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$. Consider this $(x_1, x_2, \ldots, x_k)$, and denote it by $(y_1, y_2, \ldots, y_k)$. Thus, $(y_1, y_2, \ldots, y_k) \in \{0, 1, \ldots, p-1\}^k$ satisfies $y_1 + y_2 + \cdots + y_k = n$ and $\mathbf{s} = (y_1, y_2, \ldots, y_k)$.

We have $(y_1, y_2, \ldots, y_k) \in \{0, 1, \ldots, p-1\}^k \subseteq \mathbb{N}^k$ (since $\{0, 1, \ldots, p-1\} \subseteq \mathbb{N}$). Hence, $(y_1, y_2, \ldots, y_k)$ is an $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$ (since $y_1 + y_2 + \cdots + y_k = n$). In other words,

$$(y_1, y_2, \ldots, y_k) \in \left\{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}.$$

In view of (355), this rewrites as $(y_1, y_2, \ldots, y_k) \in U$. Hence, $\mathbf{s} = (y_1, y_2, \ldots, y_k) \in U$.

Next, we shall prove that $\mathbf{s} \notin A_1 \cup A_2 \cup \cdots \cup A_k$. Indeed, assume the contrary. Thus, $\mathbf{s} \in A_1 \cup A_2 \cup \cdots \cup A_k$. In other words, $\mathbf{s} \in A_i$ for some $i \in \{1, 2, \ldots, k\}$. Consider this i. We have $(y_1, y_2, \ldots, y_k) = \mathbf{s} \in A_i$. Because of the equivalence (357), this entails that $y_i \geq p$. But from $(y_1, y_2, \ldots, y_k) \in \{0, 1, \ldots, p-1\}^k$, we obtain $y_i \in \{0, 1, \ldots, p-1\}$, so that $y_i \leq p - 1 < p$. This contradicts $y_i \geq p$. This contradiction shows that our assumption was wrong. Hence, we have proved that $\mathbf{s} \notin A_1 \cup A_2 \cup \cdots \cup A_k$.

Combining $\mathbf{s} \in U$ with $\mathbf{s} \notin A_1 \cup A_2 \cup \cdots \cup A_k$, we obtain $\mathbf{s} \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k)$.

Forget that we fixed $\mathbf{s}$. We thus have proved that $\mathbf{s} \in U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k)$ for each $\mathbf{s} \in$

Combining (358) with (359), we obtain

$$\begin{aligned} &U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k) \\ &= \left\{ (x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \;\mid\; x_1 + x_2 + \cdots + x_k = n \right\}. \end{aligned}$$

This proves Statement 1.]

Next, we claim the following:

Statement 2: Let I be a subset of $[k]$. Then,

$$\left| \{ s \in U \;\mid\; s \in A_i \text{ for all } i \in I \} \right| = \binom{n - p\,|I| + k - 1}{n - p\,|I|}.$$

[*Proof of Statement 2:* We shall use the Iverson bracket notation (as defined in Definition 1.3.15). Corollary 1.6.3 **(a)** (applied to $S = [k]$ and $T = I$) yields

$$|I| = \sum_{s \in [k]} [s \in I] = \sum_{i \in [k]} [i \in I] \tag{360}$$

(here, we have renamed the summation index s as i).

Define two sets

$$\begin{aligned} P &= \{ s \in U \;\mid\; s \in A_i \text{ for all } i \in I \} \qquad \text{and} \\ Q &= \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \;\mid\; x_1 + x_2 + \cdots + x_k = n - p\,|I| \right\}. \end{aligned}$$

We shall find a bijection from P to Q.

The definition of P shows that $P \subseteq U \subseteq \mathbb{N}^k$, so that every element of P is a k-tuple of nonnegative integers. The same holds for Q (since the definition of Q shows that $Q \subseteq \mathbb{N}^k$).

For each $i \in \{1, 2, \ldots, k\}$, we define an integer q_i by $q_i = p\,[i \in I]$. Thus, we have defined k integers $q_1, q_2, \ldots, q_k$. Their sum is

$$\begin{aligned} q_1 + q_2 + \cdots + q_k &= \underbrace{\sum_{i=1}^{k}}_{= \sum_{i \in \{1,2,\ldots,k\}} = \sum_{i \in [k]}} \underbrace{q_i}_{= p[i \in I]} \\ &\qquad \text{(by the definition of } q_i\text{)} \\ &= \sum_{i \in [k]} p\,[i \in I] = p \underbrace{\sum_{i \in [k]} [i \in I]}_{= |I| \text{ (by (360))}} \\ &= p\,|I|. \end{aligned}$$

$\left\{ (x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \;\mid\; x_1 + x_2 + \cdots + x_k = n \right\}$. In other words,

$$\left\{ (x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \;\mid\; x_1 + x_2 + \cdots + x_k = n \right\} \subseteq U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k).$$

This proves (359).

If $(y_1, y_2, \ldots, y_k) \in P$, then $(y_1 - q_1, y_2 - q_2, \ldots, y_k - q_k) \in Q$ [285]. Hence, we can define a map

$$\begin{aligned} \alpha : P &\to Q, \\ (y_1, y_2, \ldots, y_k) &\mapsto (y_1 - q_1, y_2 - q_2, \ldots, y_k - q_k). \end{aligned}$$

If $(z_1, z_2, \ldots, z_k) \in Q$, then $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in P$ [286]. Hence, we can

[285] *Proof.* Let $(y_1, y_2, \ldots, y_k) \in P$. Thus,

$$(y_1, y_2, \ldots, y_k) \in P \subseteq U = \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n \right\}.$$

In other words, $(y_1, y_2, \ldots, y_k)$ is an $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$. In other words, $(y_1, y_2, \ldots, y_k)$ is an element of $\mathbb{N}^k$ and satisfies $y_1 + y_2 + \cdots + y_k = n$.

Recall that $(y_1, y_2, \ldots, y_k) \in P = \{s \in U \mid s \in A_i \text{ for all } i \in I\}$. In other words, $(y_1, y_2, \ldots, y_k)$ is an $s \in U$ satisfying $s \in A_i$ for all $i \in I$. In other words, $(y_1, y_2, \ldots, y_k)$ is an element of U and satisfies

$$(y_1, y_2, \ldots, y_k) \in A_i \qquad \text{for all } i \in I. \tag{361}$$

Now, let $i \in \{1, 2, \ldots, k\}$. Then, $y_i \in \mathbb{N}$ (since $(y_1, y_2, \ldots, y_k)$ is an element of $\mathbb{N}^k$). We shall now show that $y_i - q_i \in \mathbb{N}$. Indeed, this is obvious in the case when $q_i = 0$ (because in this case, we have $y_i - \underbrace{q_i}_{=0} = y_i \in \mathbb{N}$). Hence, for the rest of this proof of $y_i - q_i \in \mathbb{N}$, we WLOG assume that $q_i \neq 0$. Hence, we have $i \in I$ (since otherwise, we would have $[i \in I] = 0$ and thus $q_i = p \underbrace{[i \in I]}_{=0} = 0$, which would contradict $q_i \neq 0$). Hence, (361) yields $(y_1, y_2, \ldots, y_k) \in A_i$. Because of the equivalence (357), this entails that $y_i \geq p$. Thus, $y_i - p \geq 0$, so that $y_i - p \in \mathbb{N}$. Now, $q_i = p \underbrace{[i \in I]}_{\substack{=1 \\ (\text{since } i \in I)}} = p$. Hence, $y_i - \underbrace{q_i}_{=p} = y_i - p \in \mathbb{N}$. Thus, $y_i - q_i \in \mathbb{N}$ is proved.

Now, forget that we fixed i. We thus have showed that $y_i - q_i \in \mathbb{N}$ for each $i \in \{1, 2, \ldots, k\}$. In other words, $(y_1 - q_1, y_2 - q_2, \ldots, y_k - q_k) \in \mathbb{N}^k$. Moreover,

$$(y_1 - q_1) + (y_2 - q_2) + \cdots + (y_k - q_k) = \underbrace{(y_1 + y_2 + \cdots + y_k)}_{=n} - \underbrace{(q_1 + q_2 + \cdots + q_k)}_{=p|I|} = n - p\,|I|.$$

Hence, $(y_1 - q_1, y_2 - q_2, \ldots, y_k - q_k)$ is an $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n - p\,|I|$ (since $(y_1 - q_1, y_2 - q_2, \ldots, y_k - q_k) \in \mathbb{N}^k$). In other words,

$$(y_1 - q_1, y_2 - q_2, \ldots, y_k - q_k) \in \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n - p\,|I| \right\}.$$

In other words, $(y_1 - q_1, y_2 - q_2, \ldots, y_k - q_k) \in Q$ (since $Q = \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n - p\,|I| \right\}$). Qed.

[286] *Proof.* Let $(z_1, z_2, \ldots, z_k) \in Q$. Thus,

$$(z_1, z_2, \ldots, z_k) \in Q = \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n - p\,|I| \right\}.$$

In other words, $(z_1, z_2, \ldots, z_k)$ is an $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n - p\,|I|$. In other words, $(z_1, z_2, \ldots, z_k)$ is an element of $\mathbb{N}^k$ and satisfies $z_1 + z_2 + \cdots + z_k = n - p\,|I|$.

define a map

$$\beta : Q \to P,$$
$$(z_1, z_2, \ldots, z_k) \mapsto (z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k).$$

The maps α and β are mutually inverse[287], and thus are bijective. Hence, in

---

For each $i \in \{1, 2, \ldots, k\}$, we have $z_i \in \mathbb{N}$ (since $(z_1, z_2, \ldots, z_k)$ is an element of $\mathbb{N}^k$) and thus

$$\underbrace{z_i}_{\in \mathbb{N}} + \underbrace{q_i}_{\substack{= p[i \in I] \in \mathbb{N} \\ \text{(since } p \in \mathbb{N} \text{ and } [i \in I] \in \mathbb{N}\text{)}}} \in \mathbb{N}.$$

In other words, $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in \mathbb{N}^k$. Moreover,

$$\begin{aligned}&(z_1 + q_1) + (z_2 + q_2) + \cdots + (z_k + q_k) \\ &= \underbrace{(z_1 + z_2 + \cdots + z_k)}_{= n - p|I|} + \underbrace{(q_1 + q_2 + \cdots + q_k)}_{= p|I|} = (n - p|I|) + p|I| = n.\end{aligned}$$

Hence, $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k)$ is an $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ satisfying $x_1 + x_2 + \cdots + x_k = n$ (since $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in \mathbb{N}^k$). In other words,

$$(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in \left\{ (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n \right\}.$$

In view of (355), this rewrites as $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in U$.

Now, let $i \in I$. We shall show that $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in A_i$.

Indeed, $i \in I$, so that $[i \in I] = 1$. Hence, the definition of q_i yields $q_i = p \underbrace{[i \in I]}_{=1} = p$. Also, $z_i \in \mathbb{N}$ (since $(z_1, z_2, \ldots, z_k)$ is an element of $\mathbb{N}^k$) and thus $z_i \geq 0$. Thus, $\underbrace{z_i}_{\geq 0} + \underbrace{q_i}_{=p} \geq 0 + p = p$. Hence, $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k)$ is an $(x_1, x_2, \ldots, x_k) \in U$ satisfying $x_i \geq p$ (since $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in U$). In other words,

$$(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in \{ (x_1, x_2, \ldots, x_k) \in U \mid x_i \geq p \}.$$

In view of (356), this rewrites as $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in A_i$.

Now, forget that we fixed i. We thus have showed that $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in A_i$ for all $i \in I$. Hence, $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k)$ is an $s \in U$ that satisfies ($s \in A_i$ for all $i \in I$) (since $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in U$). In other words,

$$(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in \{ s \in U \mid s \in A_i \text{ for all } i \in I \}.$$

In view of $P = \{ s \in U \mid s \in A_i \text{ for all } i \in I \}$, this rewrites as $(z_1 + q_1, z_2 + q_2, \ldots, z_k + q_k) \in P$. Qed.

[287] Indeed, the map α subtracts $q_1, q_2, \ldots, q_k$ from the entries of the k-tuple that it is applied to, whereas the map β adds $q_1, q_2, \ldots, q_k$ to the entries of the k-tuple that it is applied to. Thus, the maps α and β clearly undo each other. Hence, they are mutually inverse.

particular, α is a bijection. Thus, the bijection principle yields

$$\begin{aligned}
|P| = |Q| &= \left|\left\{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n - p\,|I|\right\}\right| \\
&\qquad \left(\text{since } Q = \left\{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid x_1 + x_2 + \cdots + x_k = n - p\,|I|\right\}\right) \\
&= \left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n - p\,|I|\right) \\
&= \binom{n - p\,|I| + k - 1}{n - p\,|I|} \qquad \text{(by Lemma 7.53.1, applied to } n - p\,|I| \text{ instead of } n\text{)}.
\end{aligned}$$

In view of $P = \{s \in U \mid s \in A_i \text{ for all } i \in I\}$, this rewrites as

$$|\{s \in U \mid s \in A_i \text{ for all } i \in I\}| = \binom{n - p\,|I| + k - 1}{n - p\,|I|}.$$

This proves Statement 2.]

Now, let us note that each subset I of $[k]$ satisfies $|I| \in \{0, 1, \ldots, k\}$ (since Theorem 1.4.7 **(b)** yields $|I| \leq |[k]| = k$).

But Statement 1 yields

$$\begin{aligned}
&U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k) \\
&= \left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}.
\end{aligned}$$

Hence,

$$\begin{aligned}
&|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k)| \\
&= \left|\left\{(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}\right| \\
&= \left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, p-1\}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right).
\end{aligned}$$

Thus,

$$\begin{aligned}
&\Big(\#\text{ of } (x_1,x_2,\ldots,x_k) \in \{0,1,\ldots,p-1\}^k \text{ satisfying } x_1+x_2+\cdots+x_k = n\Big) \\
&= \left|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_k)\right| \\
&= \sum_{I\subseteq[k]} (-1)^{|I|} \underbrace{\left|\{s \in U \mid s \in A_i \text{ for all } i \in I\}\right|}_{= \binom{n-p|I|+k-1}{n-p|I|} \text{ (by Statement 2)}} \\
&\qquad \text{(by Theorem 2.9.9 (applied to } k \text{ instead of } n)) \\
&= \sum_{I\subseteq[k]} (-1)^{|I|} \binom{n-p|I|+k-1}{n-p|I|} = \sum_{j=0}^{k} \sum_{\substack{I\subseteq[k];\\ |I|=j}} \underbrace{(-1)^{|I|} \binom{n-p|I|+k-1}{n-p|I|}}_{=(-1)^j \binom{n-pj+k-1}{n-pj} \text{ (since } |I|=j)} \\
&\qquad \left(\begin{array}{c} \text{by an application of (37), since} \\ \text{each subset } I \text{ of } [k] \text{ satisfies } |I| \in \{0,1,\ldots,k\} \end{array} \right) \\
&= \sum_{j=0}^{k} \underbrace{\sum_{\substack{I\subseteq[k];\\ |I|=j}} (-1)^j \binom{n-pj+k-1}{n-pj}}_{=(\#\text{ of subsets } I \text{ of } [k] \text{ satisfying } |I|=j)\cdot(-1)^j \binom{n-pj+k-1}{n-pj}} \\
&= \sum_{j=0}^{k} \underbrace{(\#\text{ of subsets } I \text{ of } [k] \text{ satisfying } |I|=j)}_{=(\#\text{ of } j\text{-element subsets of } [k]) = \binom{k}{j} \text{ (by Theorem 1.3.12, applied to } [k], k \text{ and } j \text{ instead of } S, n \text{ and } k)} \cdot (-1)^j \binom{n-pj+k-1}{n-pj} \\
&= \sum_{j=0}^{k} \binom{k}{j} \cdot (-1)^j \binom{n-pj+k-1}{n-pj} = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \binom{n-pj+k-1}{n-pj}.
\end{aligned}$$

This solves Exercise 2.10.6. □

7.54. Solution to Exercise 2.10.7

Our solution to Exercise 2.10.7 is taken from [Grinbe16b]. We first recall some notations and basic facts from number theory:

Definition 7.54.1. If a is an integer and b is a positive integer, then

- we let $a \mathbin{//} b$ denote the quotient obtained when dividing a by b (in the sense of division with remainder);
- we let $a\%b$ denote the remainder obtained when dividing a by b.

Proposition 7.54.2. Let b be a positive integer.
(a) We have $a = (a \mathbin{//} b) \cdot b + (a\%b)$ for every $a \in \mathbb{Z}$.
(b) We have $a\%b \in \{0, 1, \ldots, b-1\}$ for every $a \in \mathbb{Z}$.
(c) If $a \in \mathbb{N}$, then $a \mathbin{//} b \in \mathbb{N}$.
(d) Any $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, b-1\}$ satisfy $(qb+r) \mathbin{//} b = q$.
(e) Any $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, b-1\}$ satisfy $(qb+r)\%b = r$.

Proof of Proposition 7.54.2. **(a)** Proposition 7.54.2 **(a)** is [19s, Corollary 2.6.9 **(d)**] (with u and n renamed as a and b).

(b) Proposition 7.54.2 **(b)** is the first claim of [19s, Corollary 2.6.9 **(a)**] (with u and n renamed as a and b).

(c) Let $a \in \mathbb{N}$. Then, Proposition 7.54.2 **(b)** yields $a\%b \in \{0, 1, \ldots, b-1\}$, so that $a\%b \leq b-1 < b$. But Proposition 7.54.2 **(a)** yields

$$a = (a \mathbin{//} b) \cdot b + \underbrace{(a\%b)}_{<b} < (a \mathbin{//} b) \cdot b + b = ((a \mathbin{//} b) + 1)\, b.$$

Hence,

$$((a \mathbin{//} b) + 1)\, b > a \geq 0 \qquad (\text{since } a \in \mathbb{N}).$$

We can divide both sides of this inequality by b (since b is positive), and thus obtain $(a \mathbin{//} b) + 1 > 0$. In other words, $a \mathbin{//} b > -1$. Since $a \mathbin{//} b \in \mathbb{Z}$, we thus conclude that $a \mathbin{//} b \geq (-1) + 1 = 0$. In other words, $a \mathbin{//} b \in \mathbb{N}$. This proves Proposition 7.54.2 **(c)**.

(d) Proposition 7.54.2 **(d)** is [19s, Exercise 2.6.4 **(c)**] (with n renamed as b).

(e) Proposition 7.54.2 **(e)** is [19s, Exercise 2.6.4 **(d)**] (with n renamed as b). □

Solution to Exercise 2.10.7. This will be a proof by double counting. We shall count the n-tuples $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ satisfying $x_1 + x_2 + \cdots + x_n = k$ in two different ways.

The first way is easy: The equality (243) (applied to k and n instead of n and k) shows that

$$(\#\text{ of } (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \text{ satisfying } x_1 + x_2 + \cdots + x_n = k) = \binom{k+n-1}{k}$$
$$= \binom{n+k-1}{k} \tag{362}$$

(since $k+n=n+k$).

The second way is trickier. Let me first outline the idea, before showing the argument in full detail.

Outline: It is well-known (a particular case of division with remainder) that any nonnegative integer x can be written as $x = 2q + r$ for a unique $q \in \mathbb{N}$ and a unique $r \in \{0,1\}$. Thus, each n-tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ can be written uniquely in the form $(2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n)$ for some $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and some $r_1, r_2, \ldots, r_n \in \{0,1\}$. In other words, for each n-tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$, there exists a unique $2 \times n$-table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ with $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0,1\}$ satisfying $(x_1, x_2, \ldots, x_n) = (2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n)$. Moreover, an n-tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ satisfies $x_1 + x_2 + \cdots + x_n = k$ if and only if the corresponding $2 \times n$-table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ satisfies $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$. Thus, there is a bijection

$$\left\{ 2 \times n\text{-tables } \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \text{ with } q_1, q_2, \ldots, q_n \in \mathbb{N} \text{ and } r_1, r_2, \ldots, r_n \in \{0,1\} \right.$$
$$\left. \text{satisfying } 2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k \right\}$$
$$\to \{ n\text{-tuples } (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \text{ satisfying } x_1 + x_2 + \cdots + x_n = k \}$$

that sends

$$\text{each } 2 \times n\text{-table } \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$$
$$\text{to the } n\text{-tuple } (2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n).$$

Hence, the bijection principle yields

$$\begin{aligned} &(\#\text{ of } n\text{-tuples } (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \text{ satisfying } x_1 + x_2 + \cdots + x_n = k) \\ &= (\#\text{ of nice tables}), \end{aligned} \tag{363}$$

where a "*nice table*" shall mean a $2 \times n$-table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ with $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0,1\}$ satisfying $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$. It thus remains to count the nice tables. But we can do this using the sum rule: Define the *top-sum* of a nice table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ to be the sum $q_1 + q_2 + \cdots + q_n$. The top-sum of a nice table is always a nonnegative integer $\leq k$ (actually, $\leq \lfloor k/2 \rfloor$, but we will not use this stronger statement), i.e., an element of $\{0, 1, \ldots, k\}$. Moreover, for each $i \in \{0, 1, \ldots, k\}$, the product rule yields

$$(\#\text{ of nice tables with top-sum } i) = \binom{n+i-1}{i} \binom{n}{k-2i},$$

because we can construct a nice table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ with top-sum i by the following algorithm:

- First, choose the n entries $q_1, q_2, \ldots, q_n$ of the top row of the table. These n entries must belong to $\mathbb{N}$ and sum to $q_1 + q_2 + \cdots + q_n = i$; in other words, we are choosing an n-tuple $(q_1, q_2, \ldots, q_n) \in \mathbb{N}^n$ satisfying $q_1 + q_2 + \cdots + q_n = i$. Thus, (243) (applied to i and n instead of n and k) shows that the # of options at this step is $\dbinom{i+n-1}{i} = \dbinom{n+i-1}{i}$.
- Then, choose the n entries $r_1, r_2, \ldots, r_n$ of the bottom row of the table. These n entries must belong to $\{0,1\}$ and sum to $r_1 + r_2 + \cdots + r_n = k - 2i$ (since we want to have $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$, but we have $q_1 + q_2 + \cdots + q_n = i$); in other words, we are choosing an n-tuple $(r_1, r_2, \ldots, r_n) \in \{0,1\}^n$ satisfying $r_1 + r_2 + \cdots + r_n = k - 2i$. Thus, Theorem 2.10.4 (applied to $k - 2i$ and n instead of n and k) shows that the # of options at this step is $\dbinom{n}{k-2i}$.

Combining these observations using the sum rule, we obtain (# of nice tables) $= \sum_{i=0}^{k} \dbinom{n+i-1}{i} \dbinom{n}{k-2i}$. In view of (363), this rewrites as

$$\begin{aligned} &(\#\text{ of } n\text{-tuples } (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \text{ satisfying } x_1 + x_2 + \cdots + x_n = k) \\ &= \sum_{i=0}^{k} \binom{n+i-1}{i} \binom{n}{k-2i}. \end{aligned}$$

Comparing this with (362), we obtain the claim of the exercise.

Detailed argument: Here comes the detailed (and formalized) version of the argument we just outlined.

We define a *nice table* to mean a $2 \times n$-table[288] $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ with $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0,1\}$ satisfying $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$.

The *top-sum* of a nice table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is defined to be the sum $q_1 + q_2 + \cdots + q_n$.

We now state our first observation:

Statement 1: We have

$$\begin{aligned} &(\#\text{ of } (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \text{ satisfying } x_1 + x_2 + \cdots + x_n = k) \\ &= (\#\text{ of nice tables}). \end{aligned}$$

[288] i.e., a rectangular table with 2 rows and n columns

[*Proof of Statement 1:* If $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is a nice table, then $(2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n)$ is an n-tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ satisfying $x_1 + x_2 + \cdots + x_n = k$ [289]. Hence, we can define a map

$$A : \{\text{nice tables}\} \to \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1 + x_2 + \cdots + x_n = k\},$$
$$\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \mapsto (2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n).$$

Consider this map A.

Now, if $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ is an n-tuple satisfying $x_1 + x_2 + \cdots + x_n = k$, then

$$\begin{pmatrix} x_1 \,//\, 2 & x_2 \,//\, 2 & \cdots & x_n \,//\, 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix}$$

[289] *Proof.* Let $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ be a nice table. According to the definition of a "nice table", this means that $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0, 1\}$ and $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$. Hence, for each $i \in [n]$, we have $q_i \in \mathbb{N}$ (since $q_1, q_2, \ldots, q_n \in \mathbb{N}$) and $r_i \in \{0, 1\}$ (since $r_1, r_2, \ldots, r_n \in \{0, 1\}$) and thus, $2 \underbrace{q_i}_{\in \mathbb{N}} + \underbrace{r_i}_{\in \{0,1\} \subseteq \mathbb{N}} \in \mathbb{N}$. In other words, the n numbers $2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n$ all belong to $\mathbb{N}$. In other words, $(2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n) \in \mathbb{N}^n$.

Hence, $(2q_1 + r_1, 2q_2 + r_2, \ldots, 2q_n + r_n)$ is an n-tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ satisfying $x_1 + x_2 + \cdots + x_n = k$ (since

$$(2q_1 + r_1) + (2q_2 + r_2) + \cdots + (2q_n + r_n) = 2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$$

). Qed.

is a nice table[290]. Hence, we can define a map

$$B : \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1 + x_2 + \cdots + x_n = k\} \to \{\text{nice tables}\},$$
$$(x_1, x_2, \ldots, x_n) \mapsto \begin{pmatrix} x_1 \,//\, 2 & x_2 \,//\, 2 & \cdots & x_n \,//\, 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix}.$$

[290] *Proof.* Let $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ be an n-tuple satisfying $x_1 + x_2 + \cdots + x_n = k$. We have $x_1, x_2, \ldots, x_n \in \mathbb{N}$ (since $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$). Thus, for each $i \in [n]$, we have $x_i \in \mathbb{N}$ and therefore $x_i \,//\, 2 \in \mathbb{N}$ (by Proposition 7.54.2 **(c)**, applied to $a = x_i$ and $b = 2$). In other words, the n numbers $x_1 \,//\, 2, x_2 \,//\, 2, \ldots, x_n \,//\, 2$ all belong to $\mathbb{N}$. In other words, $x_1 \,//\, 2, x_2 \,//\, 2, \ldots, x_n \,//\, 2 \in \mathbb{N}$.

Furthermore, for each $i \in [n]$, we have

$$\begin{aligned} x_i \% 2 &\in \{0, 1, \ldots, 2-1\} \qquad \text{(by Proposition 7.54.2 \textbf{(b)}, applied to } a = x_i \text{ and } b = 2) \\ &= \{0, 1\}. \end{aligned}$$

In other words, the n numbers $x_1 \% 2, x_2 \% 2, \ldots, x_n \% 2$ all belong to $\{0, 1\}$. In other words, $x_1 \% 2, x_2 \% 2, \ldots, x_n \% 2 \in \{0, 1\}$.

Finally, for each $i \in [n]$, we have $x_i = (x_i \,//\, 2) \cdot 2 + (x_i \% 2)$ (by Proposition 7.54.2 **(a)**, applied to $a = x_i$ and $b = 2$). In other words, we have the n equalities

$$\begin{aligned} x_1 &= (x_1 \,//\, 2) \cdot 2 + (x_1 \% 2), \\ x_2 &= (x_2 \,//\, 2) \cdot 2 + (x_2 \% 2), \\ &\vdots \\ x_n &= (x_n \,//\, 2) \cdot 2 + (x_n \% 2). \end{aligned}$$

Adding these n equalities together, we find

$$\begin{aligned} &x_1 + x_2 + \cdots + x_n \\ &= ((x_1 \,//\, 2) \cdot 2 + (x_1 \% 2)) + ((x_2 \,//\, 2) \cdot 2 + (x_2 \% 2)) + \cdots + ((x_n \,//\, 2) \cdot 2 + (x_n \% 2)) \\ &= ((x_1 \,//\, 2) + (x_2 \,//\, 2) + \cdots + (x_n \,//\, 2)) \cdot 2 + ((x_1 \% 2) + (x_2 \% 2) + \cdots + (x_n \% 2)) \\ &= 2\,((x_1 \,//\, 2) + (x_2 \,//\, 2) + \cdots + (x_n \,//\, 2)) + ((x_1 \% 2) + (x_2 \% 2) + \cdots + (x_n \% 2)). \end{aligned}$$

Comparing this with $x_1 + x_2 + \cdots + x_n = k$, we obtain

$$2\,((x_1 \,//\, 2) + (x_2 \,//\, 2) + \cdots + (x_n \,//\, 2)) + ((x_1 \% 2) + (x_2 \% 2) + \cdots + (x_n \% 2)) = k.$$

Thus, we have proved that $x_1 \,//\, 2, x_2 \,//\, 2, \ldots, x_n \,//\, 2 \in \mathbb{N}$ and $x_1 \% 2, x_2 \% 2, \ldots, x_n \% 2 \in \{0, 1\}$ and

$$2\,((x_1 \,//\, 2) + (x_2 \,//\, 2) + \cdots + (x_n \,//\, 2)) + ((x_1 \% 2) + (x_2 \% 2) + \cdots + (x_n \% 2)) = k.$$

In other words,

$$\begin{pmatrix} x_1 \,//\, 2 & x_2 \,//\, 2 & \cdots & x_n \,//\, 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix}$$

is a $2 \times n$-table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ with $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0, 1\}$ satisfying $2\,(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$. In other words,

$$\begin{pmatrix} x_1 \,//\, 2 & x_2 \,//\, 2 & \cdots & x_n \,//\, 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix}$$

is a nice table (because this is how a "nice table" was defined). Qed.

Consider this map B.

It is easy to see that $A \circ B = \mathrm{id}$ [291] and $B \circ A = \mathrm{id}$ [292]. Combining these two equalities, we conclude that the maps A and B are mutually inverse. Hence, the

[291] *Proof.* Let $\mathbf{x} \in \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1 + x_2 + \cdots + x_n = k\}$. Thus, $\mathbf{x}$ can be written in the form $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ for some $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ satisfying $x_1 + x_2 + \cdots + x_n = k$. Consider this $(x_1, x_2, \ldots, x_n)$. The definition of B yields $B(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 // 2 & x_2 // 2 & \cdots & x_n // 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix}$. Applying the map B to both sides of the equality $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, we obtain

$$B(\mathbf{x}) = B(x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 // 2 & x_2 // 2 & \cdots & x_n // 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix}.$$

Applying the map A to both sides of this equality, we find

$$\begin{aligned} A(B(\mathbf{x})) &= A\left(\begin{pmatrix} x_1 // 2 & x_2 // 2 & \cdots & x_n // 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix}\right) \\ &= (2(x_1 // 2) + (x_1 \% 2), 2(x_2 // 2) + (x_2 \% 2), \ldots, 2(x_n // 2) + (x_n \% 2)) \end{aligned} \tag{364}$$

(by the definition of the map A).

