Discrete Mathematics I

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

1) $\binom{n}{i} = 0$ if $i < 0$ or $i > n$

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

Proof #2

Task: Pick one subset of $[n]$ of cardinality i.

This can be done in "i" steps:

Step 1: Pick 1 of the n elements. (n ways)

Step 2: — " — 1 — " — $n-1$ elements left. ($(n-1)$ ways)

$\vdots$

Step i: — " — 1 — " — $n-i+1$ elements left. ($n-i+1$ ways)

Hence, by the multiplication principle, this task can be done in $n \cdot (n-1) \cdots (n-i+1) = \dfrac{n!}{(n-i)!}$ ways.

But! By doing so we obtain $i!$ times each of the i-subsets of n. (By permuting the order of the choices).

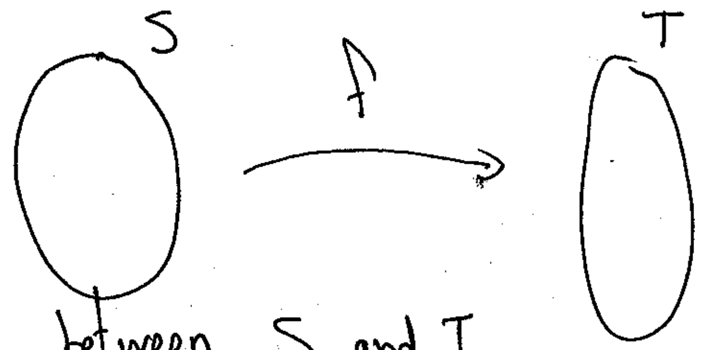
Therefore, we divide by $i!$ to get

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

$\boxtimes$

What is a Bijective Proof

Two sets:



Find a bijection between S and T.

Examples

1) $S = \{ A \subseteq [n] \mid |A| = i \}$
$T = \{ A \subseteq [n] \mid |A| = n-i \}$

$$f : S \to T \qquad f \text{ is bijective.}$$
$$A \mapsto [n] \setminus A$$

$$\Rightarrow \binom{n}{i} = \binom{n}{n-i}.$$

2) $S = \{ A \subseteq [n] : |A| = i \}$
$U = \{ A \subseteq [n] : |A| = i, 1 \in A \} \cup \{ A \subseteq [n] : |A| = i, 1 \notin A \}$

$$g : S \to U$$
$$A \mapsto A$$ (it is sent to one of the two sets forming U).

g is bijective (check!)

$$\Rightarrow \binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}.$$

3) Let $n, k, p \in \mathbb{N}$, then

$$\binom{n+k}{n+p} \cdot \binom{n+p}{p} = \binom{n+k}{n} \cdot \binom{k}{p}$$

Pf | - If $k < p$ then both side are 0.

Otherwise, consider

Task T: Select "p" employees from "n+k" applicants, where some subset of the candidates (greater than p) should pass an interview.

Task T can be split into two consecutive tasks as follows:

1) - First, select "n+p" applicants for the short list.
   - Then, from the short list, select "p" employees.

   By the M.P. there are

   $\binom{n+k}{n+p} \cdot \binom{n+p}{p}$ ways to do this. (since $p \le k$)

2) - First, reject "n" applicants from the "n+k".
   - Then, select "p" employees from the "k" remaining that passed an interview.

   By the M.P. there are

   $\binom{n+k}{n} \binom{k}{p}$ ways to do this.

We counted in two ways the same task, hence the numbers are equal. ∎

4) For all $n, i \in \mathbb{N}$ $\quad \sum_{j=0}^{n} \binom{j}{i} = \binom{n+1}{i+1}$

pf| Task: Choose a $(i+1)$-element subset of a $(n+1)$-element set.

1) The RHS counts this directly $\rightarrow \binom{n+1}{i+1}$ ways.

2) The LHS counts this task in $n+1$ disjoint classes: The j-th class counts the number of $(i+1)$-subsets where the largest element is "$j+1$"

$\hookrightarrow$ There are $\binom{j}{i}$ elements in the j-th class.

