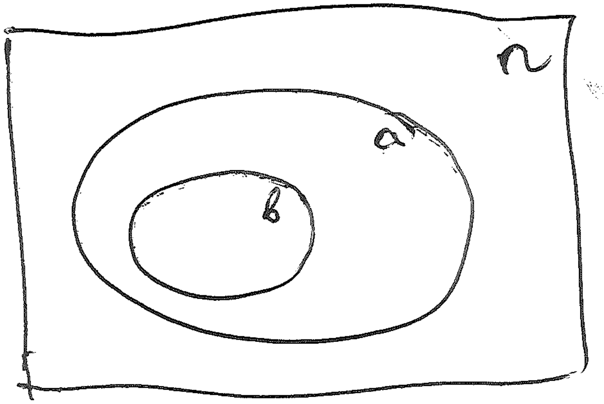
<u>Remark:</u> If $n, a, b \in \mathbb{N}$, then Prop. 2.2 can also be proven using double counting:

Consider a set $\mathcal{N}$ of n people.

$\binom{n}{a}\binom{a}{b}$ is the # of ways to choose a committee of a people from $\mathcal{N}$ and then choose a subcommittee of b people from this committee.

$\binom{n}{b}\binom{n-b}{a-b}$ is the # of ways to choose the same things, but in a different way: first choose the subcommitee, then choose $a-b$ further people to add to it, forming the commitee. $\square$



Cor. 2.3. Let $n \in \mathbb{N}$. Then, $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = [n=0]$.

1st proof (Jacob). Assume $n>0$ (WLOG).

$$\sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k}}_{=\binom{n-1}{k-1}+\binom{n-1}{k}} \cancel{= \sum_{k=0}^{n} (-1)^k \binom{n-1}{k-1} + \sum_{k=0}^{n} (-1)^k}$$

$$= \sum_{k=0}^{n} \left(\underbrace{(-1)^k}_{=-(-1)^{k-1}} \binom{n-1}{k-1} + (-1)^k \binom{n-1}{k} \right)$$

$$= \sum_{k=0}^{n} \left((-1)^k \binom{n-1}{k} - (-1)^{k-1} \binom{n-1}{k-1} \right)$$

telescope principle

$$= (-1)^n \underbrace{\binom{n-1}{n}}_{\text{Prop. 1.14: } 0} - (-1)^{0-1} \underbrace{\binom{n-1}{0-1}}_{=0} = 0. \qquad \square$$

2nd proof. Apply Thm. 1.21 to $x = -1$ and $y = 1$.

Thus,

$$((-1)+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \cancel{1^{n-k}} = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

Hence, $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = ((-1)+1)^n = 0^n = [n=0]$. $\square$

3rd proof. Rewrite $\sum_{k=0}^{n} (-1)^k \binom{n}{k}$ as

$$\sum_{k \text{ even}} \binom{n}{k} - \sum_{k \text{ odd}} \binom{n}{k},$$ where $k \in \{0, 1, \ldots, n\}$.

Thus, for $n > 0$, we must prove

$$\sum_{k \text{ even}} \binom{n}{k} = \sum_{k \text{ odd}} \binom{n}{k}. \qquad (5)$$

We can prove (5) bijectively:

The LHS of (5) is the # of subsets of $[n]$ of even size.

The RHS of (5) is the # of subsets of $[n]$ of odd size.

So we need a bijection

$$\{\text{subsets of } [n] \text{ of even size}\} \to \{\text{subsets of } [n] \text{ of odd size}\}.$$

One bijection we can use here is

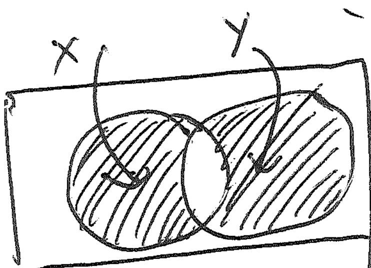
$$A \longmapsto \begin{cases} A \cup \{1\}, & \text{if } 1 \notin A; \\ A \setminus \{1\}, & \text{if } 1 \in A \end{cases}$$

(the inverse map is given by the same formula).

