

Discrete Mathematics in Computer Science

B3. Cantor's Theorem

Malte Helmert, Gabriele Röger

University of Basel

October 5, 2020

Discrete Mathematics in Computer Science

October 5, 2020 — B3. Cantor's Theorem

B3.1 Cantor's Theorem

B3.2 Consequences of Cantor's Theorem

B3.3 Sets: Summary

B3.1 Cantor's Theorem

Countable Sets

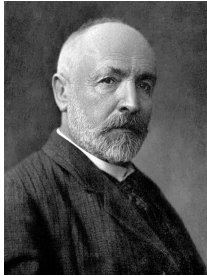
We already know:

- ▶ The **cardinality** of \mathbb{N}_0 is \aleph_0 .
- ▶ All sets with cardinality \aleph_0 are called **countably infinite**.
- ▶ A **countable** set is finite or countably infinite.
- ▶ Every subset of a countable set is countable.
- ▶ The union of countably many countable sets is countable.

These questions were still open:

- ▶ Do all infinite sets have the same cardinality?
- ▶ Does the power set of infinite set S have the same cardinality as S ?

Georg Cantor



- ▶ German mathematician (1845–1918)
- ▶ Proved that the rational numbers are countable.
- ▶ Proved that the real numbers are not countable.
- ▶ **Cantor's Theorem:** For every set S it holds that $|S| < |\mathcal{P}(S)|$.

Our Plan

- ▶ Understand Cantor's theorem
- ▶ Understand an important theoretical implication for computer science

Cantor's Diagonal Argument Illustrated on a Finite Set

$$S = \{a, b, c\}.$$

Consider an arbitrary injective function from S to $\mathcal{P}(S)$.

For example:

	a	b	c	
a	1	0	1	a mapped to $\{a, c\}$
b	1	1	0	b mapped to $\{a, b\}$
c	0	1	0	c mapped to $\{b\}$
	0	0	1	nothing was mapped to $\{c\}$.

We can identify an “unused” element of $\mathcal{P}(S)$.

Complement the entries on the main diagonal.

Works with every injective function from S to $\mathcal{P}(S)$.

→ there cannot be a bijection from S to $\mathcal{P}(S)$.

Cantor's Diagonal Argument on a Countably Infinite Set

$$S = \mathbb{N}_0.$$

Consider an arbitrary injective function from \mathbb{N}_0 to $\mathcal{P}(\mathbb{N}_0)$.

For example:

	0	1	2	3	4	...
0	1	0	1	0	1	...
1	1	1	0	1	0	...
2	0	1	0	1	0	...
3	1	1	0	0	0	...
4	1	1	0	1	1	...
⋮	⋮	⋮	⋮	⋮	⋮	⋱
	0	0	1	1	0	...

Complementing the entries on the main diagonal again results in an “unused” element of $\mathcal{P}(\mathbb{N}_0)$.

Cantor's Theorem

Theorem (Cantor's Theorem)

For every set S it holds that $|S| < |\mathcal{P}(S)|$.

Proof.

We need to show that

- ① There is an injective function from S to $\mathcal{P}(S)$.
- ② There is no bijection from S to $\mathcal{P}(S)$.

For 1, consider function $f : S \rightarrow \mathcal{P}(S)$ with $f(x) = \{x\}$. Each element of S is paired with a unique element of $\mathcal{P}(S)$

Cantor's Theorem

Proof (continued).

For 2, we show for every injective function $f : S \rightarrow \mathcal{P}(S)$ that it is not a bijection from S to $\mathcal{P}(S)$.

This is sufficient because every bijection is injective.

Let f be an arbitrary injective function with $f : S \rightarrow \mathcal{P}(S)$.

Consider $M = \{x \mid x \in S, x \notin f(x)\}$.

For every $x \in S$ it holds that $f(x) \neq M$ because $x \in f(x)$ iff not $x \notin f(x)$ iff not $x \in M$ iff $x \notin M$.

Hence, there is no $x \in S$ with $f(x) = M$. As $M \in \mathcal{P}(S)$ this implies that f is not a bijection from S to $\mathcal{P}(S)$. \square

B3.2 Consequences of Cantor's Theorem

Infinite Sets can Have Different Cardinalities

There are infinitely many different cardinalities of infinite sets:

- ▶ $|\mathbb{N}_0| < |\mathcal{P}(\mathbb{N}_0)| < |\mathcal{P}(\mathcal{P}(\mathbb{N}_0))| < \dots$
- ▶ $|\mathbb{N}_0| = \aleph_0 = \beth_0$
- ▶ $|\mathcal{P}(\mathbb{N}_0)| = \beth_1 (= |\mathbb{R}|)$
- ▶ $|\mathcal{P}(\mathcal{P}(\mathbb{N}_0))| = \beth_2$
- ▶ ...

Existence of Unsolvable Problems

There are more problems in computer science than there are programs to solve them.

There are problems that cannot be solved by a computer program!

Why can we say so?

Decision Problems

“Intuitive Definition:” Decision Problem

A **decision problem** is a Yes-No question of the form

“Does the given input have a certain property?”

- ▶ “Does the given binary tree have more than three leaves?”
- ▶ “Is the given integer odd?”
- ▶ “Given a train schedule, is there a connection from Basel to Belinzona that takes at most 2.5 hours?”

- ▶ Input can be encoded as some finite string.
- ▶ Problem can also be represented as the (possibly infinite) set of all input strings where the answer is “yes”.
- ▶ A computer program solves a decision problem if it terminates on every input and returns the correct answer.

More Problems than Programs I

- ▶ A computer program is given by a finite string.
- ▶ A decision problem corresponds to a set of strings.

More Problems than Programs II

- ▶ Consider an arbitrary finite set of symbols (an **alphabet**) Σ .
- ▶ You can think of $\Sigma = \{0, 1\}$ as internally computers operate on binary representation.
- ▶ Let S be the **set of all finite strings** made from symbols in Σ .
- ▶ There are **at most $|S|$ computer programs** with this alphabet.
- ▶ There are **at least $|\mathcal{P}(S)|$ problems** with this alphabet.
 - ▶ every subset of S corresponds to a separate decision problem
- ▶ By Cantor's theorem $|S| < |\mathcal{P}(S)|$, so **there are more problems than programs**.

B3.3 Sets: Summary

Summary

- ▶ A **set** is an **unordered collection** of **distinct** objects.
- ▶ **Set operations**: union, intersection, set difference, complement



- ▶ Commutativity, associativity and distributivity of union and intersection
- ▶ **De Morgan's law**: $\overline{A \cup B} = \bar{A} \cap \bar{B}$ and $\overline{A \cap B} = \bar{A} \cup \bar{B}$.
- ▶ The **cardinality** measures the "size" of a set.
 - ▶ For finite sets, the cardinality equals the number of elements.
 - ▶ All sets with the same cardinality as \mathbb{N}_0 are **countably infinite**.
 - ▶ All sets with cardinality $\leq |\mathbb{N}_0|$ are **countable**.
- ▶ The **power set** $\mathcal{P}(S)$ of set S is the set of all subsets of S .
 - ▶ For **finite** sets S it holds that $|\mathcal{P}(S)| = 2^{|S|}$.
 - ▶ For all sets S it holds that $|S| < |\mathcal{P}(S)|$.