Drexel University, Department of Mathematics

Math 222: Enumerative Combinatorics, Fall 2019: Homework 0

Darij Grinberg

September 27, 2019

This document serves several purposes:

1. demonstrate how mathematical prose is written in LaTeX.
2. introduce some basic conventions and facts that will be used in this combinatorics class, such as the product rule (see the solution of Exercise 1 below) or the telescope principle (see the solution of Exercise 2 below) or the conventions for empty sums and empty products.
3. give examples of rigorous proofs in combinatorics (as opposed to handwavy explanations that the reader either "gets" or doesn't).

Some caveats are in order. The use of LaTeX is highly recommended but not required; simple or short arguments can be written equally well in systems like Microsoft Office or even as plain text (LaTeX is best for long-form with lots of formulas, cross-references and citations). The proofs given below are, in many ways, more rigorous and detailed than necessary; they intend to alert you to the tacit details "under the hood" of many common-sense arguments, but you don't have to write at this level of detail.

1 Exercise 1

1.1 Problem

Let $n \in \mathbb{N}$. (Here and in the following, $\mathbb{N}$ stands for the set $\{0, 1, 2, \ldots\}$.)

(a) Show that the number of all subsets of $\{1, 2, \ldots, n\}$ is 2^n.

(b) A *composition* of n shall mean a list[1] $(i_1, i_2, \ldots, i_k)$ of positive integers such that $i_1 + i_2 + \cdots + i_k = n$. (For example, the compositions of 3 are (3), $(1, 2)$, $(2, 1)$ and $(1, 1, 1)$.)

Show that the number of all compositions of n is

$$\begin{cases} 2^{n-1}, & \text{if } n > 0; \\ 1, & \text{if } n = 0. \end{cases}$$

1.2 Solution

Let us first introduce two shorthand notations:

1. If $\mathcal{A}$ is any statement (such as "$1+1=2$" or "$1+1=1$" or "there exist infinitely many primes"), then $[\mathcal{A}]$ stands for the number

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

This number belongs to $\{0, 1\}$, and is called the *truth value* of $\mathcal{A}$. For example,

$$[1+1=2] = 1, \qquad [1+1=1] = 0, \qquad [\text{there exist infinitely many primes}] = 1.$$

This shorthand is called the *Iverson bracket notation.*

2. If $m \in \mathbb{Z}$, then $[m]$ shall mean the set $\{1, 2, \ldots, m\}$. When $m \leq 0$, this is understood to be the empty set.

These two shorthand notations use the same symbol (square brackets), but they will never clash, since the former always has a statement inside the square brackets, whereas the latter always has an integer inside the square brackets.

Recall the following basic principle (known as the *product rule*):

Proposition 1.1. *If $m \in \mathbb{N}$, and if $A_1, A_2, \ldots, A_m$ are m finite sets, then the Cartesian product $A_1 \times A_2 \times \cdots \times A_m$ is a finite set again, and satisfies*

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_m| . \tag{1}$$

(Note that if $m = 0$, then the Cartesian product $A_1 \times A_2 \times \cdots \times A_m$ has 0 factors; in this case it just consists of a single element, which is the 0-tuple $()$. Meanwhile, in this case, the right hand side of (1) becomes a product of 0 numbers, which is 1 by definition. Thus, (1) turns into "$1 = 1$" when $m = 0$.)

Applying (1) to $m = n$ and $A_i = \{0, 1\}$, we get

$$\left| \underbrace{\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}}_{n \text{ factors}} \right| = \underbrace{|\{0,1\}| \cdot |\{0,1\}| \cdot \cdots \cdot |\{0,1\}|}_{n \text{ factors}} .$$

This rewrites as

$$\left| \{0,1\}^n \right| = \left| \{0,1\} \right|^n . \tag{2}$$

[1] "List" means the same as "tuple"; lists are always ordered and finite.

Here, we are using the standard notation S^n (where S is a set and $n \in \mathbb{N}$) for the Cartesian product $\underbrace{S \times S \times \cdots \times S}_{n \text{ factors}}$. In view of $|\{0,1\}| = 2$, we can rewrite (2) as

$$|\{0,1\}^n| = 2^n. \tag{3}$$

Note that $\{0,1\}^n$ is the set of all n-tuples of elements of $\{0,1\}$. These are also known as "binary strings of length n". For example, $(0,1,1,0,1,0) \in \{0,1\}^6$.

Another basic principle (some call it the *bijection principle*) is the following:

Proposition 1.2. *If X and Y are two sets, and if $f : X \to Y$ is a bijection (i.e., a bijective map), then*

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

In other words, if there is a bijection between two sets, then these two sets have the same size.

Note that the size of a set is in general just a cardinal number. But if the set is finite, this cardinal number is an actual nonnegative integer.

Part **(a)** of the exercise asks us to show that the number of all subsets of $\{1,2,\ldots,n\}$ is 2^n. In other words, it asks us to show that the number of all subsets of $[n]$ is 2^n (since $[n] = \{1,2,\ldots,n\}$). In other words, it asks us to show that

$$|\{\text{subsets of } [n]\}| = 2^n. \tag{5}$$

We will show this by constructing a bijection from the set $\{\text{subsets of } [n]\}$ to $\{0,1\}^n$. This will then let us apply (4) and (3) and obtain (5). So let us construct such a bijection:

We define the map $A : \{\text{subsets of } [n]\} \to \{0,1\}^n$ by setting

$$A(S) = ([1 \in S], [2 \in S], \ldots, [n \in S]) \qquad \text{for each subset } S \text{ of } [n].$$

(This is well-defined, since each of the truth values $[1 \in S], [2 \in S], \ldots, [n \in S]$ belongs to $\{0,1\}$.) For example, if $n = 5$ and $S = \{2,4,5\}$, then $A(S) = (0,1,0,1,1)$. (Some call $A(S)$ the *indicator vector* of S, since its i-th entry indicates whether i belongs to S or not.)