This proves Cor. 2.3 for $n > 0$. (Again, the $n = 0$ case is easy.) $\square$

<u>Rmk.</u> If X and Y are two sets, then the <u>symmetric difference</u> of X and Y is a set called $X \triangle Y$, defined by

$$X \triangle Y = \{\text{all elements that lie in exactly one of } X \text{ and } Y\} = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y).$$



← Venn diagram of $X \triangle Y$

Note that

$$X \triangle X = \emptyset;$$
$$X \triangle Y = Y \triangle X;$$
$$(X \triangle Y) \triangle Z = X \triangle (Y \triangle Z);$$
$$X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z).$$

The bijection used in the above 3rd proof is thus given by

$$A \longmapsto A \triangle \{1\}.$$

2.2. Counting maps

How many maps are there from a set to another?

Thm. 2.4. 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. Informally: Choosing a map f from A to B means (independently) choosing an image for each $a \in A$. Thus, there are n^m ways to do this (since there are m elements $a \in A$, and for each we have n options).

More rigorously: Let $(a_1, a_2, \ldots, a_m)$ be a list of all elements of A (with no repetitions). Then,

$$\begin{aligned} \{\text{maps } A \to B\} &\longrightarrow B^m, \\ f &\longmapsto (f(a_1), f(a_2), \ldots, f(a_m)) \end{aligned}$$

is a bijection. Thus,

$$|\{\text{maps } A \to B\}| = |B^m| = |B|^m = n^m,$$

since $|B| = n$. $\square$

<u>Thm. 2.5.</u> Let $m, n \in \mathbb{N}$. Let A be an m-element set. Let B be an n-element set. Then,

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

Rmk. (a) If $m=0$, then the RHS is
$n^{\underline{0}} = (\text{empty product}) = 1$.
And indeed, there is exactly one injective map from $A=\varnothing$ to B (namely, the "empty map": it sends nothing anywhere).

(b) If $m>n$, then the RHS is
$$n^{\underline{m}} = n(n-1)\cdots\cdots \underbrace{(n-n)}_{=0}\cdots(n-m+1) = 0.$$

And thus, $\nexists$ injective maps from A to B in this case.
(See Thm. 2.6 (a) below.)

1st proof of Thm. 2.5 (informal). Let $(a_1, a_2, \ldots, a_m)$ of A (with no repetitions). Then, an injective map $f : A \to B$ can be constructed as follows:

- choose $f(a_1)$ (there are n options for this, since we want $f(a_1) \in B$);
- choose $f(a_2)$ (there are $n-1$ options for this, since we want ~~$f(a_1) \in B$~~ $f(a_2) \in B \setminus \{f(a_1)\}$);

  to be distinct from $f(a_1)$
- choose $f(a_3)$ (there are $n-2$ options for this, since we want

  $$f(a_3) \in B \setminus \underbrace{\{f(a_1), f(a_2)\}}_{\substack{\text{a 2-element set,} \\ \text{since } f(a_1) \text{ and} \\ f(a_2) \text{ are distinct}}});$$

  to be distinct from $f(a_1)$ and $f(a_2)$
- etc. (last step: choose $f(a_m)$; there are $n-(m-1)$ options).

In total, we thus have

$$n(n-1)(n-2)\cdots(n-(m-1)) = n(n-1)\cdots(n-m+1) = n^{\underline{m}} \text{ options.}$$

$\square$

I will now show 2 more proofs, which are essentially just rigorous models for the 1st proof.

I will use the notation $\operatorname{Inj}(A,B)$ for the set of all injective maps from A to B.

Thus, Thm. 2.5 states that $|\operatorname{Inj}(A,B)| = n^{\underline{m}}$, where A, B, m, n are as in Thm. 2.5.

<u>2nd proof of Thm. 2.5. (explicit bijection).</u>

WLOG assume that $A = [m]$
(since $|\operatorname{Inj}(A,B)| = |\operatorname{Inj}([m],B)|$, because we can relabel the m elements of A as $1, 2, \ldots, m$
— like in the proof of Lemma 1.31).

WLOG assume that $B = [n]$ (for similar reasons).

