Theorem

Let A and B be finite sets with $|A| = m$, $|B| = n$. Then

$$|\{f : A \to B : f \text{ is injective}\}| = n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!}$$

An informal argument

let f be an injective map $A \to B$. We can assume that $A = \{1, \dots, n\}$. Then $f(1)$ can have n possible values. Once $f(1)$ is fixed, $f(2)$ can have $n-1$ values, since we must have $f(2) \neq f(1)$. Then $f(3)$ can have $n-2$ values since $f(2) \neq f(1), f(2)$. Continuing this way we conclude that $f(k)$ can take $n-k+1$ values, for $f(k)$ cannot be equal to already fixed $f(1), \dots, f(k-1)$. Thus, the total number of injective maps from A to B is

$$\begin{aligned} & n(n-1)\cdots(n-m+1) \\ & \qquad = \frac{n(n-1)\cdots(n-m+1)(n-m)(n-m-1)\cdots 1}{(n-m)(n-m-1)\cdots 1} = \frac{n!}{(n-m)!}. \end{aligned}$$

A formal argument

Let $\mathcal{I}(m, n)$ be the set of injective maps from I_m to I_n where $I_k = \{1, \dots, k\}$. If $m = 1$ then clearly $\mathcal{I}(m, n)$ contains precisely n elements.

If $m > 1$ then $\mathcal{I}(m, n)$ is the union of sets X_i where $X_i = \{f \in \mathcal{I}(m, n) : f(m) = i\}$, $1 \leq i \leq n$.

Clearly, $X_i \cap X_j = \emptyset$ if $i \neq j$.

Also, $|X_i| = |X_j|$ for all $1 \leq i, j \leq n$, so

$$|\mathcal{I}(m, n)| = |X_1| + \cdots + |X_n| = n|X_n|.$$

Now, $|X_n| = |\mathcal{I}(m-1, n-1)|$ since if $f \in X_n$ then f is uniquely determined by $f|_{I_{m-1}}$ which is an injective map from I_{m-1} to I_{n-1}.

Thus, $|\mathcal{I}(m, n)| = n|\mathcal{I}(m-1, n-1)| = n(n-1)|\mathcal{I}(m-2, n-2)| = \cdots = n(n-1)\cdots(n-m+1)$.

Theorem

Let A, B be finite sets with $|A| = |B|$ and let $f : A \to B$ be a map. The following are equivalent:

(1) *f is injective*

(2) *f is surjective*

(3) *f is bijective*

Proof.

(1) $\Longrightarrow$ (2) If f is injective then $|\operatorname{im} f| = |A| = |B|$. Since $\operatorname{im} f \subset B$ and B is a finite set, it follows that $\operatorname{im} f = B$ that is f is surjective.
(2) $\Longrightarrow$ (1) If f is surjective then $|f^{-1}(\{b\})| \geq 1$ for all $b \in B$. Suppose that $|f^{-1}(\{b\})| > 1$ for some $b \in B$. Since $f^{-1}(\{b'\}) \cap f^{-1}(\{b''\}) = \emptyset$ for all $b' \neq b'' \in B$, we have

$$|A| = |f^{-1}(B)| = \sum_{b' \in B} |f^{-1}(\{b'\})| > |B|.$$

This is a contradiction. Thus, $|f^{-1}(b)| = 1$ for all $b \in B$, that is, f is injective. $\square$

Proof.

(3) $\implies$ (1) If f is bijective then it is injective.
(1) $\implies$ (3) If f is injective then it is also surjective (we already proved it) and so it is bijective. $\square$

The assumption that A and B are finite sets is essential. For example, if $A = \mathbb{N} = B$ then, of course, $|A| = |B|$. However, the map $f : A \to B$ defined by $f(a) = 2a$ for all $a \in A$ is injective but not surjective, as $1 \notin \operatorname{im} f$. Also, the map $f : A \to B$ defined by $f(a) = a - 1$ if $a \geq 1$ and $f(0) = 0$ is surjective but not injective.