We want to show that A is a bijection. There are two standard ways to prove that a map is a bijection: One is to show that it is injective and surjective; another is to exhibit its inverse. Either of these ways works here; we shall use the latter.

We define the map $B : \{0,1\}^n \to \{\text{subsets of } [n]\}$ by setting

$$B((i_1, i_2, \ldots, i_n)) = \{k \in [n] \mid i_k = 1\} \qquad \text{for each } (i_1, i_2, \ldots, i_n) \in \{0,1\}^n.$$

We want to show that the maps A and B are mutually inverse. In order to do this, we must show that $A \circ B = \text{id}$ and that $B \circ A = \text{id}$. (We are using the notation "id" for an identity map. We don't specify which set this map acts on, since it is clear from the context: For example, in "$A \circ B = \text{id}$", the "id" must be the identity map of $\{0,1\}^n$, because the domain of $A \circ B$ is $\{0,1\}^n$. If you really want to be precise, you could denote this identity map by $\text{id}_{\{0,1\}^n}$.) So let us prove this[2]:

- In order to show that $A \circ B = \text{id}$, we fix some $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$. We shall show that $(A \circ B)((i_1, i_2, \ldots, i_n)) = (i_1, i_2, \ldots, i_n)$.

[2] On an actual homework set, you can leave both of these proofs to the reader. I am merely demonstrating the basics of rigorous combinatorial reasoning here; otherwise I'd do the same.

Set $S = B\left(\left(i_1, i_2, \ldots, i_n\right)\right)$. Thus, $S = B\left(\left(i_1, i_2, \ldots, i_n\right)\right) = \{k \in [n] \mid i_k = 1\}$ (by the definition of B). Now,

$$\begin{aligned}
\left(A \circ B\right)\left(\left(i_1, i_2, \ldots, i_n\right)\right) &= A\left(\underbrace{B\left(\left(i_1, i_2, \ldots, i_n\right)\right)}_{=S}\right) \\
&= A\left(S\right) \\
&= \left(\left[1 \in S\right], \left[2 \in S\right], \ldots, \left[n \in S\right]\right) \qquad (6)
\end{aligned}$$

(by the definition of A). Now, we shall show that each $j \in [n]$ satisfies $[j \in S] = i_j$.

Indeed, let $j \in [n]$. Recall that $S = \{k \in [n] \mid i_k = 1\}$. Hence, if $i_j = 1$, then $j \in S$ and therefore $[j \in S] = 1 = i_j$. Therefore, we have proven $[j \in S] = i_j$ 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 $j \notin S$ (because $S = \{k \in [n] \mid i_k = 1\}$ whereas $i_j \neq 1$) and therefore $[j \in S] = 0 = i_j$. Thus, we have proven $[j \in S] = i_j$ in the case when $i_j \neq 1$. We have now proven $[j \in S] = i_j$ 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 $[j \in S] = i_j$.

Forget that we fixed j. We thus have shown that $[j \in S] = i_j$ for each $j \in [n]$. Hence,

$$\left(\left[1 \in S\right], \left[2 \in S\right], \ldots, \left[n \in S\right]\right) = \left(i_1, i_2, \ldots, i_n\right).$$

Hence, (6) becomes

$$\begin{aligned}
\left(A \circ B\right)\left(\left(i_1, i_2, \ldots, i_n\right)\right) &= \left(\left[1 \in S\right], \left[2 \in S\right], \ldots, \left[n \in S\right]\right) = \left(i_1, i_2, \ldots, i_n\right) \\
&= \operatorname{id}\left(\left(i_1, i_2, \ldots, i_n\right)\right). \qquad (7)
\end{aligned}$$

Now, forget that we fixed $\left(i_1, i_2, \ldots, i_n\right)$. We thus have proven (7) for each $\left(i_1, i_2, \ldots, i_n\right) \in \{0, 1\}^n$. Hence, $A \circ B = \operatorname{id}$.

- In order to prove that $B \circ A = \operatorname{id}$, we fix $S \in \{\text{subsets of } [n]\}$. We are going to show that $\left(B \circ A\right)\left(S\right) = S$.

  We have $A\left(S\right) = \left(\left[1 \in S\right], \left[2 \in S\right], \ldots, \left[n \in S\right]\right)$ by the definition of A. Now,

$$\begin{aligned}
\left(B \circ A\right)\left(S\right) &= B\left(\underbrace{A\left(S\right)}_{=\left(\left[1 \in S\right], \left[2 \in S\right], \ldots, \left[n \in S\right]\right)}\right) \\
&= B\left(\left(\left[1 \in S\right], \left[2 \in S\right], \ldots, \left[n \in S\right]\right)\right) \\
&= \{k \in [n] \mid [k \in S] = 1\} \qquad \left(\text{by the definition of } B\right) \\
&= \{k \in [n] \mid k \in S\} \\
&\qquad \left(\text{because for any } k \in [n], \text{ we have } [k \in S] = 1 \text{ if and only if } k \in S\right) \\
&= [n] \cap S = S \qquad \left(\text{since } S \subseteq [n]\right) \\
&= \operatorname{id}\left(S\right).
\end{aligned}$$

  Since we have proven this for each $S \in \{\text{subsets of } [n]\}$, we can thus conclude that $B \circ A = \operatorname{id}$.

