Discrete Mathematics I

SoSe 17

Week 1 Lecture I

1. Numbers & Notations

$$\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \quad \text{(Integers)}$$
$$\mathbb{N} := \{0, 1, 2, 3, \ldots\} \quad \text{(Natural numbers)}$$

$\Rightarrow (\mathbb{Z}, +, \times)$ is a ring.

$\Rightarrow (\mathbb{N}, +)$ is a monoid. ($+$ is associative and 0 is the identity)

Def: Let $a, b \in \mathbb{Z}$,

we write $a \leq b \overset{def}{\Longleftrightarrow} b - a \in \mathbb{N}$.

[$\Rightarrow$ and $a = b \Leftrightarrow a \leq b$ and $b \leq a$.]

"$\leq$" is reflexive ($a \leq a$), anti-symmetric ($(a \leq b) \,\&\, (b \leq a) \Rightarrow a = b$), and transitive ($a \leq b \,\&\, b \leq c \Rightarrow a \leq c$)

Def: Let $X \subseteq \mathbb{Z}$ and $b \in \mathbb{Z}$. If $b \leq x$, $\forall x \in X$, then b is a lower bound for X.
If $b \in X$, then b is also a least member.

Well-ordering Axiom: If $X \subseteq \mathbb{Z}$ is non-empty and has a lower bound then X has a least member.

→ This is not true for $\mathbb{Q}$.

→ This allows us to count and use induction.

→ $\mathbb{Z}$ is <u>discrete</u>.

<u>Well-ordering for $\mathbb{N}$</u>

If $X \in \mathbb{N}$ and non-empty, then X has a least member.

<u>Thm [Induction principle]</u>

Let $S \subseteq \mathbb{N}$ be such that

i) $1 \in S$,

ii) $(\forall k \in \mathbb{N}) \quad k \in S \Rightarrow k+1 \in S$

Then $S = \mathbb{N}$.

<u>Pf</u> Exercise.

<u>Notations</u>

For now, we use the following conventions:

$[n] := \{1, 2, \ldots, n\}$, for $n \geq 1$. $\quad [0] := \emptyset := \{\}$

$n! := n(n-1)(n-2) \ldots 3 \cdot 2 \cdot 1$

$0! := 1$

If $X \subseteq \mathbb{N}$ has m members then $|X| := m$ and we say that X has <u>cardinality</u> or <u>size</u> m.

The empty set $\{\}, \emptyset$ has cardinality 0.

2. Relations & Functions

Let A, B be sets, then $A \times B := \{(a,b) : a \in A, b \in B\}$

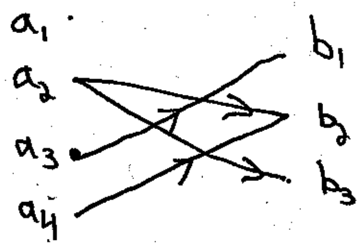
<u>Def</u>: Given two sets A and B, a <u>relation</u> R between A and B is any subset $R \subseteq A \times B$ of ordered pair in $A \times B$.

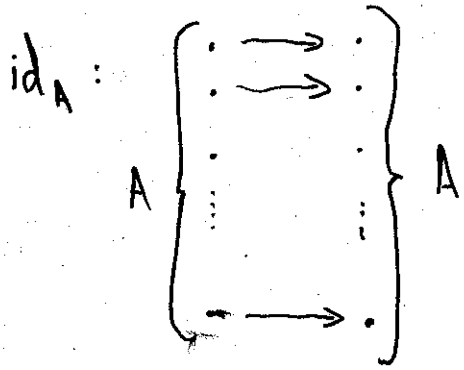
If $(a,b) \in A \times B$ and $(a,b) \in R$, "a & b are related by R"

<u>Domain</u>: $\mathrm{dom}(R) := \{a \in A \mid \exists b \in B, (a,b) \in R\}$

<u>Range/Codomain</u>: $\mathrm{codom}(R) := \{b \in B \mid \exists a \in A, (a,b) \in R\}$

<u>Ex</u>:





<u>Def</u>: A <u>function</u> f from a set A to a set B is a relation $f \subseteq A \times B$ such that $(\forall a \in A)$ if $(a, b_1) \in f$, $(a, b_2) \in f$ then $b_1 = b_2$.