On the other hand, for each $i \in [n]$, we have

$$\begin{aligned} x_i &= (x_i // 2) \cdot 2 + (x_i \% 2) \qquad \text{(by Proposition 7.54.2 \textbf{(a)}, applied to } a = x_i \text{ and } b = 2) \\ &= 2(x_i // 2) + (x_i \% 2). \end{aligned}$$

In other words, we have the n equalities

$$\begin{aligned} x_1 &= 2(x_1 // 2) + (x_1 \% 2), \\ x_2 &= 2(x_2 // 2) + (x_2 \% 2), \\ &\vdots \\ x_n &= 2(x_n // 2) + (x_n \% 2). \end{aligned}$$

Hence,

$$(x_1, x_2, \ldots, x_n) = (2(x_1 // 2) + (x_1 \% 2), 2(x_2 // 2) + (x_2 \% 2), \ldots, 2(x_n // 2) + (x_n \% 2)).$$

Comparing this with (364), we obtain

$$A(B(\mathbf{x})) = (x_1, x_2, \ldots, x_n) = \mathbf{x} = \mathrm{id}(\mathbf{x}).$$

Hence, $(A \circ B)(\mathbf{x}) = A(B(\mathbf{x})) = \mathrm{id}(\mathbf{x})$.

Forget that we fixed $\mathbf{x}$. We thus have showed that $(A \circ B)(\mathbf{x}) = \mathrm{id}(\mathbf{x})$ for each $\mathbf{x} \in \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1 + x_2 + \cdots + x_n = k\}$. In other words, $A \circ B = \mathrm{id}$.

[292] *Proof.* Let $\mathbf{T} \in \{\text{nice tables}\}$. We shall show that $(B \circ A)(\mathbf{T}) = \mathbf{T}$.

We have $\mathbf{T} \in \{\text{nice tables}\}$; in other words, $\mathbf{T}$ is a nice table. In other words, $\mathbf{T}$ is a $2 \times n$-table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ with $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0, 1\}$ satisfying $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$ (since this is how a "nice table" is defined). Consider these $q_1, q_2, \ldots, q_n$ and $r_1, r_2, \ldots, r_n$. Thus,

$$\mathbf{T} = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}. \tag{365}$$

map B is invertible, i.e., is a bijection. Thus, the bijection principle yields

$$\begin{aligned}&\left|\left\{(x_1,x_2,\ldots,x_n)\in\mathbb{N}^n \;\mid\; x_1+x_2+\cdots+x_n=k\right\}\right| \\ &= \left|\{\text{nice tables}\}\right|.\end{aligned}$$

In other words,

$$\begin{aligned}&(\#\text{ of } (x_1,x_2,\ldots,x_n)\in\mathbb{N}^n \text{ satisfying } x_1+x_2+\cdots+x_n=k) \\ &= (\#\text{ of nice tables}).\end{aligned}$$

This proves Statement 1.]

The next observation is simpler:

Statement 2: The top-sum of any nice table belongs to $\{0,1,\ldots,k\}$.

Applying the map A to both sides of this equality, we obtain

$$A(\mathbf{T}) = A\left(\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}\right) = (2q_1+r_1, 2q_2+r_2, \ldots, 2q_n+r_n) \tag{366}$$

(by the definition of A). Define an integer x_i by $x_i = 2q_i + r_i$ for each $i \in [n]$. Thus,

$$(x_1,x_2,\ldots,x_n) = (2q_1+r_1, 2q_2+r_2, \ldots, 2q_n+r_n).$$

Comparing this with (366), we obtain $A(\mathbf{T}) = (x_1,x_2,\ldots,x_n)$. Applying the map B to both sides of this equality, we find

$$B(A(\mathbf{T})) = B(x_1,x_2,\ldots,x_n) = \begin{pmatrix} x_1 \,//\, 2 & x_2 \,//\, 2 & \cdots & x_n \,//\, 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix} \tag{367}$$

(by the definition of B).

Now, let $i \in [n]$. The definition of x_i yields $x_i = 2q_i + r_i = q_i \cdot 2 + r_i$. From $q_1, q_2, \ldots, q_n \in \mathbb{N}$, we obtain $q_i \in \mathbb{N} \subseteq \mathbb{Z}$. Also, from $r_1, r_2, \ldots, r_n \in \{0,1\}$, we obtain $r_i \in \{0,1\} = \{0,1,\ldots,2-1\}$. Hence, Proposition 7.54.2 **(d)** (applied to $b=2$ and $q=q_i$ and $r=r_i$) yields $(q_i \cdot 2 + r_i) \,//\, 2 = q_i$. In view of $x_i = q_i \cdot 2 + r_i$, this rewrites as $x_i \,//\, 2 = q_i$. Furthermore, Proposition 7.54.2 **(e)** (applied to $b=2$ and $q=q_i$ and $r=r_i$) yields $(q_i \cdot 2 + r_i) \,\%2 = r_i$. In view of $x_i = q_i \cdot 2 + r_i$, this rewrites as $x_i \% 2 = r_i$.

Now, forget that we fixed i. We thus have proved that

$$x_i \,//\, 2 = q_i \qquad \text{and} \qquad x_i \% 2 = r_i$$

for each $i \in [n]$. In other words,

$$\begin{pmatrix} x_1 \,//\, 2 & x_2 \,//\, 2 & \cdots & x_n \,//\, 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix} = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}.$$

Hence, (367) becomes

$$B(A(\mathbf{T})) = \begin{pmatrix} x_1 \,//\, 2 & x_2 \,//\, 2 & \cdots & x_n \,//\, 2 \\ x_1 \% 2 & x_2 \% 2 & \cdots & x_n \% 2 \end{pmatrix} = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} = \mathbf{T}$$

(by (365)). Thus, $(B \circ A)(\mathbf{T}) = B(A(\mathbf{T})) = \mathbf{T} = \mathrm{id}(\mathbf{T})$.

Forget that we fixed $\mathbf{T}$. We thus have proved that $(B \circ A)(\mathbf{T}) = \mathrm{id}(\mathbf{T})$ for each $\mathbf{T} \in \{\text{nice tables}\}$. In other words, $B \circ A = \mathrm{id}$.

[*Proof of Statement 2:* Let $\mathbf{T}$ be a nice table. We must show that the top-sum of $\mathbf{T}$ belongs to $\{0,1,\ldots,k\}$.

We have assumed that $\mathbf{T}$ is a nice table. According to the definition of a "nice table", this means that $\mathbf{T}$ is a $2 \times n$-table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ with $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0,1\}$ satisfying $2(q_1+q_2+\cdots+q_n)+(r_1+r_2+\cdots+r_n) = k$. Consider these $q_1, q_2, \ldots, q_n$ and $r_1, r_2, \ldots, r_n$. Thus, $\mathbf{T} = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$. Hence, the top-sum of $\mathbf{T}$ is $q_1+q_2+\cdots+q_n$ (by the definition of "top-sum").

We have $r_1, r_2, \ldots, r_n \in \{0,1\}$. Thus, $r_1, r_2, \ldots, r_n$ are nonnegative integers. Hence, their sum $r_1+r_2+\cdots+r_n$ is a nonnegative integer. Thus, $r_1+r_2+\cdots+r_n \geq 0$.

Moreover, from $q_1, q_2, \ldots, q_n \in \mathbb{N}$, we obtain $q_1+q_2+\cdots+q_n \in \mathbb{N}$. Thus, $q_1+q_2+\cdots+q_n \geq 0$, so that

$$2(q_1+q_2+\cdots+q_n) \geq q_1+q_2+\cdots+q_n.$$

But from $2(q_1+q_2+\cdots+q_n)+(r_1+r_2+\cdots+r_n) = k$, we obtain

$$\begin{aligned} k &= 2(q_1+q_2+\cdots+q_n) + \underbrace{(r_1+r_2+\cdots+r_n)}_{\geq 0} \\ &\geq 2(q_1+q_2+\cdots+q_n) \geq q_1+q_2+\cdots+q_n. \end{aligned}$$

In other words, $q_1+q_2+\cdots+q_n \leq k$. Combining this with $q_1+q_2+\cdots+q_n \in \mathbb{N}$, we obtain $q_1+q_2+\cdots+q_n \in \{0,1,\ldots,k\}$. In other words, $q_1+q_2+\cdots+q_n$ belongs to $\{0,1,\ldots,k\}$. In other words, the top-sum of $\mathbf{T}$ belongs to $\{0,1,\ldots,k\}$ (since the top-sum of $\mathbf{T}$ is $q_1+q_2+\cdots+q_n$). This completes the proof of Statement 2.]

Finally, let us count the nice tables with a given top-sum $i \in \{0,1,\ldots,k\}$:

Statement 3: Let $i \in \{0,1,\ldots,k\}$. Then,

$$(\#\text{ of nice tables having top-sum } i) = \binom{n+i-1}{i}\binom{n}{k-2i}.$$

[*Proof of Statement 3:* Define a set

$$Q = \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1+x_2+\cdots+x_n = i\}.$$

Thus,

$$\begin{aligned} |Q| &= |\{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1+x_2+\cdots+x_n = i\}| \\ &= (\#\text{ of } (x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \text{ satisfying } x_1+x_2+\cdots+x_n = i) \\ &= \binom{i+n-1}{i} \\ &\qquad (\text{by (243) (applied to } i \text{ and } n \text{ instead of } n \text{ and } k)) \\ &= \binom{n+i-1}{i} \qquad (\text{since } i+n = n+i). \end{aligned} \tag{368}$$

Define a set

$$R = \left\{ (x_1, x_2, \ldots, x_n) \in \{0,1\}^n \mid x_1 + x_2 + \cdots + x_n = k - 2i \right\}.$$

Thus,

$$\begin{aligned} |R| &= \left| \left\{ (x_1, x_2, \ldots, x_n) \in \{0,1\}^n \mid x_1 + x_2 + \cdots + x_n = k - 2i \right\} \right| \\ &= \left(\#\text{ of } (x_1, x_2, \ldots, x_n) \in \{0,1\}^n \text{ satisfying } x_1 + x_2 + \cdots + x_n = k - 2i \right) \\ &= \binom{n}{k-2i} \qquad (369) \\ &\qquad \left(\text{by Theorem 2.10.4 (applied to } k-2i \text{ and } n \text{ instead of } n \text{ and } k) \right). \end{aligned}$$

Now, if $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is a nice table having top-sum i, then

$$\left((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n) \right) \in Q \times R$$

[293]. Thus, we can define a map

$$C : \{\text{nice tables having top-sum } i\} \to Q \times R,$$
$$\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \mapsto \left((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n) \right).$$

Consider this map C.

On the other hand, any element of $Q \times R$ has the form $\left((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n) \right)$ for some $(q_1, q_2, \ldots, q_n) \in \mathbb{N}^n$ and some $(r_1, r_2, \ldots, r_n) \in \{0,1\}^n$ (since any element of Q has the form $(q_1, q_2, \ldots, q_n)$ for some $(q_1, q_2, \ldots, q_n) \in \mathbb{N}^n$, whereas any element of R has the form $(r_1, r_2, \ldots, r_n)$ for some $(r_1, r_2, \ldots, r_n) \in \{0,1\}^n$). For any $\left((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n) \right) \in Q \times R$, we have

$$\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \in \{\text{nice tables having top-sum } i\}$$

---

[293] *Proof.* Let $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ be a nice table having top-sum i. We must prove that $\left((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n) \right) \in Q \times R$.

We know that $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is a nice table. According to the definition of a "nice table", this means that $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0,1\}$ and $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$.

Also, we know that the nice table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ has top-sum i. Hence, the top-sum of the nice table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is i. Thus,

$$i = \left(\text{the top-sum of the nice table } \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \right) = q_1 + q_2 + \cdots + q_n$$

(by the definition of "top-sum"). Thus, $q_1 + q_2 + \cdots + q_n = i$. Moreover, from $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$, we obtain

$$r_1 + r_2 + \cdots + r_n = k - 2\underbrace{(q_1 + q_2 + \cdots + q_n)}_{=i} = k - 2i.$$

Now, $(q_1, q_2, \ldots, q_n)$ is an element of $\mathbb{N}^n$ (since $q_1, q_2, \ldots, q_n \in \mathbb{N}$) and satisfies $q_1 + q_2 + \cdots + q_n = i$. In other words, $(q_1, q_2, \ldots, q_n)$ is an $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ satisfying $x_1 + x_2 + \cdots + x_n = i$. In other words, $(q_1, q_2, \ldots, q_n) \in \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1 + x_2 + \cdots + x_n = i\}$. This rewrites as $(q_1, q_2, \ldots, q_n) \in Q$ (since $Q = \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1 + x_2 + \cdots + x_n = i\}$).

Also, $(r_1, r_2, \ldots, r_n)$ is an element of $\{0,1\}^n$ (since $r_1, r_2, \ldots, r_n \in \{0,1\}$) and satisfies $r_1 + r_2 + \cdots + r_n = k - 2i$. In other words, $(r_1, r_2, \ldots, r_n)$ is an $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ satisfying $x_1 + x_2 + \cdots + x_n = k - 2i$. In other words, $(r_1, r_2, \ldots, r_n) \in \left\{(x_1, x_2, \ldots, x_n) \in \{0,1\}^n \mid x_1 + x_2 + \cdots + x_n = k - 2i\right\}$. This rewrites as $(r_1, r_2, \ldots, r_n) \in R$ (since $R = \left\{(x_1, x_2, \ldots, x_n) \in \{0,1\}^n \mid x_1 + x_2 + \cdots + x_n = k - 2i\right\}$).

Combining $(q_1, q_2, \ldots, q_n) \in Q$ with $(r_1, r_2, \ldots, r_n) \in R$, we obtain $\left((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n) \right) \in Q \times R$. Qed.

[294]. Hence, we can define a map

$$D : Q \times R \to \{\text{nice tables having top-sum } i\},$$
$$((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n)) \mapsto \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}.$$

Consider this map D.

The maps C and D are mutually inverse[295]. Hence, the map C is invertible, i.e., is a bijection. Thus, the bijection principle yields

$$|\{\text{nice tables having top-sum } i\}|$$
$$= |Q \times R| = |Q| \cdot |R| \qquad \text{(by Theorem 1.1.4, applied to } X = Q \text{ and } Y = R).$$

---

[294] *Proof.* Let $((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n)) \in Q \times R$. We must prove that $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \in \{\text{nice tables having top-sum } i\}$.

We have $((q_1, q_2, \ldots, q_n), (r_1, r_2, \ldots, r_n)) \in Q \times R$. In other words, $(q_1, q_2, \ldots, q_n) \in Q$ and $(r_1, r_2, \ldots, r_n) \in R$.

We have $(q_1, q_2, \ldots, q_n) \in Q = \{(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n \mid x_1 + x_2 + \cdots + x_n = i\}$. In other words, $(q_1, q_2, \ldots, q_n)$ is an $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ satisfying $x_1 + x_2 + \cdots + x_n = i$. In other words, $(q_1, q_2, \ldots, q_n) \in \mathbb{N}^n$ and $q_1 + q_2 + \cdots + q_n = i$.

We have $(r_1, r_2, \ldots, r_n) \in R = \left\{(x_1, x_2, \ldots, x_n) \in \{0,1\}^n \mid x_1 + x_2 + \cdots + x_n = k - 2i\right\}$. In other words, $(r_1, r_2, \ldots, r_n)$ is an $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ satisfying $x_1 + x_2 + \cdots + x_n = k - 2i$. In other words, $(r_1, r_2, \ldots, r_n) \in \{0,1\}^n$ and $r_1 + r_2 + \cdots + r_n = k - 2i$.

Now,

$$2\underbrace{(q_1 + q_2 + \cdots + q_n)}_{=i} + \underbrace{(r_1 + r_2 + \cdots + r_n)}_{=k-2i} = 2i + (k - 2i) = k.$$

Now, we have $q_1, q_2, \ldots, q_n \in \mathbb{N}$ (since $(q_1, q_2, \ldots, q_n) \in \mathbb{N}^n$) and $r_1, r_2, \ldots, r_n \in \{0,1\}$ (since $(r_1, r_2, \ldots, r_n) \in \{0,1\}^n$).

Thus, we know that the $2 \times n$-table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ satisfies $q_1, q_2, \ldots, q_n \in \mathbb{N}$ and $r_1, r_2, \ldots, r_n \in \{0,1\}$ and $2(q_1 + q_2 + \cdots + q_n) + (r_1 + r_2 + \cdots + r_n) = k$. In other words, $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is a nice table (because this is how a "nice table" was defined). Furthermore, the top-sum of this nice table $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is

$$q_1 + q_2 + \cdots + q_n \qquad \text{(by the definition of the "top-sum")}$$
$$= i.$$

Hence, $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix}$ is a nice table having top-sum i. In other words, $\begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ r_1 & r_2 & \cdots & r_n \end{pmatrix} \in \{\text{nice tables having top-sum } i\}$. Qed.

[295] *Proof.* This follows immediately from the definitions of C and D.

Hence,

$$\begin{aligned}
&(\text{\# of nice tables having top-sum } i) \\
&= |\{\text{nice tables having top-sum } i\}| \\
&= \underbrace{|Q|}_{\substack{=\binom{n+i-1}{i} \\ \text{(by (368))}}} \cdot \underbrace{|R|}_{\substack{=\binom{n}{k-2i} \\ \text{(by (369))}}} = \binom{n+i-1}{i}\binom{n}{k-2i}.
\end{aligned}$$

This proves Statement 3.]

Now, we have almost solved the exercise. Statement 2 shows that the top-sum of any nice table belongs to $\{0,1,\ldots,k\}$. Hence, the sum rule (specifically, Theorem 1.2.5) yields

$$\begin{aligned}
(\text{\# of nice tables}) &= \sum_{i\in\{0,1,\ldots,k\}} \underbrace{(\text{\# of nice tables having top-sum } i)}_{\substack{=\binom{n+i-1}{i}\binom{n}{k-2i} \\ \text{(by Statement 3)}}} \\
&= \underbrace{\sum_{i\in\{0,1,\ldots,k\}}}_{=\sum_{i=0}^{k}} \binom{n+i-1}{i}\binom{n}{k-2i} = \sum_{i=0}^{k}\binom{n+i-1}{i}\binom{n}{k-2i}.
\end{aligned}$$

But Statement 1 yields

$$\begin{aligned}
&(\text{\# of } (x_1,x_2,\ldots,x_n) \in \mathbb{N}^n \text{ satisfying } x_1+x_2+\cdots+x_n = k) \\
&= (\text{\# of nice tables}) = \sum_{i=0}^{k}\binom{n+i-1}{i}\binom{n}{k-2i}.
\end{aligned}$$

Comparing this with (362), we find

$$\sum_{i=0}^{k}\binom{n+i-1}{i}\binom{n}{k-2i} = \binom{n+k-1}{k}.$$

This solves Exercise 2.10.7. □

7.55. Solution to Exercise 2.10.8

Exercise 2.10.8 wants us to generalize Exercise 2.10.7 to all $n \in \mathbb{R}$. Here is this generalization:

Proposition 7.55.1. Let $n \in \mathbb{R}$ and $k \in \mathbb{N}$. Prove that

$$\sum_{i=0}^{k} \binom{n+i-1}{i} \binom{n}{k-2i} = \binom{n+k-1}{k}.$$

Proof of Proposition 7.55.1. For each $x \in \mathbb{N}$, we have

$$\sum_{i=0}^{k} \binom{x+i-1}{i} \binom{x}{k-2i} = \binom{x+k-1}{k} \tag{370}$$

(by Exercise 2.10.7 (applied to x instead of n)).

Define two polynomials P and Q (in 1 variable X, with real coefficients) by

$$P = \sum_{i=0}^{k} \binom{X+i-1}{i} \binom{X}{k-2i} \qquad \text{and} \qquad Q = \binom{X+k-1}{k}.$$

These are well-defined polynomials[296].

Now, for each $x \in \mathbb{R}$, we have

$$Q(x) = \binom{x+k-1}{k} \qquad \left(\text{by Proposition 2.6.12, since } Q = \binom{X+k-1}{k}\right)$$

and

$$P(x) = \sum_{i=0}^{k} \binom{x+i-1}{i} \binom{x}{k-2i} \qquad (\text{likewise}).$$

In view of these two equalities, we can rewrite (370) as

$$P(x) = Q(x).$$

[296] They can be written explicitly as follows:

$$\begin{aligned} P &= \sum_{i=0}^{k} \binom{X+i-1}{i} \binom{X}{k-2i} \\ &= \sum_{i=0}^{k} \frac{(X+i-1)(X+i-2)\cdots(X+1)X}{i!} \\ &\qquad \cdot \begin{cases} \dfrac{X(X-1)(X-2)\cdots(X-(k-2i)+1)}{(k-2i)!}, & \text{if } k-2i \in \mathbb{N}; \\ 0, & \text{if } k-2i \notin \mathbb{N} \end{cases} \end{aligned}$$

and

$$Q = \binom{X+k-1}{k} = \frac{(X+k-1)(X+k-2)\cdots(X+1)X}{k!}.$$

Hence, we know that $P(x) = Q(x)$ holds for all $x \in \mathbb{N}$ (because we know that (370) holds for all $x \in \mathbb{N}$). Therefore, Corollary 2.6.10 yields $P = Q$. Thus, $P(x) = Q(x)$ for all $x \in \mathbb{R}$. In other words,

$$\sum_{i=0}^{k} \binom{x+i-1}{i} \binom{x}{k-2i} = \binom{x+k-1}{k}$$

for all $x \in \mathbb{R}$ (since $Q(x) = \binom{x+k-1}{k}$ and $P(x) = \sum_{i=0}^{k} \binom{x+i-1}{i} \binom{x}{k-2i}$ for each $x \in \mathbb{R}$). Applying this to $x = n$, we obtain

$$\sum_{i=0}^{k} \binom{n+i-1}{i} \binom{n}{k-2i} = \binom{n+k-1}{k}.$$

This proves Proposition 7.55.1. □

Thus, Exercise 2.10.8 is solved.

7.56. Solution to Exercise 2.10.9

Exercise 2.10.9 is [18s-mt2s, Exercise 6], and two solutions can be found on the course website (1 and 2). Let us give another, based on the following lemma:

Lemma 7.56.1. Let n be a positive integer. Then,

$$\sum_{k=0}^{n} k \binom{n-1}{k-1} = (n+1)\, 2^{n-2}.$$

Proof of Lemma 7.56.1. We have $n - 1 \in \mathbb{N}$ (since n is a positive integer).

We can split off the addend for $k = 0$ from the sum $\sum_{k=0}^{n} k\binom{n-1}{k-1}$. This yields

$$\sum_{k=0}^{n} k\binom{n-1}{k-1} = \underbrace{0\binom{n-1}{0-1}}_{=0} + \sum_{k=1}^{n} k\binom{n-1}{k-1} = \sum_{k=1}^{n} k\binom{n-1}{k-1}$$

$$= \sum_{k=0}^{n-1} (k+1) \underbrace{\binom{n-1}{(k+1)-1}}_{=\binom{n-1}{k}}$$

(here, we have substituted $k+1$ for k in the sum)

$$= \sum_{k=0}^{n-1} \underbrace{(k+1)\binom{n-1}{k}}_{=k\binom{n-1}{k}+\binom{n-1}{k}} = \sum_{k=0}^{n-1} \left(k\binom{n-1}{k} + \binom{n-1}{k} \right)$$

$$= \underbrace{\sum_{k=0}^{n-1} k\binom{n-1}{k}}_{\substack{=(n-1)\cdot 2^{(n-1)-1} \\ \text{(by Exercise 1.3.6,} \\ \text{applied to } n-1 \text{ instead of } n)}} + \underbrace{\sum_{k=0}^{n-1} \binom{n-1}{k}}_{\substack{=2^{n-1} \\ \text{(by Corollary 1.3.27,} \\ \text{applied to } n-1 \text{ instead of } n)}}$$

$$= (n-1) \cdot \underbrace{2^{(n-1)-1}}_{=2^{n-2}} + \underbrace{2^{n-1}}_{=2\cdot 2^{n-2}} = (n-1) \cdot 2^{n-2} + 2 \cdot 2^{n-2}$$

$$= \underbrace{((n-1)+2)}_{=n+1} 2^{n-2} = (n+1)\, 2^{n-2}.$$

This proves Lemma 7.56.1. □

Solution to Exercise 2.10.9. Let $\mathbb{P} = \{1, 2, 3, \ldots\}$ be the set of all positive integers.

If α is any composition of n, then (the length of α) $\in \{0, 1, \ldots, n\}$ [297].

Let $k \in \mathbb{N}$. Then, a k-tuple of positive integers is the same as an element of $\mathbb{P}^k$ (since $\mathbb{P}$ is the set of all positive integers).

Recall that a composition of n is the same as a tuple of positive integers whose

[297] *Proof.* Let α be a composition of n.

Write α in the form $\alpha = (x_1, x_2, \ldots, x_k)$. Then, α is a k-tuple; thus, the length of α is k (by the definition of "length"). But α is a composition of n; in other words, $(x_1, x_2, \ldots, x_k)$ is a composition of n (since $\alpha = (x_1, x_2, \ldots, x_k)$). Hence, Proposition 7.52.1 yields $k \leq n$. Thus, k is an element of $\{0, 1, \ldots, n\}$ (since $k \in \mathbb{N}$). In other words, the length of α is an element of $\{0, 1, \ldots, n\}$ (since the length of α is k). In other words, (the length of α) $\in \{0, 1, \ldots, n\}$. Qed.

sum is n (by the definition of a "composition of n"). Hence,

$$\begin{aligned}
&\{\alpha \text{ is a composition of } n \mid (\text{the length of } \alpha) = k\} \\
&= \{\alpha \text{ is a tuple of positive integers whose sum is } n \mid (\text{the length of } \alpha) = k\} \\
&= \{\alpha \text{ is a tuple of positive integers whose sum is } n \mid \alpha \text{ is a } k\text{-tuple}\} \\
&\qquad \left(\begin{array}{c} \text{because a tuple } \alpha \text{ satisfies } (\text{the length of } \alpha) = k \text{ if and only if} \\ \text{it is a } k\text{-tuple} \end{array} \right) \\
&= \{\alpha \text{ is a } k\text{-tuple of positive integers whose sum is } n\} \\
&= \{(x_1, x_2, \ldots, x_k) \text{ is a } k\text{-tuple of positive integers whose sum is } n\} \\
&\qquad (\text{here, we have renamed the index } \alpha \text{ as } (x_1, x_2, \ldots, x_k)) \\
&= \{(x_1, x_2, \ldots, x_k) \text{ is a } k\text{-tuple of positive integers} \mid x_1 + x_2 + \cdots + x_k = n\} \\
&= \left\{(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \mid x_1 + x_2 + \cdots + x_k = n\right\} \\
&\qquad \left(\text{since a } k\text{-tuple of positive integers is the same as an element of } \mathbb{P}^k\right).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&|\{\alpha \text{ is a composition of } n \mid (\text{the length of } \alpha) = k\}| \\
&= \left|\left\{(x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \mid x_1 + x_2 + \cdots + x_k = n\right\}\right| \\
&= \left(\#\text{ of } (x_1, x_2, \ldots, x_k) \in \mathbb{P}^k \text{ satisfying } x_1 + x_2 + \cdots + x_k = n\right) \\
&= \begin{cases} \dbinom{n-1}{k-1}, & \text{if } n > 0; \\ [k = 0], & \text{if } n = 0 \end{cases} \qquad (\text{by (240)}) \\
&= \dbinom{n-1}{k-1} \qquad (\text{since } n > 0). \qquad (371)
\end{aligned}$$

Forget that we fixed k. We thus have proved (371) for each $k \in \mathbb{N}$.

Now,

$$\begin{aligned}
&(\text{the sum of the lengths of all compositions of } n) \\
&= \sum_{\alpha \text{ is a composition of } n} (\text{the length of } \alpha) \\
&= \sum_{k \in \{0,1,\ldots,n\}} \sum_{\substack{\alpha \text{ is a composition of } n; \\ (\text{the length of } \alpha) = k}} \underbrace{(\text{the length of } \alpha)}_{=k} \\
&\qquad \left(\begin{array}{c} \text{by (37), because if } \alpha \text{ is any composition of } n, \\ \text{then } (\text{the length of } \alpha) \in \{0,1,\ldots,n\} \end{array} \right) \\
&= \sum_{k \in \{0,1,\ldots,n\}} \underbrace{\sum_{\substack{\alpha \text{ is a composition of } n; \\ (\text{the length of } \alpha) = k}} k}_{= \left| \{\alpha \text{ is a composition of } n \mid (\text{the length of } \alpha) = k\} \right| \cdot k} \\
&= \underbrace{\sum_{k \in \{0,1,\ldots,n\}}}_{= \sum_{k=0}^{n}} \underbrace{\left| \{\alpha \text{ is a composition of } n \mid (\text{the length of } \alpha) = k\} \right|}_{= \binom{n-1}{k-1} \atop (\text{by (371)})} \cdot k \\
&= \sum_{k=0}^{n} \binom{n-1}{k-1} \cdot k = \sum_{k=0}^{n} k \binom{n-1}{k-1} = (n+1)\, 2^{n-2} \qquad (\text{by Lemma 7.56.1}) .
\end{aligned}$$

This solves Exercise 2.10.9. □

7.57. Solution to Exercise 2.11.1

Before we solve Exercise 2.11.1, let us recall the definition of the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$:

Definition 7.57.1. Let T be a set. Let $k \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_k$ be any k elements of T (not necessarily distinct). Then, $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ is the multisubset of T defined as the map

$$\begin{aligned}
&T \to \mathbb{N}, \\
&t \mapsto (\#\text{ of } i \in [k] \text{ satisfying } a_i = t) .
\end{aligned}$$

Indeed, Definition 7.57.1 is simply a restatement of the last sentence of Definition 2.11.1 **(c)**.

Solution to Exercise 2.11.1. Definition 7.57.1 shows that $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ is the multisubset of T defined as the map

$$\begin{aligned}
&T \to \mathbb{N}, \\
&t \mapsto (\#\text{ of } i \in [k] \text{ satisfying } a_i = t) .
\end{aligned}$$

Let us denote this map by f. Thus, $\{a_1, a_2, \ldots, a_k\}_{\text{multi}} = f$. Hence,

$$\begin{aligned}(\text{the size of } \{a_1, a_2, \ldots, a_k\}_{\text{multi}}) &= (\text{the size of } f) \\ &= \sum_{t \in T} \underbrace{f(t)}_{\substack{=(\#\text{ of } i \in [k] \text{ satisfying } a_i = t) \\ (\text{by the definition of } f)}} \qquad (\text{by Definition 2.11.2}) \\ &= \sum_{t \in T} (\#\text{ of } i \in [k] \text{ satisfying } a_i = t)\,.\end{aligned}$$

Comparing this with

$$\begin{aligned}k &= |[k]| \qquad (\text{since } [k] = \{1, 2, \ldots, k\} \text{ is a } k\text{-element set}) \\ &= \sum_{t \in T} (\#\text{ of } i \in [k] \text{ satisfying } a_i = t) \\ &\qquad (\text{by the sum rule (Theorem 1.2.5), since } a_i \in T \text{ for each } i \in [k])\,,\end{aligned}$$

we obtain $(\text{the size of } \{a_1, a_2, \ldots, a_k\}_{\text{multi}}) = k$. In other words, the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of T has size k. This solves Exercise 2.11.1. □

7.58. Solution to Exercise 2.11.2

Exercise 2.11.2 asks us to prove Proposition 2.11.5 and Proposition 2.11.6. We shall prove Proposition 2.11.5 first. This proof will imitate the proof of Proposition 1.4.11 that is given in [Grinbe15, proof of Theorem 2.46]. First, however, we need to build up some basics of the theory of multisubsets. Since these fundamental constructions are hard to find in the mathematical literature, I will do them in detail; very little (if anything) in them is non-obvious.

