Ideas of mathematical proof

Slides Week 23

Cantor's theorem: uncountable sets. Arithmetic of cardinalities.
Inequalities between cardinalities. Cantor–Bernstein–Schröder theorem.
Logical statements and connectives.

Not all infinite sets are countable

There may be an impression that
all infinite sets have the same cardinality,
that is, all are countable.

But this is not the case,
discovered by Georg Cantor at the end of 19th century:
there are uncountable sets.

Cantor's theorem: uncountable sets

Theorem (Cantor's theorem)

The set $(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$ *is not countable.*

That is: there is no bijection $\mathbb{N} \to (0,1)$.

Proof by contradiction: assume the opposite,

that there is a bijection $f : \mathbb{N} \to (0,1)$,

and derive a contradiction.

This will show that the assumption is false,

that is, there cannot be such a bijection.

Proof of Cantor's theorem

Recall: real numbers in $(0,1)$ are

infinite decimal fractions

(like $0.152637153548595 76\ldots$).

We suppose the opposite (aim: a contradiction):

that there is a bijection $f : \mathbb{N} \to (0,1)$,

so then all numbers in $(0,1)$ can be listed in a sequence.

We arrange this list vertically,

so that we obtain an infinite table, in which

i-th row $=$ image of i, the real number $f(i) \in (0,1)$.

Cantor's theorem: assume the opposite

.... suppose the <u>opposite</u>: $\exists$ bijection $f : \mathbb{N} \to (0,1)$...

$$
\begin{array}{rcccccccc}
f(1) = & 0 & . & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & \cdots \\
f(2) = & 0 & . & a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & \cdots \\
f(3) = & 0 & . & a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & \cdots \\
f(4) = & 0 & . & a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & \cdots \\
f(5) = & 0 & . & a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & \cdots \\
\vdots & & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots
\end{array}
$$

Here a_{ij} is the j-th decimal digit in the i-th number $f(i)$.

Proof of Cantor's theorem continued

$$\begin{array}{rccccccccc}
f(1) = & 0 & . & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & \cdots \\
f(2) = & 0 & . & a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & \cdots \\
f(3) = & 0 & . & a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & \cdots \\
\vdots & & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots
\end{array}$$

We now define another real number as a decimal fraction $b = 0.b_1 b_2 b_3 \ldots$ by the following rule:

$b_1 = 1$ or 2 but $b_1 \neq a_{11}$, next $b_2 = 1$ or 2 but $b_2 \neq a_{22}$, and so on, $b_i = 1$ or 2 but $b_i \neq a_{ii}$

Going along the red 'diagonal' and choosing $b_i \neq a_{ii}$,

for definiteness: $b_i = \begin{cases} 1 & \text{if } a_{ii} \neq 1 \\ 2 & \text{if } a_{ii} = 1 \end{cases}.$

Proof of Cantor's theorem: arriving at a contradiction

The number $b = 0.b_1 b_2 \ldots$ that we constructed is in the interval $(0, 1)$ but it is not in the list:

$b \neq f(1)$ since b differs from $f(1)$ in the 1st decimal place, by our construction;

$b \neq f(2)$ since b differs from $f(2)$ in the 2nd decimal place, by our construction;

and so on, $b \neq f(i)$ since b differs from $f(i)$ in the *i*th decimal place by our construction.

Proof of Cantor's theorem: contradiction

Recall: $b = 0.b_1 b_2 b_3 \ldots,$ where

$$b_i = \begin{cases} 1 & \text{if } a_{ii} \neq 1 \\ 2 & \text{if } a_{ii} = 1 \end{cases}.$$

$$\begin{array}{llllllllll}
b \neq & f(1) = & 0 & . & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & \cdots \\
b \neq & f(2) = & 0 & . & a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & \cdots \\
b \neq & f(3) = & 0 & . & a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & \cdots \\
b \neq & f(4) = & 0 & . & a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & \cdots \\
b \neq & f(5) = & 0 & . & a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & \cdots \\
 & & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \ddots
\end{array}$$

Proof of Cantor's theorem: contradiction

Repeat: the number $b = 0.b_1 b_2 \ldots$ that we constructed

is in the interval $(0, 1)$ but it is not in the list:

for every $i = 1, 2, \ldots$

$b \neq f(i)$ since b differs from $f(i)$

in the ith decimal place by our construction.

This is a contradiction with our assumption that f was a bijection, onto the entire interval $(0, 1)$.

Therefore our assumption that $\exists$ a bijection $f : \mathbb{N} \to (0, 1)$ is false,

so there cannot be such a bijection, as required, that is, $|(0, 1)| \neq \aleph_0$. □

$\mathbb{R}$ is uncountable

Corollary

The set of real numbers $\mathbb{R}$ is uncountable.