The equality follows from the addition principle. $\boxtimes$

5) (Vandermonde's Sum)

For all $n, m, k \in \mathbb{N}$, we have

$$\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i} \cdot \binom{m}{k-i}$$

pf| Task: Select a committee of k individuals among "n" bachelor students and "m" master students.

1) This is counted directly by $\binom{n+m}{k}$ (LHS).

The RHS also counts this in $(k+1)$ disjoint sets. The i-th class counts the commitees with "i" bachelor students. There are $\binom{n}{i}\cdot\binom{m}{k-i}$ ways to do this by the M.P. The equality holds by the A.P. ⊠

The Binomial Theorem

Let $n \in \mathbb{N}$. Then
[(and $a,b \in \mathbb{R}$) say]

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Pf| Monomials in the expansion of $(a+b)^n$ are of the form $a^i b^{n-i}$ for some $i \in \{0,1,\dots,n\}$.
To get $a^i b^{n-i}$, we need to choose "i" brackets where the a's are coming from; the other terms will give "$n-i$" b's.
There are $\binom{n}{i}$ ways to make this choice giving the formula. ⊠

Applications

1) Show that $\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$

Pf| Consider $(1+x)^n(1+x)^n = (1+x)^{2n}$

By the Binomial Thm:

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i.$$

The coefficient of x^n on the LHS is obtained by summing the pairings "x^i" with "x^{n-i}" that have coefficients $\binom{n}{i}$ and $\binom{n}{n-i}$ respectively.
Since $\binom{n}{n-i} = \binom{n}{i}$ we get that the coeff of x^n is

$$\sum_{i=0}^{n} \binom{n}{i}^2.$$

On the other hand, the coefficient of "x" in $(1+x)^{2n}$ is $\binom{2n}{n}$ by the B.T. ☒.

---

2) Let $n \in \mathbb{N} \setminus \{0\}$, then

$$\sum_{i=0}^{n} \binom{n}{i} (-1)^i = 0$$

Pf| Let $a = 1$ and $b = -1$ in the Binomial Theorem ☒

---

3) What is the coefficient of x^4 in $(3x + 5y + 7)^6$?

Solution: Write $(\underbrace{3x}_{a} + \underbrace{(5y+7)}_{b})^6 = (a+b)^6 \underset{\text{B.T.}}{=} \sum_{i=0}^{6} \binom{6}{i} a^i b^{6-i}$.

The monomial x^4 only appears when $i=4$ in the above sum.
Hence the coefficient is

$$\binom{6}{4} a^4 b^2 = \binom{6}{4} (3x)^4 (5y+7)^2 = \underbrace{\binom{6}{4} 3^4 (5y+7)^2}_{\text{Solution.}} x^4$$

4) For all $n \geq 0$,

$$n \cdot 2^{n-1} = \sum_{k=0}^{n} k \binom{n}{k}$$

Pf| From the B.T.,

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

Differenciating both sides w.r.t. x,

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

Then substitute "x" by "1" to get the desired equality. ⊠

The Inclusion-Exclusion Principle

Let $P_1, P_2, \ldots, P_r$ be properties that elements of a set S can have. Define $A_i := \{a \in S : a \text{ has property } P_i\}$.

We have

$$\left|\bigcup_{i=1}^{r} A_i\right| = \sum_{i=1}^{r} |A_i| - \sum_{1 \leq i, j \leq r} |A_i \cap A_j| + \sum_{1 \leq i < j \leq k \leq r} |A_i \cap A_j \cap A_k|$$

$$+/- \cdots + (-1)^{r-1} |A_1 \cap A_2 \cap \cdots \cap A_r|.$$

$$= \sum_{\emptyset \neq J \subseteq [r]} (-1)^{|J|-1} \left|\bigcap_{j \in J} A_j\right|.$$

By de Morgan's laws:

$$\Big|\bigcap_{i=1}^{r} \underbrace{\overline{A_i}}_{\overset{\text{def}}{\Downarrow}\ S\setminus A_i}\Big| = \Big|S-\bigcup_{i=1}^{r} A_i\Big| = |S| - \sum_{i=1}^{r}|A_i| + \sum_{1\le i<j\le r}|A_i\cap A_j|$$

$$-/+ \cdots + (-1)^r\,|A_1\cap\dots\cap A_r|.$$

Warning: the exponent "r" here is correct. Compare it with the other formula.