We recall that multisubsets of a set T have been defined as (certain) maps from T to $\mathbb{N}$. Even if we can think of them as analogues of sets, they are thus (formally speaking) maps. Hence, we will tend to use letters like f, g, h (rather than S or A) for them in this section.

Definition 7.58.1. Let T be a set. Let f be any multisubset of T. Then, we let $|f|$ denote the size of f. Thus,

$$|f| = (\text{the size of } f) = \sum_{t \in T} f(t) \tag{372}$$

(by the definition of the size of a multisubset).

Let us next define a concept of inclusion for multisubsets of T:

Definition 7.58.2. Let T be a set. Let f and g be two multisubsets of T. Then, we shall say that $f \subseteq g$ if and only if each $t \in T$ satisfies $f(t) \leq g(t)$.

Thus, we have defined a relation "$\subseteq$" between multisubsets of T. It is an analogue of the relation "$\subseteq$" between sets, but it takes the multiplicities into account: Two multisubsets f and g of T satisfy $f \subseteq g$ if and only if each element of T appears at most as often in f as it appears in g. For example, we have $\{1,3,3,5,6\}_{\text{multi}} \subseteq \{1,1,3,3,3,5,6,7\}_{\text{multi}}$, but we don't have $\{1,3,3,5\}_{\text{multi}} \subseteq \{1,1,3,5,5\}_{\text{multi}}$.

Definition 7.58.3. Let T be a set. Let f and g be two multisubsets of T. Then, the map

$$\begin{aligned} T &\to \mathbb{N}, \\ t &\mapsto f(t) + g(t) \end{aligned}$$

is a multisubset of T (by Proposition 7.58.4 **(a)** below). This multisubset of T will be denoted by $f \cup g$.

The multisubset $f \cup g$ is an analogue of the union of two sets, but it takes the multiplicities into account: If an element of T appears a times in f and appears b times in g, then it appears $a + b$ times in $f \cup g$. For example, $\{1,3,4,4,5\}_{\text{multi}} \cup \{2,3,4\}_{\text{multi}} = \{1,2,3,3,4,4,4,5\}_{\text{multi}}$.

Let us prove a few properties of this "multisubset union" $f \cup g$:

Proposition 7.58.4. Let T be a set. Let f and g be two multisubsets of T. Then:
(a) The map

$$\begin{aligned} T &\to \mathbb{N}, \\ t &\mapsto f(t) + g(t) \end{aligned}$$

is a multisubset of T.
(b) We have $|f \cup g| = |f| + |g|$.
(c) We have $f \subseteq f \cup g$ and $g \subseteq f \cup g$.
(d) We have $f \cup g = g \cup f$.

Proof of Proposition 7.58.4. We know that f and g are multisubsets of T; thus, f and g are maps from T to $\mathbb{N}$.

We know that f is a multisubset of T. According to Definition 2.11.1 **(a)**, this means that only finitely many $t \in T$ satisfy $f(t) \neq 0$. Hence, we know that only finitely many $t \in T$ satisfy $f(t) \neq 0$. In other words, the set $\{t \in T \mid f(t) \neq 0\}$ is finite. Similarly, the set $\{t \in T \mid g(t) \neq 0\}$ is finite.

(a) We know that f and g are maps from T to $\mathbb{N}$. Hence, each $t \in T$ satisfies $f(t) \in \mathbb{N}$ and $g(t) \in \mathbb{N}$ and therefore $f(t) + g(t) \in \mathbb{N}$. Thus, the map

$$\begin{aligned} T &\to \mathbb{N}, \\ t &\mapsto f(t) + g(t) \end{aligned}$$

is well-defined. Moreover, it is easy to see that this map is a multisubset of T [298]. This proves Proposition 7.58.4 **(a)**.

(b) The equality (372) yields $|f| = \sum_{t \in T} f(t)$. Also, applying (372) to g instead of f, we find $|g| = \sum_{t \in T} g(t)$. Adding these two equalities together, we obtain

$$|f| + |g| = \sum_{t \in T} f(t) + \sum_{t \in T} g(t) = \sum_{t \in T} (f(t) + g(t)).$$

[298] *Proof.* We need to show that the map

$$T \to \mathbb{N},$$
$$t \mapsto f(t) + g(t)$$

is a multisubset of T. According to Definition 2.11.1 **(a)**, this means showing that only finitely many $t \in T$ satisfy $f(t) + g(t) \neq 0$. Thus, we need to show that only finitely many $t \in T$ satisfy $f(t) + g(t) \neq 0$. In other words, we need to show that the set $\{t \in T \mid f(t) + g(t) \neq 0\}$ is finite.

Let $s \in \{t \in T \mid f(t) + g(t) \neq 0\}$. We shall show that $s \in \{t \in T \mid f(t) \neq 0\} \cup \{t \in T \mid g(t) \neq 0\}$.

Indeed, assume the contrary. Hence, $s \notin \{t \in T \mid f(t) \neq 0\} \cup \{t \in T \mid g(t) \neq 0\}$. In other words, we have both $s \notin \{t \in T \mid f(t) \neq 0\}$ and $s \notin \{t \in T \mid g(t) \neq 0\}$.

But $s \in \{t \in T \mid f(t) + g(t) \neq 0\}$. Thus, s is a $t \in T$ satisfying $f(t) + g(t) \neq 0$. In other words, $s \in T$ and $f(s) + g(s) \neq 0$.

If we had $f(s) \neq 0$, then s would be an element $t \in T$ satisfying $f(t) \neq 0$, and therefore we would have $s \in \{t \in T \mid f(t) \neq 0\}$; but this would contradict $s \notin \{t \in T \mid f(t) \neq 0\}$. Hence, we cannot have $f(s) \neq 0$. Thus, we must have $f(s) = 0$. Similarly, $g(s) = 0$. Hence, $\underbrace{f(s)}_{=0} + \underbrace{g(s)}_{=0} = 0$, which contradicts $f(s) + g(s) \neq 0$.

This contradiction shows that our assumption was false. Hence, $s \in \{t \in T \mid f(t) \neq 0\} \cup \{t \in T \mid g(t) \neq 0\}$ is proved.

Now, forget that we fixed s. We thus have proved that $s \in \{t \in T \mid f(t) \neq 0\} \cup \{t \in T \mid g(t) \neq 0\}$ for each $s \in \{t \in T \mid f(t) + g(t) \neq 0\}$. In other words,

$$\{t \in T \mid f(t) + g(t) \neq 0\} \text{ is a subset of } \{t \in T \mid f(t) \neq 0\} \cup \{t \in T \mid g(t) \neq 0\}.$$

But the set $\{t \in T \mid f(t) \neq 0\} \cup \{t \in T \mid g(t) \neq 0\}$ is finite (since it is the union of the two finite sets $\{t \in T \mid f(t) \neq 0\}$ and $\{t \in T \mid g(t) \neq 0\}$). Hence, its subset $\{t \in T \mid f(t) + g(t) \neq 0\}$ must be finite as well (since a subset of a finite set is always finite). In other words, only finitely many $t \in T$ satisfy $f(t) + g(t) \neq 0$. In other words, the map

$$T \to \mathbb{N},$$
$$t \mapsto f(t) + g(t)$$

is a multisubset of T. Qed.

Comparing this with

$$|f \cup g| = \sum_{t \in T} \underbrace{(f \cup g)(t)}_{\substack{= f(t) + g(t) \\ \text{(by the definition of } f \cup g\text{)}}} \qquad \text{(by (372), applied to } f \cup g \text{ instead of } f\text{)}$$
$$= \sum_{t \in T} (f(t) + g(t)),$$

we obtain $|f \cup g| = |f| + |g|$. This proves Proposition 7.58.4 **(b)**.

(c) Each $t \in T$ satisfies

$$(f \cup g)(t) = f(t) + \underbrace{g(t)}_{\substack{\geq 0 \\ \text{(since } g(t) \in \mathbb{N} \\ \text{(because } g \text{ is a map from } T \text{ to } \mathbb{N}\text{))}}} \qquad \text{(by the definition of } f \cup g\text{)}$$
$$\geq f(t).$$

In other words, each $t \in T$ satisfies $f(t) \leq (f \cup g)(t)$. In other words, $f \subseteq f \cup g$ (according to Definition 7.58.2). An analogous argument shows that $g \subseteq f \cup g$. Hence, Proposition 7.58.4 **(c)** is proved.

(d) For each $t \in T$, we have

$$(f \cup g)(t) = f(t) + g(t) \tag{373}$$

(by the definition of $f \cup g$) and

$$(g \cup f)(t) = g(t) + f(t) \tag{374}$$

(by the definition of $g \cup f$). Hence, for each $t \in T$, we have

$$(f \cup g)(t) = f(t) + g(t) \qquad \text{(by (373))}$$
$$= g(t) + f(t) = (g \cup f)(t) \qquad \text{(by (374))}.$$

In other words, $f \cup g = g \cup f$ (since both $f \cup g$ and $g \cup f$ are maps from T to $\mathbb{N}$). This proves Proposition 7.58.4 **(d)**. □

Proposition 7.58.5. Let T be a set. Let $k \in \mathbb{N}$ and $\ell \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_k$ be any k elements of T (not necessarily distinct). Let $b_1, b_2, \ldots, b_\ell$ be any ℓ elements of T (not necessarily distinct). Then,

$$\{a_1, a_2, \ldots, a_k\}_{\text{multi}} \cup \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}} = \{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}_{\text{multi}}.$$

Proof of Proposition 7.58.5. Definition 7.57.1 says that $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ is the multisubset of T defined as the map

$$T \to \mathbb{N},$$
$$t \mapsto (\#\text{ of } i \in [k] \text{ satisfying } a_i = t).$$

Hence, for each $t \in T$, we have[299]

$$\begin{aligned}
&\{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) \\
&= (\#\text{ of } i \in [k] \text{ satisfying } a_i = t) \\
&= (\#\text{ of times } t \text{ appears in the } k\text{-tuple } (a_1, a_2, \ldots, a_k)) . \qquad (375)
\end{aligned}$$

Likewise, for each $t \in T$, we have

$$\begin{aligned}
&\{b_1, b_2, \ldots, b_\ell\}_{\text{multi}}(t) \\
&= (\#\text{ of times } t \text{ appears in the } \ell\text{-tuple } (b_1, b_2, \ldots, b_\ell)) . \qquad (376)
\end{aligned}$$

Likewise, for each $t \in T$, we have

$$\begin{aligned}
&\{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}_{\text{multi}}(t) \\
&= (\#\text{ of times } t \text{ appears in the } (k+\ell)\text{-tuple } (a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell)) .
\end{aligned}$$

Hence, for each $t \in T$, we have

$$\begin{aligned}
&\{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}_{\text{multi}}(t) \\
&= (\#\text{ of times } t \text{ appears in the } (k+\ell)\text{-tuple } (a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell)) \\
&= \underbrace{(\#\text{ of times } t \text{ appears in the } k\text{-tuple } (a_1, a_2, \ldots, a_k))}_{\substack{= \{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) \\ \text{(by (375))}}} \\
&\qquad + \underbrace{(\#\text{ of times } t \text{ appears in the } \ell\text{-tuple } (b_1, b_2, \ldots, b_\ell))}_{\substack{= \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}}(t) \\ \text{(by (376))}}} \\
&= \{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) + \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}}(t) . \qquad (377)
\end{aligned}$$

On the other hand, for each $t \in T$, we have

$$\begin{aligned}
&(\{a_1, a_2, \ldots, a_k\}_{\text{multi}} \cup \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}})(t) \\
&= \{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) + \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}}(t) \\
&\qquad (\text{by the definition of the map } \{a_1, a_2, \ldots, a_k\}_{\text{multi}} \cup \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}}) \\
&= \{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}_{\text{multi}}(t)
\end{aligned}$$

(by (377)). In other words,

$$\{a_1, a_2, \ldots, a_k\}_{\text{multi}} \cup \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}} = \{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}_{\text{multi}}$$

(because both $\{a_1, a_2, \ldots, a_k\}_{\text{multi}} \cup \{b_1, b_2, \ldots, b_\ell\}_{\text{multi}}$ and $\{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}_{\text{multi}}$ are maps from T to $\mathbb{N}$). This proves Proposition 7.58.5. $\square$

[299] Recall that any multisubset of T is a map from T to $\mathbb{N}$. Hence, for example, the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of T is a map from T to $\mathbb{N}$, and thus can be evaluated at $t \in T$. Thus, expressions like "$\{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t)$" make sense.

Having defined the "union" $f \cup g$ of two multisubsets f and g, let us next define their "difference" $g \setminus f$. This is an analogue of the set difference of two sets, but we shall only define it in the simplest case – namely, when $f \subseteq g$. (This is the only case in which we will need it.)

Definition 7.58.6. Let T be a set. Let f and g be two multisubsets of T such that $f \subseteq g$. Then, the map

$$\begin{aligned} T &\to \mathbb{N}, \\ t &\mapsto g(t) - f(t) \end{aligned}$$

is a multisubset of T (by Proposition 7.58.7 **(a)** further below). This multisubset of T is denoted by $g \setminus f$.

Proposition 7.58.7. Let T be a set. Let f and g be two multisubsets of T such that $f \subseteq g$.

(a) The map

$$\begin{aligned} T &\to \mathbb{N}, \\ t &\mapsto g(t) - f(t) \end{aligned}$$

is a multisubset of T.

(b) We have $(g \setminus f) \cup f = g$.

(c) We have $g \setminus f \subseteq g$.

Proof of Proposition 7.58.7. **(a)** We have $f \subseteq g$. In other words, each $t \in T$ satisfies $f(t) \leq g(t)$ (by Definition 7.58.2). Hence, each $t \in T$ satisfies $g(t) - f(t) \in \mathbb{N}$ (since the previous sentence says that $f(t) \leq g(t)$, hence $g(t) \geq f(t)$ and therefore $g(t) - f(t) \in \mathbb{N}$ [300]). Thus, the map

$$\begin{aligned} T &\to \mathbb{N}, \\ t &\mapsto g(t) - f(t) \end{aligned}$$

is well-defined. Moreover, it is easy to see that this map is a multisubset of T [301]. This proves Proposition 7.58.7 **(a)**.

(b) For each $t \in T$, we have

$$(g \setminus f)(t) = g(t) - f(t) \tag{378}$$

[300] since $g(t) - f(t)$ is an integer

[301] The proof of this fact is analogous to our proof (during the proof of Proposition 7.58.4 **(a)** above) of the fact that

$$\begin{aligned} T &\to \mathbb{N}, \\ t &\mapsto f(t) + g(t) \end{aligned}$$

is a multisubset of T.

(by the definition of $g \setminus f$). Hence, for each $t \in T$, we have

$$\begin{aligned}((g \setminus f) \cup f)(t) &= (g \setminus f)(t) + f(t) \qquad \text{(by the definition of } (g \setminus f) \cup f\text{)} \\ &= g(t) \qquad \text{(by (378))}.\end{aligned}$$

In other words, $(g \setminus f) \cup f = g$ (since both $(g \setminus f) \cup f$ and g are maps from T to $\mathbb{N}$). This proves Proposition 7.58.7 **(b)**.

(c) Proposition 7.58.4 **(c)** (applied to $g \setminus f$ and f instead of f and g) yields $g \setminus f \subseteq (g \setminus f) \cup f$ and $f \subseteq (g \setminus f) \cup f$. Thus, in particular, $g \setminus f \subseteq (g \setminus f) \cup f = g$ (by Proposition 7.58.7 **(b)**). This proves Proposition 7.58.7 **(c)**. □

Proposition 7.58.7 **(b)** is a multiset analogue of the standard fact that if A and B are two sets satisfying $A \subseteq B$, then $(B \setminus A) \cup A = B$. A similar fact is that if A and B are two disjoint sets, then $(B \cup A) \setminus A = B$. This, too, has a multiset analogue (but without any disjointness requirement):

Proposition 7.58.8. Let T be a set. Let f and g be two multisubsets of T. Then, $(g \cup f) \setminus f = g$.

Proof of Proposition 7.58.8. Proposition 7.58.4 **(c)** (applied to g and f instead of f and g) yields $g \subseteq g \cup f$ and $f \subseteq g \cup f$. Hence, $(g \cup f) \setminus f$ is well-defined. Moreover, for each $t \in T$, we have

$$(g \cup f)(t) = g(t) + f(t) \tag{379}$$

(by the definition of $g \cup f$). Hence, for each $t \in T$, we have

$$\begin{aligned}((g \cup f) \setminus f)(t) &= (g \cup f)(t) - f(t) \qquad \text{(by the definition of } (g \cup f) \setminus f\text{)} \\ &= g(t) \qquad \text{(by (379))}.\end{aligned}$$

In other words, $(g \cup f) \setminus f = g$ (since both $(g \cup f) \setminus f$ and g are maps from T to $\mathbb{N}$). This proves Proposition 7.58.8. □

Next, we define the *support* of a multisubset f of T:

Definition 7.58.9. Let T be a set. Let f be a multisubset of T. Then, we define $\operatorname{Supp} f$ to be the set $\{t \in T \mid f(t) \neq 0\}$. We call this set $\operatorname{Supp} f$ the *support* of f.

Thus, the support of a multisubset f of T is the set of all $t \in T$ that occur in f (with a positive multiplicity). Thus, intuitively speaking, the support of a multisubset f is obtained by turning f into a set (by forgetting the multiplicities). From this viewpoint, the following fact should be evident:

Proposition 7.58.10. Let T be a set. Let $k \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_k$ be any k elements of T (not necessarily distinct). Then,

$$\operatorname{Supp}\left(\{a_1, a_2, \ldots, a_k\}_{\text{multi}}\right) = \{a_1, a_2, \ldots, a_k\}.$$

Proof of Proposition 7.58.10. The definition of $\operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right)$ yields

$$\begin{aligned}&\operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right)\\&= \left\{t \in T \mid \left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(t) \neq 0\right\}.\end{aligned} \tag{380}$$

Now, let $u \in \operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right)$. We shall show that $u \in \left\{a_1, a_2, \ldots, a_k\right\}$.

We have $u \in \operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right) = \left\{t \in T \mid \left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(t) \neq 0\right\}$ (by (380)). In other words, u is a $t \in T$ satisfying $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(t) \neq 0$. In other words, $u \in T$ and $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(u) \neq 0$.

But recall how the map $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}$ was defined in Definition 7.57.1. This definition shows that

$$\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(u) = (\#\text{ of } i \in [k] \text{ satisfying } a_i = u).$$

Hence, $(\#\text{ of } i \in [k] \text{ satisfying } a_i = u) = \left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(u) \neq 0$. In other words, there exists at least one $i \in [k]$ satisfying $a_i = u$. Consider this i. Hence, $u = a_i \in \left\{a_1, a_2, \ldots, a_k\right\}$.

Forget that we fixed u. We thus have proved that $u \in \left\{a_1, a_2, \ldots, a_k\right\}$ for each $u \in \operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right)$. In other words,

$$\operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right) \subseteq \left\{a_1, a_2, \ldots, a_k\right\}. \tag{381}$$

Next, let $v \in \left\{a_1, a_2, \ldots, a_k\right\}$. We shall show that $v \in \operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right)$.

We have $v \in \left\{a_1, a_2, \ldots, a_k\right\}$. In other words, $v = a_j$ for some $j \in [k]$. Consider this j. We have $v = a_j \in T$ (since $a_1, a_2, \ldots, a_k$ are elements of T). Also, $v = a_j$, so that $a_j = v$. Hence, there exists at least one $i \in [k]$ satisfying $a_i = v$ (namely, $i = j$).

Recall how the map $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}$ was defined in Definition 7.57.1. This definition shows that

$$\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(v) = (\#\text{ of } i \in [k] \text{ satisfying } a_i = v) \geq 1$$

(since there exists at least one $i \in [k]$ satisfying $a_i = v$). Thus, $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(v) \geq 1 > 0$, so that $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(v) \neq 0$.

Now, we know that $v \in T$ and $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(v) \neq 0$. In other words, v is a $t \in T$ satisfying $\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(t) \neq 0$. In other words, $v \in \left\{t \in T \mid \left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}(t) \neq 0\right\}$. In view of (380), this rewrites as $v \in \operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right)$.

Forget that we fixed v. We thus have proved that $v \in \operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right)$ for each $v \in \left\{a_1, a_2, \ldots, a_k\right\}$. In other words,

$$\left\{a_1, a_2, \ldots, a_k\right\} \subseteq \operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right).$$

Combining this with (381), we obtain $\operatorname{Supp}\left(\left\{a_1, a_2, \ldots, a_k\right\}_{\text{multi}}\right) = \left\{a_1, a_2, \ldots, a_k\right\}$. This proves Proposition 7.58.10. □

Here are three more simple properties of supports:

Proposition 7.58.11. Let T be a set. Let f be a multisubset of T. Let $u \in \operatorname{Supp} f$. Then:
(a) We have $\{u\}_{\text{multi}} \subseteq f$.
(b) We have $|f \setminus \{u\}_{\text{multi}}| = |f| - 1$.

Proof of Proposition 7.58.11. We know that f is a multisubset of T, thus a map from T to $\mathbb{N}$.

(a) The definition of $\operatorname{Supp} f$ yields $\operatorname{Supp} f = \{t \in T \mid f(t) \neq 0\} = \{s \in T \mid f(s) \neq 0\}$ (here, we have renamed the index t as s).

Definition 7.57.1 (applied to 1 and the 1-tuple (u) instead of k and the k-tuple $(a_1, a_2, \ldots, a_k)$) tells us that $\{u\}_{\text{multi}}$ is defined as the map

$$\begin{aligned} & T \to \mathbb{N}, \\ & t \mapsto (\#\text{ of } i \in [1] \text{ satisfying } u = t). \end{aligned}$$

Hence,

$$\{u\}_{\text{multi}}(t) = (\#\text{ of } i \in [1] \text{ satisfying } u = t) \tag{382}$$

for each $t \in T$.

Let $t \in T$. We shall show that $\{u\}_{\text{multi}}(t) \leq f(t)$.

Indeed, assume the contrary. Thus, $\{u\}_{\text{multi}}(t) > f(t)$. But $f(t) \in \mathbb{N}$ (since f is a map from T to $\mathbb{N}$), hence $f(t) \geq 0$. Thus, $\{u\}_{\text{multi}}(t) > f(t) \geq 0$. In view of (382), this rewrites as $(\#\text{ of } i \in [1] \text{ satisfying } u = t) > 0$. In other words, there exists at least one $i \in [1]$ satisfying $u = t$. Thus, of course, we have $u = t$ (since the statement "$u = t$" does not depend on i). Hence, $t = u \in \operatorname{Supp} f = \{s \in T \mid f(s) \neq 0\}$. In other words, t is an $s \in T$ such that $f(s) \neq 0$. In other words, $t \in T$ and $f(t) \neq 0$. From $f(t) \neq 0$, we obtain $f(t) \geq 1$ (since $f(t) \in \mathbb{N}$). Hence, $\{u\}_{\text{multi}}(t) > f(t) \geq 1$.

But (382) becomes

$$\begin{aligned} \{u\}_{\text{multi}}(t) &= (\#\text{ of } i \in [1] \text{ satisfying } u = t) \\ &= (\#\text{ of } i \in [1]) \qquad \text{(since we know that } u = t) \\ &= |[1]| = 1. \end{aligned}$$

This contradicts $\{u\}_{\text{multi}}(t) > 1$. This contradiction shows that our assumption was wrong. Hence, $\{u\}_{\text{multi}}(t) \leq f(t)$ is proven.

Forget that we fixed t. We thus have showed that each $t \in T$ satisfies $\{u\}_{\text{multi}}(t) \leq f(t)$. This means that $\{u\}_{\text{multi}} \subseteq f$ (according to Definition 7.58.2). Thus, we have shown that $\{u\}_{\text{multi}} \subseteq f$. This proves Proposition 7.58.11 **(a)**.

(b) Exercise 2.11.1 (applied to 1 and the 1-tuple (u) instead of k and the k-tuple $(a_1, a_2, \ldots, a_k)$) yields that the multisubset $\{u\}_{\text{multi}}$ of T has size 1. In other words, $|\{u\}_{\text{multi}}| = 1$ (since the size of $\{u\}_{\text{multi}}$ is denoted by $|\{u\}_{\text{multi}}|$).

We have $\{u\}_{\text{multi}} \subseteq f$ (by Proposition 7.58.11 **(a)**). Thus, Proposition 7.58.7 **(b)** (applied to $\{u\}_{\text{multi}}$ and f instead of f and g) yields $(f \setminus \{u\}_{\text{multi}}) \cup \{u\}_{\text{multi}} = f$.

Hence, $f = (f \setminus \{u\}_{\text{multi}}) \cup \{u\}_{\text{multi}}$. Thus,

$$|f| = |(f \setminus \{u\}_{\text{multi}}) \cup \{u\}_{\text{multi}}| = |f \setminus \{u\}_{\text{multi}}| + \underbrace{|\{u\}_{\text{multi}}|}_{=1}$$

$$\left(\begin{array}{c} \text{by Proposition 7.58.4 \textbf{(b)},} \\ \text{applied to } f \setminus \{u\}_{\text{multi}} \text{ and } \{u\}_{\text{multi}} \text{ instead of } f \text{ and } g \end{array} \right)$$

$$= |f \setminus \{u\}_{\text{multi}}| + 1.$$

In other words, $|f \setminus \{u\}_{\text{multi}}| = |f| - 1$. This proves Proposition 7.58.11 **(b)**. □

Proposition 7.58.12. Let T be a set. Let f be a multisubset of T.
(a) The set $\operatorname{Supp} f$ is finite.
(b) We have $|f| = \sum_{t \in \operatorname{Supp} f} f(t)$.
(c) Assume that $|f| > 0$. Then, $\operatorname{Supp} f$ is a finite nonempty subset of T.

Proof of Proposition 7.58.12. We know that f is a multisubset of T. According to Definition 2.11.1 **(a)**, this means that only finitely many $t \in T$ satisfy $f(t) \neq 0$. Hence, we know that only finitely many $t \in T$ satisfy $f(t) \neq 0$. In other words, the set $\{t \in T \mid f(t) \neq 0\}$ is finite. Since $\operatorname{Supp} f = \{t \in T \mid f(t) \neq 0\}$ (by the definition of $\operatorname{Supp} f$), we can rewrite this as follows: The set $\operatorname{Supp} f$ is finite. This proves Proposition 7.58.12 **(a)**.

(b) From (372), we obtain

$$|f| = \sum_{t \in T} f(t) = \sum_{\substack{t \in T; \\ f(t)=0}} \underbrace{f(t)}_{=0} + \sum_{\substack{t \in T; \\ f(t) \neq 0}} f(t)$$

$$\left(\text{since each } t \in T \text{ satisfies either } f(t) = 0 \text{ or } f(t) \neq 0 \text{ (but not both)} \right)$$

$$= \underbrace{\sum_{\substack{t \in T; \\ f(t)=0}} 0}_{=0} + \sum_{\substack{t \in T; \\ f(t) \neq 0}} f(t) = \sum_{\substack{t \in T; \\ f(t) \neq 0}} f(t).$$

Comparing this with

$$\underbrace{\sum_{t \in \operatorname{Supp} f}}_{\substack{= \sum_{\substack{t \in T; \\ f(t) \neq 0}} \\ (\text{since } \operatorname{Supp} f = \{t \in T \mid f(t) \neq 0\})}} \qquad f(t) = \sum_{\substack{t \in T; \\ f(t) \neq 0}} f(t),$$

we obtain $|f| = \sum_{t \in \operatorname{Supp} f} f(t)$. Thus, Proposition 7.58.12 **(b)** is proved.

(c) Proposition 7.58.12 **(b)** yields $|f| = \sum_{t \in \operatorname{Supp} f} f(t)$, thus $\sum_{t \in \operatorname{Supp} f} f(t) = |f| > 0$. If we had $\operatorname{Supp} f = \varnothing$, then we would have

$$\sum_{t \in \operatorname{Supp} f} f(t) = \sum_{t \in \varnothing} f(t) = (\text{empty sum}) = 0,$$

which would contradict $\sum_{t \in \operatorname{Supp} f} f(t) > 0$. Thus, we cannot have $\operatorname{Supp} f = \varnothing$. Hence, $\operatorname{Supp} f \neq \varnothing$. In other words, $\operatorname{Supp} f$ is nonempty. Moreover, $\operatorname{Supp} f$ is finite (by Proposition 7.58.12 **(a)**). Finally, $\operatorname{Supp} f = \{t \in T \mid f(t) \neq 0\} \subseteq T$. Hence, $\operatorname{Supp} f$ is a subset of T. Altogether, this proves Proposition 7.58.12 **(c)**. □

Proposition 7.58.13. Let T be a set. Let f and g be two multisubsets of T such that $f \subseteq g$. Then, $\operatorname{Supp} f \subseteq \operatorname{Supp} g$.

Proof of Proposition 7.58.13. Let $u \in \operatorname{Supp} f$. We shall show that $u \in \operatorname{Supp} g$.

The definition of $\operatorname{Supp} f$ yields $\operatorname{Supp} f = \{t \in T \mid f(t) \neq 0\}$. The definition of $\operatorname{Supp} g$ yields $\operatorname{Supp} g = \{t \in T \mid g(t) \neq 0\}$.

Now, $u \in \operatorname{Supp} f = \{t \in T \mid f(t) \neq 0\}$; in other words, u is a $t \in T$ satisfying $f(t) \neq 0$. In other words, $u \in T$ and $f(u) \neq 0$. But f is a multisubset of T, thus a map from T to $\mathbb{N}$. Hence, $f(u) \in \mathbb{N}$. Thus, from $f(u) \neq 0$, we obtain $f(u) > 0$.

But $f \subseteq g$. In other words, each $t \in T$ satisfies $f(t) \leq g(t)$ (by Definition 7.58.2). Applying this to $t = u$, we obtain $f(u) \leq g(u)$. Hence, $g(u) \geq f(u) > 0$, so that $g(u) \neq 0$. Hence, u is a $t \in T$ satisfying $g(t) \neq 0$ (since $u \in T$). In other words, $u \in \{t \in T \mid g(t) \neq 0\}$. This rewrites as $u \in \operatorname{Supp} g$ (since $\operatorname{Supp} g = \{t \in T \mid g(t) \neq 0\}$).

Forget that we fixed u. We thus have proved that $u \in \operatorname{Supp} g$ for each $u \in \operatorname{Supp} f$. In other words, $\operatorname{Supp} f \subseteq \operatorname{Supp} g$. This proves Proposition 7.58.13. □

Next, let us introduce a word for the kind of tuple whose existence (and uniqueness) is claimed in Proposition 2.11.5:

Definition 7.58.14. Let T be a set of integers. Let f be a multisubset of T. An *increasing list* of f shall mean a tuple $(s_1, s_2, \ldots, s_k)$ of elements of T such that $f = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_k$.

Our goal is thus to prove the following:

Proposition 7.58.15. Let T be a set of integers. Let f be a multisubset of T. Then, f has exactly one increasing list.

We shall prove this by induction on the size of this multisubset; the induction base will rely on the following simple fact (an analogue of [Grinbe15, Proposition 2.48]):

Proposition 7.58.16. Let T be a set. Let f be a multisubset of T such that $|f| = 0$. Then:

(a) We have $f = \{\}_{\text{multi}}$.