A function f is <u>partial</u> if not all $a \in A$ are related to an element of B.

Otherwise it is <u>total</u>

⌜The codomain is also called the <u>image</u>⌟

Def: Given a function $f: A \to B$ with $A \neq \emptyset$,

- suppose there is some function $g: B \to A$ such that

$$g \circ f = id_A$$

then g is a <u>left inverse</u> of f.

- suppose ——— // ——— $h: B \to A$ such that

$$f \circ h = id_B$$

then h is a <u>right inverse</u> of f.

Observe: in $g \circ f$ → f must be total and?
→ What about g?

in $f \circ h$ → h must be total
→ What about f?

Lemma Let $f: A \to B$ be a function and suppose that

$$g \circ f = id_A \quad \& \quad f \circ h = id_B$$

Then $g = h$ and g is unique.

Pf Exercise.

Def A function $f: A \to B$ is <u>invertible</u> when there is a function $g: B \to A$ such that:

$$g \circ f = id_A \quad \& \quad f \circ g = id_B$$

g is denoted f^{-1}.

Def: Let $f: A \to B$ be a function.

- f is injective (or one-to-one) $f: A \hookrightarrow B$
  when $\forall a, b \in A \quad f(a) = f(b) \Rightarrow a = b$.

- f is surjective (or onto) $f: A \twoheadrightarrow B$
  when $(\forall b \in B), (\exists a \in A)$ s.t. $b = f(a)$.
  $(\Leftrightarrow \operatorname{Im}(f) = B)$.

- f is bijective when f is injective & surjective

Thm: Let $f: A \to B$ be a function with $A \neq \emptyset$.

a) f is injective $\Leftrightarrow$ f has a left inverse

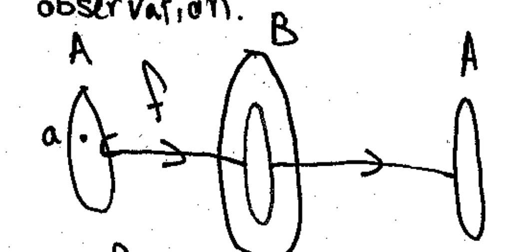
b) f is surjective $\Leftrightarrow$ f has a right inverse

c) f is bijective $\Leftrightarrow$ f is invertible

Pf]

a) $\Leftarrow$) See observation.

$\Rightarrow$)



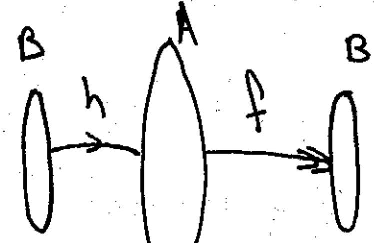
$g \circ f = Id_A$

$a \xmapsto{f} f(a) \xmapsto{g} a$ (if ~~f(a)~~ element is in $\operatorname{Im}(f)$)

$b \longmapsto a_0$ (since $A \neq \emptyset$, pick one)

b) $\Leftarrow$) See observation.

$\Rightarrow$)



Since $A \neq \emptyset$ and f is surj. $\Rightarrow B \neq \emptyset$.

$\forall b \in B \quad f^{-1}(b) = \{a \in A \mid f(a) = b\} \neq \emptyset$.

Hence $\boxed{\text{"pick"}}$ an element x_b in each

and define $h: B \to A$
$b \to x_b$

c) Lemma ④ a) + b)

<u>"pick"</u>: This requires the <u>Axiom of Choice</u> (for uncountable sets)

<u>Axiom of choice:</u> $(\forall\ R \subseteq A \times B)$, $\exists$ a partial function $f: A \to B$
$f \subseteq R$ and $\mathrm{dom}(f) = \mathrm{dom}(R)$.

