Math 222 Fall 2022, Lecture 16: Binomial coefficients

website: `https://www.cip.ifi.lmu.de/~grinberg/t/22fco`

2. Binomial coefficients (cont'd)

2.4. Counting maps

We now return to the problem of counting maps. This time, we will focus on maps with special properties.

2.4.1. All maps

In Theorem 1.5.6 (Lecture 11), we showed that (# of maps from A to B) $= |B|^{|A|}$ for any two finite sets A and B. In other words:

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,

$$(\text{\# of maps from } A \text{ to } B) = n^m.$$

2.4.2. Injective maps

Recall that a map is injective if and only if it sends distinct elements to distinct values.

How many injective maps are there from a set A to a set B ? To state the answer, we introduce a new notation:

Definition 2.4.2. Let $n \in \mathbb{R}$ and $k \in \mathbb{N}$. Then, the **falling factorial** $n^{\underline{k}}$ is defined by

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

The falling factorial is also known as the **lower factorial** or the **descending factorial**. Here are some simple properties:

Proposition 2.4.3. Let $n \in \mathbb{R}$. Then:

(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 any $k \in \mathbb{N}$.
(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 $n^{\underline{k}} \cdot (n-k) = n^{\underline{k+1}}$ for any $k \in \mathbb{N}$.

Proof. All of these are easy. (See Proposition 2.4.3 in the 2019 notes for details.) □

Now, we can count injective maps:

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,

$$(\text{\# of injective maps from } A \text{ to } B) = n^{\underline{m}}.$$

Informal proof of Theorem 2.4.4. Let $a_1, a_2, \ldots, a_m$ be the m elements of A (listed without repetition). Then, a map $f : A \to B$ is uniquely determined by its values $f(a_1), f(a_2), \ldots, f(a_m)$, and can be constructed by choosing these values arbitrarily, one by one. For this map f to be injective, these values have to be distinct. Thus, when choosing its values, we need to ensure that

$$\begin{aligned}
&f(a_1) \in B; \\
&f(a_2) \in B \setminus \{f(a_1)\}; \\
&f(a_3) \in B \setminus \{f(a_1), f(a_2)\}; \\
&f(a_4) \in B \setminus \{f(a_1), f(a_2), f(a_3)\}; \\
&\qquad \ldots.
\end{aligned}$$

This means that we can construct an injective map $f : A \to B$ by choosing its m values $f(a_1), f(a_2), \ldots, f(a_m)$ one by one. How many options do we have in this m-step procedure?

- For $f(a_1)$, we have n options, since all n elements of B qualify.
- For $f(a_2)$, we have $n-1$ options, since all n elements of B except for the already-chosen value $f(a_1)$ qualify.
- For $f(a_3)$, we have $n-2$ options, since all n elements of B except for the two already-chosen values $f(a_1)$ and $f(a_2)$ qualify (and since these two values $f(a_1)$ and $f(a_2)$ are distinct).
- For $f(a_4)$, we have $n-3$ options, since all n elements of B except for the three already-chosen values $f(a_1)$, $f(a_2)$ and $f(a_3)$ qualify (and again since these three values are distinct).

- $\cdots$.

In total, we thus have $n(n-1)(n-2)\cdots(n-m+1)$ many possibilities. Thus, by the dependent product rule, we get

$$(\text{\# of injective maps } f : A \to B) = n(n-1)(n-2)\cdots(n-m+1) = n^{\underline{m}}.$$

This proves Theorem 2.4.4. □

How can we make this proof rigorous? We could formalize the dependent product rule and the above m-step procedure for constructing an injective map $f : A \to B$, but it is easier to proceed differently, using induction to "pack" the first $m-1$ steps of the m-step procedure into a single big step. This leads to the following more formal proof:

Formal proof of Theorem 2.4.4 (sketched). Forget that we fixed m, n, 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. Thus, we must prove that

$$|\operatorname{Inj}(A, B)| \overset{?}{=} n^{\underline{m}} \qquad (1)$$

for any $m, n \in \mathbb{N}$ and any m-element set A and any n-element set B.

We shall prove (1) by induction on m:

Base case: The equality (1) holds for $m = 0$. (Indeed, there is only one map from $\varnothing$ to B, and this map is injective; thus, $|\operatorname{Inj}(\varnothing, B)| = 1 = n^{\underline{0}}$.)