We now know that $A \circ B = \operatorname{id}$ and $B \circ A = \operatorname{id}$. 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, $A : \{\text{subsets of } [n]\} \to \{0,1\}^n$ is a bijection. Thus, (4) (applied to $X = \{\text{subsets of } [n]\}$, $Y = \{0,1\}^n$ and $f = A$) yields

$$|\{\text{subsets of } [n]\}| = |\{0,1\}^n| = 2^n \qquad \left(\text{by (3)}\right).$$

This proves (5), thus solving part **(a)** of the exercise.

It remains to solve part **(b)**. If $n = 0$, then it demands us to prove that the number of all compositions of 0 is 1. This is easy enough:[3] Recall that a composition of n is defined as a tuple of positive integers whose sum is n. Thus, the compositions of 0 are the tuples of positive integers whose sum is 0. Hence, the only composition of 0 is the empty 0-tuple $()$, since any other tuple of positive integers would have a positive sum. Thus, the number of all compositions of 0 is 1.

Having thus dealt with the case $n = 0$, we can now WLOG[4] assume that $n > 0$. Thus, part **(b)** of the exercise claims that the number of all compositions of n is 2^{n-1}.

Since $n > 0$, we have $n - 1 \in \mathbb{N}$ (since n is an integer). Thus, we can apply part **(a)** of our exercise to $n - 1$ instead of n. We thus obtain that the number of all subsets of $\{1, 2, \ldots, n-1\}$ is 2^{n-1}. In other words, the number of all subsets of $[n-1]$ is 2^{n-1} (since $[n-1] = \{1, 2, \ldots, n-1\}$). In other words,

$$|\{\text{subsets of } [n-1]\}| = 2^{n-1}. \tag{8}$$

This suggests finding a bijection from $\{\text{subsets of } [n-1]\}$ to $\{\text{compositions of } n\}$. And this is indeed what we shall do.

This time we will rely on the following principle:

Proposition 1.3. *Let S be a finite set of integers. Then, there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers such that $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$.*

This proposition just says that if you have a finite set of integers, you can list its elements in increasing order in exactly one way. Obvious, right?

I will not prove Proposition 1.3 here, nor would I require such a proof in homework solutions; basic results like this can be taken for granted, as far as this course is concerned. Nevertheless, proving Proposition 1.3 becomes a necessity if one wants to fully understand the logical foundations of mathematics or implement it in a proof assistant; thus, I will give a few hints on how such a proof can be obtained:[5]

[*Outline of a proof of Proposition 1.3.* First, show that any nonempty finite set of integers has a unique largest element. Then, prove the existence part of Proposition 1.3 (that is, the claim that there exists at least one tuple $(s_1, s_2, \ldots, s_k)$ of integers such that $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$) by induction on $|S|$ (start by picking the largest element t of S, then apply the induction hypothesis to $S \setminus \{t\}$). Finally, it remains to prove the uniqueness part of Proposition 1.3. In other words, it remains to prove that if $(s_1, s_2, \ldots, s_k)$ and $(t_1, t_2, \ldots, t_j)$ are two tuples of integers such that $\{s_1, s_2, \ldots, s_k\} = S$ and $\{t_1, t_2, \ldots, t_j\} = S$ and $s_1 < s_2 < \cdots < s_k$ and $t_1 < t_2 < \cdots < t_j$, then $(s_1, s_2, \ldots, s_k) = (t_1, t_2, \ldots, t_j)$. Prove this by induction on $|S|$ again: First argue that both s_k and t_j equal the largest element of S (and thus each other); then apply the induction hypothesis to the rests of the lists (and the set $S \setminus \{t\}$, where t is the largest element of S). Details are left to the reader.]

Now, we define a map

$$C : \{\text{compositions of } n\} \to \{\text{subsets of } [n-1]\}$$

[3] ... and can be left to the reader in real homework

[4] "WLOG" means "without loss of generality".

[5] For a complete detailed proof, see [Grinbe16, Theorem 2.46].

by setting

$$\begin{aligned} C\left(\left(a_1, a_2, \ldots, a_k\right)\right) &= \left\{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\right\} \qquad (9) \\ &= \left\{a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{k-1}\right\} \\ &\qquad \text{for all compositions } \left(a_1, a_2, \ldots, a_k\right) \text{ of } n. \end{aligned}$$

[6] We first need to check that this C is well-defined – i.e., that $\{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\}$ is actually a subset of $[n-1]$ for any composition $(a_1, a_2, \ldots, a_k)$ of n. Before we do this, let us give a few examples of C:

- If $n = 4$, then $C((1,3)) = \{1\}$ and $C((1,1,2)) = \{1,2\}$ and $C((2,1,1)) = \{2,3\}$.
- If $n = 7$, then $C((2,1,1,2,1)) = \{2,3,4,6\}$.

Note that C is called the "partial-sums" map, since it sends a composition $(a_1, a_2, \ldots, a_k)$ to the set of all (nonempty, proper) partial sums $a_1 + a_2 + \cdots + a_i$ of the composition.