<u>Def</u>: A set A is <u>equinumerous</u> to a set B, $A \approx B$
when $\exists\, f: A \to B$ which is bijective.

<u>Lemma</u>: If $f: A \to B$

a) f injective, then $|A| \leq |B|$
b) f surjective, then $|B| \leq |A|$
c) f bijective, then $|A| = |B|$

Wooo! What about "infinite" sets?

<u>Def</u>:
- A set is <u>finite</u> if it is equinumerous to a set of the form $[n]$ for some $n \in \mathbb{N}$.
- A set is <u>infinite</u> when it is not finite.
- A set A is <u>countable</u> when $\exists\, f: A \hookrightarrow \mathbb{N}$ injective.

When $f: A \to A$ is bijective and A is countable
we say that A is a <u>permutation of A</u>.

<u>Lemma</u>: $\mathbb{N}$ is infinite

<u>Pf</u>| Assume the opposite, i.e. $\exists\, f: \mathbb{N} \xrightarrow{\text{bij}} [n]$ for some $n \in \mathbb{N}$.
Form $A = \{f(a) + 1 \mid a \in \mathbb{N}\}$, $|A| = n$ and the least member of $f(\mathbb{N})$ is not in A $\Rightarrow$ $|f(\mathbb{N}) \cup A| > n$ and $f(\mathbb{N}) \cup A \subset \mathbb{N}$

↯ $\boxtimes$

3. Elementary counting problems

Subsets

Let $A \subseteq \mathbb{N}$. How many sets B such that $B \subseteq A$ are there?

For $B \subseteq A$, define $\chi_B : A \to \{0,1\}$

$$\chi_B(x) = \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{if } x \notin B. \end{cases}$$

$$\to \chi : 2^A \to \{0,1\}^{|A|} \qquad 2^A := \text{Power set.}$$
$$B \mapsto \chi_B$$

- χ is bijective (Check!)

$\{0,1\}^A$ has $\underline{2^{|A|} \text{ elements}}$. $\Rightarrow 2^{|A|}$ subsets.

Permutations

Let $A \subset \mathbb{N}$, s.t. $|A| = n > 0$.

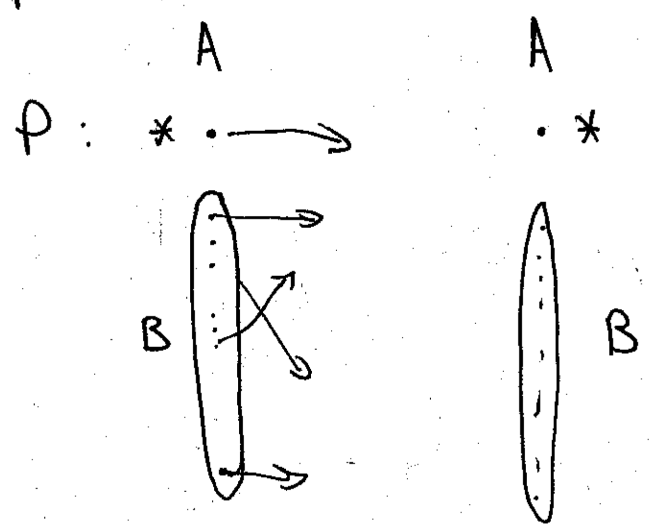
How many permutations of A (i.e. bij. $f : A \to A$) are there?

Pf | If $n=1$, Id_A is the only bijection.
If $n > 1$, let p_{n-1} be the number of permutations of a set of card. $n-1$.

Write $A = \{*\} \cup B$ B is a set of card $n-1$.   8

your favorite element in A.

Then a permutation P of A looks like:



$*$ has n possible images. <u>AND</u>

<u>after</u> for B there are $n-1$ possible images

i.e.

$$P': B \longrightarrow A \setminus \{P(*)\} \approx B$$

is a permutation of B (after relabeling).