Proof: Example earlier: $|(0,1)| = |\mathbb{R}|$,

so $\mathbb{R}$ is also not countable.

Or: by a preceding theorem, if $\mathbb{R}$ was countable, then all subsets would be countable.

Notation

The cardinality of $\mathbb{R}$ is called

the **cardinality of a continuum**,

and is denoted either $\mathbf{c}$ or $2^{\aleph_0}$.

Ever increasing cardinals (optional)

Optional remark: Cantor proved that for any set A the cardinality of $\mathscr{P}(A)$ (denoted by $2^{|A|}$) is always not equal to (=strictly greater than) $|A|$.

So there are infinitely many non-equal cardinalities:

$$\aleph_0 \lneqq \mathbf{c} = 2^{\aleph_0} \lneqq 2^{(2^{\aleph_0})} \lneqq 2^{(2^{(2^{\aleph_0})})} \lneqq \cdots$$

Arithmetic of cardinals

Definition

If A and B are disjoint sets, $A \cap B = \varnothing$,

then the sum of their cardinalities

is defined as the cardinality of their union:

$|A| + |B| := |A \mathbin{\dot{\cup}} B|$.

Definition

The product of the cardinalities

is defined as the cardinality of the Cartesian product:

$|A| \cdot |B| := |A \times B|$.

Some sums and products of cardinals

For finite sets, the sum and product are ‘the same’ as usual. Different for infinite cardinals:

Example

We showed $|\mathbb{Z}| = |\mathbb{N}|$,

and $\mathbb{Z} = \{0\} \,\dot{\cup}\, \mathbb{N} \,\dot{\cup}\, \{\text{negative integers}\}$ (also $\aleph_0$).

Thus, $1 + \aleph_0 + \aleph_0 = \aleph_0$.

Example

We also showed earlier: $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$,

thus, $\aleph_0 \cdot \aleph_0 = \aleph_0$.

Example

Prove that $\aleph_0 + k = \aleph_0$ for any finite cardinal $k \in \mathbb{N}$.

Proof: add (disjointly) k elements $\{a_1, \ldots, a_k\}$ to $\mathbb{N}$; then we can easily enumerate the resulting set:

$$\begin{array}{cccccccccc}
1 & 2 & \ldots & k & k+1 & k+2 & \text{k+3} & k+4 & \text{k+5} & \ldots \\
\downarrow & \downarrow & \ldots & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \ldots \\
a_1 & a_2 & \ldots & a_k & 1 & 2 & 3 & 4 & 5 & \ldots
\end{array}$$

This is a bijection $\mathbb{N} \to \{a_1, \ldots, a_k\} \mathbin{\dot\cup} \mathbb{N}$,

so $\aleph_0 = k + \aleph_0$.

Theorem

For any infinite cardinal $|A|$, *we have* $|A| + \aleph_0 = |A|$.

Proof. First choose a countable infinite subset in A:

by induction: a_1 any element,

then a_2 any element $\neq a_1$, and so on,

when $a_1, \ldots, a_k$ already chosen to be all different,

they cannot exhaust all of A since A is infinite,

so there is $a_{k+1} \in A$ that is different from all $a_1, \ldots, a_k$.

By this recursive definition, we obtain a sequence

$A_1 = \{a_1, a_2, \ldots\}$ of pairwise different elements of A.

Proving $|A| = |A| + \aleph_0$

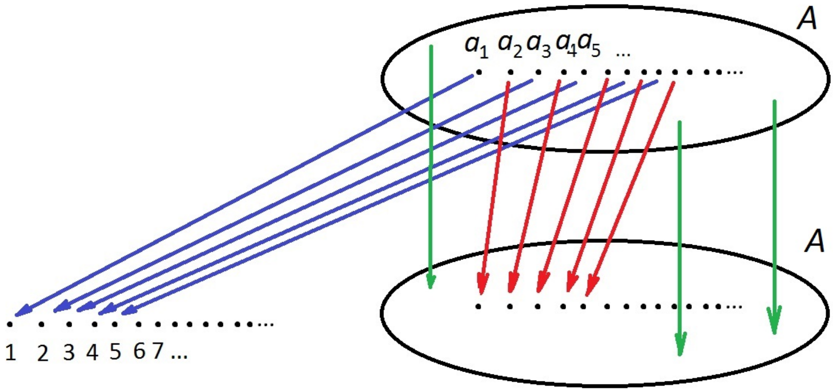
Consider $A \mathbin{\dot\cup} \mathbb{N}$ (can assume $A \cap \mathbb{N} = \varnothing$, can always 'paint' $\mathbb{N}$ in a different colour). Need a bijection $A \to A \mathbin{\dot\cup} \mathbb{N}$.