Let us now show that C is well-defined:

[*Proof of the well-definedness of C.* Let $(a_1, a_2, \ldots, a_k)$ be a composition of n. We must show that $\{a_1 + a_2 + \cdots + a_i \mid i \in [k-1]\}$ is actually a subset of $[n-1]$. In other words, we must show that $a_1 + a_2 + \cdots + a_i \in [n-1]$ for each $i \in [k-1]$. So let us fix $i \in [k-1]$. Then, $i \geq 1$, so that $a_1 + a_2 + \cdots + a_i$ is a nonempty sum of positive integers (because $a_1, a_2, \ldots, a_k$ are positive integers). Thus, $a_1 + a_2 + \cdots + a_i$ is itself a positive integer. Also, from $i \in [k-1]$, we obtain $i \leq k-1$. Hence, $a_{i+1} + a_{i+2} + \cdots + a_k$ is a nonempty sum of positive integers as well (because $a_1, a_2, \ldots, a_k$ are positive integers). Thus, $a_{i+1} + a_{i+2} + \cdots + a_k$ is itself a positive integer. Hence, $a_{i+1} + a_{i+2} + \cdots + a_k \geq 1$. But now,

$$(a_1 + a_2 + \cdots + a_i) + (a_{i+1} + a_{i+2} + \cdots + a_k) = a_1 + a_2 + \cdots + a_k = n$$

(since $(a_1, a_2, \ldots, a_k)$ is a composition of n). Therefore,

$$a_1 + a_2 + \cdots + a_i = n - \underbrace{(a_{i+1} + a_{i+2} + \cdots + a_k)}_{\geq 1} \leq n - 1.$$

Since $a_1 + a_2 + \cdots + a_i$ is a positive integer, this shows that $a_1 + a_2 + \cdots + a_i \in [n-1]$. But this is precisely what we wanted to show. Hence, C is well-defined.]

Next, we define a map

$$D : \{\text{subsets of } [n-1]\} \to \{\text{compositions of } n\}$$

as follows: Let S be a subset of $[n-1]$. Then, Proposition 1.3 shows that there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers such that $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$. Consider this tuple, and extend it further by setting $s_0 = 0$ and $s_{k+1} = n$. Then, we have the following inequalities:

- $s_1 < s_2 < \cdots < s_k$;
- $s_0 < s_i$ for each $i \in [k]$ (because each $i \in [k]$ satisfies $s_i \in \{s_1, s_2, \ldots, s_k\} = S \subseteq [n-1]$, so that $s_i > 0 = s_0$);
- $s_i < s_{k+1}$ for each $i \in [k]$ (because each $i \in [k]$ satisfies $s_i \in \{s_1, s_2, \ldots, s_k\} = S \subseteq [n-1]$, so that $s_i \leq n - 1 < n = s_{k+1}$);

[6] Note that every composition $(a_1, a_2, \ldots, a_k)$ of n satisfies $k \geq 1$. Indeed, if it wouldn't, then it would satisfy $k = 0$ and therefore $a_1 + a_2 + \cdots + a_k = a_1 + a_2 + \cdots + a_0 = (\text{empty sum}) = 0$, which would contradict $a_1 + a_2 + \cdots + a_k = n > 0$.

- $s_0 < s_{k+1}$ (since $s_{k+1} = n > 0 = s_0$).

Combining these inequalities, we obtain $s_0 < s_1 < \cdots < s_{k+1}$. Now, set

$$D(S) = (s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k).$$

This defines D.

In fact, we again need to prove that D is well-defined – i.e., that $(s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k)$ is actually a composition of n. But this is easy: The tuple $(s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k)$ consists of positive integers (since $s_0 < s_1 < \cdots < s_{k+1}$), and the sum of these integers is

$$\begin{aligned}
&(s_1 - s_0) + (s_2 - s_1) + \cdots + (s_{k+1} - s_k) \\
&= \underbrace{(s_1 + s_2 + \cdots + s_{k+1})}_{=(s_1+s_2+\cdots+s_k)+s_{k+1}} - \underbrace{(s_0 + s_1 + \cdots + s_k)}_{=s_0+(s_1+s_2+\cdots+s_k)} \\
&= ((s_1 + s_2 + \cdots + s_k) + s_{k+1}) - (s_0 + (s_1 + s_2 + \cdots + s_k)) \\
&= s_{k+1} - s_0 = n - 0 \qquad \left(\text{since } s_{k+1} = n \text{ and } s_0 = 0\right) \\
&= n.
\end{aligned}$$

Thus, D is indeed well-defined.

Note that the map D depends on n. For example, if $n = 5$, then $D(\{1,3\}) = (1,2,2)$, but if $n = 7$, then $D(\{1,3\}) = (1,2,4)$. But n is fixed in our current setting, which allows us to leave it out of our notation.

We now claim that the maps C and D are mutually inverse.

Proving this is again a fairly straightforward matter, so we restrict ourselves to an outline:

- In order to prove that $C \circ D = \mathrm{id}$, we fix some subset S of $[n-1]$, and we try to show that $(C \circ D)(S) = S$.

  Proposition 1.3 shows that there exists a unique tuple $(s_1, s_2, \ldots, s_k)$ of integers such that $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$. Consider this tuple, and extend it further by setting $s_0 = 0$ and $s_{k+1} = n$. The definition of D shows that

  $$D(S) = (s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k). \qquad (10)$$

  Now,

  $$\begin{aligned}
  (C \circ D)(S) &= C(D(S)) = C((s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k)) \qquad \left(\text{by } (10)\right) \\
  &= \{(s_1 - s_0) + (s_2 - s_1) + \cdots + (s_i - s_{i-1}) \mid i \in [k+1-1]\}
  \end{aligned}$$