Example

In how many ways can 5 tasks be distributed among 10 employees, assuming that one task is given to precisely one employee?

This is precisely the number of injective maps from a set of 5 elements (tasks) to the set of 10 elements (employees); the map specifies to which employee a specific task is assigned. So, the answer is $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 30240$.

Example

In how many ways can we select 3 students from a group of 5 students to stand in line for a picture? In how many ways can we arrange all five of these students in a line for a picture?

Example

How many ways are there for 6 women and 4 men to stand in a line so that no two men stand next to each other?

Example: Birthday paradox

We already discussed that, by the pigeonhole principle, in any group of 367 people where are at least two who share a birthday.

Question

What is the probability that at least two people in a group of N, $N < 367$, share a birthday?

Let S be some set of people and let $f : S \to \{1, \ldots, 366\}$ be the map which assigns to each person in S his or her birthday (we number all days of year from 1 to 366). Let $N = |S|$.

The statement "No two people in S share a birthday" means that this map is injective (in particular, $N \leq 366$).

The total number of maps from S to $\{1, \ldots, 366\}$ is $366^{|S|} = 366^N$, while the number of injective maps is $366(366-1)\cdots(366-N+1)$.

So, the probability that no two people in S share a birthday is

$$\frac{366(366-1)\cdots(366-N+1)}{366^N} = \left(1 - \frac{1}{366}\right)\left(1 - \frac{2}{366}\right)\cdots\left(1 - \frac{N-1}{366}\right).$$

Denote by $p(N)$ the probability of two people in a group of N having the same birthday. Then

$$p(N) = 1 - \left(1 - \frac{1}{366}\right)\left(1 - \frac{2}{366}\right)\cdots\left(1 - \frac{N-1}{366}\right).$$

Some of its approximate values are shown in the following table

N	$p(N)$	N	$p(N)$
22	47.48%	28	65.34%
23	50.63%	29	67.99%
24	53.74%	30	70.53%
25	56.77%	40	89.06%
26	59.72%	50	97.01%
27	62.58%	60	99.4%

Permutations

The word *permutation* has two meanings in combinatorics.

Definition

A permutation of a set of distinct objects is an ordered arrangement of these objects.
An ordered arrangement of r elements of a set is called an r-permutation.

Example

Let $S = \{1, 2, 3, 4, 5, 6\}$. Then $(1, 2, 3, 4, 5, 6)$, $(2, 1, 4, 3, 6, 5)$, $(4, 3, 1, 6, 5, 2)$ and $(3, 1, 6, 5, 4, 2)$ are examples of permutations of S.
Note that we use the tuple notation and not the set notation, to emphasize that the *order* is important.
$(3, 1, 2)$ and $(4, 6, 5)$ are 3-permutations of S, while $(6, 1, 4, 5)$ and $(5, 2, 3, 4)$ are 4-permutations.
Let $X = \{a, b, c, d, e, f, g, h\}$. Then (a, c, f, g), (f, a, c, g) are 4-permutations of X, and (h, g, a, b, f, e, c, d) is a permutation of X.

The second meaning of *permutation of a set S* is *a bijective map from S to itself*.

The two meanings are connected as follows:

Theorem

Let S be a finite set with $|S| = n$. A permutation of S is given by a bijective map $f : \{1, \dots, n\} \to S$. Likewise, an r-permutation of S, $1 \leq r \leq n$, is given by an injective map $f : \{1, \dots, r\} \to S$

Many counting questions reduce to finding the number of permutations (or r-permutations) of a finite set or the number of permutations with certain properties.

Example

How many ways are there to rearrange the string $ABCDEFGHIJK$ so that the resulting string contains the string $ABCD$?

Example

How many permutations of the string $ABCDEFG$ leave A, D and G in their place?

Example

Find the number of *distinct* permutations of the string $ABBCDEEF$.

Example

How many bit strings of length 10 contain exactly four 1s?