Idea: first a bijection $A_1 \to A_1 \mathbin{\dot\cup} \mathbb{N}$:

$$\begin{array}{cccccccccc}
a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & \dots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \dots \\
1 & a_1 & 2 & a_2 & 3 & a_3 & 4 & a_4 & 5 & \dots
\end{array}$$

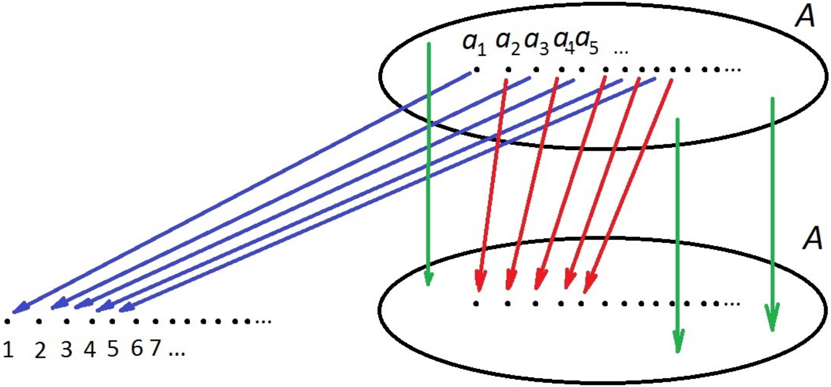
This infinite table gives a bijection $f : A_1 \to A_1 \mathbin{\dot\cup} \mathbb{N}$.

Then we extend the mapping f to the remaining parts, which are the same: $A \setminus A_1$ and $(A \mathbin{\dot\cup} \mathbb{N}) \setminus (A_1 \mathbin{\dot\cup} \mathbb{N})$, by $x \to x$ for all $x \in A \setminus A_1$.



$$\begin{array}{ccccccccccc}
A_1 & = & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & \dots \\
\downarrow & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \dots \\
\mathbb{N} \mathbin{\dot\cup} A_1 & = & 1 & a_1 & 2 & a_2 & 3 & a_3 & 4 & a_4 & 5 & \dots
\end{array}$$

green arrows: $x \rightarrow x$ for all $x \in A \setminus A_1$.



To be precise: we define $g(x) = \begin{cases} f(x) & \text{if } x \in A_1 \\ x & \text{if } x \in A \setminus A_1 \end{cases}$.

Then $\mathbb{N} \dot{\cup} A$ is covered by images: $= g(A)$.

So, $|\mathbb{N} \dot{\cup} A| = |A|$, means $|A| + \aleph_0 = |A|$, as req. □

Existence of irrational numbers

Corollary 1 of Cantor's theorem

There exist irrational numbers.

Proof: We have $|\mathbb{R}| \neq |\mathbb{Q}|$, so $\mathbb{R} \neq \mathbb{Q}$. □

This is a "pure existence theorem",

does not give us any particular irrational number!

Cardinality of irrational numbers

We can even say that irrationals are in a 'majority'.

Corollary 2 of Cantor's theorem.

The cardinality of irrational numbers is that of a continuum: $|\mathbb{R} \setminus \mathbb{Q}| = \mathbf{c}$.

Proof: Indeed, $\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \,\dot{\cup}\, \mathbb{Q}$,

so $\quad \mathbf{c} = |\mathbb{R}| = |\mathbb{R} \setminus \mathbb{Q}| + \aleph_0 = |\mathbb{R} \setminus \mathbb{Q}|$

by the preceding theorem

(note that $\mathbb{R} \setminus \mathbb{Q}$ cannot be finite,

for then $\mathbb{R}$ would be countable by an example above). $\square$

Optional: existence of transcendental numbers

Optional remark: Another corollary: there exist **transcendental numbers** — numbers that are not roots of polynomials with rational coefficients.

Moreover, their cardinality is that of a continuum.

Again pure existence theorem: proving that, e.g., π or e is transcendental is quite difficult.

Proof is in showing that the set of algebraic numbers (=roots of polynomials with rational coefficients) is countable.

More examples about cardinalities

Example

Produce a bijection between $(1, 2)$ and $(3, \infty)$ by a formula.

Idea: for example, $f(x) \to \infty$ as $x \to 2^-$:

$f(x) = \dfrac{c}{2-x}$ would do, with any constant $c > 0$.

When $x = 1$, $f(1) = \dfrac{c}{2-1} = c$.

Put $c = 3$. So we guess $f(x) = \dfrac{3}{2-x}$.

Guess: $f(x) = \dfrac{3}{2-x}$ is a bijection between $(1,2)$ and $(3,\infty)$.

Injective: $\dfrac{3}{2-x_1} = \dfrac{3}{2-x_2} \Rightarrow x_1 = x_2$.