Pf] Take $s\in S$.

- If s is not in $\bigcup_{i=1}^{r} A_i$ then it is not counted in any part of the RHS. (and not on the LHS either...)
- Else, let $I\subseteq[r]$ be the set of indices i s.t. $s\in A_i$.
  - In the 1^{st} sum, "s" is in $|I|$ summand ($|I|\geq 1$).
  - In the 2^{nd} sum, "s" is in $\binom{|I|}{2}$ — // —

    ⋮

  - In the $|I|^{th}$ sum, "s" is in $\binom{|I|}{|I|}$ — // —

Hence "s" is counted a total of

$$\underbrace{\binom{|I|}{1}-\binom{|I|}{2}+\binom{|I|}{3} +/- \cdots + (-1)^{|I|-1}\binom{|I|}{|I|}}_{=:K} \text{ times.}$$

We can write, after setting $|I|=:t$

$$-(K-1) = 1-\binom{t}{1}+\binom{t}{2}-\binom{t}{3}+\cdots+(-1)^{t-1}\binom{t}{t}.$$

$$= \sum_{i=0}^{t}\binom{t}{i}(-1)^{t-i} = (1-1)^t = 0. \quad (\forall t\in\{1,\dots,r\})$$

$$\Rightarrow K=1 \quad \boxtimes.$$

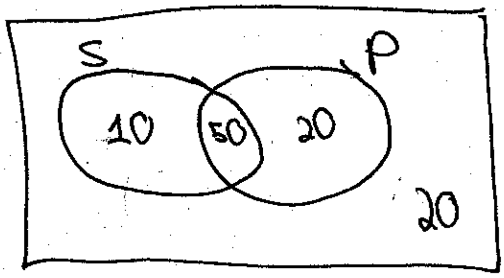
Example

At the last exam

- 60 students studied (Set S)
- 70 " passed (Set P)
- 50 " did both (Set $P \cap S$)
- 20 " did not do either (Set $(P \cup S)^c$)

How many students were at the exam?

Answer: The class "C"



$$|C| = |(P \cup S)^c| + |P \cup S| = 20 + (60 + 70 - 50) = 100$$

Example: (Dérangements)

A new Iphone virus (or feature?) permutes the phone numbers in the ~~address~~ contacts book. [Assume each entry has one number only] in the ~~address~~ contacts book

If an Iphone gets the virus and has n contacts, in how many ways can the virus permute the numbers so that no contact gets it own number?

For $n=0$, $D(0) = 1$ $\quad n=2$, $D(2) = 1$

$n=1$, $D(1) = 0$

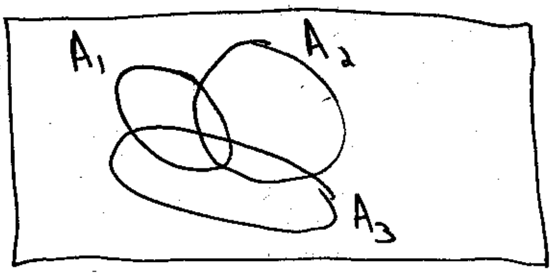
<u>$n=3$</u>

Person A	Person B	Person C
# B	# C	# A
# C	# A	# B

↳ Method: Go through each permutation and check for each n...

... This is long and inefficient.

⇝ Use Inclusion - Exclusion principle!