  (by (9), applied to $k+1$ and $(s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k)$ instead of k and $(a_1, a_2, \ldots, a_k)$). Since

  $$\begin{aligned}
  &(s_1 - s_0) + (s_2 - s_1) + \cdots + (s_i - s_{i-1}) \\
  &= \underbrace{(s_1 + s_2 + \cdots + s_i)}_{=(s_1+s_2+\cdots+s_{i-1})+s_i} - \underbrace{(s_0 + s_1 + \cdots + s_{i-1})}_{=s_0+(s_1+s_2+\cdots+s_{i-1})} \\
  &= ((s_1 + s_2 + \cdots + s_{i-1}) + s_i) - (s_0 + (s_1 + s_2 + \cdots + s_{i-1})) \\
  &= s_i - \underbrace{s_0}_{=0} = s_i
  \end{aligned}$$

  for each $i \in [k+1-1]$, this becomes

  $$\begin{aligned}
  (C \circ D)(S) &= \left\{ \underbrace{(s_1 - s_0) + (s_2 - s_1) + \cdots + (s_i - s_{i-1})}_{=s_i} \mid i \in [k+1-1] \right\} \\
  &= \left\{ s_i \mid i \in \left[\underbrace{k+1-1}_{=k} \right] \right\} = \{s_i \mid i \in [k]\} = \{s_1, s_2, \ldots, s_k\} = S = \mathrm{id}(S).
  \end{aligned}$$

  Since we have proven this for each subset S of $[n-1]$, we thus conclude that $C \circ D = \mathrm{id}$.

- In order to prove $D \circ C = \operatorname{id}$, we fix some composition $(a_1, a_2, \ldots, a_j)$ of n. We shall show that $(D \circ C)((a_1, a_2, \ldots, a_j)) = (a_1, a_2, \ldots, a_j)$.

  Let S be the set $C((a_1, a_2, \ldots, a_j))$. Then, S is a subset of $[n-1]$ (since C is well-defined).

  Recall that $(a_1, a_2, \ldots, a_j)$ is a composition of n. Thus, $a_1, a_2, \ldots, a_j$ are positive integers whose sum is n. Hence, $a_1 + a_2 + \cdots + a_j = n > 0$, so that $j > 0$ (since otherwise, $a_1 + a_2 + \cdots + a_j$ would be an empty sum and therefore equal to 0). Since $a_1, a_2, \ldots, a_j$ are positive integers, we have

$$a_1 < a_1 + a_2 < a_1 + a_2 + a_3 < \cdots < a_1 + a_2 + \cdots + a_{j-1}.$$

  Moreover,

$$S = C((a_1, a_2, \ldots, a_j)) = \{a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{j-1}\}$$

  (by the definition of C). Hence, the $(j-1)$-tuple

$$(a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{j-1})$$

  is a tuple $(s_1, s_2, \ldots, s_k)$ of integers such that $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$.

  But Proposition 1.3 shows that there is a **unique** tuple $(s_1, s_2, \ldots, s_k)$ of integers such that $\{s_1, s_2, \ldots, s_k\} = S$ and $s_1 < s_2 < \cdots < s_k$. This unique tuple must be the $(j-1)$-tuple $(a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{j-1})$ (because as we have just seen, the latter $(j-1)$-tuple is such a tuple). Consider this tuple; thus,

$$(s_1, s_2, \ldots, s_k) = (a_1,\ a_1 + a_2,\ a_1 + a_2 + a_3,\ \ldots,\ a_1 + a_2 + \cdots + a_{j-1}).$$

  In other words, $k = j - 1$ and

$$s_i = a_1 + a_2 + \cdots + a_i \qquad \text{for each } i \in [k]. \tag{11}$$

  Extend the k-tuple $(s_1, s_2, \ldots, s_k)$ further by setting $s_0 = 0$ and $s_{k+1} = n$. The definition of D then shows that

$$D(S) = (s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k). \tag{12}$$

  But $a_1 + a_2 + \cdots + a_0$ is an empty sum and thus equals 0. Also, $k = j - 1$ leads to $k + 1 = j$, so that $a_1 + a_2 + \cdots + a_{k+1} = a_1 + a_2 + \cdots + a_j = n$. Now, the equality (11) holds not only for each $i \in [k]$, but also for $i = 0$ (since $s_0 = 0 = a_1 + a_2 + \cdots + a_0$) and for $i = k + 1$ (since $s_{k+1} = n = a_1 + a_2 + \cdots + a_{k+1}$). Hence, this equality holds for all $i \in \{0, 1, \ldots, k+1\}$. In other words, we have

$$s_i = a_1 + a_2 + \cdots + a_i \qquad \text{for each } i \in \{0, 1, \ldots, k+1\}. \tag{13}$$

  Hence, for each $i \in [k+1]$, we have

$$\begin{aligned} \underbrace{s_i}_{\substack{= a_1 + a_2 + \cdots + a_i \\ \text{(by (13))}}} - \underbrace{s_{i-1}}_{\substack{= a_1 + a_2 + \cdots + a_{i-1} \\ \text{(by (13), applied to } i-1 \text{ instead of } i\text{)}}} &= (a_1 + a_2 + \cdots + a_i) - (a_1 + a_2 + \cdots + a_{i-1}) \\ &= a_i. \end{aligned}$$

  Thus,

$$(s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k) = (a_1, a_2, \ldots, a_{k+1}) = (a_1, a_2, \ldots, a_j)$$

  (since $k + 1 = j$). Thus, (12) becomes

$$D(S) = (s_1 - s_0, s_2 - s_1, \ldots, s_{k+1} - s_k) = (a_1, a_2, \ldots, a_j).$$

Now,

$$\begin{aligned}(D \circ C)\left((a_1, a_2, \ldots, a_j)\right) &= D\left(\underbrace{C\left((a_1, a_2, \ldots, a_j)\right)}_{=S}\right) = D(S) \\ &= (a_1, a_2, \ldots, a_j) = \operatorname{id}\left((a_1, a_2, \ldots, a_j)\right).\end{aligned}$$

This shows that $D \circ C = \operatorname{id}$.

