Cardinality

Cardinality represents “the number” of elements in a set. If our set contains finitely many elements then it is (at least, intuitively) clear what we mean by that. But what if S is infinite?

The idea is to compare sizes of sets using maps.

Definition

- We define the cardinality of $\emptyset$ to be 0 and write $|\emptyset| = 0$.
- Let n be a positive integer. We define the cardinality of the set $\{1, 2, \ldots, n\} = \{k \in \mathbb{Z} : 1 \leq k \leq n\}$ to be n and write $|\{1, 2, \ldots, n\}| = n$.
- Let A and B be non-empty sets. We say that the cardinality of B is equal to the cardinality of A and write $|A| = |B|$ if there exists a *bijective* map $f : A \to B$.
- We say that a set S is finite if S is empty or if $|S| = |\{1, 2, \ldots, n\}|$ for some positive integer n. In this case we write $|S| = n$.

The cardinality of $\mathbb{N}$ is denoted $\aleph_0$.

Example

- The cardinality of $S = \{a, b, a, b, c, a, a, b\}$ is 3.
- The cardinality of $\{0,1\}^3$ is 8 because

$$\begin{aligned}\{0,1\}^3 = \{&(0,0,0),(0,0,1),(0,1,0),(1,0,0),\\ &(0,1,1),(1,0,1),(1,1,0),(1,1,1)\}\end{aligned}$$

and we can map this set bijectively to $\{1,\ldots,8\}$ via $(a_0, a_1, a_2) \mapsto 1 + a_0 + 2a_1 + 4a_2$. For example, $(1,0,1) \mapsto 1 + 1 + 2 \cdot 0 + 4 \cdot 1 = 6$ and $(0,1,1) \mapsto 1 + 0 + 2 \cdot 1 + 4 \cdot 1 = 7$.

Theorem

Let A, B and C be sets. Then

(a) $|A| = |A|$

(b) $|A| = |B|$ *if and only if* $|B| = |A|$

(c) $|A| = |B|$, $|B| = |C|$ *imply that* $|A| = |C|$.

Proof.

(a) Since $\mathrm{id}_A : A \to A$ is bijective, $|A| = |A|$

(b) Let $|A| = |B|$. Thus, there exists a bijective map $f : A \to B$. Then f has the inverse map $g : B \to A$ which is also bijective (since f is its inverse). Therefore, $|B| = |A|$

(c) If $|A| = |B|$ and $|B| = |C|$ then we have bijective maps $f : A \to B$ and $g : B \to C$. Their composition $g \circ f$ is a bijective map $A \to C$. Thus, $|A| = |C|$.

□

Comparison of cardinalities

Definition

- We say that the cardinality of A is less than or equal to the cardinality of B and write $|A| \leq |B|$ if there exists an *injective* map $f : A \to B$.
- If $|A| \leq |B|$ and $|A| \neq |B|$ we say that the cardinality of A is strictly less than the cardinality of B and write $|A| < |B|$.
- We say that a set S is *countable* if $|S| \leq |\mathbb{N}|$. We say that S is *uncountable* if $|\mathbb{N}| < |S|$.

Theorem

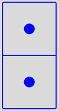
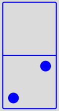
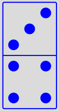
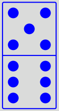
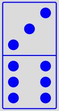
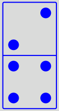
Comparison of cardinalities is well defined in the sense that if $|A| = |A'|$, $|B| = |B'|$ *and* $|A| \leq |B|$ *then* $|A'| \leq |B'|$.

Proof.

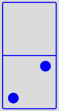
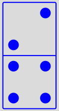
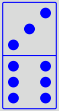
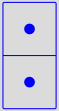
Suppose that $|A| = |A'|$, $|B| = |B'|$ and $|A| \leq |B|$. Then we have a bijective map $f : A' \to A$ (since $|A| = |A'|$, $|A'| = |A|$), a bijective map $g : B \to B'$ and an injective map $h : A \to B$. Then $g \circ h \circ f$ is a map $A' \to B'$. Since all maps involved are injective, so is their composition. □

Example

Consider the sets $A = \{\spadesuit, \clubsuit, \diamondsuit, \heartsuit\}$ and

$B = \{$, , , , , $\}$

Define $f : A \to B$ by

$f(\spadesuit) =$ , $f(\clubsuit) =$ , $f(\diamondsuit) =$ , $f(\heartsuit) =$ .

Since f is injective, $|A| \leq |B|$. In fact, $|A| = 4$ and $|B| = 6$ so this agrees with the usual comparison.

Why does this make sense?

Theorem

Let A, B and C be sets. Then

(a) $|A| \leq |B|$, $|B| \leq |C|$ *imply that* $|A| \leq |C|$.

(b) *If* $A \subset B$ *then* $|A| \leq |B|$.

Proof.