Induction step: Let m be a positive integer. Let us assume that (1) holds for $m-1$ instead of m. Let us now prove (1) for m.

Thus, let A be an m-element set, and let B be an n-element set. We want to prove that

$$|\operatorname{Inj}(A, B)| \overset{?}{=} n^{\underline{m}}.$$

The set A is nonempty, since its size is $|A| = m > 0$. So we can pick an element $a \in A$. Let us pick one and keep it fixed from now on.

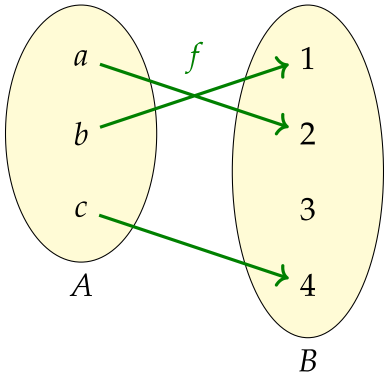
Then, $A \setminus \{a\}$ is an $(m-1)$-element set. Hence, by the induction hypothesis, we have

$$|\operatorname{Inj}(A \setminus \{a\}, B)| = n^{\underline{m-1}}.$$

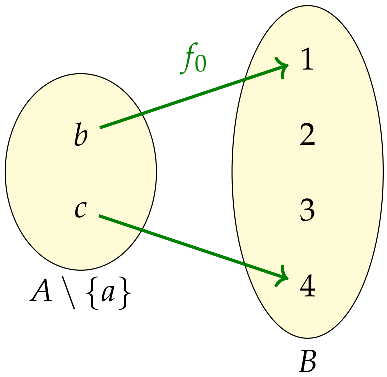
It remains to connect $\operatorname{Inj}(A, B)$ with $\operatorname{Inj}(A \setminus \{a\}, B)$.

The easiest way to do so is by restriction: For any map $f : A \to B$, we can consider its **restriction** f_0 to the subset $A \setminus \{a\}$. This restriction is simply the map that sends each $x \in A \setminus \{a\}$ to $f(x)$. In other words, the restriction f_0 is obtained from f by "forgetting" the value $f(a)$.

For example,

if $f =$ 

,

then $f_0 =$ 

.

Clearly, if a map $f : A \to B$ is injective, then so is its restriction f_0. In other words, for every $f \in \operatorname{Inj}(A, B)$, we have $f_0 \in \operatorname{Inj}(A \setminus \{a\}, B)$.

This allows us to "classify" maps $f \in \operatorname{Inj}(A, B)$ according to their restriction. In particular, by the sum rule,

$$\begin{aligned} &(\#\text{ of all } f \in \operatorname{Inj}(A, B)) \\ &= \sum_{g \in \operatorname{Inj}(A \setminus \{a\},\, B)} (\#\text{ of all } f \in \operatorname{Inj}(A, B) \text{ such that } f_0 = g). \end{aligned} \tag{2}$$

We shall now try to compute the addends of the sum on the RHS.

Indeed, fix an injective map $g \in \operatorname{Inj}(A \setminus \{a\}, B)$. How many injective maps $f \in \operatorname{Inj}(A, B)$ have restriction $f_0 = g$?

We let $\operatorname{Im} g$ be the set of all values of g. This is also known as the **image** (or **range**) of the map g, and can also be denoted $g(A \setminus \{a\})$. Since the map g is injective, all its values are distinct, so that it has exactly $m - 1$ many values (since $|A \setminus \{a\}| = m - 1$). In other words, $|\operatorname{Im} g| = m - 1$. Since $\operatorname{Im} g$ is a subset of B, we have $|B \setminus \operatorname{Im} g| = \underbrace{|B|}_{=n} - \underbrace{|\operatorname{Im} g|}_{=m-1} = n - (m - 1) = n - m + 1$.