Surjective: for any $y > 3$, need $y = \dfrac{3}{2-x}$;

Solve for x: $2 - x = \dfrac{3}{y}$; $x = 2 - \dfrac{3}{y}$.

But also must be $x \in (1,2)$.

Since $y > 3$, we have $0 < \dfrac{3}{y} < 1$; $0 > -\dfrac{3}{y} > -1$;

$2 > 2 - \dfrac{3}{y} > 1$, as req.

Example

Another proof that $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad f((m, n)) = 2^m \cdot 3^n$.

Claim: f is injective:

$f((m_1, n_1)) = f((m_2, n_2)) \;\Rightarrow\; (m_1, n_1) = (m_2, n_2)$.

$2^{m_1} \cdot 3^{n_1} = 2^{m_2} \cdot 3^{n_2} \;\Rightarrow\; m_1 = m_2$ and $n_1 = n_2$

by uniqueness of prime-power factorization (assumed as known).

Apply a Theorem in previous lectures, part (b): injective $B \to A$ and $|A| = \aleph_0 \;\Rightarrow\; |B| = \aleph_0$ or finite.

We have injective $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and $|\mathbb{N}| = \aleph_0$, hence $|\mathbb{N} \times \mathbb{N}| = \aleph_0$.

Countable set as a sequence

Recall: a bijection $\mathbb{N} \to A$ means

representing A as a sequence:

$$A = \{a_1, a_2, a_3, \dots\}$$

with every element of A occurring exactly once.

Example

Prove that $|\mathbb{N} \times \{u, v\}| = \aleph_0$.

Need a bijection $\mathbb{N} \to \mathbb{N} \times \{u, v\}$.

Recall: $\mathbb{N} \times \{u, v\}$ is the set of pairs (k, u), (m, v), where $k, m \in \mathbb{N}$.

This set of pairs can be arranged as a sequence:

$(1, u)$, $(1, v)$, $(2, u)$, $(2, v)$, $(3, u)$, $(3, v)$, $(4, u)$,
$(4, v)$, $(5, u)$, $(5, v)$, ...

So this is a bijection $\mathbb{N} \to \mathbb{N} \times \{u, v\}$,

so $|\mathbb{N} \times \{u, v\}| = \aleph_0$.

Cardinality of a power set $\mathscr{P}(A)$

When A is finite, write $A = \{a_1, a_2, \ldots, a_n\}$.

Every subset $X \subseteq A$ can be encoded

as a string of 0s and 1s:

0 if the element is not included, 1 if it is included.

E.g.: $A = \{a_1, a_2, a_3, a_4\}$:

$\{a_1, a_3\} \leftrightarrow (1, 0, 1, 0)$;

$\{a_2, a_3, a_4\} \leftrightarrow (0, 1, 1, 1)$;

$\varnothing \leftrightarrow (0, 0, 0, 0)$.

This is a bijection. Note: $|\mathscr{P}(A)| = 2^n$.

$\mathscr{P}(\mathbb{N})$ as set of sequences of 0s and 1s

Every subset $X \subseteq \mathbb{N}$ corresponds
to a sequence of 0s and 1s:

going over $1, 2, 3, \ldots$ write in turn

0 if the element is not included in X,
1 if it is included in X.

E.g.: all even numbers $\leftrightarrow (0, 1, 0, 1, 0, 1, \ldots)$.

E.g.: all primes $\leftrightarrow (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, \ldots)$.

This is a bijection between $\mathscr{P}(\mathbb{N})$ and

the set S of all sequences of 0s and 1s.

Thus, $|\mathscr{P}(\mathbb{N})| = |S|$.

Theorem

$\mathscr{P}(\mathbb{N})$ *is uncountable:* $|\mathscr{P}(\mathbb{N})| \neq \aleph_0$.

Proof. Since $|\mathscr{P}(\mathbb{N})| = |S|$, the same as $|S| \neq \aleph_0$.

Use Cantor's diagonal method. Proof by contradiction: suppose the opposite, that is, that there is a bijection $f : \mathbb{N} \to S$; aim: a contradiction.