(a) Since $|A| \leq |B|$, there exists an injective map $f : A \to B$. Since $|B| \leq |C|$, there exists an injective map $g : B \to C$. Then $g \circ f : A \to C$ is injective and so $|A| \leq |C|$.

(b) If $A \subset B$, we can turn $\mathrm{id}_A : A \to A$ into a map $A \to B$ which is manifestly injective.

□

Theorem (Schroeder-Bernstein)

Let A and B be sets. If $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.

Theorem

Let A and B be sets. Then either $|A| < |B|$, or $|B| < |A|$ or $|A| = |B|$ (trichotomy law).

Theorem

The comparison of cardinalities agrees with the comparison of integers, that is, if A and B are finite with $|A| = m$ and $|B| = n$ then $|A| < |B|$ if and only if $m < n$.

Example

The set $\mathcal{B}$ of *ALL* infinite bit strings is *uncountable*.

Indeed, suppose that $\mathcal{B}$ is countable and number its elements as $\mathbf{b}_0$, $\mathbf{b}_1$, $\mathbf{b}_2$ etc. Write $\mathbf{b}_n = b_{n,0}b_{n,1}b_{n,2}\cdots$.

Let $\mathbf{a} = a_0a_1\cdots$ be the bit string defined by

$$a_i = \begin{cases} 1, & b_{i,i} = 0 \\ 0, & b_{i,i} = 1 \end{cases}$$

For example, if $\mathbf{b}_0 = 10111\cdots$, $\mathbf{b}_1 = 110111\cdots$, $\mathbf{b}_2 = 01111\cdots$, $\mathbf{b}_3 = 000011\cdots$ then $\mathbf{a} = 0001\cdots$

By construction, $\mathbf{a} \neq \mathbf{b}_i$ for all $i \in \mathbb{N}$. Yet $\mathbf{a} \in \mathcal{B}$ and so $\mathbf{a} = \mathbf{b}_i$ for some $i \in \mathbb{N}$. This is a contradiction.

What makes countable sets special?

Theorem

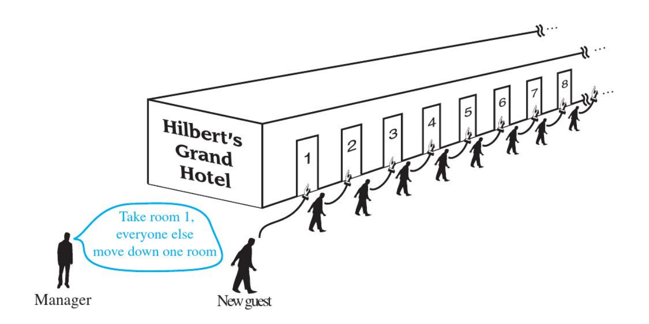
Let S be an infinite set. Then S contains an infinite countable subset. In particular, $\aleph_0$ is the smallest infinite cardinality (that is, if $|S| < \aleph_0$ then S is finite and for any infinite S, $\aleph_0 \leq |S|$).

We already saw that $\aleph_0 < |\mathbb{R}|$. It is conjectured that there is no set S such that $\aleph_0 < |S| < |\mathbb{R}|$. This is known as the *Continuum Hypothesis*.

Example (Hilbert's Grand Hotel)

This is a nice model for understanding infinite countable sets. The hotel has countably many rooms (so we may assume without loss of generality that rooms are numbered by non-negative integers).

Suppose that the Grand Hotel is fully occupied. But an arriving guest can always be accommodated as shown below.



The pigeonhole principle (or Dirichlet box principle)

Informal statement

If we have m pigeons and n pigeonholes and $m > n$ then there is at least one pigeonhole where more than one pigeon is sitting

Formal statement

If A, B are sets and $|B| < |A|$ then no map $f : A \to B$ is injective.

Proof.

Suppose that there is an injective map $f : A \to B$. Then $|A| \leq |B|$. Since we also have $|B| < |A|$ it follows that $|A| < |A|$ which is absurd. □

Example

- Assume you have a bag containing a mixture of black socks and blue socks. What is the minimum number of socks you need to pull out of the bag to *guarantee* that you will have a pair of the same color?
- What if you have a mixture of black, blue and white socks?

The "pigeonholes" here are colors, and "pigeons" are socks; we have 2 pigeonholes (colors), so if we take 3 socks two of them are necessarily of the same color; likewise, for three colors if we take 4 socks two of them are necessarily going to be of the same color and so on.

Later we will see that if we want to obtain 2 matching pairs from the collection of socks of 3 different colors we will need at least 10 socks.

Example

- In a group of 13 people at least two were born in the same month; in a group of 366 people at least two share the same birthday
- In a class of 30 students there are at least two students whose last name begins with the same letter.
- A lossless compression algorithm, while making some inputs smaller (as the name compression suggests), will also make some other inputs larger. Otherwise, the set of all input sequences up to a given length L could be mapped to the smaller set of all sequences of length less than L without collisions (because the compression is lossless).