(b) Now, assume that T is a set of integers. Then, the multisubset f has exactly one increasing list: namely, the empty list $()$.

Of course, the multisubset $\{\}_{\text{multi}}$ is a multiset analogue of the empty set $\varnothing$.

Proof of Proposition 7.58.16. This is an essentially trivial argument that takes long to explain due to the notational awkwardness of working with the empty multisubset and the empty list. So here we go:

From (372), we obtain $|f| = \sum_{t \in T} f(t)$. Hence, $\sum_{t \in T} f(t) = |f| = 0$.

But f is a multisubset of T, thus a map from T to $\mathbb{N}$. Hence, each $t \in T$ satisfies $f(t) \in \mathbb{N}$. Therefore, all addends of the sum $\sum_{t \in T} f(t)$ are nonnegative integers. Thus, $\sum_{t \in T} f(t)$ is a sum of nonnegative integers. But this sum equals 0 (since $\sum_{t \in T} f(t) = 0$).

If a sum of nonnegative integers equals 0, then all its addends must be 0 (since otherwise, the sum would be positive rather than 0). We can apply this to the sum $\sum_{t \in T} f(t)$ (because $\sum_{t \in T} f(t)$ is a sum of nonnegative integers and equals 0). Thus, we conclude that all addends of this sum must be 0. In other words,

$$f(t) = 0 \qquad \text{for each } t \in T. \tag{383}$$

Let us denote the 0-tuple $()$ by $(a_1, a_2, \ldots, a_0)$. Thus, $(a_1, a_2, \ldots, a_0) = ()$, so that $\{a_1, a_2, \ldots, a_0\}_{\text{multi}} = \{\}_{\text{multi}}$.

Definition 7.57.1 (applied to 0 and the 0-tuple $(a_1, a_2, \ldots, a_0)$ instead of k and the k-tuple $(a_1, a_2, \ldots, a_k)$) tells us that $\{a_1, a_2, \ldots, a_0\}_{\text{multi}}$ is defined as the map

$$\begin{aligned} &T \to \mathbb{N}, \\ &t \mapsto (\#\text{ of } i \in [0] \text{ satisfying } a_i = t). \end{aligned}$$

[302] Hence, for each $t \in T$, we have

$$\{a_1, a_2, \ldots, a_0\}_{\text{multi}}(t) = (\#\text{ of } i \in [0] \text{ satisfying } a_i = t) = 0 \tag{384}$$

(since there exist no $i \in [0]$ satisfying $a_i = t$ (because $[0]$ is an empty set)).

Now, for each $t \in T$, we have

$$\begin{aligned} f(t) &= 0 \qquad \text{(by (383))} \\ &= \underbrace{\{a_1, a_2, \ldots, a_0\}_{\text{multi}}}_{=\{\}_{\text{multi}}}(t) \qquad \text{(by (384))} \\ &= \{\}_{\text{multi}}(t). \end{aligned}$$

In other words, $f = \{\}_{\text{multi}}$ (since both f and $\{\}_{\text{multi}}$ are maps from T to $\mathbb{N}$). This proves Proposition 7.58.16 **(a)**.

(b) The empty list $()$ satisfies $f = \{\}_{\text{multi}}$ (as we have just proved). Thus, the empty list $()$ is a tuple $(s_1, s_2, \ldots, s_k)$ of elements of T such that $f = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_k$ (indeed, the chain of inequalities $s_1 \leq s_2 \leq \cdots \leq s_k$ is vacuously true for the empty list $()$, because it contains no inequality signs). In other

[302] Being able to write down this map is the reason why we denoted the 0-tuple $()$ by $(a_1, a_2, \ldots, a_0)$.

words, the empty list $()$ is an increasing list of f (by the definition of an increasing list). It remains to show that it is the only increasing list of f.

Let $(s_1, s_2, \ldots, s_k)$ be any increasing list of f. Thus, $(s_1, s_2, \ldots, s_k)$ is a tuple of elements of T such that $f = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_k$ (by the definition of an increasing list). But Exercise 2.11.1 (applied to $a_i = s_i$) yields that the multisubset $\{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ of T has size k. In other words, the multisubset f of T has size k (since $f = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$). In other words, $|f| = k$ (since the size of f is denoted by $|f|$). Thus, $k = |f| = 0$. Hence, $(s_1, s_2, \ldots, s_k) = (s_1, s_2, \ldots, s_0) = ()$.

Now, forget that we fixed $(s_1, s_2, \ldots, s_k)$. We thus have shown that if $(s_1, s_2, \ldots, s_k)$ is any increasing list of f, then $(s_1, s_2, \ldots, s_k) = ()$. In other words, any increasing list of f is $()$. Therefore, the multisubset f has exactly one increasing list: namely, the empty list $()$ (since we already know that $()$ is an increasing list of f). This proves Proposition 7.58.16 **(b)**. □

The induction step of our proof of Proposition 7.58.15 will rely on the following fact (an analogue of [Grinbe15, Proposition 2.49]):

Proposition 7.58.17. Let T be a set of integers. Let f be a multisubset of T such that $|f| > 0$. Let m be the largest element of $\operatorname{Supp} f$. Let $(s_1, s_2, \ldots, s_k)$ be an increasing list of f. Then:

(a) We have $k \geq 1$ and $s_k = m$.

(b) We have $\{m\}_{\text{multi}} \subseteq f$.

(c) The list $(s_1, s_2, \ldots, s_{k-1})$ is an increasing list of the multisubset $f \setminus \{m\}_{\text{multi}}$ of T.

Proof of Proposition 7.58.17. We know that $(s_1, s_2, \ldots, s_k)$ is an increasing list of f. In other words, $(s_1, s_2, \ldots, s_k)$ is a list of elements of T such that $f = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_k$ (by the definition of an "increasing list").

Exercise 2.11.1 (applied to $a_i = s_i$) yields that the multisubset $\{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ of T has size k. In other words, the multisubset f of T has size k (since $f = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$). In other words, $|f| = k$ (since the size of f is denoted by $|f|$). Hence, $k = |f| > 0$. Thus, $k \geq 1$ (since k is an integer). Therefore, s_k is well-defined. Clearly, $k \in [k]$ (since $k \geq 1$).

Proposition 7.58.10 (applied to $a_i = s_i$) yields
$\operatorname{Supp}\left(\{s_1, s_2, \ldots, s_k\}_{\text{multi}}\right) = \{s_1, s_2, \ldots, s_k\}$. Thus,

$$\begin{aligned} \operatorname{Supp} \underbrace{f}_{=\{s_1, s_2, \ldots, s_k\}_{\text{multi}}} &= \operatorname{Supp}\left(\{s_1, s_2, \ldots, s_k\}_{\text{multi}}\right) \\ &= \{s_1, s_2, \ldots, s_k\}. \end{aligned} \tag{385}$$

We have $s_1 \leq s_2 \leq \cdots \leq s_k$. Hence, the largest element of $\{s_1, s_2, \ldots, s_k\}$ is s_k. In view of (385), this rewrites as follows: The largest element of $\operatorname{Supp} f$ is s_k. In other words, m is s_k (since m is the largest element of $\operatorname{Supp} f$). In other words, $m = s_k$. Hence, $s_k = m$. This completes the proof of Proposition 7.58.17 **(a)**.

(b) We have $m = s_k \in \{s_1, s_2, \ldots, s_k\} = \operatorname{Supp} f$ (by (385)). Hence, Proposition 7.58.11 **(a)** (applied to $u = m$) yields $\{m\}_{\text{multi}} \subseteq f$. This proves Proposition 7.58.17 **(b)**.

(c) From $s_1 \leq s_2 \leq \cdots \leq s_k$, we obtain $s_1 \leq s_2 \leq \cdots \leq s_{k-1}$.

Furthermore, $k-1 \in \mathbb{N}$ (since $k \geq 1$). Hence, Proposition 7.58.5 (applied to $k-1$ and 1 and the $(k-1)$-tuple $(s_1, s_2, \ldots, s_{k-1})$ and the 1-tuple (s_k) instead of k and ℓ and the k-tuple $(a_1, a_2, \ldots, a_k)$ and the ℓ-tuple $(b_1, b_2, \ldots, b_\ell)$) yields

$$\{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}} \cup \{s_k\}_{\text{multi}} = \{s_1, s_2, \ldots, s_{k-1}, s_k\}_{\text{multi}} = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}.$$

Now, Proposition 7.58.8 (applied to $\{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}}$ and $\{s_k\}_{\text{multi}}$ instead of g and f) yields

$$(\{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}} \cup \{s_k\}_{\text{multi}}) \setminus \{s_k\}_{\text{multi}} = \{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}}.$$

Hence,

$$\begin{aligned}\{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}} &= \underbrace{(\{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}} \cup \{s_k\}_{\text{multi}})}_{\substack{=\{s_1,s_2,\ldots,s_k\}_{\text{multi}}=f \\ (\text{since } f=\{s_1,s_2,\ldots,s_k\}_{\text{multi}})}} \setminus \left\{ \underbrace{s_k}_{=m} \right\}_{\text{multi}} \\ &= f \setminus \{m\}_{\text{multi}}.\end{aligned}$$

Thus, $f \setminus \{m\}_{\text{multi}} = \{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}}$.

Now, we know that $(s_1, s_2, \ldots, s_{k-1})$ is a list of elements of T such that $f \setminus \{m\}_{\text{multi}} = \{s_1, s_2, \ldots, s_{k-1}\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_{k-1}$. In other words, $(s_1, s_2, \ldots, s_{k-1})$ is an increasing list of $f \setminus \{m\}_{\text{multi}}$ (by the definition of an "increasing list"). This proves Proposition 7.58.17 **(c)**. □

We are now ready to prove Proposition 7.58.15:

Proof of Proposition 7.58.15. We shall prove Proposition 7.58.15 by induction on $|f|$:

Induction base: Proposition 7.58.15 holds under the condition that $|f| = 0$ [303]. This completes the induction base.

Induction step: Let $g \in \mathbb{N}$. Assume that Proposition 7.58.15 holds under the condition that $|f| = g$. We shall now show that Proposition 7.58.15 holds under the condition that $|f| = g + 1$.

We have assumed that Proposition 7.58.15 holds under the condition that $|f| = g$. In other words,

$$\left(\begin{array}{c} \text{if } f \text{ is a multisubset of } T \text{ satisfying } |f| = g, \\ \text{then } f \text{ has exactly one increasing list} \end{array} \right). \tag{386}$$

[303] *Proof.* Let f be as in Proposition 7.58.15, and assume that $|f| = 0$. We must show that the claim of Proposition 7.58.15 holds.

Indeed, Proposition 7.58.16 **(b)** shows that the multisubset f has exactly one increasing list. Thus, the claim of Proposition 7.58.15 holds. This completes our proof.

Now, let f be a multisubset of T satisfying $|f| = g+1$. We want to prove that f has exactly one increasing list.

We have $|f| = g+1 > g \geq 0$. Hence, Proposition 7.58.12 **(c)** shows that $\operatorname{Supp} f$ is a finite nonempty subset of T. Hence, $\operatorname{Supp} f$ is a finite nonempty set of integers (since T is a set of integers). Thus, $\operatorname{Supp} f$ has a largest element (since any finite nonempty set of integers has a largest element). Let m be this largest element.

Thus, m is the largest element of $\operatorname{Supp} f$. Hence, in particular, m is an element of $\operatorname{Supp} f$, so that we have $m \in \operatorname{Supp} f$. Hence, Proposition 7.58.11 **(a)** (applied to $u = m$) yields $\{m\}_{\text{multi}} \subseteq f$. Also, Proposition 7.58.11 **(b)** (applied to $u = m$) yields $|f \setminus \{m\}_{\text{multi}}| = |f| - 1 = g$ (since $|f| = g+1$). Hence, (386) (applied to $f \setminus \{m\}_{\text{multi}}$ instead of f) shows that $f \setminus \{m\}_{\text{multi}}$ has exactly one increasing list. Let $(t_1, t_2, \ldots, t_j)$ be this list. We extend this list to a $(j+1)$-tuple $(t_1, t_2, \ldots, t_{j+1})$ by setting $t_{j+1} = m$. Thus, $t_{j+1} = m \in \operatorname{Supp} f \subseteq T$ (since $\operatorname{Supp} f$ is a subset of T).

Recall that $\{m\}_{\text{multi}} \subseteq f$. Hence, Proposition 7.58.7 **(c)** (applied to $\{m\}_{\text{multi}}$ and f instead of f and g) yields $f \setminus \{m\}_{\text{multi}} \subseteq f$. Therefore, Proposition 7.58.13 (applied to $f \setminus \{m\}_{\text{multi}}$ and f instead of f and g) yields $\operatorname{Supp}\left(f \setminus \{m\}_{\text{multi}}\right) \subseteq \operatorname{Supp} f$.

We have defined $(t_1, t_2, \ldots, t_j)$ as an increasing list of the multisubset $f \setminus \{m\}_{\text{multi}}$. In other words, $(t_1, t_2, \ldots, t_j)$ is a tuple of elements of T such that $f \setminus \{m\}_{\text{multi}} = \{t_1, t_2, \ldots, t_j\}_{\text{multi}}$ and $t_1 \leq t_2 \leq \cdots \leq t_j$ (by the definition of an "increasing list"). Thus, $t_1, t_2, \ldots, t_j$ are elements of T (since $(t_1, t_2, \ldots, t_j)$ is a tuple of elements of T).

Proposition 7.58.10 (applied to j and the j-tuple $(t_1, t_2, \ldots, t_j)$ instead of k and the k-tuple $(a_1, a_2, \ldots, a_k)$) yields

$$\operatorname{Supp}\left(\{t_1, t_2, \ldots, t_j\}_{\text{multi}}\right) = \{t_1, t_2, \ldots, t_j\}.$$

In view of $f \setminus \{m\}_{\text{multi}} = \{t_1, t_2, \ldots, t_j\}_{\text{multi}}$, this rewrites as

$$\operatorname{Supp}\left(f \setminus \{m\}_{\text{multi}}\right) = \{t_1, t_2, \ldots, t_j\}.$$

Hence,

$$\{t_1, t_2, \ldots, t_j\} = \operatorname{Supp}\left(f \setminus \{m\}_{\text{multi}}\right) \subseteq \operatorname{Supp} f.$$

We claim that

$$t_1 \leq t_2 \leq \cdots \leq t_{j+1}. \tag{387}$$

[*Proof of (387):* If $j+1 \leq 1$, then the chain of inequalities (387) is vacuously true (since it contains no inequality signs). Thus, for the rest of this proof of (387), we WLOG assume that we don't have $j+1 \leq 1$. Hence, $j+1 > 1$, so that $j > 0$ and thus $j \geq 1$ (since j is an integer). Hence, t_j is well-defined. We have $j \geq 1$ and thus $j \in [j]$. Hence, $t_j \in \{t_1, t_2, \ldots, t_j\} \subseteq \operatorname{Supp} f$.

But m is the largest element of $\operatorname{Supp} f$. Hence, $m \geq x$ for each $x \in \operatorname{Supp} f$. Applying this to $x = t_j$, we obtain $m \geq t_j$ (since $t_j \in \operatorname{Supp} f$). Thus, $t_j \leq m = t_{j+1}$ (since $t_{j+1} = m$). Combining the chain of inequalities $t_1 \leq t_2 \leq \cdots \leq t_j$ with the single inequality $t_j \leq t_{j+1}$, we obtain the longer chain of inequalities $t_1 \leq t_2 \leq \cdots \leq t_j \leq t_{j+1}$. In other words, $t_1 \leq t_2 \leq \cdots \leq t_{j+1}$. This proves (387).]

Next, we shall prove that

$$f = \left\{t_1, t_2, \ldots, t_{j+1}\right\}_{\text{multi}}. \tag{388}$$

[*Proof of (388):* We have $\{m\}_{\text{multi}} \subseteq f$ and thus $(f \setminus \{m\}_{\text{multi}}) \cup \{m\}_{\text{multi}} = f$ (by Proposition 7.58.7 **(b)**, applied to $\{m\}_{\text{multi}}$ and f instead of f and g). Thus,

$$f = \left(\underbrace{f \setminus \{m\}_{\text{multi}}}_{=\left\{t_1, t_2, \ldots, t_j\right\}_{\text{multi}}}\right) \cup \left\{\underbrace{m}_{=t_{j+1}}\right\}_{\text{multi}} = \left\{t_1, t_2, \ldots, t_j\right\}_{\text{multi}} \cup \left\{t_{j+1}\right\}_{\text{multi}}$$

$$= \left\{t_1, t_2, \ldots, t_j, t_{j+1}\right\}_{\text{multi}}$$

$$\left(\begin{array}{c}\text{by Proposition 7.58.5, applied to the numbers } j \text{ and } 1 \text{ and} \\ \text{the } j\text{-tuple } \left(t_1, t_2, \ldots, t_j\right) \text{ and the 1-tuple } \left(t_{j+1}\right) \text{ instead of the numbers } k \\ \text{and } \ell \text{ and the } k\text{-tuple } \left(a_1, a_2, \ldots, a_k\right) \text{ and the } \ell\text{-tuple } \left(b_1, b_2, \ldots, b_\ell\right)\end{array}\right)$$

$$= \left\{t_1, t_2, \ldots, t_{j+1}\right\}_{\text{multi}}.$$

This proves (388).]

Clearly, $t_1, t_2, \ldots, t_{j+1}$ are elements of the set T (since $t_1, t_2, \ldots, t_j$ are elements of T, and since $t_{j+1} \in T$). Hence, $\left(t_1, t_2, \ldots, t_{j+1}\right)$ is a tuple of elements of T.

Thus, $\left(t_1, t_2, \ldots, t_{j+1}\right)$ is a tuple of elements of T such that $f = \left\{t_1, t_2, \ldots, t_{j+1}\right\}_{\text{multi}}$ (by (388)) and $t_1 \leq t_2 \leq \cdots \leq t_{j+1}$ (by (387)). In other words, $\left(t_1, t_2, \ldots, t_{j+1}\right)$ is an increasing list of f (by the definition of an "increasing list"). Hence, the multisubset f has **at least** one increasing list (namely, $\left(t_1, t_2, \ldots, t_{j+1}\right)$).

We shall next show that $\left(t_1, t_2, \ldots, t_{j+1}\right)$ is the only increasing list of f. Indeed, let $(s_1, s_2, \ldots, s_k)$ be any increasing list of f. Then, Proposition 7.58.17 **(a)** shows that $k \geq 1$ and $s_k = m$. Also, Proposition 7.58.17 **(c)** shows that the list $(s_1, s_2, \ldots, s_{k-1})$ is an increasing list of the multisubset $f \setminus \{m\}_{\text{multi}}$ of T.

But recall that $f \setminus \{m\}_{\text{multi}}$ has exactly one increasing list. Thus, in particular, $f \setminus \{m\}_{\text{multi}}$ has **at most** one increasing list. In other words, any two increasing lists of $f \setminus \{m\}_{\text{multi}}$ are equal. Hence, the lists $(s_1, s_2, \ldots, s_{k-1})$ and $\left(t_1, t_2, \ldots, t_j\right)$ must be equal (since both of these lists are increasing lists of $f \setminus \{m\}_{\text{multi}}$). In other words, $(s_1, s_2, \ldots, s_{k-1}) = \left(t_1, t_2, \ldots, t_j\right)$. In other words, $k - 1 = j$ and

$$\left(s_i = t_i \text{ for each } i \in \{1, 2, \ldots, k-1\}\right). \tag{389}$$

From $k - 1 = j$, we obtain $k = j + 1$. Hence, $t_k = t_{j+1} = m$. Next, we claim that

$$s_i = t_i \text{ for each } i \in \{1, 2, \ldots, k\}. \tag{390}$$

[*Proof of (390):* Let $i \in \{1, 2, \ldots, k\}$. We must prove that $s_i = t_i$. If $i \in \{1, 2, \ldots, k-1\}$, then this follows from (389). Hence, for the rest of this proof, we WLOG assume that we don't have $i \in \{1, 2, \ldots, k-1\}$. Hence, $i \notin \{1, 2, \ldots, k-1\}$. Combining $i \in \{1, 2, \ldots, k\}$ with $i \notin \{1, 2, \ldots, k-1\}$, we obtain

$$i \in \{1, 2, \ldots, k\} \setminus \{1, 2, \ldots, k-1\} = \{k\}.$$

In other words, $i = k$. Hence, $s_i = s_k = m = t_k$ (since $t_k = m$). In view of $k = i$, this rewrites as $s_i = t_i$. This proves (390).]

From (390), we obtain $(s_1, s_2, \ldots, s_k) = (t_1, t_2, \ldots, t_k) = \left(t_1, t_2, \ldots, t_{j+1}\right)$ (since $k = j + 1$).

Now, forget that we fixed $(s_1, s_2, \ldots, s_k)$. We thus have proven that if $(s_1, s_2, \ldots, s_k)$ is any increasing list of f, then $(s_1, s_2, \ldots, s_k) = \left(t_1, t_2, \ldots, t_{j+1}\right)$. In other words, any increasing list of f equals $\left(t_1, t_2, \ldots, t_{j+1}\right)$. Thus, the multisubset f has **at most** one increasing list. Since we also know that the multisubset f has **at least** one increasing list, we thus conclude that f has exactly one increasing list.

Now, forget that we fixed f. We thus have shown that

$$\left(\begin{array}{c}\text{if } f \text{ is a multisubset of } T \text{ satisfying } |f| = g+1, \\ \text{then } f \text{ has exactly one increasing list}\end{array}\right).$$

In other words, Proposition 7.58.15 holds under the condition that $|f| = g + 1$. This completes the induction step. Hence, Proposition 7.58.15 is proven by induction. □

It is now easy to prove the two propositions that Exercise 2.11.2 wants us to prove:

Proof of Proposition 2.11.5. Proposition 7.58.15 (applied to $f = S$) shows that S has exactly one increasing list. In other words, there exists exactly one increasing list of S. In other words, there exists a unique increasing list of S. In other words, there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of elements of T such that $S = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_k$ (because an increasing list of S is defined to be a tuple $(s_1, s_2, \ldots, s_k)$ of elements of T such that $S = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_k$). In other words, there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers in T satisfying $S = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$ and $s_1 \leq s_2 \leq \cdots \leq s_k$ (because elements of T are the same as integers in T). In other words, there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers in T satisfying $\{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_k$ (because "$S = \{s_1, s_2, \ldots, s_k\}_{\text{multi}}$" is equivalent to "$\{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S$"). This proves Proposition 2.11.5. □

Now, Proposition 2.11.6 can be derived from Proposition 2.11.5 in the same way as Proposition 1.4.13 was derived from Proposition 1.4.11 (in the solution to Exercise 1.4.2):

Proof of Proposition 2.11.6. Proposition 2.11.5 yields that there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers in T satisfying $\{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_k$. Consider this tuple, and denote it by $\left(t_1, t_2, \ldots, t_p\right)$. Thus, $\left(t_1, t_2, \ldots, t_p\right)$ is the unique tuple of integers in T satisfying $\left\{t_1, t_2, \ldots, t_p\right\}_{\text{multi}} = S$ and $t_1 \leq t_2 \leq \cdots \leq t_p$.

Exercise 2.11.1 (applied to p and t_i instead of k and a_i) yields that the multisubset $\left\{t_1, t_2, \ldots, t_p\right\}_{\text{multi}}$ of T has size p. In other words, the multisubset S of T has size p (since $\left\{t_1, t_2, \ldots, t_p\right\}_{\text{multi}} = S$). This rewrites as $|S| = p$ (since the size of S is

denoted by $|S|$). But we know that S has size m; in other words, we have $|S| = m$ (since the size of S is denoted by $|S|$). Comparing this with $|S| = p$, we obtain $p = m$.

Recall that the tuple $(t_1, t_2, \ldots, t_p)$ is a p-tuple of integers in T satisfying $\{t_1, t_2, \ldots, t_p\}_{\text{multi}} = S$ and $t_1 \leq t_2 \leq \cdots \leq t_p$. In view of $p = m$, we can rewrite this as follows: The tuple $(t_1, t_2, \ldots, t_m)$ is an m-tuple of integers in T satisfying $\{t_1, t_2, \ldots, t_m\}_{\text{multi}} = S$ and $t_1 \leq t_2 \leq \cdots \leq t_m$. Hence, there exists **at least one** m-tuple $(s_1, s_2, \ldots, s_m)$ of integers in T satisfying $\{s_1, s_2, \ldots, s_m\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_m$ (namely, the m-tuple $(t_1, t_2, \ldots, t_m)$). Furthermore, there exists **at most one** such m-tuple $(s_1, s_2, \ldots, s_m)$ [304]. Combining the claims of the preceding two sentences, we conclude that there exists a **unique** m-tuple $(s_1, s_2, \ldots, s_m)$ of integers in T satisfying $\{s_1, s_2, \ldots, s_m\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_m$. This proves Proposition 2.11.6. □

Thus, Proposition 2.11.5 and Proposition 2.11.6 are proven, so that Exercise 2.11.2 is solved.

7.59. Solution to Exercise 2.12.1

In order to solve Exercise 2.12.1, we need to prove Proposition 2.12.4.

Proof of Proposition 2.12.4. By assumption, we have $n_1 + n_2 + \cdots + n_k = n$, so that $n = n_1 + n_2 + \cdots + n_k$.

For each $i \in [k+1]$, we define a nonnegative integer $s_i \in \mathbb{N}$ by $s_i = n_i + n_{i+1} + \cdots + n_k$. Thus, in particular, $s_1 = n_1 + n_2 + \cdots + n_k = n$ and $s_{k+1} = n_{k+1} + n_{k+2} + \cdots + n_k = (\text{empty sum}) = 0$.

For each $i \in [k+1]$, we have

$$\begin{aligned} \underbrace{n}_{=n_1+n_2+\cdots+n_k} - n_1 - n_2 - \cdots - n_{i-1} &= (n_1 + n_2 + \cdots + n_k) - n_1 - n_2 - \cdots - n_{i-1} \\ &= n_i + n_{i+1} + \cdots + n_k = s_i \end{aligned} \tag{391}$$

(since s_i is defined by $s_i = n_i + n_{i+1} + \cdots + n_k$).

(a) It is easy to see that Proposition 2.12.4 **(a)** holds if $k = 0$ [305]. Hence, for the rest of this proof, we WLOG assume that $k \neq 0$. Hence, $k \geq 1$.

We shall now show two simple observations:

[304] *Proof.* Recall that $(t_1, t_2, \ldots, t_p)$ is the **unique** tuple $(s_1, s_2, \ldots, s_k)$ of integers in T satisfying $\{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_k$. Hence, if $(s_1, s_2, \ldots, s_k)$ is any tuple of integers in T satisfying $\{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_k$, then $(s_1, s_2, \ldots, s_k)$ must equal $(t_1, t_2, \ldots, t_p)$. Applying this to $k = m$, we conclude that if $(s_1, s_2, \ldots, s_m)$ is any m-tuple of integers in T satisfying $\{s_1, s_2, \ldots, s_m\}_{\text{multi}} = S$ and $s_1 \leq s_2 \leq \cdots \leq s_m$, then $(s_1, s_2, \ldots, s_m)$ must equal $(t_1, t_2, \ldots, t_p)$. Thus, there exists **at most one** such m-tuple $(s_1, s_2, \ldots, s_m)$.

[305] *Proof.* Assume that $k = 0$. Then,

$$\begin{aligned} n &= n_1 + n_2 + \cdots + n_k = (\text{empty sum}) \qquad (\text{since } k = 0) \\ &= 0. \end{aligned}$$

Observation 1: We have $\dbinom{n-n_1-n_2-\cdots-n_{i-1}}{n_i} = \dfrac{s_i!}{n_i! \cdot s_{i+1}!}$ for each $i \in [k]$.

[*Proof of Observation 1:* Let $i \in [k]$. Then, the definition of s_{i+1} yields $s_{i+1} = n_{i+1} + n_{i+2} + \cdots + n_k$. But the definition of s_i yields

$$s_i = n_i + n_{i+1} + \cdots + n_k = n_i + \underbrace{\left(n_{i+1} + n_{i+2} + \cdots + n_k\right)}_{=s_{i+1}} = n_i + s_{i+1}.$$

Hence, $s_i - n_i = s_{i+1} \geq 0$ (since $s_{i+1} \in \mathbb{N}$), so that $n_i \leq s_i$. Thus, Proposition 1.3.9 (applied to s_i and n_i instead of n and k) yields

$$\binom{s_i}{n_i} = \frac{s_i!}{n_i! \cdot (s_i - n_i)!} = \frac{s_i!}{n_i! \cdot s_{i+1}!} \qquad \left(\text{since } s_i - n_i = s_{i+1}\right).$$

But (391) yields $n - n_1 - n_2 - \cdots - n_{i-1} = s_i$. Thus,

$$\binom{n-n_1-n_2-\cdots-n_{i-1}}{n_i} = \binom{s_i}{n_i} = \frac{s_i!}{n_i! \cdot s_{i+1}!}.$$

This proves Observation 1.]

Thus, the definition of $\dbinom{n}{n_1, n_2, \ldots, n_k}$ yields

$$\begin{aligned}
\binom{n}{n_1, n_2, \ldots, n_k} &= \frac{n!}{n_1! n_2! \cdots n_k!} = \frac{1}{n_1! n_2! \cdots n_0!} \\
&\qquad \left(\text{since } \underbrace{n}_{=0}! = 0! = 1 \text{ and } k = 0\right) \\
&= \frac{1}{1} \qquad (\text{since } n_1! n_2! \cdots n_0! = (\text{empty product}) = 1) \\
&= 1.
\end{aligned}$$

Moreover, the products

$$\prod_{i=1}^{k} \binom{n-n_1-n_2-\cdots-n_{i-1}}{n_i},$$

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\underbrace{\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}}_{=1},$$

$$\prod_{i=1}^{k-1} \binom{n-n_1-n_2-\cdots-n_{i-1}}{n_i}$$

are all empty products (since $k = 0$) and thus equal 1 as well. Hence, the claim of Proposition 2.12.4 **(a)** boils down to $1 = 1 = 1 = 1$, which is obvious. Thus, Proposition 2.12.4 **(a)** is proved under the assumption that $k = 0$.

Observation 2: We have $\dbinom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = 1$.

[*Proof of Observation 2:* We have $k \in [k]$ (since $k \geq 1$). From $n = n_1+n_2+\cdots+n_k$, we obtain

$$\underbrace{n}_{=n_1+n_2+\cdots+n_k} - n_1 - n_2 - \cdots - n_{k-1} = (n_1+n_2+\cdots+n_k) - n_1 - n_2 - \cdots - n_{k-1} = n_k.$$

Hence, $\dbinom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \dbinom{n_k}{n_k} = 1$ (by Exercise 1.3.2, applied to n_k instead of n). This proves Observation 2.]