Next, set $G = [n] \times [n-1] \times \cdots \times [n-m+1]$
$= \{(i_1, i_2, \ldots, i_m) \mid i_k \in [n-k+1] \ \forall k \in [m]\}$.

(Here, $[p] = \{1, 2, \ldots, p\}$ $\forall p \in \mathbb{Z}$. This means $[p] = \varnothing$ if $p \leq 0$.)

Observation 1: $|G| = n^{\underline{m}}$.

[Proof: If $m > n$, then both sides are 0 (since one of the factors in G is $\emptyset$).

Else, $|G| = |[n] \times [n-1] \times \cdots \times [n-m+1]|$

$$= \underbrace{|[n]|}_{=n} \cdot \underbrace{|[n-1]|}_{=n-1} \cdot \cdots \cdot \underbrace{|[n-m+1]|}_{=n-m+1}$$

$$= n(n-1)\cdots(n-m+1) = n^{\underline{m}}. \quad \square]$$

Now, we want a bijection from $\operatorname{Inj}(A,B)$ to G:

- Define a map $L : \operatorname{Inj}(A,B) \to G$ that sends each $f \in \operatorname{Inj}(A,B)$ to $(g_1, g_2, \ldots, g_m) \in G$, where g_i is such that $f(i)$ is the g_i-th smallest element of $B \setminus \{f(1), \ldots, f(i-1)\}$.

- To define a map $M : G \to \operatorname{Inj}(A,B)$, we send $(g_1, g_2, \ldots, g_m) \in G$ to the injective map $f \in \operatorname{Inj}(A,B)$

defined recursively as follows:

If $f(1), f(2), \ldots, f(i-1)$ are already defined, then $f(i)$ shall be the g_i-th smallest element of $B \setminus \{f(1), \ldots, f(i-1)\}$.

It is easy to see that L and M are well-defined & mutually inverse. So L is a bijection. Thus,

$|\operatorname{Inj}(A, B)| = |G| = n^{\underline{m}}$ (by Observation 1). $\square$

<u>3rd proof (induction).</u> Induction on m.

<u>Base</u>: $m = 0$. Here, $A = \varnothing$. Trivial (see Rmk (a) above).

<u>Step</u>: Let $k \in \mathbb{N}$. Assume (as $\underbrace{\text{IH}}_{\text{ind. hyp.}}$) that Thm. 2.5 holds for $m = k$. Now let us prove it for $k+1$.

Let A be a $(k+1)$-element set, and B an n-element set for some $n \in \mathbb{N}$. We must show

$$|\operatorname{Inj}(A,B)| = n^{\underline{k+1}}.$$

Fix $a \in A$. (This exists, since $|A| = k+1 > 0$.)
The set $A \setminus \{a\}$ has size $|A \setminus \{a\}| = |A| - 1 = (k+1) - 1 = k$.
Thus, the IH yields

$$(6) \qquad |\operatorname{Inj}(A \setminus \{a\}, B)| = n^{\underline{k}}.$$

The map

$$R : \operatorname{Inj}(A,B) \to \operatorname{Inj}(A \setminus \{a\}, B),$$
$$f \mapsto f|_{A \setminus \{a\}}$$

is well-defined.

<u>Observation 1:</u> Let $g \in \operatorname{Inj}(A \setminus \{a\}, B)$. Then, there are precisely $n-k$ maps $f \in \operatorname{Inj}(A,B)$ such that $R(f) = g$.

[<u>Proof:</u> To construct an $f \in \operatorname{Inj}(A,B)$ such that $R(f) = g$, we only need to choose a value $f(a)$. This value must be distinct from all values of g (in order for

f to be injective); there are precisely k values to avoid (because g is injective & thus takes exactly k different values). Thus, in total, there are $n-k$ options for $f(a)$. This proves Obs. 1.]