Arrange the set S as a list vertically:

$$
\begin{array}{llllllll}
f(1) = (& a_{11}, & a_{12}, & a_{13}, & a_{14}, & a_{15}, & \dots) & \\
f(2) = (& a_{21}, & a_{22}, & a_{23}, & a_{24}, & a_{25}, & \dots) & \\
f(3) = (& a_{31}, & a_{32}, & a_{33}, & a_{34}, & a_{35}, & \dots) & \\
f(4) = (& a_{41}, & a_{42}, & a_{43}, & a_{44}, & a_{45}, & \dots) & \\
\vdots & & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \quad \ddots
\end{array}
$$

Define a sequence $B = (b_1, b_2, b_3, \dots)$ by the rule: $b_1 = 1$ or 0 but $b_1 \neq a_{11}$, then $b_2 = 1$ or 0 but $b_2 \neq a_{22}$, and so on, $b_i = 1$ or 0 but $b_i \neq a_{ii}$

$$\begin{array}{lllllll}
f(1) = (& {\color{red}a_{11},} & a_{12}, & a_{13}, & a_{14}, & a_{15}, & \dots) \\
f(2) = (& a_{21}, & {\color{red}a_{22},} & a_{23}, & a_{24}, & a_{25}, & \dots) \\
f(3) = (& a_{31}, & a_{32}, & {\color{red}a_{33},} & a_{34}, & a_{35}, & \dots) \\
f(4) = (& a_{41}, & a_{42}, & a_{43}, & {\color{red}a_{44},} & a_{45}, & \dots) \\
f(5) = (& a_{51}, & a_{52}, & a_{53}, & a_{54}, & {\color{red}a_{55},} & \dots) \\
\vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \quad \ddots
\end{array}$$

going along the red "diagonal" and choosing values

$b_i \neq a_{ii}$ by the rule $b_i = \begin{cases} 1 & \text{if } a_{ii} = 0 \\ 0 & \text{if } a_{ii} = 1. \end{cases}$

Then our sequence $B = (b_1, b_2, b_3, \dots)$ consists of 0s and 1s, so it is in our set S, but it is not in the list:

$B \neq f(1)$ since B differs from $f(1)$ in the 1st element by construction;

$B \neq f(2)$ since $b_2 \neq$ 2nd element of $f(2)$ by construction;

and so on, $B \neq f(i)$ since $b_i \neq$ the ith element of $f(i)$by construction.

Contradiction with the assumption that f was a bijection, onto the entire set S.

Hence the assumption that there is a bijection $\mathbb{N} \to S$ is false, this precisely means that there cannot be such a bijection, as required: $|\mathscr{P}(\mathbb{N})| \neq \aleph_0$. □

Optional: In fact, $|\mathscr{P}(\mathbb{N})| = \mathbf{c} = |(0,1)|$.

Same as $|S| = \mathbf{c}$. Simply write numbers r between 0 and 1 as binary (not decimal) fractions: $r = 0.a_1a_2a_3\ldots$, where $a_i = 0, 1$. Namely, $a_1 = 1$ if $r \geq 0.5$, and 0 if $r < 0.5$, then divide the half into two halves, write 1 or 0 depending on which smaller half contains r, and so on.

Then $f(r) = (a_1, a_2, a_3, \ldots)$ is an injection $f : (0,1) \to S$.

Not covered: sequences with 'tails of 1s'. The set of such sequences T is countable. We have $S = f((0,1)) \cup T$ (disjoint union).

So $|S| = |f((0,1))| + \aleph_0 = |f((0,1))| = |(0,1)| = \mathbf{c}$.

This also explains why notation $\mathbf{c} = 2^{\aleph_0}$ makes sense.

Inequalities between cardinals

Definition

$|A| \leq |B|$ if there is an injective mapping $f : A \to B$.

This agrees with what we have for finite sets.

Must be well defined: if $|A_1| = |A|$, $|B_1| = |B|$,

then $|A| \leq |B| \Rightarrow |A_1| \leq |B_1|$ (independent of sets).

Indeed:

$$A_1 \xrightarrow{\text{bijection}} A \xrightarrow{\text{injection}} B \xrightarrow{\text{bijection}} B_1.$$

Composite is defined,

composite of injections is an injection (proved earlier).

Example

$|\mathbb{N}| \leq |\mathbb{Z}|$: injection $k \to k$.

(Here, in fact, $|\mathbb{N}| = |\mathbb{Z}|$, as we saw above.)

Example

$|\mathbb{N}| \leq |\mathbb{R}|$: injection $k \to k$.

But here $|\mathbb{N}| \neq |\mathbb{R}|$ by Cantor's theorem,

so strict inequality $|\mathbb{N}| < |\mathbb{R}|$, or $\aleph_0 < \mathbf{c}$.

Theorem

Inequality between cardinals is a total order relation.

Partial proof:

Reflexive: clearly, $A \to A$, $x \to x$, is injective,

so $|A| \leq |A|$.

Transitive: need $|A| \leq |B|$ and $|B| \leq |C| \Rightarrow |A| \leq |C|$.

$|A| \leq |B|$ means $\exists$ injection $f : A \to B$;

$|B| \leq |C|$ means $\exists$ injection $g : B \to C$.

Then the composite $g \circ f : A \to C$

is also an injection (proved in the lectures earlier);

so $|A| \leq |C|$.