Combining $C \circ D = \operatorname{id}$ with $D \circ C = \operatorname{id}$, we conclude that the maps C and D are mutually inverse.

Thus, the map

$$C : \{\text{compositions of } n\} \to \{\text{subsets of } [n-1]\}$$

is invertible, i.e., is a bijection. Hence, using (4) again[7], we obtain

$$\left|\{\text{compositions of } n\}\right| = \left|\{\text{subsets of } [n-1]\}\right| = 2^{n-1}$$

(by (8)). In other words, the number of all compositions of n is 2^{n-1}. This completes our solution to part **(b)** of the exercise (since this is what part **(b)** claims for $n > 0$).

---

2 Exercise 2

2.1 Problem

For any real number x and any $k \in \mathbb{N}$, we define a number $x^{\underline{k}}$ by[8]

$$x^{\underline{k}} = x(x-1)(x-2)\cdots(x-k+1) = \prod_{i=0}^{k-1}(x-i).$$

(Note that if $k = 0$, then the product on the right hand side of this equality is an empty product, and thus equals 1 by definition. Hence, $x^{\underline{0}} = 1$ for every real x. Also, $x^{\underline{1}} = x$, $x^{\underline{2}} = x(x-1)$, and so on. The notation $x^{\underline{n}}$ is called the *n-th falling factorial of x*.)

Let $k \in \mathbb{N}$ and $n \in \mathbb{N}$. Prove that

$$\sum_{i=0}^{n} i^{\underline{k}} = \frac{1}{k+1}(n+1)^{\underline{k+1}}. \qquad (14)$$

2.2 Remark

Remark 2.1. This may remind you of the classical formula

$$\int_0^n x^k dx = \frac{1}{k+1} n^{k+1}$$

[7] this time, applied to $X = \{\text{compositions of } n\}$, $Y = \{\text{subsets of } [n-1]\}$ and $f = C$

[8] Note that the letter i does **not** stand for the imaginary unit $\sqrt{-1}$ in combinatorics, unless we explicitly say that it does.

from calculus; in fact, (14) is something like a "discrete version" of this formula (with the integral replaced by a finite sum, and the k-th power x^k replaced by the falling factorial $x^{\underline{k}}$).

The equality (14) rewrites as

$$0^{\underline{k}} + 1^{\underline{k}} + \cdots + n^{\underline{k}} = \frac{1}{k+1} (n+1)^{\underline{k+1}}.$$

For example, for $k = 1$, this simplifies to

$$0 + 1 + \cdots + n = \frac{1}{2} (n+1) n,$$

which is a famous formula. (It is common to start the sum at 1 rather than 0, but this doesn't matter.)

2.3 Solution

There are several ways to solve this exercise; the two simplest are probably the one by induction on n, and the one using the telescope principle. In truth they are "essentially the same" (i.e., you can easily translate one into the other). I shall show the second one only.

Let me state the telescope principle first:

Proposition 2.2. *Let $m \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_m$ be $m+1$ real numbers*[9]*. Then,*

$$\sum_{i=1}^{m} (a_i - a_{i-1}) = a_m - a_0.$$

Proposition 2.2 is known as the "telescope principle" since it contracts the sum $\sum\limits_{i=1}^{m} (a_i - a_{i-1})$ to the single difference $a_m - a_0$, like folding a telescope.

The simplest way to convince yourself that Proposition 2.2 is true is by expanding the left hand side:

$$\sum_{i=1}^{m} (a_i - a_{i-1}) = (a_1 - a_0) + (a_2 - a_1) + (a_3 - a_2) + \cdots + (a_m - a_{m-1})$$

and watching all the terms cancel each other out except for the $-a_0$ and the a_m. More formally, this argument can be emulated by an induction on m. Here is a different proof (which illustrates a few of the basic rules for manipulating sums):

Proof of Proposition 2.2. If $m = 0$, then

$$\sum_{i=1}^{m} (a_i - a_{i-1}) = \sum_{i=1}^{0} (a_i - a_{i-1}) = (\text{empty sum}) = 0 = a_m - a_0$$

(since $m = 0$ leads to $a_m = a_0$). Thus, Proposition 2.2 holds if $m = 0$. Hence, for the rest of this proof, we can WLOG assume that $m \neq 0$. Let us assume this.[10] Thus, $m \geq 1$. Hence,

$$\sum_{i=1}^{m} a_i = \sum_{i=1}^{m-1} a_i + a_m$$

[9] I am saying "real numbers" just for the sake of saying something definite. You could just as well say "complex numbers" or "rational numbers" or "elements of an abelian group (where the operation of the group is written as addition)". The telescope principle is a general property of sums and differences; it does not depend on what exactly we are summing.

[10] In actual homework, feel free to just say "Assume WLOG that $m \neq 0$" without giving the justification that we just gave. The reader can be trusted to fill it in.

and

$$\sum_{i=1}^{m} a_{i-1} = \underbrace{a_{1-1}}_{=a_0} + \sum_{i=2}^{m} a_{i-1} = a_0 + \sum_{i=2}^{m} a_{i-1} = a_0 + \sum_{i=1}^{m-1} a_i$$

(here, we have substituted i for $i-1$ in the sum). Thus,

$$\sum_{i=1}^{m} (a_i - a_{i-1}) = \underbrace{\sum_{i=1}^{m} a_i}_{=\sum_{i=1}^{m-1} a_i + a_m} - \underbrace{\sum_{i=1}^{m} a_{i-1}}_{=a_0 + \sum_{i=1}^{m-1} a_i} = \left(\sum_{i=1}^{m-1} a_i + a_m\right) - \left(a_0 + \sum_{i=1}^{m-1} a_i\right) = a_m - a_0.$$