Now,

$$\prod_{i=1}^{k} \underbrace{\binom{n-n_1-n_2-\cdots-n_{i-1}}{n_i}}_{= \frac{s_i!}{n_i! \cdot s_{i+1}!} \text{ (by Observation 1)}}$$

$$= \prod_{i=1}^{k} \frac{s_i!}{n_i! \cdot s_{i+1}!} = \frac{\prod_{i=1}^{k} s_i!}{\left(\prod_{i=1}^{k} n_i!\right) \cdot \left(\prod_{i=1}^{k} s_{i+1}!\right)}$$

$$= \frac{s_1! \cdot (s_2! s_3! \cdots s_k!)}{(n_1! n_2! \cdots n_k!) \cdot (s_2! s_3! \cdots s_k!) \cdot s_{k+1}!}$$

$$\left(\begin{array}{c} \text{since } \prod_{i=1}^{k} s_i! = s_1! s_2! \cdots s_k! = s_1! \cdot (s_2! s_3! \cdots s_k!) \\ \text{and } \prod_{i=1}^{k} n_i! = n_1! n_2! \cdots n_k! \\ \text{and } \prod_{i=1}^{k} s_{i+1}! = s_2! s_3! \cdots s_{k+1}! = (s_2! s_3! \cdots s_k!) \cdot s_{k+1}! \end{array} \right)$$

$$= \frac{s_1!}{(n_1! n_2! \cdots n_k!) \cdot s_{k+1}!} = \frac{n!}{(n_1! n_2! \cdots n_k!) \cdot 1} \qquad \left(\text{since } s_1 = n \text{ and } \underbrace{s_{k+1}}_{=0}! = 0! = 1 \right)$$

$$= \frac{n!}{n_1! n_2! \cdots n_k!}. \tag{392}$$

But the definition of $\binom{n}{n_1, n_2, \ldots, n_k}$ yields

$$\begin{aligned}
\binom{n}{n_1, n_2, \ldots, n_k} &= \frac{n!}{n_1! n_2! \cdots n_k!} \\
&= \prod_{i=1}^{k} \binom{n - n_1 - n_2 - \cdots - n_{i-1}}{n_i} \qquad \text{(by (392))} \\
&= \binom{n}{n_1} \binom{n - n_1}{n_2} \binom{n - n_1 - n_2}{n_3} \cdots \binom{n - n_1 - n_2 - \cdots - n_{k-1}}{n_k} \\
&= \binom{n}{n_1} \binom{n - n_1}{n_2} \binom{n - n_1 - n_2}{n_3} \cdots \binom{n - n_1 - n_2 - \cdots - n_{k-2}}{n_{k-1}} \\
&\qquad \cdot \underbrace{\binom{n - n_1 - n_2 - \cdots - n_{k-1}}{n_k}}_{\substack{=1 \\ \text{(by Observation 2)}}} \\
&\qquad \text{(here, we have split off the last factor from our product)} \\
&= \binom{n}{n_1} \binom{n - n_1}{n_2} \binom{n - n_1 - n_2}{n_3} \cdots \binom{n - n_1 - n_2 - \cdots - n_{k-2}}{n_{k-1}} \\
&= \prod_{i=1}^{k-1} \binom{n - n_1 - n_2 - \cdots - n_{i-1}}{n_i}.
\end{aligned}$$

Thus, Proposition 2.12.4 **(a)** is proved.

(b) Proposition 2.12.4 **(a)** yields

$$\binom{n}{n_1, n_2, \ldots, n_k} = \prod_{i=1}^{k} \underbrace{\binom{n - n_1 - n_2 - \cdots - n_{i-1}}{n_i}}_{\substack{= \binom{s_i}{n_i} \\ \text{(since (391) yields } n - n_1 - n_2 - \cdots - n_{i-1} = s_i\text{)}}} = \prod_{i=1}^{k} \underbrace{\binom{s_i}{n_i}}_{\substack{\in \mathbb{N} \\ \text{(by Lemma 1.3.17,} \\ \text{applied to } s_i \text{ and } n_i \\ \text{instead of } n \text{ and } k\text{)}}} \in \mathbb{N}$$

(since any product of elements of $\mathbb{N}$ must itself belong to $\mathbb{N}$). This proves Proposition 2.12.4 **(b)**. [306] □

7.60. Solution to Exercise 2.12.2

In order to solve Exercise 2.12.2, we first introduce a convenient notation:

Definition 7.60.1. Let A be a set. Let $k \in \mathbb{N}$. Let $n_1, n_2, \ldots, n_k \in \mathbb{N}$. A map $f : A \to [k]$ is said to be $(n_1, n_2, \ldots, n_k)$-*fine* if it satisfies

$$(\#\text{ of } a \in A \text{ such that } f(a) = i) = n_i \qquad \text{for each } i \in [k]. \tag{393}$$

[306] This proof of Proposition 2.12.4 **(b)** is essentially taken from [Grinbe15, solution to Exercise 3.1].

Example 7.60.2. The map $f : \{2,5,6,9,10\} \to [2]$ that sends $2,6,9$ to 1 and sends $5,10$ to 2 is $(3,2)$-fine, since it satisfies

$$(\#\text{ of } a \in \{2,5,6,9,10\} \text{ such that } f(a) = 1) = |\{2,6,9\}| = 3 \qquad \text{and}$$
$$(\#\text{ of } a \in \{2,5,6,9,10\} \text{ such that } f(a) = 2) = |\{5,10\}| = 2.$$

We can now (slightly) generalize Proposition 2.12.5 as follows:

Proposition 7.60.3. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n$. Let A be a set such that $|A| = n$. Then, the # of $(n_1, n_2, \ldots, n_k)$-fine maps $f : A \to [k]$ is $\dbinom{n}{n_1, n_2, \ldots, n_k}$.

Proposition 2.12.5 is the particular case of Proposition 7.60.3 when $A = [n]$.

We shall now prove Proposition 7.60.3.

Proof of Proposition 7.60.3. We shall prove Proposition 7.60.3 by induction on k.

Induction base: It is easy to see that Proposition 7.60.3 holds when $k = 0$ [307]. This completes the induction base.

Induction step: Let m be a positive integer. Assume that Proposition 7.60.3 holds when $k = m - 1$. We must prove that Proposition 7.60.3 holds when $k = m$.

[307] *Proof.* Consider the situation of Proposition 7.60.3, and assume that $k = 0$. We must show that Proposition 7.60.3 holds.

Definition 2.12.1 yields

$$\begin{aligned}\binom{n}{n_1, n_2, \ldots, n_k} &= \frac{n!}{n_1! n_2! \cdots n_k!} = \frac{0!}{n_1! n_2! \cdots n_0!} \qquad (\text{since } k = 0 \text{ and } n = 0) \\ &= \frac{0!}{1} \qquad (\text{since } n_1! n_2! \cdots n_0! = (\text{empty product}) = 1) \\ &= 0! = 1.\end{aligned}$$

We have

$$\begin{aligned}|A| = n &= n_1 + n_2 + \cdots + n_k = n_1 + n_2 + \cdots + n_0 \qquad (\text{since } k = 0) \\ &= (\text{empty sum}) = 0.\end{aligned}$$

Hence, $A = \varnothing$. Also, $k = 0$ and thus $[k] = [0] = \varnothing$. Thus, there exists no $i \in [k]$.

Both sets A and $[k]$ are empty (since $A = \varnothing$ and $[k] = \varnothing$). Hence, there exists exactly one map $f : A \to [k]$ (namely, the map that sends nothing to nothing). This map f satisfies (393) (since (393) is a vacuously true statement (because there exists no $i \in [k]$)), and thus is $(n_1, n_2, \ldots, n_k)$-fine (by the definition of "$(n_1, n_2, \ldots, n_k)$-fine"). Thus, there exists exactly one $(n_1, n_2, \ldots, n_k)$-fine map $f : A \to [k]$ (namely, the map we just found). In other words, the # of $(n_1, n_2, \ldots, n_k)$-fine maps $f : A \to [k]$ is 1. In view of $\dbinom{n}{n_1, n_2, \ldots, n_k} = 1$, we can rewrite this as follows: The # of $(n_1, n_2, \ldots, n_k)$-fine maps $f : A \to [k]$ is $\dbinom{n}{n_1, n_2, \ldots, n_k}$. Hence, Proposition 7.60.3 is proved (under the assumption that $k = 0$). Thus, Proposition 7.60.3 holds when $k = 0$.

Note that $m \in [m]$ (since m is positive).

We have assumed that Proposition 7.60.3 holds when $k = m - 1$. In other words, the following statement holds:

> *Statement 1:* Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_{m-1} \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_{m-1} = n$. Let A be a set such that $|A| = n$. Then, the # of $(n_1, n_2, \ldots, n_{m-1})$-fine maps $f : A \to [m-1]$ is $\dbinom{n}{n_1, n_2, \ldots, n_{m-1}}$.

We must prove that Proposition 7.60.3 holds when $k = m$. In other words, we must prove the following statement:

> *Statement 2:* Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_m \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_m = n$. Let A be a set such that $|A| = n$. Then, the # of $(n_1, n_2, \ldots, n_m)$-fine maps $f : A \to [m]$ is $\dbinom{n}{n_1, n_2, \ldots, n_m}$.

[*Proof of Statement 2:* The following proof is rather similar to the 1st approach to counting $\operatorname{sur}(m, n)$ in Subsection 2.4.5.

From $n_1 + n_2 + \cdots + n_m = n$, we obtain

$$n = n_1 + n_2 + \cdots + n_m = (n_1 + n_2 + \cdots + n_{m-1}) + n_m.$$

Thus, $n - n_m = n_1 + n_2 + \cdots + n_{m-1} \in \mathbb{N}$ (since $n_1, n_2, \ldots, n_{m-1} \in \mathbb{N}$). Hence, $n - n_m \geq 0$, so that $n_m \leq n$. Thus, Theorem 1.3.9 (applied to $k = n_m$) yields

$$\binom{n}{n_m} = \frac{n!}{n_m! \cdot (n - n_m)!}. \tag{394}$$

But A is an n-element set (since $|A| = n$). Hence, Theorem 1.3.12 (applied to $k = n_m$ and $S = A$) yields

$$\begin{aligned}\binom{n}{n_m} &= (\text{\# of } n_m\text{-element subsets of } A) \\ &= (\text{\# of subsets } J \text{ of } A \text{ satisfying } |J| = n_m).\end{aligned}$$

Comparing this with (394), we obtain

$$(\text{\# of subsets } J \text{ of } A \text{ satisfying } |J| = n_m) = \frac{n!}{n_m! \cdot (n - n_m)!}. \tag{395}$$

Given a map $f : A \to [m]$, we let J_f be the set of all $a \in A$ such that $f(a) = m$. [308] Clearly, this set J_f is a subset of A. Moreover, if $f : A \to [m]$ is an $(n_1, n_2, \ldots, n_m)$-fine map, then this subset J_f of A satisfies $\left|J_f\right| = n_m$ [309]. Hence, the sum rule

[308] For example, if $A = \{2, 5, 6, 9, 13\}$ and $m = 2$, and if $f : A \to [m]$ is the map written in two-line notation as $\begin{pmatrix} 2 & 5 & 6 & 9 & 13 \\ 2 & 1 & 2 & 2 & 1 \end{pmatrix}$, then $J_f = \{2, 6, 9\}$, because $2, 6, 9$ are precisely the $a \in A$ such that $f(a) = 2$.

[309] *Proof.* Let $f : A \to [m]$ be an $(n_1, n_2, \ldots, n_m)$-fine map. Thus, we have

$$(\text{\# of } a \in A \text{ such that } f(a) = i) = n_i \qquad \text{for each } i \in [m]$$

yields

$$\begin{aligned}&(\#\text{ of all } (n_1,n_2,\ldots,n_m)\text{-fine maps } f: A\to[m])\\&=\sum_{\substack{J\subseteq A;\\ |J|=n_m}}\left(\#\text{ of all } (n_1,n_2,\ldots,n_m)\text{-fine maps } f: A\to[m] \text{ satisfying } J_f=J\right).\end{aligned} \tag{396}$$

Now, fix a subset J of A that satisfies $|J|=n_m$. What is the # of all $(n_1,n_2,\ldots,n_m)$-fine maps $f: A\to[m]$ satisfying $J_f=J$? Such a map f must satisfy

$$J=J_f=\{a\in A \mid f(a)=m\} \qquad \left(\text{by the definition of } J_f\right).$$

In other words, such a map f must send all elements of J, but no other elements, to m. In other words, it must send all elements of J to m, and send all other elements of A to numbers different from m. The latter numbers are, of course, the elements of $[m]\setminus\{m\}=[m-1]$. Thus, an $(n_1,n_2,\ldots,n_m)$-fine map $f: A\to[m]$ satisfying $J_f=J$ must send all elements of J to m, and send all elements of $A\setminus J$ to elements of $[m-1]$. Hence, if f is such a map, then f is uniquely determined by its values at the elements of $A\setminus J$, and said values must belong to $[m-1]$. In other words, if f is such a map, then f is uniquely determined by its restriction $f\mid_{A\setminus J}$, and furthermore this restriction must "actually" be a map from $A\setminus J$ to $[m-1]$, in the sense that all its values belong to $[m-1]$. Moreover, in order for the map f to be $(n_1,n_2,\ldots,n_m)$-fine, its restriction $f\mid_{A\setminus J}$ (regarded as a map from $A\setminus J$ to $[m-1]$) must be $(n_1,n_2,\ldots,n_{m-1})$-fine[310]. This is actually a necessary

(by the definition of "$(n_1,n_2,\ldots,n_m)$-fine"). We can apply this to $i=m$ (since $m\in[m]$), and thus obtain

$$(\#\text{ of } a\in A \text{ such that } f(a)=m)=n_m.$$

But J_f was defined as the set of all $a\in A$ such that $f(a)=m$. Hence,

$$\left|J_f\right|=(\#\text{ of } a\in A \text{ such that } f(a)=m)=n_m.$$

Qed.

[310] *Proof.* Let $f: A\to[m]$ be a map satisfying $J_f=J$. We must prove that the map f is $(n_1,n_2,\ldots,n_m)$-fine if and only if its restriction $f\mid_{A\setminus J}$ (regarded as a map from $A\setminus J$ to $[m-1]$) is $(n_1,n_2,\ldots,n_{m-1})$-fine.

For each $i\in[m]$, we let $\mathcal{A}_i$ be the logical statement "(# of $a\in A$ such that $f(a)=i)=n_i$". Recall that $J_f=J$, so that

$$J=J_f=\{a\in A \mid f(a)=m\} \qquad \left(\text{by the definition of } J_f\right).$$

Hence, $|J|=|\{a\in A \mid f(a)=m\}|=(\#\text{ of } a\in A \text{ such that } f(a)=m)$. Therefore,

$$(\#\text{ of } a\in A \text{ such that } f(a)=m)=|J|=n_m.$$

In other words, the statement $\mathcal{A}_m$ holds (since $\mathcal{A}_m$ was defined to be the logical statement "(# of $a\in A$ such that $f(a)=m)=n_m$"). In logical notation, this rewrites as follows: $\mathcal{A}_m\iff(\text{true})$.

and sufficient condition; i.e., if $f : A \to [m]$ is a map satisfying $J_f = J$, and if its restriction $f\mid_{A\setminus J}$ (regarded as a map from $A \setminus J$ to $[m-1]$) is $(n_1, n_2, \ldots, n_{m-1})$-fine,

---

Now, let $i \in [m-1]$. Then, $i \leq m-1 < m$, so that $i \neq m$. But $J = \{a \in A \mid f(a) = m\}$. Hence,

$$\text{each } a \in J \text{ satisfies } f(a) = m. \tag{397}$$

Hence, if there was an element $a \in A$ satisfying both $f(a) = i$ and $a \in J$ at the same time, then this element would satisfy $f(a) = m$ (by (397)), which would contradict $f(a) = i \neq m$. Thus, there is no such element a. In other words, there exists no $a \in A$ such that $f(a) = i$ and $a \in J$. In other words,

$$(\#\text{ of } a \in A \text{ such that } f(a) = i \text{ and } a \in J) = 0.$$

But each $a \in A$ satisfies either $a \in J$ or $a \notin J$ (but not both at the same time). Hence, the sum rule yields

$$\begin{aligned}
&(\#\text{ of } a \in A \text{ such that } f(a) = i) \\
&= \underbrace{(\#\text{ of } a \in A \text{ such that } f(a) = i \text{ and } a \in J)}_{=0} + (\#\text{ of } a \in A \text{ such that } f(a) = i \text{ and } a \notin J) \\
&= (\#\text{ of } a \in A \text{ such that } f(a) = i \text{ and } a \notin J) \\
&= (\#\text{ of } a \in A \text{ such that } a \notin J \text{ and } f(a) = i) \\
&= (\#\text{ of } a \in A \setminus J \text{ such that } f(a) = i)
\end{aligned}$$

(since the $a \in A$ satisfying $a \notin J$ are precisely the elements of $A \setminus J$).

Now, forget that we fixed i. We thus have proved that

$$\begin{aligned}
&(\#\text{ of } a \in A \text{ such that } f(a) = i) \\
&= (\#\text{ of } a \in A \setminus J \text{ such that } f(a) = i)
\end{aligned} \tag{398}$$

for each $i \in [m-1]$.

We have the following chain of logical equivalences:

$$\begin{aligned}
&\left(f\mid_{A\setminus J} \text{ (regarded as a map from } A \setminus J \text{ to } [m-1]\text{) is } (n_1, n_2, \ldots, n_{m-1})\text{-fine}\right) \\
&\iff \left(\left(\#\text{ of } a \in A \setminus J \text{ such that } \underbrace{\left(f\mid_{A\setminus J}\right)(a)}_{=f(a)} = i\right) = n_i \text{ for each } i \in [m-1]\right) \\
&\qquad \left(\text{by the definition of "}(n_1, n_2, \ldots, n_{m-1})\text{-fine"}\right) \\
&\iff \left(\underbrace{(\#\text{ of } a \in A \setminus J \text{ such that } f(a) = i)}_{=(\#\text{ of } a\in A \text{ such that } f(a)=i) \text{ (by (398))}} = n_i \text{ for each } i \in [m-1]\right) \\
&\iff \left(\underbrace{(\#\text{ of } a \in A \text{ such that } f(a) = i) = n_i}_{\iff (\mathcal{A}_i \text{ holds})} \qquad \text{for each } i \in [m-1]\right) \\
&\qquad \left(\text{since } \mathcal{A}_i \text{ is the logical statement "}(\#\text{ of } a\in A \text{ such that } f(a)=i)=n_i\text{"}\right) \\
&\iff (\mathcal{A}_i \text{ holds for each } i \in [m-1]) \\
&\iff (\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}).
\end{aligned} \tag{399}$$

then the map f itself must be $(n_1, n_2, \ldots, n_m)$-fine[311]. Thus, in order to construct an $(n_1, n_2, \ldots, n_m)$-fine map $f : A \to [m]$ satisfying $J_f = J$, we need to construct an $(n_1, n_2, \ldots, n_{m-1})$-fine map $f : A \setminus J \to [m-1]$. Hence,

$$\begin{aligned} &\left(\#\text{ of all } (n_1, n_2, \ldots, n_m)\text{-fine maps } f : A \to [m] \text{ satisfying } J_f = J\right) \\ &= \left(\#\text{ of all } (n_1, n_2, \ldots, n_{m-1})\text{-fine maps } f : A \setminus J \to [m-1]\right). \end{aligned} \tag{400}$$

(Formally speaking, this can be proved using the bijection principle[312].)

On the other hand, $J \subseteq A$, and thus an application of Theorem 1.4.7 **(a)** yields $|A \setminus J| = \underbrace{|A|}_{=n} - \underbrace{|J|}_{=n_m} = n - n_m \in \mathbb{N}$. Also, recall that $n - n_m = n_1 + n_2 + \cdots + n_{m-1}$, so that $n_1 + n_2 + \cdots + n_{m-1} = n - n_m$. Hence, Statement 1 (applied to $n - n_m$ and $A \setminus J$ instead of n and A) yields that the # of $(n_1, n_2, \ldots, n_{m-1})$-fine maps

---

On the other hand, we have the following chain of logical equivalences:

$$\begin{aligned} &(f \text{ is } (n_1, n_2, \ldots, n_m)\text{-fine}) \\ &\iff \left(\underbrace{(\#\text{ of } a \in A \text{ such that } f(a) = i) = n_i}_{\substack{\iff (\mathcal{A}_i \text{ holds}) \\ (\text{since } \mathcal{A}_i \text{ is the logical statement ``}(\#\text{ of } a \in A \text{ such that } f(a)=i)=n_i\text{''})}} \qquad \text{for each } i \in [m] \right) \\ &\qquad (\text{by the definition of ``}(n_1, n_2, \ldots, n_m)\text{-fine''}) \\ &\iff (\mathcal{A}_i \text{ holds for each } i \in [m]) \\ &\iff (\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_m) \\ &\iff \left((\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}) \wedge \underbrace{\mathcal{A}_m}_{\iff (\text{true})} \right) \\ &\iff ((\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}) \wedge (\text{true})) \\ &\iff (\mathcal{A}_1 \wedge \mathcal{A}_2 \wedge \cdots \wedge \mathcal{A}_{m-1}) \\ &\iff \left(f \mid_{A \setminus J} \text{ (regarded as a map from } A \setminus J \text{ to } [m-1]) \text{ is } (n_1, n_2, \ldots, n_{m-1})\text{-fine} \right) \end{aligned}$$

(by (399)). In other words, the map f is $(n_1, n_2, \ldots, n_m)$-fine if and only if its restriction $f \mid_{A \setminus J}$ (regarded as a map from $A \setminus J$ to $[m-1]$) is $(n_1, n_2, \ldots, n_{m-1})$-fine. Qed.

[311] This was proven in the previous footnote.

[312] More precisely, we need to apply the bijection principle to the bijection

$$\begin{aligned} &\left\{(n_1, n_2, \ldots, n_m)\text{-fine maps } f : A \to [m] \text{ satisfying } J_f = J\right\} \\ &\to \{(n_1, n_2, \ldots, n_{m-1})\text{-fine maps } f : A \setminus J \to [m-1]\} \end{aligned}$$

that sends each f to its restriction $f \mid_{A \setminus J}$ (considered as a map from $A \setminus J$ to $[m-1]$).

Here, of course, we are using the fact that if an $(n_1, n_2, \ldots, n_m)$-fine map $f : A \to [m]$ satisfies $J_f = J$, then the restriction $f \mid_{A \setminus J}$ can be considered as a map from $A \setminus J$ to $[m-1]$, since it does not take the value m.

$f : A \setminus J \to [m-1]$ is $\binom{n-n_m}{n_1, n_2, \ldots, n_{m-1}}$. In other words,

$$\begin{aligned}&(\#\text{ of all } (n_1, n_2, \ldots, n_{m-1})\text{-fine maps } f : A \setminus J \to [m-1])\\ &= \binom{n-n_m}{n_1, n_2, \ldots, n_{m-1}} = \frac{(n-n_m)!}{n_1! n_2! \cdots n_{m-1}!}\end{aligned}$$

(by the definition of $\binom{n-n_m}{n_1, n_2, \ldots, n_{m-1}}$). Thus, (400) becomes

$$\begin{aligned}&\left(\#\text{ of all } (n_1, n_2, \ldots, n_m)\text{-fine maps } f : A \to [m] \text{ satisfying } J_f = J\right)\\ &= (\#\text{ of all } (n_1, n_2, \ldots, n_{m-1})\text{-fine maps } f : A \setminus J \to [m-1])\\ &= \frac{(n-n_m)!}{n_1! n_2! \cdots n_{m-1}!}. \qquad (401)\end{aligned}$$

Now, forget that we fixed J. We thus have proved (401) for each subset J of A satisfying $|J| = n_m$. Hence, (396) becomes

$$\begin{aligned}&(\#\text{ of all } (n_1, n_2, \ldots, n_m)\text{-fine maps } f : A \to [m])\\ &= \sum_{\substack{J \subseteq A;\\ |J| = n_m}} \underbrace{\left(\#\text{ of all } (n_1, n_2, \ldots, n_m)\text{-fine maps } f : A \to [m] \text{ satisfying } J_f = J\right)}_{\substack{= \frac{(n-n_m)!}{n_1! n_2! \cdots n_{m-1}!} \\ \text{(by (401))}}}\\ &= \sum_{\substack{J \subseteq A;\\ |J| = n_m}} \frac{(n-n_m)!}{n_1! n_2! \cdots n_{m-1}!} = \underbrace{(\#\text{ of subsets } J \text{ of } A \text{ satisfying } |J| = n_m)}_{\substack{= \frac{n!}{n_m! \cdot (n-n_m)!} \\ \text{(by (395))}}} \frac{(n-n_m)!}{n_1! n_2! \cdots n_{m-1}!}\\ &= \frac{n!}{n_m! \cdot (n-n_m)!} \cdot \frac{(n-n_m)!}{n_1! n_2! \cdots n_{m-1}!} = \frac{n!}{n_m! \cdot (n_1! n_2! \cdots n_{m-1}!)} = \frac{n!}{n_1! n_2! \cdots n_m!}\\ &\qquad (\text{since } n_m! \cdot (n_1! n_2! \cdots n_{m-1}!) = (n_1! n_2! \cdots n_{m-1}!) \cdot n_m! = n_1! n_2! \cdots n_m!)\\ &= \binom{n}{n_1, n_2, \ldots, n_m}\end{aligned}$$

(since $\binom{n}{n_1, n_2, \ldots, n_m}$ was defined to be $\frac{n!}{n_1! n_2! \cdots n_m!}$). In other words, the # of $(n_1, n_2, \ldots, n_m)$-fine maps $f : A \to [m]$ is $\binom{n}{n_1, n_2, \ldots, n_m}$. This proves Statement 2.]

Now, Statement 2 is proven. In other words, Proposition 7.60.3 holds when $k = m$. This completes the induction step. Thus, Proposition 7.60.3 is proved. □

Proof of Proposition 2.12.5. We have $|[n]| = n$. Hence, Proposition 7.60.3 (applied to $A = [n]$) yields that the # of $(n_1, n_2, \ldots, n_k)$-fine maps $f : [n] \to [k]$ is $\binom{n}{n_1, n_2, \ldots, n_k}$.

In other words, the # of maps $f : [n] \to [k]$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } f(a) = i) = n_i \qquad \text{for each } i \in [k] \tag{402}$$

is $\binom{n}{n_1, n_2, \ldots, n_k}$ (because the $(n_1, n_2, \ldots, n_k)$-fine maps $f : [n] \to [k]$ are precisely the maps $f : [n] \to [k]$ satisfying (402)[313]). This proves Proposition 2.12.5. □

Thus, Exercise 2.12.2 is solved.

7.61. Solution to Exercise 2.12.3

Solution to Exercise 2.12.3. Write the n-tuple $\alpha \in X^n$ in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Thus,

$$(\#\text{ of times } i \text{ appears in } \alpha) = (\#\text{ of } a \in [n] \text{ such that } \alpha_a = i). \tag{403}$$

We have assumed that β is an anagram of the n-tuple α. Thus, β is an n-tuple that can be obtained from α by permuting its entries (by the definition of an "anagram"). In other words, β is an n-tuple of the form $\left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}\right)$, where σ is a permutation of $[n]$. Consider this σ.

Thus, $\beta = \left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}\right)$. Thus,

$$(\#\text{ of times } i \text{ appears in } \beta) = \left(\#\text{ of } b \in [n] \text{ such that } \alpha_{\sigma(b)} = i\right). \tag{404}$$

But σ is a permutation of $[n]$. In other words, σ is a bijection from $[n]$ to $[n]$ (by the definition of a permutation). Hence, its inverse map $\sigma^{-1} : [n] \to [n]$ is well-defined.

If $a \in [n]$ satisfies $\alpha_a = i$, then the element $\sigma^{-1}(a)$ is a $b \in [n]$ such that $\alpha_{\sigma(b)} = i$ [314]. Hence, the map

$$f : \{a \in [n] \mid \alpha_a = i\} \to \left\{b \in [n] \mid \alpha_{\sigma(b)} = i\right\},$$
$$a \mapsto \sigma^{-1}(a)$$

is well-defined. Consider this map f.

[313] by the definition of "$(n_1, n_2, \ldots, n_k)$-fine"

[314] *Proof.* Let $a \in [n]$ satisfy $\alpha_a = i$. We must prove that the element $\sigma^{-1}(a)$ is a $b \in [n]$ such that $\alpha_{\sigma(b)} = i$.

Clearly, $\sigma^{-1}(a) \in [n]$. Also, $\sigma\left(\sigma^{-1}(a)\right) = a$, so that $\alpha_{\sigma\left(\sigma^{-1}(a)\right)} = \alpha_a = i$. Thus, $\sigma^{-1}(a)$ is a $b \in [n]$ such that $\alpha_{\sigma(b)} = i$ (since $\sigma^{-1}(a) \in [n]$ and $\alpha_{\sigma\left(\sigma^{-1}(a)\right)} = i$). Qed.

If $b \in [n]$ satisfies $\alpha_{\sigma(b)} = i$, then the element $\sigma(b)$ is an $a \in [n]$ such that $\alpha_a = i$ [315]. Hence, the map

$$g : \left\{ b \in [n] \mid \alpha_{\sigma(b)} = i \right\} \to \{ a \in [n] \mid \alpha_a = i \}, \\ b \mapsto \sigma(b)$$

is well-defined. Consider this map g.

It is easy to see that $f \circ g = \mathrm{id}$ [316]. Similarly, $g \circ f = \mathrm{id}$. Combining $f \circ g = \mathrm{id}$ with $g \circ f = \mathrm{id}$, we conclude that the maps f and g are mutually inverse. Hence, the map $f : \{ a \in [n] \mid \alpha_a = i \} \to \left\{ b \in [n] \mid \alpha_{\sigma(b)} = i \right\}$ is invertible, i.e., is bijective. Thus, the bijection principle yields

$$\left| \{ a \in [n] \mid \alpha_a = i \} \right| = \left| \left\{ b \in [n] \mid \alpha_{\sigma(b)} = i \right\} \right|.$$

Now, (403) yields

$$\begin{aligned} (\#\text{ of times } i \text{ appears in } \alpha) &= (\#\text{ of } a \in [n] \text{ such that } \alpha_a = i) \\ &= \left| \{ a \in [n] \mid \alpha_a = i \} \right| = \left| \left\{ b \in [n] \mid \alpha_{\sigma(b)} = i \right\} \right| \\ &= \left(\#\text{ of } b \in [n] \text{ such that } \alpha_{\sigma(b)} = i \right) \\ &= (\#\text{ of times } i \text{ appears in } \beta) \qquad \text{(by (404))}. \end{aligned}$$

In other words, (# of times i appears in β) = (# of times i appears in α). This solves Exercise 2.12.3. □

7.62. Solution to Exercise 2.12.4

Instead of solving Exercise 2.12.4 directly, we shall first prove a more general statement (stated in the more flexible language of maps instead of tuples):

Theorem 7.62.1. Let A and B be two finite sets. Let X be any set. Let $f : A \to X$ and $g : B \to X$ be two maps. Assume that

$$(\#\text{ of } a \in A \text{ such that } f(a) = i) \\ = (\#\text{ of } b \in B \text{ such that } g(b) = i) \tag{405}$$

[315] *Proof.* Let $b \in [n]$ satisfy $\alpha_{\sigma(b)} = i$. We must prove that the element $\sigma(b)$ is an $a \in [n]$ such that $\alpha_a = i$. In other words, we must prove that $\sigma(b) \in [n]$ and $\alpha_{\sigma(b)} = i$. But this is obvious. Qed.

[316] *Proof.* Let $c \in \left\{ b \in [n] \mid \alpha_{\sigma(b)} = i \right\}$. We shall show that $(f \circ g)(c) = \mathrm{id}(c)$.