Question

How many integers should we select to guarantee that at least two of them have the same remainder when divided by 5?

The remainder of an integer, when divided by 5, can only take values $0, 1, 2, 3, 4$ (5 values). By the pigeonhole principle, we need at least $5 + 1 = 6$ integers to make sure that two of them have the same remainder.

The fundamental principles of counting

The four fundamental principles

Let A and B be finite sets.

- (*Addition*) If $A \cap B = \emptyset$ then $|A \cup B| = |A| + |B|$;
  More generally, if $A_1, \ldots, A_n$ are finite and *pairwise disjoint*, that is, $A_i \cap A_j = \emptyset$ if $1 \leq i \neq j \leq n$ then $|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$.
- (*Subtraction*) If $A \subset B$ then $|B \setminus A| = |B| - |A|$;
- (*Multiplication*) $|A \times B| = |A||B|$;
  More generally, if $A_1, \ldots, A_n$ are finite then
  $|A_1 \times \cdots \times A_n| = |A_1| \cdots |A_n|$.
  In particular, if A is finite then $|A^n| = |A|^n$.
- (*Power rule*) If A and B are non-empty then there are $|B|^{|A|}$ maps from A to B.

Applications to counting

If we want to count the number of elements in the Cartesian product of collection of sets, we multiply their cardinalities.

Example

- Telephone numbers in North America are of the form $NXX - NXX - XXXX$ where X can be any digit between 0 and 9 and N can be any digit between 2 and 9. How many different phone numbers can be assigned?

Example

- Standard license plates for passenger vehicles in California are of the form $NMLMXXX$ where N is a digit between 1 and 9, L is any letter, M is any letter except I, O and Q, and and X is a digit between 0 and 9. Assuming that no letter sequences are prohibited, how many license plates are available?

Example (Counting Internet addresses)

In Version 4 of the Internet Protocol an address is a string of 32 bits. It begins with a *network number (netid)* which is followed by a *host number (hostid)*. The formats are shown in the following table

Bit number	0	1	2	3	4	8	16	24	31
Class A	0	netid				hostid			
Class B	1	0	netid				hostid		
Class C	1	1	0	netid				hostid	
Class D	1	1	1	0	Multicast Address				
Class E	1	1	1	1	0	Address			

Class A addresses are used for large networks, consist of 0 followed by a 7-bit netid and a 24-bit hostid.

Class B addresses are used for medium-size networks, consist of 10 followed by a 14-bit netid and a 16-bit hostid.

Class C addresses are used for small networks, consist of 110 followed by a 21-bit netid and an 8-bit hostid.

There are also some restrictions: a Class A network cannot have 1111111 as its netid, and a hostid cannot consist of all 0 or all 1.

Example (Counting Internet addresses)

- How many hosts can be in a network of each of the first 3 types?
  In a Class A network the 24-bit hostid is used so we have $2^{24} - 2 = 16,777,214$ possibilities (all 0 and all 1 are excluded)
  In a Class B network the hostid is 16-bit so we have $2^{16} - 2 = 65,534$ possibilities
  In a Class C network the hostid is 8-bit so we have $2^{8} - 2 = 254$ possibilities.
- How many computers can be in all Class A networks put together?
  The netid for a Class A network is 7-bit, so there are $2^7 - 1 = 127$ Class A networks (1111111 cannot be a netid).
  Since each Class A network can have up to $16,777,214$ hosts we obtain $2,130,706,178$ (about two billions) possibilities.

A stronger form of the pigeonhole principle

Theorem (Generalized pigeonhole principle)

Suppose that N objects are distributed into k boxes. Then there is a box that contains at least N/k objects and a box that contains at most N/k objects.

Note that N/k does not have to be an integer; if it is not an integer then we are guaranteed that there is a box that contains at least $\lceil N/k \rceil$ (the least integer $\geq N/k$) and a box that contains at most $\lfloor N/k \rfloor$ (the maximal integer $\leq N/k$) objects.

Example

- How many cards must be selected from a deck of 52 cards to guarantee that 3 of the same suit are chosen?
- Phone numbers in North America are of the form $NXX - NXX - XXXX$, where X can be any digit between 0 and 9 and N is a digit between 2 and 9.

  How many area codes are necessary to guarantee that $25,000,000$ different phone numbers can be assigned?

Example

Suppose that a computer laboratory has 15 workstations and 8 servers.
A cable can be used to directly connect a workstation to a server.
For each server, only one direct connection to that server can be active at any time.
We want to guarantee that at any time any set of 8 or fewer workstations can simultaneously access different servers via direct connections.
Although we could do this by connecting every workstation directly to every server (using $15 \cdot 8 = 120$ connections), what is the minimum number of direct connections needed to achieve this goal?