There are
- P_{n-1} choices for P'
- n choices for the image of $*$.

$\Rightarrow n \cdot P_{n-1} \Rightarrow n!$.

Cycles

A permutation p of $A = \{a_1, \dots, a_n\}$ is cyclic if it can be written as

$$a_1 \xrightarrow{p} a_2 \xrightarrow{p} \cdots \xrightarrow{p} a_{n-1} \to a_n \to a_1$$

$(a_i \neq a_j$ for $i \neq j)$
$i, j \in [n]$.

How many cyclic permutations are there?
Let $\mathcal{C}_n$ be the number of cyclic permutations of A.

A cycle can start anywhere.
Fix a_1 to be the first element written.

- Then any permutation of $A \setminus \{a_1\}$ gives distinct cycles:
  Hence at least $(n-1)! \Rightarrow |\mathcal{C}_n| \geq (n-1)!$
- Any cycle gives rise to such a permutation p of $A \setminus \{a_1\}$
  (once we fix an ordering of $A \setminus \{a_1\}$)

$$a_1 \to \underbrace{a_2 \to \cdots \to a_n}_{p} \to a_1$$

$$\Rightarrow |\mathcal{C}_n| \leq (n-1)!$$

- Therefore $|\mathcal{C}_n| = (n-1)!$.

Combining things

Addition principle

If $A_1, A_2, \ldots, A_n$ are mutually disjoint finite sets then

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|$$

pf) If $x \in A_i$ it is counted once on each side.
If $x \notin A_i$, $\forall i \in [n]$, it is never counted $\boxtimes$

Interpretation

$$\underbrace{\text{Task } T}_{r+s \text{ ways}} = \underbrace{\text{Task } R}_{r \text{ ways}} \ \underset{\text{(exclusive)}}{\underline{\text{or}}} \ \underbrace{\text{Task } S}_{s \text{ ways}}$$

Multiplication principle

Given n finite sets $A_1, A_2, \ldots, A_n$ the number of ways to select one element from each set independently is

$$|A_1| \cdot |A_2| \cdot \ldots \cdot |A_n| = |A_1 \times \ldots \times A_n|$$

Interpretation:

$$\underbrace{\text{Task } R}_{r \text{ ways}} \ \underline{\text{followed by}} \ \underbrace{\text{Task } S}_{s \text{ ways}} = \underbrace{\text{Task } T}_{r \times s \text{ ways.}}$$

Week 1 Lecture 2

Standard Proof Techniques

- Double counting vs algebraic proof

(Double counting can be ambiguous...)

One set: S Two ways to count $|S|$.

- The number of subsets of $[n]$ is 2^n: each element of $[n]$ is in or not. [Forming a committee...]
  By the multiplication principle we get 2^n choices.

- The number of subsets of $[n]$ is $\sum_{i=0}^{n} \binom{n}{i}$
  - There is $\binom{n}{0}$ ways to get 0 element from $[n]$
  - $\binom{n}{1}$ ——— 1 ——//——
  - ⋮
  - There is $\binom{n}{n}$ ——— n ——//——

Thus $\boxed{2^n = \sum_{i=0}^{n} \binom{n}{i}}$, where $\binom{n}{i}$ is the number of i-subsets of an n-element set.

What is $\binom{n}{i}$?

- $\binom{n}{i} = 0$ if $i<0$ or $i>n$ ✓
- $\binom{n}{i} = \dfrac{n!}{i!\,(n-i)!}$

pf

1) Permute the n-set : $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n)\end{pmatrix}$ Two-line notation

   There are $n!$ ways to do this

2) Pick the first "i" entries to be the i-subset.

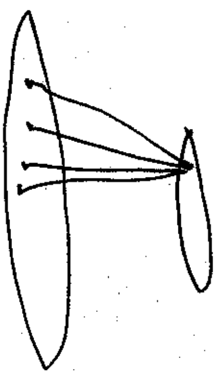
   (*) Every "i"-subset is constructible

3) We over constructed.