Let $S := \{ \text{permutations of } [n] \}$

$A_i := \{ \text{permutations of } [n] \text{ that fix "} i \text{"} \}$

$D := \{ \text{dérangements of } [n] \} = \{ \text{permutations of } [n] \text{ without fixed points} \}$

Then $D = \bigcap_{i=1}^{n} \overline{A_i} = S - \bigcup_{i=1}^{n} A_i$.

By the Incl.-Excl. principle

$$|D| = |S| - \sum_{i=1}^{n} |A_i| + \sum_{1 \le i < j \le n} |A_i \cap A_j| -/+ \dots + (-1)^n |A_1 \cap \dots \cap A_n|$$

$|A_i| = (n-1)!$ because "i" is fixed and the rest is permuted.

$|A_i \cap A_j| = (n-2)!$ because 2 elements are fixed ——〃——.

Therefore

$$|D| = n! - \sum_{i=1}^{n} (n-1)! + \sum_{1 \le i < j \le n} (n-2)! \; -/+ \cdots + (-1)^n \cdot 1$$

$$= n! - n! + \binom{n}{2}(n-2)! \; -/+ \cdots + (-1)^n \cdot 1$$

$$= n! - n! + \frac{n!}{2!} \; -/+ \cdots + (-1)^n \frac{n!}{n!}$$

$$= n!\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right)$$

$$= \boxed{n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}}$$

Example: (Euler's totient function)

For $n \in \mathbb{N}$, let $\varphi(n) = \#$ integers m such that $m < n$ and $(m,n) = 1$.

$$\varphi(n) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

Pf] Let $P = \{ p_i \mid p_i \mid n \}$ (prime.) and $|P| = k$

and $A_i = \{ j : j \leq n \text{ and } p_i \mid j \}$

We want $\left| [n] \setminus \bigcup_{i=1}^{k} A_i \right|$

$$= n - \sum_{i=1}^{k} |A_i| + \sum_{1 \leq i \leq j \leq k} |A_i \cap A_j| -/+ \cdots +(-1)^k |A_1 \cap \cdots \cap A_k|$$

$$= n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{i \leq j} \frac{n}{p_i p_j} -/+ \cdots + (-1)^k \cdot \frac{n}{p_1 \cdots p_k}$$

$$= n \cdot \left[1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i \leq j} \frac{1}{p_i p_j} -/+ \cdots + (-1)^k \frac{1}{p_1 \cdots p_k} \right]$$

$$= n \left[\prod_{p \in P} \left(1 - \frac{1}{p} \right) \right]$$

$\square$

The Pigeonhole Principle

Theorem (Pigeonhole Principle)
No set of the form $[n]$ is equinumerous to a proper subset of itself, where $n \in \mathbb{N}$.

Pf|

Claim: If $f : [n] \to [n]$ is injective then it is surjective (thus bijective).

Suppose $[n]$ is in bijection with a proper subset of itself.

That is, there exists $g : [n] \hookrightarrow [n]$ where $\underset{\overset{\shortparallel}{Im(g)}}{A}$ is a proper subset of $[n]$

By the claim g is also surjective.

$\lightning$ contradiction with the fact that A is a proper subset $\square$

Take Home:
"If m objects are distributed into n boxes, and $m > n$, then at least one box receives at least two objects."

Theorem (Sharper Pigeonhole Principle)
Let $f : N \to R$ be a function with $|N| = n > r = |R|$.
Then, $\exists\, a \in R$ such that $|f^{-1}(a)| \geq \lfloor \frac{n-1}{r} \rfloor + 1$.

Pf| If $|f^{-1}(a)| \leq \lfloor \frac{n-1}{r} \rfloor$, $\forall a \in R$, then

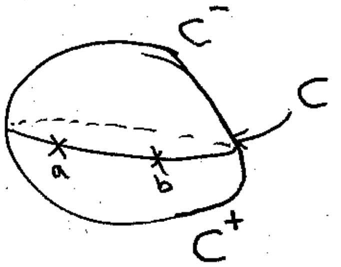
$$n = \sum_{a \in R} |f^{-1}(a)| \leq r \left\lfloor \frac{n-1}{r} \right\rfloor < n . \quad \lightning \qquad \square$$

Application of the Pigeonhole Principle

1) Given 5 pts on a sphere, there is a closed hemisphere containing at least four of them.