Indeed, the definition of g yields $g(c) = \sigma(c)$. But $(f \circ g)(c) = f(g(c)) = \sigma^{-1}(g(c))$ (by the definition of f). Thus, $(f \circ g)(c) = \sigma^{-1}\left(\underbrace{g(c)}_{=\sigma(c)} \right) = \sigma^{-1}(\sigma(c)) = c = \mathrm{id}(c)$.

Forget that we fixed c. We thus have shown that $(f \circ g)(c) = \mathrm{id}(c)$ for each $c \in \left\{ b \in [n] \mid \alpha_{\sigma(b)} = i \right\}$. In other words, $f \circ g = \mathrm{id}$.

for each $i \in X$. Then, there exists a bijection $\sigma : A \to B$ such that $f = g \circ \sigma$.

Proof of Theorem 7.62.1. The set A is finite; i.e., there are only finitely many $a \in A$. Likewise, there are only finitely many $b \in B$.

Let Y be the subset $\{f(a) \mid a \in A\}$ of X. Then, Y is finite (since there are only finitely many $a \in A$).

Let Z be the subset $\{g(b) \mid b \in B\}$ of X. Then, Z is finite (since there are only finitely many $b \in B$).

Let W be the union $Y \cup Z$. This set W is a finite set (since it is the union of the two finite sets Y and Z) and is a subset of X (since Y and Z are subsets of X).

It is easy to see that

$$f(c) \in W \qquad \text{for each } c \in A \tag{406}$$

[317]. Likewise,

$$g(d) \in W \qquad \text{for each } d \in B. \tag{407}$$

Let $i \in W$. We shall construct a bijection from the set $\{a \in A \mid f(a) = i\}$ to the set $\{b \in B \mid g(b) = i\}$.

Indeed, $i \in W \subseteq X$. Also, we have

$$\begin{aligned} |\{a \in A \mid f(a) = i\}| &= (\#\text{ of } a \in A \text{ such that } f(a) = i) \\ &= (\#\text{ of } b \in B \text{ such that } g(b) = i) \qquad \text{(by (405))} \\ &= |\{b \in B \mid g(b) = i\}|. \end{aligned}$$

In other words, $\{a \in A \mid f(a) = i\}$ and $\{b \in B \mid g(b) = i\}$ are two sets of the same size. Thus, Theorem 1.1.7 (applied to $\{a \in A \mid f(a) = i\}$ and $\{b \in B \mid g(b) = i\}$ instead of X and Y) yields that there exists a bijection from $\{a \in A \mid f(a) = i\}$ to $\{b \in B \mid g(b) = i\}$. Choose such a bijection, and denote it by h_i.

Forget that we fixed i. Thus, for each $i \in W$, we have found

$$\text{a bijection } h_i \text{ from } \{a \in A \mid f(a) = i\} \text{ to } \{b \in B \mid g(b) = i\}.$$

[318]

We shall now "glue" these bijections h_i together to a single bijection $u : A \to B$ which will satisfy $f = g \circ u$. Here is how this is done in detail:

[317] *Proof.* Let $c \in A$. We have $Y = \{f(a) \mid a \in A\}$ (by the definition of Y). But from $c \in A$, we obtain $f(c) \in \{f(a) \mid a \in A\} = Y \subseteq Y \cup Z = W$ (since W was defined to be $Y \cup Z$). This proves (406).

[318] If you are aware of the Axiom of Choice, you might wonder whether we have used it here. The answer is "no, not really". We have made a choice (namely, choosing a bijection h_i) for each $i \in W$. This amounts to finitely many choices (since W is a finite set). But you can make finitely many choices without invoking the Axiom of Choice (indeed, this can easily be proved by induction on the number of choices). Thus, we are not using the Axiom of Choice here.

For each $c \in A$, the element $h_{f(c)}(c) \in B$ is well-defined[319]. Hence, we can define a map

$$u : A \to B,$$
$$c \mapsto h_{f(c)}(c).$$

For each $d \in B$, the element $\left(h_{g(d)}\right)^{-1}(d) \in A$ is well-defined[320]. Hence, we can define a map

$$v : B \to A,$$
$$d \mapsto \left(h_{g(d)}\right)^{-1}(d).$$

We have $u \circ v = \mathrm{id}$ [321] and $v \circ u = \mathrm{id}$ [322]. Thus, the maps u and v are mutually inverse. Hence, the map $u : A \to B$ is invertible, i.e., bijective. In other

[319] *Proof.* Let $c \in A$. Let $i = f(c)$. Then, c is an $a \in A$ satisfying $f(a) = i$ (since $c \in A$ and $f(c) = i$). In other words, $c \in \{a \in A \mid f(a) = i\}$.

But $i = f(c) \in W$ (by (406)). Hence, h_i is a bijection from $\{a \in A \mid f(a) = i\}$ to $\{b \in B \mid g(b) = i\}$ (by the definition of h_i). Therefore, $h_i(c)$ is a well-defined element of $\{b \in B \mid g(b) = i\}$ (since $c \in \{a \in A \mid f(a) = i\}$). Thus, $h_i(c) \in \{b \in B \mid g(b) = i\} \subseteq B$. In view of $i = f(c)$, this rewrites as $h_{f(c)}(c) \in B$. Thus, the element $h_{f(c)}(c) \in B$ is well-defined. Qed.

[320] *Proof.* Let $d \in B$. Let $i = g(d)$. Then, d is a $b \in B$ satisfying $g(b) = i$ (since $d \in B$ and $g(d) = i$). In other words, $d \in \{b \in B \mid g(b) = i\}$.

But $i = g(d) \in W$ (by (407)). Hence, h_i is a bijection from $\{a \in A \mid f(a) = i\}$ to $\{b \in B \mid g(b) = i\}$ (by the definition of h_i). Thus, the inverse map $(h_i)^{-1}$ is a bijection from $\{b \in B \mid g(b) = i\}$ to $\{a \in A \mid f(a) = i\}$. Therefore, $(h_i)^{-1}(d)$ is a well-defined element of $\{a \in A \mid f(a) = i\}$ (since $d \in \{b \in B \mid g(b) = i\}$). Thus, $(h_i)^{-1}(d) \in \{a \in A \mid f(a) = i\} \subseteq A$. In view of $i = g(d)$, this rewrites as $\left(h_{g(d)}\right)^{-1}(d) \in A$. Thus, the element $\left(h_{g(d)}\right)^{-1}(d) \in A$ is well-defined. Qed.

[321] *Proof.* Let $d \in B$. Let $i = g(d)$. Then, d is a $b \in B$ satisfying $g(b) = i$ (since $d \in B$ and $g(d) = i$). In other words, $d \in \{b \in B \mid g(b) = i\}$.

But $i = g(d) \in W$ (by (407)). Hence, h_i is a bijection from $\{a \in A \mid f(a) = i\}$ to $\{b \in B \mid g(b) = i\}$ (by the definition of h_i). Thus, the inverse map $(h_i)^{-1}$ is a bijection from $\{b \in B \mid g(b) = i\}$ to $\{a \in A \mid f(a) = i\}$. Therefore, $(h_i)^{-1}(d)$ is a well-defined element of $\{a \in A \mid f(a) = i\}$ (since $d \in \{b \in B \mid g(b) = i\}$). Thus, $(h_i)^{-1}(d) \in \{a \in A \mid f(a) = i\}$.

But the definition of v yields $v(d) = \left(h_{g(d)}\right)^{-1}(d) = (h_i)^{-1}(d)$ (since $g(d) = i$). Hence, $h_i(v(d)) = d$.

Also, $v(d) = (h_i)^{-1}(d) \in \{a \in A \mid f(a) = i\}$. In other words, $v(d)$ is an $a \in A$ satisfying $f(a) = i$. In other words, $v(d) \in A$ and $f(v(d)) = i$. Now,

$$\begin{aligned}(u \circ v)(d) &= u(v(d)) = h_{f(v(d))}(v(d)) \qquad \text{(by the definition of } u\text{)} \\ &= h_i(v(d)) \qquad \text{(since } f(v(d)) = i\text{)} \\ &= d = \mathrm{id}(d).\end{aligned}$$

Forget that we fixed d. We thus have proved that $(u \circ v)(d) = \mathrm{id}(d)$ for each $d \in B$. In other words, $u \circ v = \mathrm{id}$.

[322] *Proof.* Let $c \in A$. Let $i = f(c)$. Then, c is an $a \in A$ satisfying $f(a) = i$ (since $c \in A$ and $f(c) = i$).

words, $u : A \to B$ is a bijection. Moreover, we have $f = g \circ u$ [323]. Hence, there exists a bijection $\sigma : A \to B$ such that $f = g \circ \sigma$ (namely, $\sigma = u$). This proves Theorem 7.62.1. $\square$

Exercise 2.12.4 now easily follows:

Solution to Exercise 2.12.4. Write the n-tuple $\alpha \in X^n$ in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Thus, for each $i \in X$, we have

$$(\#\text{ of times } i \text{ appears in } \alpha) = (\#\text{ of } a \in [n] \text{ such that } \alpha_a = i)\,. \tag{408}$$

Write the n-tuple $\beta \in X^n$ in the form $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$. Thus, for each $i \in X$, we have

$$(\#\text{ of times } i \text{ appears in } \beta) = (\#\text{ of } b \in [n] \text{ such that } \beta_b = i)\,. \tag{409}$$

Define a map

$$\begin{aligned} f : [n] &\to X, \\ a &\mapsto \beta_a. \end{aligned}$$

In other words, $c \in \{a \in A \mid f(a) = i\}$.

But $i = f(c) \in W$ (by (406)). Hence, h_i is a bijection from $\{a \in A \mid f(a) = i\}$ to $\{b \in B \mid g(b) = i\}$ (by the definition of h_i). Therefore, $h_i(c)$ is a well-defined element of $\{b \in B \mid g(b) = i\}$ (since $c \in \{a \in A \mid f(a) = i\}$). Thus, $h_i(c) \in \{b \in B \mid g(b) = i\} \subseteq B$.

But the definition of u yields $u(c) = h_{f(c)}(c) = h_i(c)$ (since $f(c) = i$).

Also, $u(c) = h_i(c) \in \{b \in B \mid g(b) = i\}$. In other words, $u(c)$ is a $b \in B$ satisfying $g(b) = i$. In other words, $u(c) \in B$ and $g(u(c)) = i$. Now,

$$\begin{aligned} (v \circ u)(c) = v(u(c)) &= \left(h_{g(u(c))}\right)^{-1}(u(c)) \qquad \text{(by the definition of } v\text{)} \\ &= (h_i)^{-1}(u(c)) \qquad (\text{since } g(u(c)) = i) \\ &= c \qquad (\text{since } u(c) = h_i(c)) \\ &= \mathrm{id}(c)\,. \end{aligned}$$

Forget that we fixed c. We thus have proved that $(v \circ u)(c) = \mathrm{id}(c)$ for each $c \in A$. In other words, $v \circ u = \mathrm{id}$.

[323] *Proof.* Let $c \in A$. Let $i = f(c)$. Then, c is an $a \in A$ satisfying $f(a) = i$ (since $c \in A$ and $f(c) = i$). In other words, $c \in \{a \in A \mid f(a) = i\}$.

But $i = f(c) \in W$ (by (406)). Hence, h_i is a bijection from $\{a \in A \mid f(a) = i\}$ to $\{b \in B \mid g(b) = i\}$ (by the definition of h_i). Therefore, $h_i(c)$ is a well-defined element of $\{b \in B \mid g(b) = i\}$ (since $c \in \{a \in A \mid f(a) = i\}$). Thus, $h_i(c) \in \{b \in B \mid g(b) = i\}$.

But the definition of u yields $u(c) = h_{f(c)}(c) = h_i(c)$ (since $f(c) = i$). Hence, $u(c) = h_i(c) \in \{b \in B \mid g(b) = i\}$. In other words, $u(c)$ is a $b \in B$ satisfying $g(b) = i$. In other words, $u(c) \in B$ and $g(u(c)) = i$. Comparing $f(c) = i$ with $(g \circ u)(c) = g(u(c)) = i$, we obtain $f(c) = (g \circ u)(c)$.

Forget that we fixed c. We thus have proved that $f(c) = (g \circ u)(c)$ for each $c \in A$. In other words, $f = g \circ u$.

Define a map

$$\begin{aligned} g : [n] &\to X, \\ b &\mapsto \alpha_b. \end{aligned}$$

For each $i \in X$, we have

$$\begin{aligned} &\left(\#\text{ of } a \in [n] \text{ such that } \underbrace{f(a)}_{\substack{=\beta_a \\ \text{(by the definition of } f\text{)}}} = i \right) \\ &= (\#\text{ of } a \in [n] \text{ such that } \beta_a = i) \\ &= (\#\text{ of } b \in [n] \text{ such that } \beta_b = i) \qquad \text{(here, we have renamed the index } a \text{ as } b\text{)} \\ &= (\#\text{ of times } i \text{ appears in } \beta) \end{aligned} \tag{410}$$

(by (409)). Likewise, for each $i \in X$, we have

$$\begin{aligned} &(\#\text{ of } b \in [n] \text{ such that } g(b) = i) \\ &= (\#\text{ of times } i \text{ appears in } \alpha). \end{aligned} \tag{411}$$

Now, for each $i \in X$, we have

$$\begin{aligned} &(\#\text{ of } a \in [n] \text{ such that } f(a) = i) \\ &= (\#\text{ of times } i \text{ appears in } \beta) \qquad \text{(by (410))} \\ &= (\#\text{ of times } i \text{ appears in } \alpha) \qquad \text{(by (254))} \\ &= (\#\text{ of } b \in [n] \text{ such that } g(b) = i) \qquad \text{(by (411))}. \end{aligned}$$

Hence, Theorem 7.62.1 (applied to $A = [n]$ and $B = [n]$) yields that there exists a bijection $\sigma : [n] \to [n]$ such that $f = g \circ \sigma$. Consider this σ.

The map σ is a bijection from $[n]$ to $[n]$. In other words, σ is a permutation of $[n]$. Moreover, we have $\beta_i = \alpha_{\sigma(i)}$ for each $i \in [n]$ [324]. In other words, $(\beta_1, \beta_2, \ldots, \beta_n) = \left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}\right)$.

Hence, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) = \left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, \ldots, \alpha_{\sigma(n)}\right)$. Thus, the n-tuple β is obtained from the n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ by permuting its entries (namely, using the permutation σ). In other words, β is an anagram of $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ (by the definition of an anagram). In other words, β is an anagram of α (since $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$). This solves Exercise 2.12.4. □

[324] *Proof.* Let $i \in [n]$. The definition of f yields $f(i) = \beta_i$. Hence, $\beta_i = \underbrace{f}_{=g\circ\sigma}(i) = (g \circ \sigma)(i) = g(\sigma(i)) = \alpha_{\sigma(i)}$ (by the definition of g). Qed.

7.63. Solution to Exercise 2.12.5

To solve Exercise 2.12.5, we need to prove Proposition 2.12.13. This proof is a straightforward generalization of the proof of Proposition 2.12.10; we give it here for the sake of convenience:

Proof of Proposition 2.12.13. We define a *good tuple* to mean an n-tuple $(u_1, u_2, \ldots, u_n) \in [k]^n$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } u_a = i) = n_i \qquad \text{for each } i \in [k]\,.$$

Then, Proposition 2.12.7 shows that the # of good tuples is $\binom{n}{n_1, n_2, \ldots, n_k}$.

Now, we shall show that the good tuples are precisely the anagrams of α. In order to do so, we must prove the following two claims:

Claim 1: Each good tuple is an anagram of α.

Claim 2: Each anagram of α is a good tuple.

[*Proof of Claim 1:* Let β be a good tuple. Thus, β is an n-tuple $(u_1, u_2, \ldots, u_n) \in [k]^n$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } u_a = i) = n_i \qquad \text{for each } i \in [k] \tag{412}$$

(by the definition of a "good tuple"). Consider this $(u_1, u_2, \ldots, u_n)$. Hence, $\beta = (u_1, u_2, \ldots, u_n) \in [k]^n$.

For each $i \in [k]$, we have

$$\begin{aligned}
&(\#\text{ of } a \in [n] \text{ such that } u_a = i) \\
&= n_i \qquad (\text{by (412)}) \\
&= (\#\text{ of times } i \text{ appears in } \alpha) \qquad (\text{by (255)})\,.
\end{aligned}$$

Hence, for each $i \in [k]$, we have

$$\begin{aligned}
&(\#\text{ of times } i \text{ appears in } \alpha) \\
&= (\#\text{ of } a \in [n] \text{ such that } u_a = i) \\
&= (\#\text{ of times } i \text{ appears in } (u_1, u_2, \ldots, u_n)) \\
&= (\#\text{ of times } i \text{ appears in } \beta) \qquad (\text{since } (u_1, u_2, \ldots, u_n) = \beta)\,.
\end{aligned}$$

In other words, for each $i \in [k]$, we have

$$(\#\text{ of times } i \text{ appears in } \beta) = (\#\text{ of times } i \text{ appears in } \alpha)\,.$$

So we have $\alpha \in [k]^n$ and $\beta \in [k]^n$, and we have shown that

$$(\#\text{ of times } i \text{ appears in } \beta) = (\#\text{ of times } i \text{ appears in } \alpha)$$

for each $i \in [k]$. Therefore, Exercise 2.12.4 (applied to $X = [k]$) yields that β is an anagram of α.

Forget that we fixed β. We thus have shown that each good tuple β is an anagram of α. This proves Claim 1.]

[*Proof of Claim 2:* Let β be an anagram of α. Then, for each $i \in [k]$, we have

$$\begin{aligned}
&(\#\text{ of times } i \text{ appears in } \beta) \\
&= (\#\text{ of times } i \text{ appears in } \alpha) \qquad (\text{by Exercise 2.12.3, applied to } X = [k]) \\
&= n_i \qquad (\text{by (255)}) . \qquad (413)
\end{aligned}$$

Moreover, β is an anagram of α, and therefore is an n-tuple (since α is an n-tuple). Hence, we can write β in the form $\beta = (u_1, u_2, \ldots, u_n)$. Consider this $(u_1, u_2, \ldots, u_n)$. Hence, $\beta = (u_1, u_2, \ldots, u_n) \in [k]^n$. Moreover, for each $i \in [k]$, we have

$$\begin{aligned}
&(\#\text{ of } a \in [n] \text{ such that } u_a = i) \\
&= (\#\text{ of times } i \text{ appears in } (u_1, u_2, \ldots, u_n)) \\
&= (\#\text{ of times } i \text{ appears in } \beta) \qquad (\text{since } (u_1, u_2, \ldots, u_n) = \beta) \\
&= n_i \qquad (\text{by (413)}) . \qquad (414)
\end{aligned}$$

We have now shown that β is an n-tuple $(u_1, u_2, \ldots, u_n) \in [k]^n$ satisfying

$$(\#\text{ of } a \in [n] \text{ such that } u_a = i) = n_i \qquad \text{for each } i \in [k]$$

(by (414)). In other words, β is a good tuple (by the definition of a good tuple).

Forget that we fixed β. We thus have shown that if β is an anagram of α, then β is a good tuple. In other words, each anagram of α is a good tuple. This proves Claim 2.]

Combining Claim 1 with Claim 2, we see that the anagrams of α are precisely the good tuples. Hence,

$$(\#\text{ of anagrams of } \alpha) = (\#\text{ of good tuples}) = \binom{n}{n_1, n_2, \ldots, n_k}$$

(since we have already shown that the # of good tuples is $\binom{n}{n_1, n_2, \ldots, n_k}$). In other words, the # of distinct anagrams of α is $\binom{n}{n_1, n_2, \ldots, n_k}$. This proves Proposition 2.12.13. $\square$

7.64. Solution to Exercise 2.12.6

In order to solve Exercise 2.12.6, we need to prove Theorem 2.12.16. We shall do this, after first proving a lemma:

Lemma 7.64.1. Let $n \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k \in \mathbb{N}$ be such that $n_1 + n_2 + \cdots + n_k = n > 0$. Let $i \in [k]$. Then,

$$\underbrace{\binom{n-1}{n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k}}_{\text{This should be interpreted as 0 if } n_i = 0} = \frac{n_i}{n} \cdot \binom{n}{n_1, n_2, \ldots, n_k}.$$

Proof of Lemma 7.64.1. We first observe that the multinomial coefficient $\binom{n}{n_1, n_2, \ldots, n_k}$ is well-defined, since $n_1 + n_2 + \cdots + n_k = n$. Its definition yields

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}. \tag{415}$$

If $n_i = 0$, then the claim of Lemma 7.64.1 is easily seen to be true[325]. Hence, for the rest of this proof, we WLOG that $n_i \neq 0$. Therefore, $n_i \geq 1$ (since $n_i \in \mathbb{N}$), so that $n_i - 1 \in \mathbb{N}$. Moreover, $n \geq 1$ (since $n \in \mathbb{N}$ and $n > 0$), so that $n - 1 \in \mathbb{N}$. Proposition 1.3.2 yields $n! = (n-1)! \cdot n$, so that $(n-1)! = n!/n$. Moreover, Proposition 1.3.2 (applied to n_i instead of n) yields $n_i! = (n_i - 1)! \cdot n_i$, so that $(n_i - 1)! = n_i!/n_i$.

The multinomial coefficient $\binom{n-1}{n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k}$ is well-defined, since

$$n_1 + \cdots + n_{i-1} + (n_i - 1) + n_{i+1} + \cdots + n_k = \underbrace{(n_1 + n_2 + \cdots + n_k)}_{=n} - 1 = n - 1$$

(and since $n - 1 \in \mathbb{N}$ and since $n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k \in \mathbb{N}$). Its definition

[325] *Proof.* Assume that $n_i = 0$. Then,

$$\underbrace{\binom{n-1}{n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k}}_{\text{This should be interpreted as 0 if } n_i = 0} = 0 \qquad (\text{since } n_i = 0).$$

Comparing this with

$$\begin{aligned} \frac{n_i}{n} \cdot \binom{n}{n_1, n_2, \ldots, n_k} &= \frac{0}{n} \cdot \binom{n}{n_1, n_2, \ldots, n_k} \qquad (\text{since } n_i = 0) \\ &= 0, \end{aligned}$$

we obtain $\underbrace{\binom{n-1}{n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k}}_{\text{This should be interpreted as 0 if } n_i = 0} = \frac{n_i}{n} \cdot \binom{n}{n_1, n_2, \ldots, n_k}$. Thus, Lemma 7.64.1 is true (under the assumption that $n_i = 0$).

yields

$$\begin{aligned}
&\binom{n-1}{n_1,\ldots,n_{i-1},n_i-1,n_{i+1},\ldots,n_k} \\
&= \frac{(n-1)!}{n_1!\cdots n_{i-1}!\,(n_i-1)!n_{i+1}!\cdots n_k!} \\
&= \frac{n!/n}{n_1!\cdots n_{i-1}!\cdot(n_i!/n_i)\cdot n_{i+1}!\cdots n_k!} \qquad \left(\begin{array}{c}\text{since } (n-1)!=n!/n \\ \text{and } (n_i-1)!=n_i!/n_i\end{array}\right) \\
&= \frac{n_i}{n}\cdot\frac{n!}{n_1!\cdots n_{i-1}!\cdot n_i!\cdot n_{i+1}!\cdots n_k!} \\
&= \frac{n_i}{n}\cdot \underbrace{\frac{n!}{n_1!n_2!\cdots n_k!}}_{=\binom{n}{n_1,n_2,\ldots,n_k}\text{ (by (415))}} \qquad (\text{since } n_1!\cdots n_{i-1}!\cdot n_i!\cdot n_{i+1}!\cdots n_k! = n_1!n_2!\cdots n_k!) \\
&= \frac{n_i}{n}\cdot\binom{n}{n_1,n_2,\ldots,n_k}.
\end{aligned}$$

This proves Lemma 7.64.1. □

We are now ready to prove Theorem 2.12.16 (and thus solve Exercise 2.12.6):

Proof of Theorem 2.12.16. We have

$$\sum_{i=1}^{k}\frac{n_i}{n} = \frac{\sum_{i=1}^{k} n_i}{n} = 1 \qquad \left(\text{since } \sum_{i=1}^{k} n_i = n_1+n_2+\cdots+n_k = n\right).$$

Now,

$$\begin{aligned}
\sum_{i=1}^{k}\underbrace{\binom{n-1}{n_1,\ldots,n_{i-1},n_i-1,n_{i+1},\ldots,n_k}}_{=\frac{n_i}{n}\cdot\binom{n}{n_1,n_2,\ldots,n_k}\text{ (by Lemma 7.64.1)}} &= \sum_{i=1}^{k}\frac{n_i}{n}\cdot\binom{n}{n_1,n_2,\ldots,n_k} \\
&= \underbrace{\left(\sum_{i=1}^{k}\frac{n_i}{n}\right)}_{=1}\cdot\binom{n}{n_1,n_2,\ldots,n_k} \\
&= \binom{n}{n_1,n_2,\ldots,n_k}.
\end{aligned}$$

This proves Theorem 2.12.16. □

7.65. Solution to Exercise 3.3.1

Our solution to Exercise 3.3.1 will rest on the following two basic facts about permutations:

Proposition 7.65.1. **(a)** If σ_1 and σ_2 are two permutations of a set S, then their composition $\sigma_1 \circ \sigma_2$ is a permutation of S.

(b) If σ is a permutation of a set S, then its inverse σ^{-1} is a permutation of S.

Proof of Proposition 7.65.1. Recall that a permutation of a set S is the same as a bijection from S to S. Thus, Proposition 7.65.1 **(a)** follows from the well-known fact that the composition of two bijections is a bijection. Likewise, Proposition 7.65.1 **(b)** follows from the fact that the inverse of a bijection is a bijection. □

Solution to Exercise 3.3.1. For any two k-tuples $\mathbf{p}, \mathbf{q} \in A^k$, we have the logical equivalence

$$\left(\mathbf{p} \underset{\text{perm}}{\sim} \mathbf{q}\right) \iff (\mathbf{p} \text{ is an anagram of } \mathbf{q}) \tag{416}$$

(by the definition of the relation $\underset{\text{perm}}{\sim}$). Using this, we quickly obtain the following two observations:

> *Observation 1:* Let $(a_1, a_2, \ldots, a_k) \in A^k$ and $(b_1, b_2, \ldots, b_k) \in A^k$ be two k-tuples such that $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$. Then, there exists a permutation π of $[k]$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$.
>
> *Observation 2:* Let $(a_1, a_2, \ldots, a_k) \in A^k$ and $(b_1, b_2, \ldots, b_k) \in A^k$ be two k-tuples, and let ω be a permutation of $[k]$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\omega(1)}, b_{\omega(2)}, \ldots, b_{\omega(k)}\right)$. Then, $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$.

[*Proof of Observation 1:* Applying (416) to $\mathbf{p} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{q} = (b_1, b_2, \ldots, b_k)$, we obtain the logical equivalence

$$\begin{aligned} &\left((a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)\right) \\ \iff &\left((a_1, a_2, \ldots, a_k) \text{ is an anagram of } (b_1, b_2, \ldots, b_k)\right). \end{aligned}$$

Hence, $(a_1, a_2, \ldots, a_k)$ is an anagram of $(b_1, b_2, \ldots, b_k)$ (since we have $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$). In other words, $(a_1, a_2, \ldots, a_k)$ is a k-tuple of the form $\left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$, where π is a permutation of $[k]$ (since an anagram of $(b_1, b_2, \ldots, b_k)$ is defined to be a k-tuple of the form $\left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$, where π is a permutation of $[k]$). In other words, there exists a permutation π of $[k]$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$. This proves Observation 1.]

[*Proof of Observation 2:* We have $(a_1, a_2, \ldots, a_k) = \left(b_{\omega(1)}, b_{\omega(2)}, \ldots, b_{\omega(k)}\right)$. Hence, there exists a permutation π of $[k]$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$ (namely, $\pi = \omega$). In other words, the tuple $(a_1, a_2, \ldots, a_k)$ is a k-tuple of the form $\left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$, where π is a permutation of $[k]$. In other words, the tuple $(a_1, a_2, \ldots, a_k)$ is an anagram of $(b_1, b_2, \ldots, b_k)$ (since an anagram of $(b_1, b_2, \ldots, b_k)$ is defined to be a k-tuple of the form $\left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$, where π is a permutation of $[k]$).

However, applying (416) to $\mathbf{p} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{q} = (b_1, b_2, \ldots, b_k)$, we obtain the logical equivalence

$$\begin{aligned}&\left((a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)\right)\\ &\iff \left((a_1, a_2, \ldots, a_k) \text{ is an anagram of } (b_1, b_2, \ldots, b_k)\right).\end{aligned}$$

Therefore, we have $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$ (since $(a_1, a_2, \ldots, a_k)$ is an anagram of $(b_1, b_2, \ldots, b_k)$). This proves Observation 2.]

Now, let us prove that the relation $\underset{\text{perm}}{\sim}$ is an equivalence relation. To that end, we need to prove that this relation $\underset{\text{perm}}{\sim}$ is reflexive, symmetric and transitive. We shall prove these three properties one by one:

[*Proof of reflexivity:* We must show that the relation $\underset{\text{perm}}{\sim}$ is reflexive. In other words, we must prove that every $a \in A^k$ satisfies $a \underset{\text{perm}}{\sim} a$.

So let $a \in A^k$ be arbitrary. Write this k-tuple a in the form $a = (a_1, a_2, \ldots, a_k)$.

Now, let id denote the identity map $\mathrm{id}_{[k]} : [k] \to [k]$. This identity map id is a permutation of $[k]$. Moreover, each $i \in [k]$ satisfies $a_i = a_{\mathrm{id}(i)}$ (since $i = \mathrm{id}(i)$). In other words, $(a_1, a_2, \ldots, a_k) = \left(a_{\mathrm{id}(1)}, a_{\mathrm{id}(2)}, \ldots, a_{\mathrm{id}(k)}\right)$. Hence, Observation 2 (applied to $(b_1, b_2, \ldots, b_k) = (a_1, a_2, \ldots, a_k)$ and $\omega = \mathrm{id}$) yields $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (a_1, a_2, \ldots, a_k)$. In view of $a = (a_1, a_2, \ldots, a_k)$, we can rewrite this as $a \underset{\text{perm}}{\sim} a$.

We thus have shown that every $a \in A^k$ satisfies $a \underset{\text{perm}}{\sim} a$. In other words, the relation $\underset{\text{perm}}{\sim}$ is reflexive.]

[*Proof of symmetry:* We must show that the relation $\underset{\text{perm}}{\sim}$ is symmetric. In other words, we must prove that every $a, b \in A^k$ satisfying $a \underset{\text{perm}}{\sim} b$ satisfy $b \underset{\text{perm}}{\sim} a$.

So let $a, b \in A^k$ satisfy $a \underset{\text{perm}}{\sim} b$. Write the k-tuples a and b in the forms

$$a = (a_1, a_2, \ldots, a_k) \qquad \text{and} \qquad b = (b_1, b_2, \ldots, b_k). \tag{417}$$

We have $a \underset{\text{perm}}{\sim} b$. In view of (417), we can rewrite this as

$$(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k) .$$

Hence, Observation 1 shows that there exists a permutation π of $[k]$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$. Consider this π. Proposition 7.65.1 **(b)** (applied to $S = [k]$ and $\sigma = \pi$) yields that π^{-1} is a permutation of $[k]$. Moreover, each $i \in [k]$ satisfies

$$a_i = b_{\pi(i)} \tag{418}$$

(since $(a_1, a_2, \ldots, a_k) = \left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$).