Antisymmetric:

need $|A| \leq |B|$ and $|B| \leq |A| \Rightarrow |A| = |B|$.

Clearly true for finite sets. Not obvious for infinite.

Actually, true, but is a difficult theorem

(without proof). $\square$

Inequality of cardinals is antisymmetric

Cantor–Bernstein–Schröder theorem

If $|A| \leq |B|$ *and* $|B| \leq |A|$, *then* $|A| = |B|$.

In other words:

if there are injections $A \to B$ and $B \to A$,

then there is a bijection $A \leftrightarrow B$.

Assumed without proof,

but you are required to know it and be able to apply.

Optional: any two cardinals are comparable

Optional Remark: any two cardinals are comparable:

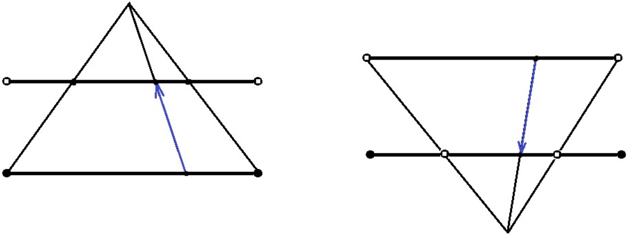
for any two sets either $|A| \leq |B|$ or $|B| \leq |A|$.

So inequality between cardinals is a total order.

Example

Use C–B–S theorem to prove that $|(0,1)| = |[0,1]|$ (when not required to produce an explicit bijection).

Geometric constructions with injective mappings are explained by the picture.



Hence, $|[0,1]| \leq |(0,1)|$ and $|(0,1)| \leq |[0,1]|$; therefore $|(0,1)| = |[0,1]|$ by the C–B–S theorem.

$\aleph_0$ as the smallest infinite cardinal

The earlier theorem about $\aleph_0$ can now be stated as

Theorem

$\aleph_0$ *is the smallest infinite cardinal.*

Proof: Indeed, a smaller infinite cardinal $|B| \leq \aleph_0$ means $\exists$ injection $B \to A$, where $|A| = \aleph_0$. By that theorem earlier, then $|B| = \aleph_0$, so there is no smaller infinite cardinal. □

Example

Use C–B–S theorem to show that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Injection: $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, for example, $f((m,n)) = 2^m \cdot 3^n$;

so $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$. (Can stop here by that theorem...)

But just as an example for C–B–S theorem:

Injection: $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$, for example, $f(k) = (1, k)$;

so $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$.

Together with $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$,

by C–B–S theorem, $\Rightarrow |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Optional: Continuum Hypothesis.

Optional remark: Continuum Hypothesis.

We know $\aleph_0 \lneqq \mathbf{c}$. But is there anything in between?

Continuum Hypothesis stated that there no intermediate cardinal:

if $\aleph_0 \leq |A| \leq \mathbf{c}$, then either $|A| = \aleph_0$ or $|A| = \mathbf{c}$.

In other words, any subset of $\mathbb{R}$ is either countable, or of cardinality $\mathbf{c}$.

Almost 100 years remained a major open problem.

Answered only in the 1960s: Paul Cohen proved that this cannot be proved, and the negation also cannot be proved.

This means: Continuum Hypothesis, or its negation,
can be assumed as an additional axiom,
in each case giving rise to a perfectly consistent
mathematical theory.

The proof is quite difficult and belongs to Mathematical Logic.

This situation similar to the 5th Postulate of Euclidean geometry, which can either be assumed, or its negation, each giving rise to perfectly legitimate geometry.

Non-Euclidean geometry is now widely used in applications (in physical theories).

So far Continuum Hypothesis had only theoretical significance.

Optional: more facts on arithmetic of cardinalities

Other interesting facts (**optional**):

$\aleph_0 \times \mathbf{c} = \mathbf{c}$

$\mathbf{c} \times \mathbf{c} = \mathbf{c}$

Both can be proved by using C–B–S theorem.

Cantor also proved $|A| \lneqq |\mathscr{P}(A)|$ for any set.

Recap of Chapter 2:

Sets: Venn diagrams; operations on sets and their properties; power set; Cartesian product.

Relations: diagrams; transitive, reflexive, symmetric, antisymmetric; equivalence and equivalence classes; partial order, infimum, supremum.

Mappings: diagrams; domain, image, inverse image; injective, surjective, bijective; composite mapping.

Cardinalities: countable infinite sets; countability of $\mathbb{Q}$; explicit bijections; injections into countable set; Cantor's theorem, uncountable sets; arithmetic of cardinals; inequalities between cardinals,
Cantor–Bernstein–Schröder theorem.

3. Elements of mathematical logic

Consider **statements**,

denoted by letters, like P, Q, etc., which can

take exactly one of two values, true or false,

denoted T, F (fixed notation).