This proves Proposition 2.2. □

Now, let us come back to the problem at hand. We want to prove (14) using Proposition 2.2. The key turns out to be the following formula:

Lemma 2.3. *Let i be a real number, and $k \in \mathbb{N}$. Then,*

$$(i-1)^{\underline{k}} = \frac{1}{k+1} i^{\underline{k+1}} - \frac{1}{k+1} (i-1)^{\underline{k+1}}.$$

Proof of Lemma 2.3. The definition of $(i-1)^{\underline{k}}$ yields

$$(i-1)^{\underline{k}} = (i-1)((i-1)-1)((i-1)-2)\cdots((i-1)-k+1) = (i-1)(i-2)\cdots(i-k).$$

But the definition of $i^{\underline{k+1}}$ yields

$$\begin{aligned} i^{\underline{k+1}} &= i(i-1)(i-2)\cdots(i-(k+1)+1) = i(i-1)(i-2)\cdots(i-k) \\ &= i\underbrace{((i-1)(i-2)\cdots(i-k))}_{=(i-1)^{\underline{k}}} = i(i-1)^{\underline{k}}. \end{aligned}$$

On the other hand, the definition of $(i-1)^{\underline{k+1}}$ yields

$$\begin{aligned} (i-1)^{\underline{k+1}} &= (i-1)((i-1)-1)((i-1)-2)\cdots((i-1)-(k+1)+1) \\ &= (i-1)(i-2)\cdots(i-k-1) \\ &= \underbrace{((i-1)(i-2)\cdots(i-k))}_{=(i-1)^{\underline{k}}}(i-k-1) = (i-1)^{\underline{k}}(i-k-1). \end{aligned}$$

Subtracting the preceding two equalities from each other, we find

$$\begin{aligned} i^{\underline{k+1}} - (i-1)^{\underline{k+1}} &= i(i-1)^{\underline{k}} - (i-1)^{\underline{k}}(i-k-1) \\ &= \underbrace{(i-(i-k-1))}_{=k+1}(i-1)^{\underline{k}} = (k+1)(i-1)^{\underline{k}}. \end{aligned}$$

We can divide this equality by $k+1$ (since $k+1>0$), and thus obtain

$$\frac{i^{\underline{k+1}} - (i-1)^{\underline{k+1}}}{k+1} = (i-1)^{\underline{k}}.$$

In other words,

$$(i-1)^{\underline{k}} = \frac{i^{\underline{k+1}} - (i-1)^{\underline{k+1}}}{k+1} = \frac{1}{k+1} i^{\underline{k+1}} - \frac{1}{k+1}(i-1)^{\underline{k+1}}.$$

This proves Lemma 2.3. □

We also note that the definition of $0^{\underline{k+1}}$ yields

$$0^{\underline{k+1}} = 0(0-1)(0-2)\cdots(0-(k+1)+1) = 0(0-1)(0-2)\cdots(0-k) = 0.$$

Now, let us substitute $i-1$ for i in the sum $\sum\limits_{i=0}^{n} i^{\underline{k}}$. Thus, we find

$$\begin{aligned}
\sum_{i=0}^{n} i^{\underline{k}} &= \sum_{i=1}^{n+1} \underbrace{(i-1)^{\underline{k}}}_{\substack{=\frac{1}{k+1}i^{\underline{k+1}}-\frac{1}{k+1}(i-1)^{\underline{k+1}} \\ \text{(by Lemma 2.3)}}} = \sum_{i=1}^{n+1}\left(\frac{1}{k+1}i^{\underline{k+1}} - \frac{1}{k+1}(i-1)^{\underline{k+1}}\right) \\
&= \frac{1}{k+1}(n+1)^{\underline{k+1}} - \frac{1}{k+1}\underbrace{0^{\underline{k+1}}}_{=0} \\
&\qquad \left(\text{by Proposition 2.2, applied to } m=n+1 \text{ and } a_i = \frac{1}{k+1}i^{\underline{k+1}}\right) \\
&= \frac{1}{k+1}(n+1)^{\underline{k+1}} - \frac{1}{k+1}0 = \frac{1}{k+1}(n+1)^{\underline{k+1}}.
\end{aligned}$$

This solves the exercise.

---

3 Exercise 3

3.1 Problem

Let n be a positive integer.

An n-tuple $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$ is said to be *even* if the sum $i_1 + i_2 + \cdots + i_n$ is even. (For example, the 4-tuple $(1,0,0,1)$ is even, whereas $(1,0,1,1)$ is not.)

Prove that the number of all even n-tuples $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$ is 2^{n-1}.

3.2 Solution

Let E_n be the set of all even n-tuples $(i_1, i_2, \ldots, i_n) \in \{0,1\}^n$. Then, the exercise wants us to show that $|E_n| = 2^{n-1}$.

We shall achieve this by finding a bijection from E_n to $\{0,1\}^{n-1}$.

Define a map $A : E_n \to \{0,1\}^{n-1}$ by setting

$$A((i_1, i_2, \ldots, i_n)) = (i_1, i_2, \ldots, i_{n-1}) \qquad \text{for each } (i_1, i_2, \ldots, i_n) \in E_n.$$

Thus, the map A simply throws away the last entry of an even n-tuple.