Now, let $j \in [k]$. Then, $\pi^{-1}(j) \in [k]$. Thus, (418) (applied to $i = \pi^{-1}(j)$) yields $a_{\pi^{-1}(j)} = b_{\pi\left(\pi^{-1}(j)\right)} = b_j$ (since $\pi\left(\pi^{-1}(j)\right) = j$). In other words, $b_j = a_{\pi^{-1}(j)}$.

Forget that we fixed j. We thus have shown that $b_j = a_{\pi^{-1}(j)}$ for each $j \in [k]$. In other words,

$$(b_1, b_2, \ldots, b_k) = \left(a_{\pi^{-1}(1)}, a_{\pi^{-1}(2)}, \ldots, a_{\pi^{-1}(k)}\right) .$$

Hence, Observation 2 (applied to $(b_1, b_2, \ldots, b_k)$, $(a_1, a_2, \ldots, a_k)$ and π^{-1} instead of $(a_1, a_2, \ldots, a_k)$, $(b_1, b_2, \ldots, b_k)$ and ω) yields $(b_1, b_2, \ldots, b_k) \underset{\text{perm}}{\sim} (a_1, a_2, \ldots, a_k)$. In view of (417), we can rewrite this as $b \underset{\text{perm}}{\sim} a$.

We thus have shown that every $a, b \in A^k$ satisfying $a \underset{\text{perm}}{\sim} b$ satisfy $b \underset{\text{perm}}{\sim} a$. In other words, the relation $\underset{\text{perm}}{\sim}$ is symmetric.]

[*Proof of transitivity:* We must show that the relation $\underset{\text{perm}}{\sim}$ is transitive. In other words, we must prove that every $a, b, c \in A^k$ satisfying $a \underset{\text{perm}}{\sim} b$ and $b \underset{\text{perm}}{\sim} c$ satisfy $a \underset{\text{perm}}{\sim} c$.

So let $a, b, c \in A^k$ satisfy $a \underset{\text{perm}}{\sim} b$ and $b \underset{\text{perm}}{\sim} c$. Write the k-tuples a, b and c in the forms

$$a = (a_1, a_2, \ldots, a_k) , \tag{419}$$
$$b = (b_1, b_2, \ldots, b_k) , \qquad \text{and} \tag{420}$$
$$c = (c_1, c_2, \ldots, c_k) . \tag{421}$$

We have $a \underset{\text{perm}}{\sim} b$. In view of (419) and (420), we can rewrite this as

$$(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k) .$$

Hence, Observation 1 shows that there exists a permutation π of $[k]$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\pi(1)}, b_{\pi(2)}, \ldots, b_{\pi(k)}\right)$. Let us denote this π by σ. Thus, σ is a

permutation of $[k]$ and satisfies $(a_1, a_2, \ldots, a_k) = \left(b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(k)}\right)$. Each $i \in [k]$ satisfies

$$a_i = b_{\sigma(i)} \tag{422}$$

(since $(a_1, a_2, \ldots, a_k) = \left(b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(k)}\right)$).

We have $b \underset{\text{perm}}{\sim} c$. In view of (420) and (421), we can rewrite this as

$$(b_1, b_2, \ldots, b_k) \underset{\text{perm}}{\sim} (c_1, c_2, \ldots, c_k).$$

Therefore, Observation 1 (applied to $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_k)$ instead of $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_k)$) shows that there exists a permutation π of $[k]$ such that $(b_1, b_2, \ldots, b_k) = \left(c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(k)}\right)$. Consider this π. Each $j \in [k]$ satisfies

$$b_j = c_{\pi(j)} \tag{423}$$

(since $(b_1, b_2, \ldots, b_k) = \left(c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(k)}\right)$).

Note that π and σ are permutations of $[k]$. Hence, their composition $\pi \circ \sigma$ is a permutation of $[k]$ as well (by Proposition 7.65.1 **(a)**, applied to $S = [k]$, $\sigma_1 = \pi$ and $\sigma_2 = \sigma$).

Now, let $i \in [k]$. Then, $\sigma(i) \in [k]$. Thus, (423) (applied to $j = \sigma(i)$) yields $b_{\sigma(i)} = c_{\pi(\sigma(i))} = c_{(\pi \circ \sigma)(i)}$ (since $\pi(\sigma(i)) = (\pi \circ \sigma)(i)$). However, (422) yields $a_i = b_{\sigma(i)} = c_{(\pi \circ \sigma)(i)}$.

Forget that we fixed i. We thus have shown that $a_i = c_{(\pi \circ \sigma)(i)}$ for each $i \in [k]$. In other words,

$$(a_1, a_2, \ldots, a_k) = \left(c_{(\pi \circ \sigma)(1)}, c_{(\pi \circ \sigma)(2)}, \ldots, c_{(\pi \circ \sigma)(k)}\right).$$

Hence, Observation 2 (applied to $(c_1, c_2, \ldots, c_k)$ and $\pi \circ \sigma$ instead of $(b_1, b_2, \ldots, b_k)$ and ω) yields $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (c_1, c_2, \ldots, c_k)$ (since $\pi \circ \sigma$ is a permutation of $[k]$). In view of (419) and (421), we can rewrite this as $a \underset{\text{perm}}{\sim} c$.

We thus have shown that every $a, b, c \in A^k$ satisfying $a \underset{\text{perm}}{\sim} b$ and $b \underset{\text{perm}}{\sim} c$ satisfy $a \underset{\text{perm}}{\sim} c$. In other words, the relation $\underset{\text{perm}}{\sim}$ is transitive.]

We have now proved that the relation $\underset{\text{perm}}{\sim}$ is reflexive, symmetric and transitive. In other words, this relation $\underset{\text{perm}}{\sim}$ is an equivalence relation. This solves Exercise 3.3.1. □

7.66. Solution to Exercise 3.3.2

In order to solve Exercise 3.3.2, we first derive a few properties of multisubsets. The first one is a kind of converse to Exercise 2.11.1:

Proposition 7.66.1. Let T be a set. Let $m \in \mathbb{N}$. Let S be a multisubset of T having size m. Then, there exists an m-tuple $(s_1, s_2, \ldots, s_m)$ of elements of T satisfying $\{s_1, s_2, \ldots, s_m\}_{\text{multi}} = S$.

Note that this proposition is a weaker version of Proposition 2.11.5 (weaker because it neither provides for $s_1 \leq s_2 \leq \cdots \leq s_m$ nor claims uniqueness), which however has the advantage of holding for any set T (rather than only for sets of integers).

Proof of Proposition 7.66.1. We shall prove Proposition 7.66.1 by induction on m:

Induction base: Proposition 7.66.1 holds for $m = 0$ [326]. This completes the induction base.

Induction step: Let $g \in \mathbb{N}$. Assume that Proposition 7.66.1 holds for $m = g$. We shall now show that Proposition 7.66.1 holds for $m = g + 1$.

We have assumed that Proposition 7.66.1 holds for $m = g$. In other words,

$$\left(\begin{array}{c} \text{if } T \text{ is a set, and if } S \text{ is a multisubset of } T \\ \text{having size } g, \text{ then there exists} \\ \text{a } g\text{-tuple } \left(s_1, s_2, \ldots, s_g\right) \text{ of elements of } T \\ \text{satisfying } \left\{s_1, s_2, \ldots, s_g\right\}_{\text{multi}} = S \end{array} \right). \tag{424}$$

Now, let T be a set, and let S be a multisubset of T having size $g+1$. We want to prove that there exists a $(g+1)$-tuple $\left(s_1, s_2, \ldots, s_{g+1}\right)$ of elements of T satisfying $\left\{s_1, s_2, \ldots, s_{g+1}\right\}_{\text{multi}} = S$.

We shall use Definition 7.58.2, Definition 7.58.3, Definition 7.58.6 and Definition 7.58.9.

We have assumed that S has size $g+1$. In other words, $|S| = g+1$ (since $|S|$ denotes the size of S). Thus, $|S| = g+1 > g \geq 0$. Hence, Proposition 7.58.12 **(c)** (applied to $f = S$) shows that $\operatorname{Supp} S$ is a finite nonempty subset of T. Hence, there exists some $u \in \operatorname{Supp} S$ (since $\operatorname{Supp} S$ is nonempty). Consider this u.

Now, Proposition 7.58.11 **(a)** (applied to $f = S$) yields $\{u\}_{\text{multi}} \subseteq S$. Also, Proposition 7.58.11 **(b)** (applied to $f = S$) yields $|S \setminus \{u\}_{\text{multi}}| = |S| - 1 = g$ (since $|S| = g+1$). In other words, the multisubset $S \setminus \{u\}_{\text{multi}}$ of T has size g.

Hence, (424) (applied to $S \setminus \{u\}_{\text{multi}}$ instead of S) shows that there exists a g-tuple $\left(s_1, s_2, \ldots, s_g\right)$ of elements of T satisfying $\left\{s_1, s_2, \ldots, s_g\right\}_{\text{multi}} = S \setminus \{u\}_{\text{multi}}$. Let us pick such a g-tuple $\left(s_1, s_2, \ldots, s_g\right)$ and denote it by $\left(t_1, t_2, \ldots, t_g\right)$.

[326] *Proof.* Let T be a set. Let S be a multisubset of T having size 0. We must prove that there exists a 0-tuple $(s_1, s_2, \ldots, s_0)$ of elements of T satisfying $\{s_1, s_2, \ldots, s_0\}_{\text{multi}} = S$.

The multisubset S has size 0. In other words, $|S| = 0$ (since $|S|$ denotes the size of S). Hence, Proposition 7.58.16 **(a)** (applied to $f = S$) yields $S = \{\}_{\text{multi}}$. Thus, $\{\}_{\text{multi}} = S$. In other words, if we denote the 0-tuple $()$ by $(s_1, s_2, \ldots, s_0)$, then $\{s_1, s_2, \ldots, s_0\}_{\text{multi}} = S$.

Hence, there exists a 0-tuple $(s_1, s_2, \ldots, s_0)$ of elements of T satisfying $\{s_1, s_2, \ldots, s_0\}_{\text{multi}} = S$ (namely, the 0-tuple $()$).

Forget that we fixed T and S. We thus have shown that if T is a set, and if S is a multisubset of T having size 0, then there exists a 0-tuple $(s_1, s_2, \ldots, s_0)$ of elements of T satisfying $\{s_1, s_2, \ldots, s_0\}_{\text{multi}} = S$. In other words, Proposition 7.66.1 holds for $m = 0$.

We extend this g-tuple $(t_1, t_2, \ldots, t_g)$ to a $(g+1)$-tuple $(t_1, t_2, \ldots, t_{g+1})$ by setting $t_{g+1} = u$. Thus, $t_{g+1} = u \in \operatorname{Supp} S \subseteq T$ (since $\operatorname{Supp} S$ is a subset of T). Therefore, $\{t_{g+1}\} \subseteq T$.

We have defined $(t_1, t_2, \ldots, t_g)$ as a g-tuple $(s_1, s_2, \ldots, s_g)$ of elements of T satisfying $\{s_1, s_2, \ldots, s_g\}_{\text{multi}} = S \setminus \{u\}_{\text{multi}}$. In other words, $(t_1, t_2, \ldots, t_g)$ is a g-tuple of elements of T and satisfies

$$\{t_1, t_2, \ldots, t_g\}_{\text{multi}} = S \setminus \{u\}_{\text{multi}}. \tag{425}$$

Note that $t_1, t_2, \ldots, t_g$ are elements of T (since $(t_1, t_2, \ldots, t_g)$ is a g-tuple of elements of T). Therefore, $\{t_1, t_2, \ldots, t_g\} \subseteq T$.

Next, we shall prove that

$$S = \{t_1, t_2, \ldots, t_{g+1}\}_{\text{multi}}. \tag{426}$$

[*Proof of (426):* We have $\{u\}_{\text{multi}} \subseteq S$ and thus $(S \setminus \{u\}_{\text{multi}}) \cup \{u\}_{\text{multi}} = S$ (by Proposition 7.58.7 **(b)**, applied to $\{u\}_{\text{multi}}$ and S instead of f and g). Thus,

$$S = \underbrace{(S \setminus \{u\}_{\text{multi}})}_{\substack{=\{t_1,t_2,\ldots,t_g\}_{\text{multi}} \\ \text{(by (425))}}} \cup \left\{ \underbrace{u}_{=t_{g+1}} \right\}_{\text{multi}} = \{t_1, t_2, \ldots, t_g\}_{\text{multi}} \cup \{t_{g+1}\}_{\text{multi}}$$

$$= \{t_1, t_2, \ldots, t_g, t_{g+1}\}_{\text{multi}}$$

$$\left(\begin{array}{c} \text{by Proposition 7.58.5, applied to the numbers } g \text{ and } 1 \text{ and} \\ \text{the } g\text{-tuple } (t_1, t_2, \ldots, t_g) \text{ and the 1-tuple } (t_{g+1}) \text{ instead of the numbers } k \\ \text{and } \ell \text{ and the } k\text{-tuple } (a_1, a_2, \ldots, a_k) \text{ and the } \ell\text{-tuple } (b_1, b_2, \ldots, b_\ell) \end{array} \right)$$

$$= \{t_1, t_2, \ldots, t_{g+1}\}_{\text{multi}}.$$

This proves (425).]

Clearly,

$$\{t_1, t_2, \ldots, t_{g+1}\} = \underbrace{\{t_1, t_2, \ldots, t_g\}}_{\subseteq T} \cup \underbrace{\{t_{g+1}\}}_{\subseteq T} \subseteq T \cup T = T.$$

Thus, $t_1, t_2, \ldots, t_{g+1}$ are elements of the set T. Hence, $(t_1, t_2, \ldots, t_{g+1})$ is a $(g+1)$-tuple of elements of T.

Altogether, we have now shown that $(t_1, t_2, \ldots, t_{g+1})$ is a $(g+1)$-tuple of elements of T and satisfies $\{t_1, t_2, \ldots, t_{g+1}\}_{\text{multi}} = S$ (by (426)). Hence, there exists a $(g+1)$-tuple $(s_1, s_2, \ldots, s_{g+1})$ of elements of T satisfying $\{s_1, s_2, \ldots, s_{g+1}\}_{\text{multi}} = S$ (namely, the $(g+1)$-tuple $(t_1, t_2, \ldots, t_{g+1})$).

Forget that we fixed T and S. We thus have shown that

$$\left(\begin{array}{c} \text{if } T \text{ is a set, and if } S \text{ is a multisubset of } T \\ \text{having size } g+1, \text{ then there exists} \\ \text{a } (g+1)\text{-tuple } (s_1, s_2, \ldots, s_{g+1}) \text{ of elements of } T \\ \text{satisfying } \{s_1, s_2, \ldots, s_{g+1}\}_{\text{multi}} = S \end{array} \right).$$

In other words, Proposition 7.66.1 holds for $m = g+1$. This completes the induction step. Hence, Proposition 7.66.1 is proven by induction. □

Our next proposition is an easy consequence of Exercise 2.12.3:

Proposition 7.66.2. Let A be a set, and let $k \in \mathbb{N}$. Let $(a_1, a_2, \ldots, a_k) \in A^k$ and $(b_1, b_2, \ldots, b_k) \in A^k$ be two k-tuples of elements of A that satisfy

$$(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k).$$

Then,

$$\{a_1, a_2, \ldots, a_k\}_{\text{multi}} = \{b_1, b_2, \ldots, b_k\}_{\text{multi}}.$$

Proof of Proposition 7.66.2. For any two k-tuples $\mathbf{p} \in A^k$ and $\mathbf{q} \in A^k$, we have the logical equivalence

$$\left(\mathbf{p} \underset{\text{perm}}{\sim} \mathbf{q}\right) \Longleftrightarrow (\mathbf{p} \text{ is an anagram of } \mathbf{q})$$

(by the definition of the relation $\underset{\text{perm}}{\sim}$). Applying this to $\mathbf{p} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{q} = (b_1, b_2, \ldots, b_k)$, we obtain the equivalence

$$\begin{aligned} &\left((a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)\right) \\ &\Longleftrightarrow \ ((a_1, a_2, \ldots, a_k) \text{ is an anagram of } (b_1, b_2, \ldots, b_k)). \end{aligned}$$

Hence, $(a_1, a_2, \ldots, a_k)$ is an anagram of $(b_1, b_2, \ldots, b_k)$ (since we have $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$). Thus, each $t \in A$ satisfies

$$\begin{aligned} &(\#\text{ of times } t \text{ appears in } (a_1, a_2, \ldots, a_k)) \\ &= (\#\text{ of times } t \text{ appears in } (b_1, b_2, \ldots, b_k)) \end{aligned} \tag{427}$$

(by Exercise 2.12.3, applied to $X = A$, $n = k$, $\alpha = (b_1, b_2, \ldots, b_k)$, $\beta = (a_1, a_2, \ldots, a_k)$ and $i = t$).

Both $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ and $\{b_1, b_2, \ldots, b_k\}_{\text{multi}}$ are multisubsets of A. Hence, both $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ and $\{b_1, b_2, \ldots, b_k\}_{\text{multi}}$ are maps from A to $\mathbb{N}$ (since any multisubset of A is a map from A to $\mathbb{N}$).

Definition 7.57.1 (applied to $T = A$) says that the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ is defined as the map

$$\begin{aligned} &A \to \mathbb{N}, \\ &t \mapsto (\#\text{ of } i \in [k] \text{ satisfying } a_i = t). \end{aligned}$$

Thus, for each $t \in A$, we have

$$\{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) = (\#\text{ of } i \in [k] \text{ satisfying } a_i = t). \tag{428}$$

Similarly, for each $t \in A$, we have

$$\{b_1, b_2, \ldots, b_k\}_{\text{multi}}(t) = (\#\text{ of } i \in [k] \text{ satisfying } b_i = t). \tag{429}$$

Hence, for each $t \in A$, we have

$$\begin{aligned}
\{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) &= (\#\text{ of } i \in [k] \text{ satisfying } a_i = t) \qquad \text{(by (428))} \\
&= (\#\text{ of times } t \text{ appears in } (a_1, a_2, \ldots, a_k)) \\
&= (\#\text{ of times } t \text{ appears in } (b_1, b_2, \ldots, b_k)) \qquad \text{(by (427))} \\
&= (\#\text{ of } i \in [k] \text{ satisfying } b_i = t) \\
&= \{b_1, b_2, \ldots, b_k\}_{\text{multi}}(t) \qquad \text{(by (429))}.
\end{aligned}$$

This shows that $\{a_1, a_2, \ldots, a_k\}_{\text{multi}} = \{b_1, b_2, \ldots, b_k\}_{\text{multi}}$ (because both $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ and $\{b_1, b_2, \ldots, b_k\}_{\text{multi}}$ are maps from A to $\mathbb{N}$). Thus, Proposition 7.66.2 is proven. □

The converse of Proposition 7.66.2 is an easy consequence of Exercise 2.12.4:

Proposition 7.66.3. Let A be a set, and let $k \in \mathbb{N}$. Let $(a_1, a_2, \ldots, a_k) \in A^k$ and $(b_1, b_2, \ldots, b_k) \in A^k$ be two k-tuples of elements of A that satisfy

$$\{a_1, a_2, \ldots, a_k\}_{\text{multi}} = \{b_1, b_2, \ldots, b_k\}_{\text{multi}}.$$

Then,

$$(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k).$$

Proof of Proposition 7.66.3. Definition 7.57.1 (applied to $T = A$) says that the multi-subset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of A is defined as the map

$$\begin{aligned}
A &\to \mathbb{N}, \\
t &\mapsto (\#\text{ of } i \in [k] \text{ satisfying } a_i = t).
\end{aligned}$$

Thus, for each $t \in A$, we have

$$\{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) = (\#\text{ of } i \in [k] \text{ satisfying } a_i = t). \tag{430}$$

Similarly, for each $t \in A$, we have

$$\{b_1, b_2, \ldots, b_k\}_{\text{multi}}(t) = (\#\text{ of } i \in [k] \text{ satisfying } b_i = t). \tag{431}$$

Now, for each $t \in A$, we have

$$\begin{aligned}
&(\#\text{ of times } t \text{ appears in } (a_1, a_2, \ldots, a_k)) \\
&= (\#\text{ of } i \in [k] \text{ satisfying } a_i = t) \\
&= \{a_1, a_2, \ldots, a_k\}_{\text{multi}}(t) \qquad \text{(by (430))} \\
&= \{b_1, b_2, \ldots, b_k\}_{\text{multi}}(t) \qquad \text{(since } \{a_1, a_2, \ldots, a_k\}_{\text{multi}} = \{b_1, b_2, \ldots, b_k\}_{\text{multi}}\text{)} \\
&= (\#\text{ of } i \in [k] \text{ satisfying } b_i = t) \qquad \text{(by (431))} \\
&= (\#\text{ of times } t \text{ appears in } (b_1, b_2, \ldots, b_k)).
\end{aligned}$$

Renaming the index t as i in this sentence, we obtain the following: For each $i \in A$, we have

$$(\#\text{ of times } i \text{ appears in } (a_1, a_2, \ldots, a_k)) = (\#\text{ of times } i \text{ appears in } (b_1, b_2, \ldots, b_k)).$$

Now, $(b_1, b_2, \ldots, b_k) \in A^k$ and $(a_1, a_2, \ldots, a_k) \in A^k$ are two k-tuples, and we know that

$$(\#\text{ of times } i \text{ appears in } (a_1, a_2, \ldots, a_k)) = (\#\text{ of times } i \text{ appears in } (b_1, b_2, \ldots, b_k))$$

for each $i \in A$ (according to the previous sentence). Hence, Exercise 2.12.4 (applied to $X = A$, $n = k$, $\alpha = (b_1, b_2, \ldots, b_k)$ and $\beta = (a_1, a_2, \ldots, a_k)$) shows that $(a_1, a_2, \ldots, a_k)$ is an anagram of $(b_1, b_2, \ldots, b_k)$.

For any two k-tuples $\mathbf{p} \in A^k$ and $\mathbf{q} \in A^k$, we have the logical equivalence

$$\left(\mathbf{p} \underset{\text{perm}}{\sim} \mathbf{q}\right) \Longleftrightarrow (\mathbf{p} \text{ is an anagram of } \mathbf{q})$$

(by the definition of the relation $\underset{\text{perm}}{\sim}$). Applying this to $\mathbf{p} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{q} = (b_1, b_2, \ldots, b_k)$, we obtain the equivalence

$$\begin{aligned} &\left((a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)\right) \\ &\Longleftrightarrow ((a_1, a_2, \ldots, a_k) \text{ is an anagram of } (b_1, b_2, \ldots, b_k)). \end{aligned}$$

Hence, $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$ (since $(a_1, a_2, \ldots, a_k)$ is an anagram of $(b_1, b_2, \ldots, b_k)$). This proves Proposition 7.66.3. □

We can now easily solve Exercise 3.3.2:

Solution to Exercise 3.3.2. We begin with three simple observations:

> *Observation 1:* Each $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ can be written in the form $[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$.

[*Proof of Observation 1:* Let $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$. Thus, α is an unordered k-tuple of elements of A. In other words, α is an equivalence class of $\underset{\text{perm}}{\sim}$ (since the unordered k-tuples of elements of A are defined to be the equivalence classes of $\underset{\text{perm}}{\sim}$). In other words, $\alpha = [\mathbf{a}]_{\underset{\text{perm}}{\sim}}$ for some $\mathbf{a} \in A^k$. Consider this $\mathbf{a}$. We can write $\mathbf{a}$ in the form $(a_1, a_2, \ldots, a_k)$ (since $\mathbf{a} \in A^k$). If we write $\mathbf{a}$ in this form, then we obtain

$$\alpha = [\mathbf{a}]_{\underset{\text{perm}}{\sim}} = [(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}} \qquad (\text{since } \mathbf{a} = (a_1, a_2, \ldots, a_k)).$$

Thus, we conclude that α can be written in the form $[(a_1, a_2, \ldots, a_k)]_{\sim \text{perm}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$.

Forget that we fixed α. We thus have shown that each $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ can be written in the form $[(a_1, a_2, \ldots, a_k)]_{\sim \text{perm}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$. This proves Observation 1.]

> *Observation 2:* Let $(a_1, a_2, \ldots, a_k) \in A^k$. Then, the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of A has size k.

[*Proof of Observation 2:* Clearly, $a_1, a_2, \ldots, a_k$ are k elements of A (since $(a_1, a_2, \ldots, a_k) \in A^k$). Hence, Exercise 2.11.1 (applied to $T = A$) shows that the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of A has size k. This proves Observation 2.]

> *Observation 3:* Let $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$. Assume that α has been written in the form $[(a_1, a_2, \ldots, a_k)]_{\sim \text{perm}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$. Then, the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of A depends only on α (but not on the choice of $(a_1, a_2, \ldots, a_k)$).

[*Proof of Observation 3:* We must show that any two choices of $(a_1, a_2, \ldots, a_k) \in A^k$ satisfying $\alpha = [(a_1, a_2, \ldots, a_k)]_{\sim \text{perm}}$ will lead to one and the same multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$.

So let $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_k)$ be two choices of $(a_1, a_2, \ldots, a_k) \in A^k$ satisfying $\alpha = [(a_1, a_2, \ldots, a_k)]_{\sim \text{perm}}$. We must prove that

$$\{b_1, b_2, \ldots, b_k\}_{\text{multi}} = \{c_1, c_2, \ldots, c_k\}_{\text{multi}}.$$

We have $\alpha = [(b_1, b_2, \ldots, b_k)]_{\sim \text{perm}}$ (since $(b_1, b_2, \ldots, b_k)$ is a choice of $(a_1, a_2, \ldots, a_k) \in A^k$ satisfying $\alpha = [(a_1, a_2, \ldots, a_k)]_{\sim \text{perm}}$). Similarly, $\alpha = [(c_1, c_2, \ldots, c_k)]_{\sim \text{perm}}$. Comparing these two equalities, we obtain $[(b_1, b_2, \ldots, b_k)]_{\sim \text{perm}} = [(c_1, c_2, \ldots, c_k)]_{\sim \text{perm}}$.

Exercise 3.3.1 shows that $\sim_{\text{perm}}$ is an equivalence relation on the set A^k. Hence, Proposition 3.3.21 **(e)** (applied to $S = A^k$, $\sim = \sim_{\text{perm}}$, $x = (b_1, b_2, \ldots, b_k)$ and $y = (c_1, c_2, \ldots, c_k)$) shows that we have $(b_1, b_2, \ldots, b_k) \sim_{\text{perm}} (c_1, c_2, \ldots, c_k)$ if and only if $[(b_1, b_2, \ldots, b_k)]_{\sim \text{perm}} = [(c_1, c_2, \ldots, c_k)]_{\sim \text{perm}}$. Thus, we have

$$(b_1, b_2, \ldots, b_k) \sim_{\text{perm}} (c_1, c_2, \ldots, c_k)$$

(since we have $[(b_1, b_2, \ldots, b_k)]_{\sim \text{perm}} = [(c_1, c_2, \ldots, c_k)]_{\sim \text{perm}}$). Therefore, Proposition 7.66.2 (applied to $(b_1, b_2, \ldots, b_k)$ and $(c_1, c_2, \ldots, c_k)$ instead of $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_k)$) yields

$$\{b_1, b_2, \ldots, b_k\}_{\text{multi}} = \{c_1, c_2, \ldots, c_k\}_{\text{multi}}.$$

Thus, we have proved $\{b_1, b_2, \ldots, b_k\}_{\text{multi}} = \{c_1, c_2, \ldots, c_k\}_{\text{multi}}$. As explained, this shows that any any two choices of $(a_1, a_2, \ldots, a_k) \in A^k$ satisfying $\alpha = [(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$ will lead to one and the same multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$. Thus, Observation 3 is proven.]

Now, let Φ denote the map

$$\{\text{unordered } k\text{-tuples of elements of } A\} \to \{\text{size-}k \text{ multisubsets of } A\},$$
$$[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}} \mapsto \{a_1, a_2, \ldots, a_k\}_{\text{multi}}.$$

This map is well-defined, because:

- Each $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ can be written in the form $[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$ (by Observation 1).
- If we write an element $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ in the form $[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$, then $\{a_1, a_2, \ldots, a_k\}_{\text{multi}} \in \{\text{size-}k \text{ multisubsets of } A\}$ (since Observation 2 shows that the multisubset $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ of A has size k).
- If we write an element $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ in the form $[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$, then $\{a_1, a_2, \ldots, a_k\}_{\text{multi}}$ depends only on α (but not on the choice of $(a_1, a_2, \ldots, a_k)$) (by Observation 3).

Now, we shall show that the map Φ is bijective. Indeed, let us prove that Φ is injective and surjective:

[*Proof of the injectivity of* Φ*:* Let $\alpha, \beta \in \{\text{unordered } k\text{-tuples of elements of } A\}$ be such that $\Phi(\alpha) = \Phi(\beta)$. We must show that $\alpha = \beta$.

Observation 1 shows that the element α can be written in the form $[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$ for some $(a_1, a_2, \ldots, a_k) \in A^k$. Similarly, the element β can be written in the form $[(b_1, b_2, \ldots, b_k)]_{\underset{\text{perm}}{\sim}}$ for some $(b_1, b_2, \ldots, b_k) \in A^k$. Consider this $(a_1, a_2, \ldots, a_k)$ and this $(b_1, b_2, \ldots, b_k)$.

From $\alpha = [(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$, we obtain

$$\Phi(\alpha) = \Phi\left([(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}\right) = \{a_1, a_2, \ldots, a_k\}_{\text{multi}} \tag{432}$$

(by the definition of the map Φ). Similarly, from $\beta = [(b_1, b_2, \ldots, b_k)]_{\underset{\text{perm}}{\sim}}$, we obtain

$$\Phi(\beta) = \{b_1, b_2, \ldots, b_k\}_{\text{multi}}.$$

Thus,

$$\Phi(\alpha) = \Phi(\beta) = \{b_1, b_2, \ldots, b_k\}_{\text{multi}}.$$

Comparing this with (432), we obtain

$$\{a_1, a_2, \ldots, a_k\}_{\text{multi}} = \{b_1, b_2, \ldots, b_k\}_{\text{multi}}.$$

Thus, Proposition 7.66.3 yields

$$(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k).$$

Exercise 3.3.1 shows that $\underset{\text{perm}}{\sim}$ is an equivalence relation on the set A^k. Hence, Proposition 3.3.21 **(e)** (applied to $S = A^k$, $\sim = \underset{\text{perm}}{\sim}$, $x = (a_1, a_2, \ldots, a_k)$ and $y = (b_1, b_2, \ldots, b_k)$) shows that we have $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$ if and only if $[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}} = [(b_1, b_2, \ldots, b_k)]_{\underset{\text{perm}}{\sim}}$. Thus, we have

$$[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}} = [(b_1, b_2, \ldots, b_k)]_{\underset{\text{perm}}{\sim}}$$

(since we have $(a_1, a_2, \ldots, a_k) \underset{\text{perm}}{\sim} (b_1, b_2, \ldots, b_k)$). In other words, $\alpha = \beta$ (since $\alpha = [(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}}$ and $\beta = [(b_1, b_2, \ldots, b_k)]_{\underset{\text{perm}}{\sim}}$).

Forget that we fixed α and β. We thus have shown that if $\alpha, \beta \in \{\text{unordered } k\text{-tuples of elements of } A\}$ are two elements such that $\Phi(\alpha) = \Phi(\beta)$, then $\alpha = \beta$. In other words, the map Φ is injective.]