Simple examples of statements:

"London is the capital of UK" has truth value T;

"$2 = 5$" has truth value F;

"Are you asleep?" is not a statement;

"$x > 0$" becomes a statement for various values of x, and these statements may be true or false.

Mathematically we do not distinguish between statements which make the same assertion, expressed differently.

E.g. “The capital of UK is London”

is regarded as the same as

“London is the capital of UK”.

Compound statements

Compound statements are composed from simple ones

by using **logical operations**

(also called **connectives**).

Negation = NOT

Definition

For a statement P the **negation** of P, denoted by $\neg P$, is a new statement defined by the following truth table:

values of $\neg P$ defined depending on values of P:

P	$\neg P$
T	F
F	T

This agrees with our common sense use of negations: if R is "It is raining", then $\neg R$ is "It is not raining". Or if P is $2 = 5$ (which is false), then $\neg P$ is $2 \neq 5$ (true).

Alternative notation

Remark: Sometimes other signs are used for negations: like $\bar{P}$, or $\sim P$.

In this module we use $\neg P$ for negation.

Conjunction = AND

Definition

For statements P and Q, the **conjunction** (logical **and**)

denoted by $P \wedge Q$ (read: “P and Q”)

is a new statement <u>defined</u> by the following truth table:

the truth values of $P \wedge Q$ defined

depending on all possible values of P, Q:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Remark: Sometimes the symbol $P\&Q$ is used for $P \wedge Q$.

Conjunction agrees with common use of "and":

"P and Q is true" only if **both are true**.

If P is "$2 = 5$", and Q is "$3 > 2$",

then $P \wedge Q$ is false,

but $\neg P \wedge Q$ is true.

Notation convention for negation

Remark: We agree that $\neg$ is only applied to the next symbol,

to avoid using too many brackets:

$\neg P \wedge Q = (\neg P) \wedge Q$,

which is <u>not</u> $\neg(P \wedge Q)$.

Connection with natural language

Example

Let $S =$ sun is shining and $R =$ it is raining.

Then $S \wedge R$ is "sun is shining and it is raining"

the same as "it is raining but sun is shining"

the same as "sun is shining although it is raining".

Disjunction = inclusive OR

Definition.

For statements P and Q, the **disjunction** (logical **inclusive or**) denoted by $P \vee Q$ is a new statement defined by the following truth table: the truth values of $P \vee Q$ are defined depending on all possible values of P, Q:

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Remark: In what follows, by “or” we always mean “inclusive or”.

Example

Let $S =$ sun is shining and $B =$ there is a rainbow.

Then $S \vee B$ is “sun is shining or there is a rainbow” or both, also formally true.

Exclusive “or”

Example

Express “exclusive or”: either P or Q but not both.

Solution: $(P \vee Q) \wedge (\neg(P \wedge Q))$

(actually exactly “or and not both”).

Truth tables

But to be precise we use truth table. We fill its columns successively going from left to right based on definitions. Columns are created according to how the formula is built from P and Q step-by-step: here we shall need $P \vee Q$, then $P \wedge Q$, then $\neg(P \wedge Q)$, and finally $(P \vee Q) \wedge (\neg(P \wedge Q))$:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q)$

Then successively fill the columns using definitions and the columns on the left that are already filled. But first we write all possible combinations of true or false for P and Q in the first two columns:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q$
T	T				
T	F				
F	T				
F	F				

We now fill the $P \vee Q$ column depending on the values of P and Q:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q)$
T	T	T			
T	F	T			
F	T	T			
F	F	F			

We fill the $P \wedge Q$ column depending on the values of P and Q:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q)$
T	T	T	T		
T	F	T	F		
F	T	T	F		
F	F	F	F		

Now the $\neg(P \wedge Q)$ column depending only on the values of $P \wedge Q$ (no need to look at preceding columns):

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q)$
T	T	T	T	F	
T	F	T	F	T	
F	T	T	F	T	
F	F	F	F	T	

Finally the last column $(P \vee Q) \wedge (\neg(P \wedge Q))$ depending on the values of $P \vee Q$ and $\neg(P \wedge Q)$:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q)$
T	T	T	T	F	F
T	F	T	F	T	T
F	T	T	F	T	T
F	F	F	F	T	F

We see that the last column is as required: true exactly when either P or Q is true but not both.

Logical equivalence

Definition

Two compound statements M, N

formed from simple statements P, Q, R,...

are **logically equivalent**, denoted $M \equiv N$,

if they have the same truth values

for all possible input data for P, Q, R,...

Example

Show that

$\neg(P \wedge Q)$ is logically equivalent to $(\neg P) \vee (\neg Q)$.