Now,

$$|\mathrm{Inj}(A,B)| = (\#\text{ of all } f \in \mathrm{Inj}(A,B))$$

$$= \sum_{g \in \mathrm{Inj}(A \setminus \{a\}, B)} \underbrace{(\#\text{ of all } f \in \mathrm{Inj}(A,B) \text{ such that } R(f) = g)}_{= n-k \text{ (by Obs. 1)}}$$

$$= \sum_{g \in \mathrm{Inj}(A \setminus \{a\}, B)} (n-k)$$

$$= \underbrace{|\mathrm{Inj}(A\setminus\{a\}, B)|}_{\overset{(6)}{=} n^{\underline{k}}} \cdot (n-k)$$

$$= n^{\underline{k}} \cdot (n-k) = n(n-1)\cdots(n-k+1)\cdot(n-k)$$

$$= n^{\underline{k+1}}.$$

This concludes the induction step. $\square$

Thm. 2.6. (Pigeonhole Principle for Injections).

Let $f: A \to B$ be an injective map between finite sets. Then:

(a) $|A| \leq |B|$.

(b) If $|A| = |B|$, then f is bijective.

<u>Proof.</u> Induction, LTTR. (see also [detnotes]) $\square$

<u>Rmk.</u> (b) is false if A, B are not finite.
For example, the map $\mathbb{N} \to \mathbb{N}$, $i \mapsto i+1$ is injective,
but NOT bijective.

<u>Thm. 2.7. (Pigeonhole Principle for Surjections).</u>
Let $f: A \to B$ be a surjective map between finite sets,

Then:
(a) $|A| \geq |B|$.
(b) If $|A| = |B|$, then f is ~~surjective~~ bijective.

<u>Rmk.</u> (b) is false if A, B are not finite.
For example, the map $\mathbb{N} \to \mathbb{N}$, $i \longmapsto \begin{cases} i-1 & \text{if } i > 0; \\ 0 & \text{if } i = 0 \end{cases}$

is surjective, but NOT bijective.

<u>Cor. 2.8.</u> Let X be a finite set. Then,

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

<u>Proof.</u> Thm. 2.6 (b) shows that every injective map from X to X is bijective. The converse also holds. Thus,

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

Hence,

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

But the LHS is (by Thm. 2.5, applied to $m = |X|$, $n = |X|$, $A = X$ and $B = X$) equal to

$$|X|^{\underline{|X|}} = |X| \cdot (|X|-1) \cdot \cdots \cdot \underbrace{(|X|-|X|+1)}_{=1} = |X|!.$$

Thus, the RHS is $|X|!$. $\square$

Now, let us count surjective maps $A \to B$.

Def. Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Then, $\operatorname{sur}(m,n)$ means the # of surjective maps from $[m]$ to $[n]$.

Prop. 2.9. Let $m, n \in \mathbb{N}$. Let A be an m-element set. Let B be an n-element set. Then,

(# of surjective maps from A to B) $= \operatorname{sur}(m,n)$.

Proof. Relabel the elements of A as $1, 2, \ldots, m$.
Relabel the elements of B as $1, 2, \ldots, n$.
(Like in the proof of Lem. 1.31.) $\square$

Prop. 2.10. (a) $\operatorname{sur}(m,0) = [m=0]$ for all $m \in \mathbb{N}$.

(b) $\operatorname{sur}(m,1) = [m \neq 0] = 1 - [m=0]$ for all $m \in \mathbb{N}$.

(c) $\operatorname{sur}(m,2) = 2^m - 2 + [m=0]$ for all $m \in \mathbb{N}$.

(d) $\operatorname{sur}(0,k) = [k=0]$ for all $k \in \mathbb{N}$.

(e) $\operatorname{sur}(1,k) = [k=1]$ for all $k \in \mathbb{N}$.

(f) $\operatorname{sur}(m,n) = 0$ if $m<n$.

<u>Proof.</u> (a) If $m \neq 0$, then $\nexists$ surjections $[m] \to [0]$ (since the arrows have nowhere to point).
If $m=0$, then there is exactly 1.

(b) There is always exactly 1 map $[m] \to [1]$.
It is surjective if & only if $m \neq 0$.

(c), (d), (e) LTTR.

(f) Thm. 2.7 (a) says that $\exists$ no surjections $[m] \to [n]$ when $m<n$. $\square$

Now, let us look for recursive formulas for $\operatorname{sur}(m,n)$.