   (**) Each i-subset appear $\underbrace{i!}_{\substack{\text{permutes}\\ \text{the } i \text{ first}\\ \text{entries}}}\ \underbrace{(n-i)!}_{\substack{\# \\ \# \ n-i \text{ last}\\ \text{entries}}}$ times

4) We partitionned the permutations into $\dfrac{n!}{i!(n-i)!}$ types

   $\rightsquigarrow \binom{n}{i} = \dfrac{n!}{i!(n-i)!}$



$f : [\text{Perm. of } [n]] \longrightarrow [i\text{-subsets of } [n]]$

(*) f is surjective

(**) $f^{-1}(x)$ has card. $i!(n-i)!$

$\Rightarrow$ # i-subsets of $[n]$ is $\dfrac{n!}{i!(n-i)!}$

⊠

Algebraic proof of $2^n = \sum_{i=0}^{n} \binom{n}{i}$

Claim: $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$ for $0 \le i \le n-1$

Pf of claim: Compute

$$\frac{n!}{i!(n-i)!} + \frac{n!}{(i+1)!(n-i-1)!} = \frac{n!(i+1) + n!(n-i)}{(i+1)!\,(n-i)!}$$

$$= \frac{(n+1)!}{(i+1)!(n-i)!} = \binom{n+1}{i+1}$$ ┘

Pf $\underline{n=1}$: $2^0 = 1 = \sum_{i=0}^{0} \binom{0}{i} = 1$ ✓

$\underline{n>1}$:

$$2^n = 2 \cdot 2^{n-1} \overset{\text{ind. hyp.}}{=} 2 \cdot \left(\sum_{i=0}^{n-1} \binom{n-1}{i} \right)$$

$$= \binom{n-1}{0} + \binom{n-1}{1} + \cdots + \binom{n-1}{n-2} + \binom{n-1}{n-1}$$

$$+ \binom{n-1}{0} + \cdots + \binom{n-1}{n-3} + \binom{n-1}{n-2} + \binom{n-1}{n-1}$$

$$= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-2} + \binom{n}{n-1} + \binom{n}{n}$$

$$= \sum_{i=0}^{n} \binom{n}{i}. \quad \boxtimes$$

Examples (Week 1)

1) How many 6 letters password is there?

Answer: By the multiplication principle there is $(26)^6$ possible pass words.

2) How many strings (or words) of 3 or 4 letters, all different, contain at least 1 vowel and 1 consonant?

Answer: Let $C_n = \{$ Strings of n distinct letters $\}$

Disjoint sets
$A_n = \{$ Strings of n distinct vowels $\}$
$B_n = \{$ —— II —— consonants $\}$
$X_n = \{$ Stings of n distinct letters w/ at least 1 vowel and 1 consonants $\}$

$$C_n = A_n \cup B_n \cup X_n$$

By the addition principle, $|C_n| = |A_n| + |B_n| + |X_n|$

We are looking for $|X_3 \cup X_4| = |X_3| + |X_4| = |C_3| - |A_3| - |B_3| + |C_4| - |A_4| - |B_4|$.

$|C_3| = 26 \cdot 25 \cdot 24$ $\quad$ $|C_4| = 26 \cdot 25 \cdot 24 \cdot 23$

$|A_3| = 6 \cdot 5 \cdot 4$ $\quad$ $|A_4| = 6 \cdot 5 \cdot 4 \cdot 3$

$|B_3| = 20 \cdot 19 \cdot 18$ $\quad$ $|B_4| = 20 \cdot 19 \cdot 18 \cdot 17$

$\Rightarrow |X_3| = 8640$ $\quad$ $\Rightarrow |X_4| = 242\ 160$

$$\Rightarrow |X_3 \cup X_4| = 250\ 800.$$