Clearly, a map $f \in \operatorname{Inj}(A, B)$ has restriction $f_0 = g$ if and only if its values on all elements of $A \setminus \{a\}$ coincide with the corresponding values of g. Thus, the only freedom we have when we choose such a map is the freedom of choosing its remaining value $f(a)$. In order for f to be injective, this value $f(a)$ must be distinct from all the existing values, i.e., distinct from all the values of g. In other words, this value $f(a)$ must come from the set $B \setminus \operatorname{Im} g$. This leaves us $n-m+1$ options, since $|B \setminus \operatorname{Im} g| = n-m+1$.

Thus, we have convinced ourselves that an injective map $f \in \operatorname{Inj}(A,B)$ that has restriction $f_0 = g$ can be chosen in $n-m+1$ many ways. Hence,

$$(\text{\# of all } f \in \operatorname{Inj}(A,B) \text{ such that } f_0 = g) = n-m+1. \tag{3}$$

(If you want this argument formalized further, you can rephrase it as an application of the bijection principle[1].)

We have proved (3) for every $g \in \operatorname{Inj}(A \setminus \{a\},\ B)$. Therefore, (2) becomes

$$\begin{aligned}
&(\text{\# of all } f \in \operatorname{Inj}(A,B)) \\
&= \sum_{g \in \operatorname{Inj}(A\setminus\{a\},\ B)} \underbrace{(\text{\# of all } f \in \operatorname{Inj}(A,B) \text{ such that } f_0 = g)}_{\substack{=n-m+1 \\ \text{(by (3))}}} \\
&= \sum_{g \in \operatorname{Inj}(A\setminus\{a\},\ B)} (n-m+1) = \underbrace{|\operatorname{Inj}(A\setminus\{a\},\ B)|}_{\substack{=n^{\underline{m-1}} \\ =n(n-1)(n-2)\cdots(n-m+2)}} \cdot (n-m+1) \\
&= n(n-1)(n-2)\cdots(n-m+2)\cdot(n-m+1) \\
&= n(n-1)(n-2)\cdots(n-m+1) = n^{\underline{m}}.
\end{aligned}$$

In other words, $|\operatorname{Inj}(A,B)| = n^{\underline{m}}$. This completes the induction step, and thus (1) is proved. As we explained above, this proves Theorem 2.4.4. □

2.4.3. The pigeonhole principles

The **pigeonhole principles** are two fundamental facts about maps between finite sets. We shall state them without proof here, since they are common-sense. (A skeptical reader can find proofs in §2.4.3 of the 2019 notes.) We begin with the **pigeonhole principle for injections**:

---

[1]Namely: We argue that the map

$$\{f \in \operatorname{Inj}(A,B) \mid f_0 = g\} \to B \setminus \operatorname{Im} g, \quad f \mapsto f(a)$$

(that is, the map that assigns to each injective map $f \in \operatorname{Inj}(A,B)$ satisfying $f_0 = g$ its value $f(a)$) is a bijection. (The proof of this is elementary set-theoretical reasoning and can be found in §2.4.2 of the 2019 notes.) Thus, the bijection principle yields

$$|\{f \in \operatorname{Inj}(A,B) \mid f_0 = g\}| = |B \setminus \operatorname{Im} g| = n-m+1.$$

In other words, $(\text{\# of all } f \in \operatorname{Inj}(A,B) \text{ such that } f_0 = g) = n-m+1$. This proves (3).

Theorem 2.4.5 (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.

Somewhat informally, this can be restated as follows:

(a) If m pigeons are distributed in n pigeonholes, and no two pigeons share a hole[2], then $m \leq n$.

(b) If n pigeons are distributed in n pigeonholes, and no two pigeons share a hole, then each hole has a pigeon in it[3].

Next comes a "dual" variant of Theorem 2.4.5 – the **pigeonhole principle for surjections**:

Theorem 2.4.6 (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.

Somewhat informally, this can be restated as follows:

(a) If m pigeons are distributed in n pigeonholes, and no hole is empty, then $m \geq n$.

(b) If n pigeons are distributed in n pigeonholes, and no hole is empty, then no two pigeons share a hole.

Remark 2.4.7. If we allow the sets A and B to be infinite, then parts **(a)** of both pigeonhole principles (Theorem 2.4.5 and Theorem 2.4.6) remain valid (as long as we understand $|A|$ and $|B|$ to be cardinalities), but parts **(b)** both become false. (See Remark 2.4.8 in the 2019 notes for counterexamples.)