We want to prove that A is bijective. We can achieve this by proving that A is injective and surjective: [11]

- Let us first show that A is injective. This means showing that if $(i_1, i_2, \ldots, i_n)$ and $(j_1, j_2, \ldots, j_n)$ are two elements of E_n (that is, even n-tuples) satisfying

$$A((i_1, i_2, \ldots, i_n)) = A((j_1, j_2, \ldots, j_n)), \tag{15}$$

[11] Again, there is much more detail in the following argumentation than you need when writing up your homework.

then

$$(i_1, i_2, \ldots, i_n) = (j_1, j_2, \ldots, j_n) . \qquad (16)$$

So let $(i_1, i_2, \ldots, i_n)$ and $(j_1, j_2, \ldots, j_n)$ be two elements of E_n satisfying (15). We must prove (16).

The definition of A yields

$$A((i_1, i_2, \ldots, i_n)) = (i_1, i_2, \ldots, i_{n-1}) \qquad \text{and} \qquad A((j_1, j_2, \ldots, j_n)) = (j_1, j_2, \ldots, j_{n-1}) .$$

Thus, (15) rewrites as

$$(i_1, i_2, \ldots, i_{n-1}) = (j_1, j_2, \ldots, j_{n-1}) .$$

In other words,

$$i_k = j_k \qquad \text{for each } k \in [n-1] . \qquad (17)$$

Hence, $i_1 + i_2 + \cdots + i_{n-1} = j_1 + j_2 + \cdots + j_{n-1}$.

On the other hand, the n-tuple $(i_1, i_2, \ldots, i_n)$ is even (since $(i_1, i_2, \ldots, i_n) \in E_n$). In other words, $i_1 + i_2 + \cdots + i_n$ is even. In other words, $i_1 + i_2 + \cdots + i_n \equiv 0 \mod 2$. Similarly, $j_1 + j_2 + \cdots + j_n \equiv 0 \mod 2$. Now,

$$\underbrace{(i_1 + i_2 + \cdots + i_{n-1})}_{=j_1+j_2+\cdots+j_{n-1}} + j_n = (j_1 + j_2 + \cdots + j_{n-1}) + j_n = j_1 + j_2 + \cdots + j_n \equiv 0$$
$$\equiv i_1 + i_2 + \cdots + i_n = (i_1 + i_2 + \cdots + i_{n-1}) + i_n \mod 2.$$

Subtracting $i_1 + i_2 + \cdots + i_{n-1}$ from both sides of this congruence, we obtain $j_n \equiv i_n \mod 2$. But j_n and i_n are two elements of $\{0, 1\}$, and thus can only be congruent to each other modulo 2 if they are equal. Hence, from $j_n \equiv i_n \mod 2$, we obtain $j_n = i_n$. In other words, $i_n = j_n$. Hence, $i_k = j_k$ holds not only for $k \in [n-1]$ (as we have shown in (17)), but also for $k = n$. In other words, we have $i_k = j_k$ for all $k \in [n]$. In other words, $(i_1, i_2, \ldots, i_n) = (j_1, j_2, \ldots, j_n)$. Thus, (16) is proven. So we have shown that A is injective.

- Let us now prove that A is surjective. To do that, we need to show that for each $(j_1, j_2, \ldots, j_{n-1}) \in \{0, 1\}^{n-1}$, there exists some $(i_1, i_2, \ldots, i_n) \in E_n$ such that

$$A((i_1, i_2, \ldots, i_n)) = (j_1, j_2, \ldots, j_{n-1}) .$$

So let us fix some $(j_1, j_2, \ldots, j_{n-1}) \in \{0, 1\}^{n-1}$. We need to show that there exists some $(i_1, i_2, \ldots, i_n) \in E_n$ such that $A((i_1, i_2, \ldots, i_n)) = (j_1, j_2, \ldots, j_{n-1})$.

Indeed, let us construct this $(i_1, i_2, \ldots, i_n)$ as follows:

We set $i_k = j_k$ for each $k \in [n-1]$. This defines $n-1$ elements $i_1, i_2, \ldots, i_{n-1}$ of $\{0, 1\}$. Next, we define a further element i_n of $\{0, 1\}$ by

$$i_n = \begin{cases} 0, & \text{if } i_1 + i_2 + \cdots + i_{n-1} \text{ is even;} \\ 1, & \text{if } i_1 + i_2 + \cdots + i_{n-1} \text{ is odd.} \end{cases}$$

Then, the number $i_1 + i_2 + \cdots + i_n$ is even (because we can write it as the sum $(i_1 + i_2 + \cdots + i_{n-1}) + i_n$ of the two numbers $i_1 + i_2 + \cdots + i_{n-1}$ and i_n, which are either both even or both odd). In other words, the n-tuple $(i_1, i_2, \ldots, i_n) \in \{0, 1\}^n$ is even. In other words, $(i_1, i_2, \ldots, i_n) \in E_n$. Finally, the definition of A yields

$$A((i_1, i_2, \ldots, i_n)) = (i_1, i_2, \ldots, i_{n-1}) = (j_1, j_2, \ldots, j_{n-1})$$

(since $i_k = j_k$ for each $k \in [n-1]$). Thus, we have constructed an $(i_1, i_2, \ldots, i_n) \in E_n$ such that $A((i_1, i_2, \ldots, i_n)) = (j_1, j_2, \ldots, j_{n-1})$. This completes our proof of the surjectivity of A.

We now know that the map A is both injective and surjective. Hence, A is bijective. In other words, $A : E_n \to \{0,1\}^{n-1}$ is a bijection. Hence, (4) (applied to $X = E_n$, $Y = \{0,1\}^{n-1}$ and $f = A$) yields

$$|E_n| = \left|\{0,1\}^{n-1}\right| = 2^{n-1}$$

(where the last equality sign follows from (3), applied to $n-1$ instead of n). This solves the exercise.

References

[Grinbe16] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`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/2019-01-10` .