Pf) Take two points. There is a great circle C passing through them.

Split the sphere S into two dis-joint sets



$$S = C^- \sqcup (C \sqcup C^+)$$

open hemispheres

Then, by the pigeonhole principle either C^- or $C \sqcup C^+$ contains at least 2 of the 3 other pts.

Say C^-, then $C \sqcup C^-$ is the closed hemisphere.

Otherwise, $C \sqcup C^+$ —— // —— .

∎

2) Erdös-Szekeres Theorem '35

Let $n \geq 0$. Every sequence of length n^2+1 of pairwise distinct natural numbers must contain either an increasing subsequence or a decreasing subsequence of length $n+1$.

Pf) (Seidenberg '59)

Label each natural number in the sequence by a pair of positive natural numbers as follows.

Let s_i be the i-th number in the sequence.

s_i receives label (a_i, b_i) where

a_i = length of the longest increasing seq. ending at s_i.

b_i = —— // —— decreasing —— // ——.

For $i<j$, then

either $s_i < s_j \Rightarrow a_i < a_j$.

or $s_i > s_j \Rightarrow b_i < b_j$.

$\Rightarrow$ all labels are distinct!

We have n^2+1 distinct label hence one of them has to contain an entry $> n$ by the pigeonhole principle. ☒

---

3) <u>Chinese Remainder Theorem</u>

Let m and n be relatively prime positive integers.

The system

$$x \equiv a \pmod m$$
$$x \equiv b \pmod n$$

has a solution for x.

<u>pf</u> • Consider the numbers

$$\underbrace{a,\ m+a,\ 2m+a,\ \ldots,\ (n-1)m+a}_{n \text{ numbers that are } \equiv a \pmod m}.$$

• Consider then $im+a$ and $jm+a$ with $0 \leq i < j < n$.

Suppose that $im + a \equiv jm + a \pmod n$.

$$\Rightarrow \begin{aligned} im + a &= q_i n + r \pmod n \\ jm + a &= q_j n + r \pmod n \end{aligned}$$

for some q_i, q_j, r.

Substracting: $(j-i)m = (q_j - q_i)n$.

Since $(m,n) = 1 \Rightarrow n \mid (j-i) \Rightarrow i = j$. $\lightning$ (with the choice of i, j).

Every number in 0 to $n-1$ appears as remainder mod n, in particular, "b" does. ☒

---

4) Ramsey's Thm (a first version)

In any group of six people there are 3 people that mutually know each other or three people that do not know each other.

Pf| Take one person in the group, say "A".

The other 5 either know or don't know "A".

By the sharper pigeonhole principle either

i) 3 don't know A, $\}$ =: group "B"

or ii) 3 know A.

Case i) - If 2 among group "B" don't know each other, 3 people mutually don't know each other.

- Otherwise they form 3 people that know each other.

$\downarrow$ group B

Case ii) is similar.

☒

5) Lossless data compression algorithm

"Lossless data compression algorithm cannot guarantee compression for all input data sets."

That is, "For any lossless d.c.a., there is a data set that does not get smaller."

Pf) Let A be a lossless d.c.a. and $S = \{ f : f \text{ a finite binary file} \}$ be some set of files encoded as binary strings. ↳ f is a sequence of 0's and 1's

Assume: 1) "A" compresses files in S such that

"new length of f $\leq$ length of f"

2) $\exists f \in S$, such that "new length of f < length of f".

Let $s \in S$ be the shortest file satisfying 2).

Let M be the length of "s".

Let N be the compressed length of "s", i.e. $N < M$.

Together with "s", there are $2^N + 1$ files compressed into 2^N files of length N.

By the pigeonhole principle, there are two files which are compressed to the same output.

↯ "A" can not be lossless: how to recover the two files from one compresed?

That means that lossless d.c.a. have to make some files longer!