[*Proof of the surjectivity of* Φ: Let $S \in \{\text{size-}k \text{ multisubsets of } A\}$. We shall construct an $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ such that $S = \Phi(\alpha)$.

Indeed, S is a size-k multisubset of A (since $S \in \{\text{size-}k \text{ multisubsets of } A\}$). In other words, S is a multisubset of A having size k. Hence, Proposition 7.66.1 (applied to $T = A$ and $m = k$) yields that there exists a k-tuple $(s_1, s_2, \ldots, s_k)$ of elements of A satisfying $\{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S$. Consider this $(s_1, s_2, \ldots, s_k)$. Consider the corresponding unordered k-tuple $[(s_1, s_2, \ldots, s_k)]_{\underset{\text{perm}}{\sim}}$ of elements of A.

The definition of Φ yields

$$\Phi\left([(s_1, s_2, \ldots, s_k)]_{\underset{\text{perm}}{\sim}}\right) = \{s_1, s_2, \ldots, s_k\}_{\text{multi}} = S.$$

Hence, $S = \Phi\left([(s_1, s_2, \ldots, s_k)]_{\underset{\text{perm}}{\sim}}\right)$. Thus, there exists an $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ such that $S = \Phi(\alpha)$ (namely, $\alpha = [(s_1, s_2, \ldots, s_k)]_{\underset{\text{perm}}{\sim}}$).

Forget that we fixed S. We thus have shown that for each $S \in \{\text{size-}k \text{ multisubsets of } A\}$, there exists an $\alpha \in \{\text{unordered } k\text{-tuples of elements of } A\}$ such that $S = \Phi(\alpha)$. In other words, the map Φ is surjective.]

We have now proved that the map Φ is injective and that the map Φ is surjective. Hence, the map Φ is bijective. In other words, the map

$$\{\text{unordered } k\text{-tuples of elements of } A\} \to \{\text{size-}k \text{ multisubsets of } A\},$$
$$[(a_1, a_2, \ldots, a_k)]_{\underset{\text{perm}}{\sim}} \mapsto \{a_1, a_2, \ldots, a_k\}_{\text{multi}}$$

is bijective (since this map is precisely the map we called Φ). Moreover, as we have already seen, this map is well-defined. Since this map is bijective, we conclude that the unordered k-tuples of elements of A are in bijection with the size-k multisubsets of A. Thus, Exercise 3.3.2 is solved. □

7.67. Solution to Exercise 3.3.3

In order to solve Exercise 3.3.3, we need to prove Proposition 3.3.29.

Proof of Proposition 3.3.29. Let us first prove that the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ is an equivalence relation. To that end, we need to prove that this relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ is reflexive, symmetric and transitive. We shall prove these three properties one by one:

[*Proof of reflexivity:* We must show that the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ is reflexive. In other words, we must prove that every $a \in \{\text{maps } A \to X\}$ satisfies $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} a$.

So let $a \in \{\text{maps } A \to X\}$ be arbitrary. Thus, a is a map from A to X. Now, the identity maps $\mathrm{id}_X : X \to X$ and $\mathrm{id}_A : A \to A$ are permutations of X and A, respectively, and satisfy $a = \mathrm{id}_X \circ a \circ \mathrm{id}_A$. Hence, there exist a permutation σ of X and a permutation τ of A such that $a = \sigma \circ a \circ \tau$ (namely, $\sigma = \mathrm{id}_X$ and $\tau = \mathrm{id}_A$). In other words, we have $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} a$ (by the definition of the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$).

We thus have shown that every $a \in \{\text{maps } A \to X\}$ satisfies $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} a$. In other words, the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ is reflexive.]

[*Proof of symmetry:* We must show that the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ is symmetric. In other words, we must prove that every $a, b \in \{\text{maps } A \to X\}$ satisfying $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} b$ satisfy $b \underset{\text{ball}}{\overset{\text{box}}{\sim}} a$.

So let $a, b \in \{\text{maps } A \to X\}$ satisfy $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} b$. Thus, a and b are maps from A to X. From $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} b$, we conclude that there exist a permutation σ of X and a permutation τ of A such that $a = \sigma \circ b \circ \tau$ (by the definition of the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$). Let us consider these σ and τ, and denote them by ξ and α, respectively. Thus, ξ is a permutation

of X, and α is a permutation of A, and they satisfy $a = \xi \circ b \circ \alpha$. The two maps ξ and α are bijective (since they are permutations), therefore invertible. Hence, their inverses ξ^{-1} and α^{-1} exist.

However, Proposition 7.65.1 **(b)** (applied to $S = X$ and $\sigma = \xi$) yields that ξ^{-1} is a permutation of X (since ξ is a permutation of X). Likewise, α^{-1} is a permutation of A. Moreover, solving the equality $a = \xi \circ b \circ \alpha$ for b, we obtain $b = \xi^{-1} \circ a \circ \alpha^{-1}$ (since $\xi^{-1} \circ \underbrace{a}_{=\xi\circ b\circ\alpha} \circ\alpha^{-1} = \underbrace{\xi^{-1} \circ \xi}_{=\mathrm{id}_X} \circ b \circ \underbrace{\alpha \circ \alpha^{-1}}_{=\mathrm{id}_A} = b$). Thus, there exist a permutation σ of X and a permutation τ of A such that $b = \sigma \circ a \circ \tau$ (namely, $\sigma = \xi^{-1}$ and $\tau = \alpha^{-1}$). In other words, we have $b \overset{\text{box}}{\underset{\text{ball}}{\sim}} a$ (by the definition of the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$).

We thus have shown that every $a, b \in \{\text{maps } A \to X\}$ satisfying $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} b$ satisfy $b \overset{\text{box}}{\underset{\text{ball}}{\sim}} a$. In other words, the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$ is symmetric.]

[*Proof of transitivity:* We must show that the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$ is transitive. In other words, we must prove that every $a, b, c \in \{\text{maps } A \to X\}$ satisfying $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} b$ and $b \overset{\text{box}}{\underset{\text{ball}}{\sim}} c$ satisfy $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} c$.

So let $a, b, c \in \{\text{maps } A \to X\}$ satisfy $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} b$ and $b \overset{\text{box}}{\underset{\text{ball}}{\sim}} c$. Thus, a, b and c are maps from A to X.

From $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} b$, we conclude that there exist a permutation σ of X and a permutation τ of A such that $a = \sigma \circ b \circ \tau$ (by the definition of the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$). Let us consider these σ and τ, and denote them by σ_1 and τ_1, respectively. Thus, σ_1 is a permutation of X, and τ_1 is a permutation of A, and they satisfy $a = \sigma_1 \circ b \circ \tau_1$.

From $b \overset{\text{box}}{\underset{\text{ball}}{\sim}} c$, we conclude that there exist a permutation σ of X and a permutation τ of A such that $b = \sigma \circ c \circ \tau$ (by the definition of the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$). Let us consider these σ and τ, and denote them by σ_2 and τ_2, respectively. Thus, σ_2 is a permutation of X, and τ_2 is a permutation of A, and they satisfy $b = \sigma_2 \circ c \circ \tau_2$.

Proposition 7.65.1 **(a)** (applied to $S = X$) yields that $\sigma_1 \circ \sigma_2$ is a permutation of X (since σ_1 and σ_2 are permutations of X). Likewise, using Proposition 7.65.1 **(a)**, we see that $\tau_2 \circ \tau_1$ is a permutation of A (since τ_2 and τ_1 are permutations of A). Moreover, we have

$$a = \sigma_1 \circ \underbrace{b}_{=\sigma_2\circ c\circ\tau_2} \circ\tau_1 = \sigma_1 \circ \sigma_2 \circ c \circ \tau_2 \circ \tau_1 = (\sigma_1 \circ \sigma_2) \circ c \circ (\tau_2 \circ \tau_1) .$$

Thus, there exist a permutation σ of X and a permutation τ of A such that $a = \sigma \circ c \circ \tau$ (namely, $\sigma = \sigma_1 \circ \sigma_2$ and $\tau = \tau_2 \circ \tau_1$). In other words, we have $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} c$ (by

the definition of the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$).

We thus have shown that every $a, b, c \in \{\text{maps } A \to X\}$ satisfying $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} b$ and $b \overset{\text{box}}{\underset{\text{ball}}{\sim}} c$ satisfy $a \overset{\text{box}}{\underset{\text{ball}}{\sim}} c$. In other words, the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$ is transitive.]

We have now proved that the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$ is reflexive, symmetric and transitive. In other words, this relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$ is an equivalence relation. Analogous arguments show that the relations $\overset{\text{box}}{\sim}$ and $\overset{\text{ball}}{\sim}$ are equivalence relations. Thus, Proposition 3.3.29 is proved. □

7.68. Solution to Exercise 3.3.4

In order to solve Exercise 3.3.4, we need to prove Proposition 3.3.32 and Corollary 3.3.33. Let us do this:

Proof of Proposition 3.3.32. **(a)** Assume that f is injective. We must prove that g is injective.

We have assumed that $f \overset{\text{box}}{\sim} g$ or $f \overset{\text{ball}}{\sim} g$ or $f \overset{\text{box}}{\underset{\text{ball}}{\sim}} g$. Thus, we are in one of the following three cases:

Case 1: We have $f \overset{\text{box}}{\sim} g$.
Case 2: We have $f \underset{\text{ball}}{\sim} g$.
Case 3: We have $f \overset{\text{box}}{\underset{\text{ball}}{\sim}} g$.

We shall only consider Case 3, since the arguments in the other two cases are very similar.

So let us consider Case 3. In this case, we have $f \overset{\text{box}}{\underset{\text{ball}}{\sim}} g$. In other words, there exist a permutation σ of X and a permutation τ of A such that $f = \sigma \circ g \circ \tau$ (by the definition of the relation $\overset{\text{box}}{\underset{\text{ball}}{\sim}}$). Consider these σ and τ.

The maps σ and τ are bijective (because they are permutations), and thus invertible. Hence, their inverses σ^{-1} and τ^{-1} are well-defined. These inverses σ^{-1} and τ^{-1} are furthermore invertible, thus bijective, thus injective.

Moreover, from $f = \sigma \circ g \circ \tau$, we obtain

$$\sigma^{-1} \circ \underbrace{f}_{=\sigma \circ g \circ \tau} \circ \tau^{-1} = \underbrace{\sigma^{-1} \circ \sigma}_{=\mathrm{id}_X} \circ g \circ \underbrace{\tau \circ \tau^{-1}}_{=\mathrm{id}_A} = g.$$

However, a composition of several injective maps is always injective. Thus, the map $\sigma^{-1} \circ f \circ \tau^{-1}$ is injective (since it is the composition of the injective maps σ^{-1}, f and τ^{-1}). In other words, the map g is injective (since $\sigma^{-1} \circ f \circ \tau^{-1} = g$). Hence, we

have completed the proof of Proposition 3.3.32 **(a)** in Case 3. As we said above, the other two cases are very similar. Hence, Proposition 3.3.32 **(a)** is proven.

(b) The proof of Proposition 3.3.32 **(b)** is analogous to the proof of Proposition 3.3.32 **(a)**; we just need to replace the word "injective" by the word "surjective" everywhere. □

Proof of Corollary 3.3.33. **(a)** Assume that C contains an injective map. We must prove that every map in C is injective.

We have assumed that C is a $U \to L$ placement or an $L \to U$ placement or a $U \to U$ placement. Thus, we are in one of the following three cases:

Case 1: The set C is a $U \to L$ placement.

Case 2: The set C is an $L \to U$ placement.

Case 3: The set C is a $U \to U$ placement.

We shall only consider Case 3, since the arguments in the other two cases are analogous.

So let us consider Case 3. In this case, C is a $U \to U$ placement. In other words, C is a $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$-equivalence class (since the $U \to U$ placements are defined to be the $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$-equivalence classes). In other words, $C = [a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}}$ for some $a \in \{\text{maps } A \to X\}$ (since the $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$-equivalence classes are defined to be the sets of the form $[a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}}$ for $a \in \{\text{maps } A \to X\}$). Consider this a.

Recall that the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ is an equivalence relation, thus is transitive.

We have assumed that C contains an injective map. Let f be this map. Thus, f is an injective map from A to X, and belongs to C. Hence, $f \in C = [a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}} \subseteq \{\text{maps } A \to X\}$. However, Proposition 3.3.21 **(c)** (applied to $S = \{\text{maps } A \to X\}$, $\sim = \underset{\text{ball}}{\overset{\text{box}}{\sim}}$, $x = f$ and $y = a$) yields that we have $f \underset{\text{ball}}{\overset{\text{box}}{\sim}} a$ if and only if $f \in [a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}}$. Hence, we have $f \underset{\text{ball}}{\overset{\text{box}}{\sim}} a$ (since we have $f \in [a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}}$).

Now, let $g \in C$ be arbitrary. Thus, $g \in C = [a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}} \subseteq \{\text{maps } A \to X\}$. However, Proposition 3.3.21 **(d)** (applied to $S = \{\text{maps } A \to X\}$, $\sim = \underset{\text{ball}}{\overset{\text{box}}{\sim}}$, $x = a$ and $y = g$) yields that we have $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} g$ if and only if $g \in [a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}}$. Thus, we have $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} g$ (since we have $g \in [a]_{\underset{\text{ball}}{\overset{\text{box}}{\sim}}}$).

Combining $f \underset{\text{ball}}{\overset{\text{box}}{\sim}} a$ and $a \underset{\text{ball}}{\overset{\text{box}}{\sim}} g$, we obtain $f \underset{\text{ball}}{\overset{\text{box}}{\sim}} g$ (since the relation $\underset{\text{ball}}{\overset{\text{box}}{\sim}}$ is transitive). Therefore, Proposition 3.3.32 **(a)** yields that g is injective (since f is injective).

Forget that we fixed g. We thus have proved that every $g \in C$ is injective. In other words, every map in C is injective. This proves Corollary 3.3.33 **(a)** in Case

3. As we mentioned above, the other two cases are analogous. Hence, Corollary 3.3.33 **(a)** is proven.

(b) The proof of Corollary 3.3.33 **(b)** is analogous to the proof of Corollary 3.3.33 **(a)**; we just need to replace the word "injective" by the word "surjective" everywhere (and use Proposition 3.3.32 **(b)** instead of Proposition 3.3.32 **(a)**). □

References

[17f-hw1s] Darij Grinberg, *UMN Fall 2017 Math 4707 & Math 4990 homework set #1 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw1s.pdf`

[17f-hw2s] Darij Grinberg, *UMN Fall 2017 Math 4707 & Math 4990 homework set #2 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw2s.pdf`

[17f-hw3s] Darij Grinberg, *UMN Fall 2017 Math 4990 homework set #3 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw3os.pdf`

[17f-hw4s] Darij Grinberg, *UMN Fall 2017 Math 4990 homework set #4 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw4os.pdf`

[17f-hw5s] Darij Grinberg, *UMN Fall 2017 Math 4990 homework set #5 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw5os.pdf`

[17f-hw6s] Darij Grinberg, *UMN Fall 2017 Math 4990 homework set #6 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw6os.pdf`

[17f-hw7s] Darij Grinberg, *UMN Fall 2017 Math 4990 homework set #7 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw7os.pdf`

[17f-hw8s] Darij Grinberg, *UMN Fall 2017 Math 4990 homework set #8 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw8os.pdf`

[18f] Darij Grinberg, *UMN Fall 2018 Math 5705: "black"board notes*, `https://www.cip.ifi.lmu.de/~grinberg/t/18f/`

[18f-hw1s] Darij Grinberg, *UMN Fall 2018 Math 5705 homework set #1 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw1s.pdf`

[18f-hw2s] Darij Grinberg, *UMN Fall 2018 Math 5705 homework set #2 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw2s.pdf`

[18f-hw3s] Darij Grinberg, *UMN Fall 2018 Math 5705 homework set #3 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw3s.pdf`

[18f-hw4s] Darij Grinberg, *UMN Fall 2018 Math 5705 homework set #4 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw4s.pdf`

[18f-mt1s] Darij Grinberg, *UMN Fall 2018 Math 5705 midterm #1 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18f/mt1s.pdf

[18f-mt2s] Darij Grinberg, *UMN Fall 2018 Math 5705 midterm #2 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18f/mt2s.pdf

[18f-mt3s] Darij Grinberg, *UMN Fall 2018 Math 5705 midterm #3 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18f/mt3s.pdf

[18s] Darij Grinberg, *UMN Spring 2018 Math 4707: "black"board notes*, https://www.cip.ifi.lmu.de/~grinberg/t/18s/

[18s-hw1s] Darij Grinberg, *UMN Spring 2018 Math 4707 homework set #1 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18s/hw1s.pdf

[18s-hw2s] Darij Grinberg, *UMN Spring 2018 Math 4707 homework set #2 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18s/hw2s.pdf

[18s-hw3s] Darij Grinberg, *UMN Spring 2018 Math 4707 homework set #3 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18s/hw3s.pdf

[18s-hw4s] Darij Grinberg, *UMN Spring 2018 Math 4707 homework set #4 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18s/hw4s.pdf

[18s-hw5s] Darij Grinberg, *UMN Spring 2018 Math 4707 homework set #5 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18s/hw5s.pdf

[18s-mt1s] Darij Grinberg, *UMN Spring 2018 Math 4707 midterm #1 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18s/mt1s.pdf

[18s-mt2s] Darij Grinberg, *UMN Spring 2018 Math 4707 midterm #2 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/18s/mt2s.pdf

[19f-hw0s] Darij Grinberg, *Drexel Fall 2019 Math 222 homework set #0 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/hw0s.pdf

[19f-hw1s] Darij Grinberg, *Drexel Fall 2019 Math 222 homework set #1 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/hw1s.pdf

[19f-hw2s] Darij Grinberg, *Drexel Fall 2019 Math 222 homework set #2 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/hw2s.pdf

[19f-hw3s] Darij Grinberg, *Drexel Fall 2019 Math 222 homework set #3 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/hw3s.pdf

[19f-hw4s] Darij Grinberg, *Drexel Fall 2019 Math 222 homework set #4 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/hw4s.pdf

[19f-mt1s] Darij Grinberg, *Drexel Fall 2019 Math 222 midterm #1 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/mt1s.pdf

[19f-mt2s] Darij Grinberg, *Drexel Fall 2019 Math 222 midterm #2 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/mt2s.pdf

[19f-mt3s] Darij Grinberg, *Drexel Fall 2019 Math 222 midterm #3 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19fco/mt3s.pdf

[19s] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019.
http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf

[19s-hw0s] Darij Grinberg, *UMN Spring 2019 Math 4281 homework set #0 with solutions*, http://www.cip.ifi.lmu.de/~grinberg/t/19s/hw0s.pdf

[21s] Darij Grinberg, *Algebraic Combinatorics (Drexel Spring 2021 Math 701 lecture notes)*, 4 May 2021.
https://www.cip.ifi.lmu.de/~grinberg/t/21s/lecs.pdf

[Aigner07] Martin Aigner, *A Course in Enumeration*, Graduate Texts in Mathematics #238, Springer 2007.

[AigZie14] Martin Aigner, Günter M. Ziegler, *Proofs from the Book*, 6th edition, Springer 2018.

[AndEri04] George E. Andrews, Kimmo Eriksson, *Integer Partitions*, Cambridge University Press 2004.

[AndFen04] Titu Andreescu, Zuming Feng, *A Path to Combinatorics for Undergraduates: Counting Strategies*, Springer 2004.

[Andrew16] George E. Andrews, *Euler's Partition Identity – Finite Version*, 2016.
http://www.personal.psu.edu/gea1/pdf/317.pdf

[ArdSta10] Federico Ardila, Richard P. Stanley, *Tilings*, The Mathematical Intelligencer **32** (2010), pp. 32–43. A preprint can be found at arXiv:math/0501170v3 .

[BCHR11] Fred Butler, Mahir Can, Jim Haglund, Jeffrey B. Remmel, *Rook Theory Notes*, 3 January 2011.
https://mathweb.ucsd.edu/~remmel/files/Book.pdf

[BenDre07] Arthur T. Benjamin and Gregory P. Dresden, *A Combinatorial Proof of Vandermonde's Determinant*, The American Mathematical Monthly, Vol. 114, No. 4 (Apr., 2007), pp. 338–341.
(Also available at http://scholarship.claremont.edu/hmc_fac_pub/524/ .)

[BenQui03] Arthur T. Benjamin and Jennifer J. Quinn, *Proofs that Really Count: The Art of Combinatorial Proof*, Dolciani Mathematical Expositions **27**, The Mathematical Association of America, 2003.

[BenQui04] Arthur T. Benjamin and Jennifer J. Quinn, *Proofs that Really Count: The Magic of Fibonacci Numbers and More*, Mathematical Adventures for Students and Amateurs, (David F. Hayes and Tatiana Shubin, editors), Spectrum Series of MAA, pp. 83–98, 2004.

[BenQui08] Arthur T. Benjamin and Jennifer J. Quinn, *An Alternate Approach to Alternating Sums: A Method to DIE for*, The College Mathematics Journal, Volume 39, Number 3, May 2008, pp. 191-202(12).

[Bona22] Miklos Bóna, *Combinatorics of Permutations*, 3rd edition, Taylor&Francis 2022.
https://doi.org/10.1201/9780429274107

[Bourba68] Nicolas Bourbaki, *Theory of Sets*, Springer 1968.

[Chu19] Hùng Việt Chu, *The Fibonacci Sequence and Schreier-Zeckendorf Sets*, Journal of Integer Sequences, **22** (2019), Article 19.6.5.
https://cs.uwaterloo.ca/journals/JIS/VOL22/Chu2/chu9.html

[CoLiOs15] David A. Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 4th edition, Springer 2015.

[Comtet74] Louis Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, D. Reidel Publishing Company, 1974.

[Day16] Martin V. Day, *An Introduction to Proofs and the Mathematical Vernacular*, 7 December 2016.
https://web.archive.org/web/20180712152432/https://www.math.vt.edu/people/day/ProofsBook/IPaMV.pdf .

[Elman22] Richard Elman, *Lectures on Abstract Algebra*, 8 September 2022.
https://www.math.ucla.edu/~rse/algebra_book.pdf

[GalQua22] Jean Gallier and Jocelyn Quaintance, *Algebra, Topology, Differential Calculus, and Optimization Theory For Computer Science and Machine Learning*, 18 March 2022.
https://www.cis.upenn.edu/~jean/gbooks/geomath.html

[Galvin17] David Galvin, *Basic discrete mathematics*, 13 December 2017.
http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf
(The URL might change, and the text may get updated. In order to reliably obtain the version of 13 December 2017, you can use the archive.org Wayback Machine: https://web.archive.org/web/20180205122609/http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf .)

[Goodma15] Frederick M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6, 1 May 2015.
http://homepage.math.uiowa.edu/~goodman/algebrabook.dir/book.2.6.pdf .

[Gould72] H. W. Gould, *A New Symmetrical Combinatorial Identity*, Journal of Combinatorial Theory A **13** (1972), pp. 278–286.

[Granvi05] Andrew Granville, *Binomial coefficients modulo prime powers*, preprint.
https://web.archive.org/web/20181024055320/http://ebooks.bharathuniv.ac.in/gdlc1/gdlc1/EngineeringMergedLibraryv3.0/AndrewGranville/BinomialCoefficientsModuloPrimePowers(5579)/BinomialCoefficientsModuloPrimePowers-AndrewGranville.pdf

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 15 September 2022.
http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2022-09-15c .

[Grinbe16a] Darij Grinberg, *Notes on linear algebra*, version of 13 December 2016.
https://github.com/darijgr/lina

[Grinbe16b] Darij Grinberg, *4th QEDMO, Problem 13 with solution*, version of 28 May 2016.
http://www.cip.ifi.lmu.de/~grinberg/QEDMO4P13.pdf

[Grinbe17] Darij Grinberg, *The Lucas and Babbage congruences*, 10 January 2019.
https://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf

[GrKnPa94] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.
See https://www-cs-faculty.stanford.edu/~knuth/gkp.html for errata.

[Guicha20] David Guichard, *An Introduction to Combinatorics and Graph Theory*, 4 March 2023.
https://www.whitman.edu/mathematics/cgt_online/book/

[Hammac15] Richard Hammack, *Book of Proof*, 3rd edition.
https://www.people.vcu.edu/~rhammack/BookOfProof/

[Joyce17] David Joyce, *Introduction to Modern Algebra*, 5 December 2017.
https://mathcs.clarku.edu/~djoyce/ma225/algebra.pdf

[Joyner08] W. D. Joyner, *Mathematics of the Rubik's cube*, 19 August 2008. https://web.archive.org/web/20160304122348/http://www.permutationpuzzles.org/rubik/webnotes/ (link to the PDF at the bottom).

[Kastel61] P. W. Kasteleyn, *The statistics of dimers on a lattice: I. The number of dimer arrangements on a quadratic lattice*, Physica **27** (1961), pp. 1209–1225. https://doi.org/10.1016/0031-8914(61)90063-5

[Knapp16] Anthony W. Knapp, *Basic Algebra*, digital second edition 2016. http://www.math.stonybrook.edu/~aknapp/download.html

[Knuth93] Donald E. Knuth, *Johann Faulhaber and sums of powers*, Math. Comp. **61** (1993), no. 203, 277–294. https://www.ams.org/journals/mcom/1993-61-203/S0025-5718-1993-1197512-7/

[Kratte17] Christian Krattenthaler, *Lattice Path Enumeration*, arXiv:1503.05930v3, published in: Handbook of Enumerative Combinatorics, M. Bóna (ed.), Discrete Math. and Its Appl., CRC Press, Boca Raton-London-New York, 2015, pp. 589–678. https://arxiv.org/abs/1503.05930v3

[LeLeMe16] Eric Lehman, F. Thomson Leighton, Albert R. Meyer, *Mathematics for Computer Science*, revised Tuesday 6th June 2018, https://courses.csail.mit.edu/6.042/spring18/mcs.pdf .

[LLPT95] D. Laksov, A. Lascoux, P. Pragacz, and A. Thorup, *The LLPT Notes*, edited by A. Thorup, 1995, https://web.math.ku.dk/noter/filer/sympol.pdf .

[Loehr11] Nicholas A. Loehr, *Bijective Combinatorics*, Chapman & Hall/CRC 2011.

[Loehr20] Nicholas A. Loehr, *An Introduction to Mathematical Proofs*, CRC Press 2020.

[Mestro14] Romeo Meštrović, *Lucas' theorem: its generalizations, extensions and applications (1878–2014)*, arXiv:1409.3820v1.

[MusPro07] Gregg Musiker, James Propp, *Combinatorial Interpretations for Rank-Two Cluster Algebras of Affine Type*, The Electronic Journal of Combinatorics **14** (2007), #R15. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v14i1r15

[Newste19] Clive Newstead, *An Infinite Descent into Pure Mathematics*, version 0.4, 1 January 2020. https://infinitedescent.xyz

[Niven69] Ivan Niven, *Formal Power Series*, The American Mathematical Monthly **76**, No. 8 (Oct., 1969), pp. 871–889.
https://www.maa.org/programs/maa-awards/writing-awards/formal-power-series

[Read80] Ronald C. Read, *A Note on Tiling Rectangles with Dominoes*, Fibonacci Quarterly **18** (1980), pp. 24–27.
https://www.fq.math.ca/Scanned/18-1/read.pdf

[Sagan01] Bruce Sagan, *The Symmetric Group*, Graduate Texts in Mathematics **203**, 2nd edition 2001.
https://doi.org/10.1007/978-1-4757-6804-6
See https://users.math.msu.edu/users/bsagan/Books/Sym/errata.pdf for errata.

[Sagan19] Bruce Sagan, *Combinatorics: The Art of Counting*, preliminary version, 7 January 2020.
https://users.math.msu.edu/users/bsagan/Books/Aoc/final.pdf

[sage] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2019, https://www.sagemath.org .

[SageBook] Paul Zimmermann et al, *Computational Mathematics with SageMath*, December 2018.
https://www.sagemath.org/sagebook/

[Siu84] Man-Keung Siu, *Proof without words: Sum of squares*, Mathematics Magazine **57** (1984), issue 2, page 92.

[Smid09] Vita Smid, *Inclusion-Exclusion Principle: Proof by Mathematical Induction*, 2 December 2009.
https://faculty.math.illinois.edu/~nirobles/files453/iep_proof.pdf

[Stanle15] Richard P. Stanley, *Catalan Numbers*, 1st edition 2015.
See http://math.mit.edu/~rstan/catalan/ for errata.

[Stanle11] Richard P. Stanley, *Enumerative Combinatorics, volume 1*, Second edition, version of 15 July 2011. Available at http://math.mit.edu/~rstan/ec/ .
See http://math.mit.edu/~rstan/ec/ for errata.

[Stanle01] Richard P. Stanley, *Enumerative Combinatorics, volume 2*, First edition, Cambridge University Press 2001.
See http://math.mit.edu/~rstan/ec/ for errata.

[Strick13] Neil Strickland, *MAS201 Linear Mathematics for Applications*, lecture notes, 28 September 2013.
https://neilstrickland.github.io/linear_maths/

[Stucky15] Eric Stucky, *An Exposition of Kasteleyn's Solution of the Dimer Model*, senior thesis at Harvey Mudd College, 2015.
https://scholarship.claremont.edu/hmc_theses/89/

[Tou17] Erik R. Tou, *Math Origins: The Totient Function*, Convergence (September 2017), DOI:10.4169/convergence20170923.
https://www.maa.org/press/periodicals/convergence/math-origins-the-totient-function

[Uecker17] Torsten Ueckerdt, *Lecture Notes Combinatorics (2017)*, 30 May 2017.
http://www.math.kit.edu/iag6/lehre/combinatorics2017s/media/script.pdf
See http://www.cip.ifi.lmu.de/~grinberg/algebra/ueckerdt-script2017-errata.pdf for an inofficial list of errata.

[UspHea39] J. V. Uspensky, M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill 1939.

[Vorobi02] Nicolai N. Vorobiev, *Fibonacci Numbers*, Translated from the Russian by Mircea Martin, Springer 2002 (translation of the 6th Russian edition).

[Walker87] Elbert A. Walker, *Introduction to Abstract Algebra*, Random House/Birkhauser, New York, 1987.

[Ward91] James Ward, *100 years of Dixon's identity*, Irish Mathematical Society Bulletin **27** (1991), pp. 46–54.
https://www.maths.tcd.ie/pub/ims/bull27/bull27_46-54.pdf

[Warner71] Seth Warner, *Classical Modern Algebra*, Prentice-Hall 1971.

[White10] Dennis White, *Math 4707: Inclusion-Exclusion and Derangements*, 18 October 2010.
https://www-users.cse.umn.edu/~reiner/Classes/Derangements.pdf

[Wilf04] Herbert S. Wilf, *generatingfunctionology*, 2nd edition 2004.
https://www2.math.upenn.edu/~wilf/DownldGF.html

[Wilf09] Herbert S. Wilf, *Lectures on Integer Partitions*, 2009.
https://www2.math.upenn.edu/~wilf/PIMS/PIMSLectures.pdf

[Yashin15] Allan Yashinski, *Math 325 – Equivalence Relations, Well-definedness, Modular Arithmetic, and the Rational Numbers*, 13 October 2015.
https://math.hawaii.edu/~allan/WellDefinedness.pdf