L.h.s. says that it is false that both P and Q hold.

This means that either P is false, or Q (or both).

In turn, P false means the negation $\neg P$ is true, same for Q.

So this is $\neg P$ is true or $\neg Q$ is true,
$=$ disjunction on r.h.s.

But in mathematical logic we can and should prove formally, based on definitions of connectives, by filling the truth table.

Proving by truth table

Proving that
$\neg(P \wedge Q)$ is logically equivalent to $(\neg P) \vee (\neg Q)$.

Recall: truth table is built successively by filling columns from left to right based on definitions and using values in preceding columns. Columns are defined as needed for the formula; all possible combinations of values of P, Q are entered:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T					
T	F					
F	T					
F	F					

First $P \wedge Q$:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	T				
T	F	F				
F	T	F				
F	F	F				

Now $\neg(P \wedge Q)$:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	T	F			
T	F	F	T			
F	T	F	T			
F	F	F	T			

Now $\neg P$ and $\neg Q$:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	T	F	F	F	
T	F	F	T	F	T	
F	T	F	T	T	F	
F	F	F	T	T	T	

Now $(\neg P) \vee (\neg Q)$:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

We see that the columns for $\neg(P \wedge Q)$ and $(\neg P) \vee (\neg Q)$ are the same, which means that
$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$.

Now $(\neg P) \vee (\neg Q)$:

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

We see that the columns for $\neg(P \wedge Q)$ and $(\neg P) \vee (\neg Q)$ are the same, which means that
$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$.

Implication = IMPLIES

Definition

Given two statements P and Q

the **implication** $P \Rightarrow Q$ is a new statement

defined by the following truth table:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note: the implication $P \Rightarrow Q$ is not true only if P is true while Q is false.

Implication as a promise under a condition

Note that $P \Rightarrow Q$ is true if P is false

whatever the value of Q:

"anything follows from a wrong statement".

This agrees with natural language:

"If condition A holds, then I will do B".

When condition A is false (does not hold),

and I do not do B, my statement is still true:

I keep my promise.

Example

Let $P(x)$ be “x is a cod”,

and $Q(x)$ be “x is a fish”.

Implication $P(x) \Rightarrow Q(x)$ is (always) true:

For $x =$ cod we have both P and Q true;

for $x =$ plaice P is false and Q is true;

for $x =$ orange, $P(x)$ is false and $Q(x)$ is false,

and there are no x such that $P(x)$ is true but $Q(x)$ is false.

Example

Let $P(x)$ be "$x > 3$", and $Q(x)$, "$x > 1$".

Implication $P(x) \Rightarrow Q(x)$ is always true:

E.g., for $x = 4$ we have both P and Q true;

for $x = 2$ P is false and Q is true;

for $x = 0$, say, $P(x)$ is false and $Q(x)$ is false,

and there are no x such that $P(x)$ is true but $Q(x)$ is false.

Theorems as implications

Many theorems in mathematics have this form: $P \Rightarrow Q$.

"If $x < -3$, then $x^2 > 9$"

Here $P =$ "$x < -3$" and $Q =$ "$x^2 > 9$".

The same: $x < -3 \Rightarrow x^2 > 9$.

Pythagoras: in a right triangle ABC with $\angle C = 90^\circ$ we have $AB^2 = BC^2 + AC^2$.

The same: "If in a triangle ABC we have $\angle C = 90^\circ$, then $AB^2 = BC^2 + AC^2$."

or: "... $\angle C = 90^\circ \Rightarrow AB^2 = BC^2 + AC^2$."

Terminology

In a theorem “$P \Rightarrow Q$”:

premise P is called the *hypothesis*,

and Q *conclusion*.

Other terms are sometimes used:

hypothesis = condition = premise = assumption.

Example (Translating logic into natural language)

Denote the following natural language statements by symbols: "On a given day ....

H ... Jane is on holiday";

S ... Jane goes swimming";

L ... Jane studies logic".

$S \Rightarrow \neg L$: When Jane swims, she does not study logic.

$L \wedge (H \Rightarrow S)$: Jane studies logic, and she swims if she is on holiday.

$H \Rightarrow (S \vee L)$: If Jane is on holiday, she studies logic or swims (or both). = Jane studies logic or swims (or both) whenever she is on holiday.

Example (Translating into logical expressions)

On the day, either Jane is on holiday and swims, or she studies logic (may also be on holiday): $(H \wedge S) \vee L$.

Jane studies logic only when she is on holiday and swims: $L \Rightarrow (H \wedge S)$.

Note that "only" means implication $\Rightarrow$.

If we write $(H \wedge S) \Rightarrow L$, then the meaning is completely different:
Whenever Jane swims being on holiday, she studies logic (but may also study logic under other conditions).