The pigeonhole principles might look like the most trivial results in mathematics, but they have a number of surprising applications. See [20f, Chapter 6], [21f-2], [Bona17, Chapter 1], [Engel98, Chapter 4], [AndDos10, Chapter 20] or [GelAnd17, §1.3] for some applications (or search for "Pigeonhole Principle" anywhere on the internet).

[2]i.e., the map that sends each pigeon to its hole is injective
[3]i.e., the map that sends each pigeon to its hole is surjective

2.4.4. Permutations

Theorem 1.7.2 in Lecture 12 says that if X is an n-element set (for $n \in \mathbb{N}$), then

$$(\text{\# of permutations of } X) = n!.$$

We can now formally prove this:

Proof of Theorem 1.7.2. The set X is finite. Thus, by the Pigeonhole Principle for Injections, every injective map $f : X \to X$ is bijective, thus is a permutation of X. Conversely, every permutation of X is bijective, thus injective. Therefore,

$$\{\text{permutations of } X\} = \{\text{injective maps from } X \text{ to } X\}.$$

Hence,

$$\begin{aligned}(\text{\# of permutations of } X) &= (\text{\# of injective maps from } X \text{ to } X) \\ &= n^{\underline{n}} \qquad (\text{by Theorem 2.4.4}) \\ &= n! \qquad (\text{by Proposition 2.4.3 } \mathbf{(d)}),\end{aligned}$$

qed. □

2.4.5. Surjective maps

So much for counting injective maps. Counting surjective maps is harder. The numbers will not have an explicit formula as nice as n^m or $n^{\underline{m}}$, so let us give them a name:

> **Definition 2.4.8.** Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Then, $\operatorname{sur}(m, n)$ shall mean the # of surjective maps from $[m]$ to $[n]$.

For instance, $\operatorname{sur}(3, 2) = 6$, because the surjective maps from $[3]$ to $[2]$ (written in one-line notation) are

$$(1,1,2), \qquad (1,2,1), \qquad (1,2,2), \qquad (2,1,1), \qquad (2,1,2), \qquad (2,2,1).$$

(We have previously defined one-line notation only for permutations of $[n]$, but we can similarly define it for maps from $[m]$ to $[n]$.)

We begin our study of surjective maps with a quasi-obvious fact:

> **Proposition 2.4.9.** 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. Apply the isomorphism principle. (That is, we relabel the elements of A as $1, 2, \ldots, m$, and we relabel the elements of B as $1, 2, \ldots, n$. The # of surjective maps from A to B clearly does not change when we do this. Hence, the # of surjective maps from A to B equals the # of surjective maps from $[m]$ to $[n]$; but the latter # is $\operatorname{sur}(m, n)$.) □

The problem of computing $\operatorname{sur}(m, n)$ is not that easy, so we approach it by first finding some particular values (again using the Iverson bracket notation):

Proposition 2.4.10. **(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 $\operatorname{sur}(0, n) = [n = 0]$ for all $n \in \mathbb{N}$.
(e) We have $\operatorname{sur}(1, n) = [n = 1]$ for all $n \in \mathbb{N}$.
(f) We have $\operatorname{sur}(m, n) = 0$ whenever $m < n$.

Proof. Try it yourself (and make sure your reasoning accounts for the empty set!). For a detailed proof, see Proposition 2.4.12 in the 2019 notes. □

References

[20f] Darij Grinberg, *Math 235: Mathematical Problem Solving*, 25 December 2021.
`http://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf`

[21f-2] Darij Grinberg, *Math 235 Fall 2021, Worksheet 2: The Pigeonhole Principles*, 5 October 2021.
`http://www.cip.ifi.lmu.de/~grinberg/t/21f/lec2.pdf`

[AndDos10] Titu Andreescu, Gabriel Dospinescu, *Problems from the Book*, 2nd edition, XYZ Press 2010.

[Bona17] Miklós Bóna, *A walk through combinatorics : an introduction to enumeration and graph theory*, World Scientific 2017.

[Engel98] Arthur Engel, *Problem-Solving Strategies*, Springer 1998.

[GelAnd17] Răzvan Gelca, Titu Andreescu, *Putnam and Beyond*, 2nd edition, Springer 2017.