Countability

How do you precisely describe the intuition that there are more real numbers than integers?
When do we say that two infinite sets A and B have the same size?

Def. Given two sets A and B, we say that they have the same cardinality and write $|A| = |B|$ if there is a bijection from A to B.

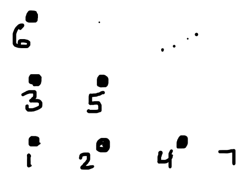
For example, $|\mathbb{Z}| = |2\mathbb{Z}|$. Mapping each x in $\mathbb{Z}$ to $2x$ yields a bijection

$$2\mathbb{Z} = \{2y : y \in \mathbb{Z}\}$$

Try showing that $|\mathbb{Z}| = |\mathbb{N}|$.

Def. A set A is countably infinite if $|A| = |\mathbb{N}|$.
A set A is countable if it is finite or countably infinite.

$\mathbb{N}_0^2$ is countable. We can number them as
$(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), \cdots$



Note that we can compose bijections to create new bijections
$\Rightarrow \mathbb{Z}^2$ is countable.

More generally, if A and B are countable, then $A \times B$ is countable.
(Extends to cartesian product of a finite number of countable sets)

Is $\mathbb{Q}$ countable?

It suffices to get a bijection from $\mathbb{Q}$ to $\mathbb{Z}^2$.

How would we do this? Not all (a,b) correspond to a distinct a/b.

We can easily construct an injective function: $\mathbb{Q} \to \mathbb{Z}^2$ by mapping p/q in lowest form to (p,q).

$\Rightarrow$ There is a one-one function from $\mathbb{Q}$ to $\mathbb{N}$.

(composing with bijection)

Def. Let A and B be sets. We write $|A| \leq |B|$ if there is an injection from A to B.

So $|\mathbb{Q}| \leq |\mathbb{N}|$.

We also have $|\mathbb{N}| \leq |\mathbb{Q}|$. (identity mapping)

Can we conclude that there is a bijection?

Theo. [Cantor-Schröder-Bernstein]

There is a bijection from A to B if and only if there is an injection from A to B and an injection from B to A.

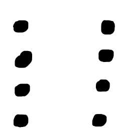
That is,

$$|A| = |B| \text{ iff } |A| \leq |B| \text{ and } |B| \leq |A|.$$

Idea of proof. Let $f: A \to B$ and $g: B \to A$ be one-one.

Consider a directed graph where edges correspond to functional values.

$(a \to f(a)$ and $b \to g(b))$ We just want a perfect matching.



Consider infinite chains obtained by following the arrows.

one-one $\Rightarrow$ each node is in a unique chain.

A chain either starts at an A node, starts at a B node, or starts nowhere (doubly infinite / cyclic) — types A, B, and C.

In case C, just pick all the edges in one direction, say from A to B.

In case A, just pick all the edges from A to B.

In case B, just pick all the edges from B to A.

This gives a bijection.

So, we have that $|\mathbb{Q}| = |\mathbb{N}|$.

Example. The set S of all finite length strings made of [A-Z] is countably infinite.

The mapping $S \to \mathbb{N}$ wherein we consider each element of S as a number in base 27 is one-one. We should omit zero and consider [A-Z] as the non-zero digits.

The mapping $\mathbb{N} \to S$, $n \mapsto A^n$ is also one-one.

$\Rightarrow |S| = |\mathbb{N}|$.

Let S be the set of all infinitely long binary strings. Prove that $|T| = |\mathbb{R}|$.

Show that $|\mathbb{R}^2| = |\mathbb{R}|$.

(bijection by interleaving infinite strings)

$|A| \leq |B|$ if there is an injection from A to B.

Equivalently, using the Axiom of Choice, there is a surjection from B to A.

Def. A is uncountable if it is infinite but not countably infinite.

Equivalently, there is no surjection from $\mathbb{N}$ to A.

How do we show that something is uncountable?

We shall prove that $P(\mathbb{N})$ is uncountable.

power set

Take any function $f : \mathbb{N} \to P(\mathbb{N})$

We can think of any element of $P(\mathbb{N})$ as a countably infinite binary string.

Make a binary table where $T_{ij} = 1$ iff $j \in f(i)$

Now, consider the diagonal of the table and flip it. That is, consider the set S where $i \in S$ iff $i \notin f(i)$.

Due to the nature of our construction, $S \neq f(i)$ for any i.
(it differs at the i^{th} position)

$\Rightarrow f$ is not a surjection.

$\Rightarrow P(\mathbb{N})$ is uncountable.

This method of proof is known as
<u>Cantor's Diagonalisation Argument</u>.

More generally, there is no onto function $f: A \to P(A)$ for any set A.
(Similarly consider the set $S = \{x \in A : x \notin f(x)\}$)

Since $|\mathbb{R}| = |P(\mathbb{N})|$, $\mathbb{R}$ is uncountable.

We denote by $\aleph_0$ the cardinality of $\mathbb{N}$ and by $\aleph_k$ the cardinality of $\underbrace{P(P(\cdots P(\mathbb{N})\cdots))}_{k \text{ times}}$.

$(\aleph_1 = |\mathbb{R}|)$

Are there intermediate infinities between $\aleph_k$ and $\aleph_{k+1}$? This is known as the continuum hypothesis.