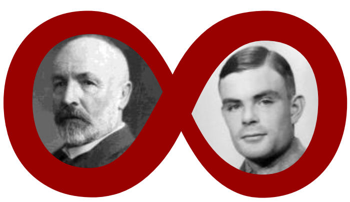
Great Theoretical Ideas in CS

Lecture 7:
Cantor's Legacy

Anil Ada
Ariel Procaccia (this time)

Our Protagonists



Georg Cantor
1845-1918
Father of set theory

Alan Turing
1912-1954
Father of CS

Carl Friedrich Gauss
1777-1855

"Infinity is nothing more than a figure of speech which helps us talk about limits. The notion of a completed infinity doesn't belong in mathematics."

Cantor's Contributions

- Infinite sets are mathematical objects
- Different levels of infinity
- Explicit definition and use of 1-1 correspondences
- $|\mathbb{N}| < |\mathbb{R}|$ even though they are both infinite
- $|\mathbb{N}| = |\mathbb{Z}|$ even though $\mathbb{N} \subsetneq \mathbb{Z}$

Henri Poincaré
1854-1912

"Most of the ideas of Cantorian set theory should be banished from mathematics once and for all!"

Leopold Kronecker
1823-1891

"I don't know what predominates in Cantor's theory — philosophy or theology."

"Scientific charlatan."

"Corruptor of youth."

Ludwig Wittgenstein
1889-1951

"Wrong."

"Utter nonsense."

"Laughable."

David Hilbert
1862-1943

"No one should expel us from the Paradise that Cantor has created."

Ludwig Wittgenstein
1889-1951

"If one person can see it as a paradise, why should not another see it as a joke?"

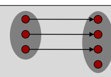
Ariel Procaccia
1979-?

"Enough monkeying around, let's get down to business."

3 Types of Functions

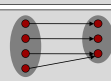
Injective, 1-1:
$f: A \to B$ is injective if
$a \neq a' \Rightarrow f(a) \neq f(a')$

$$f: A \rightarrowtail B$$



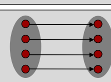
Surjective, onto:
$f: A \to B$ is surjective if
$\forall b \in B\ \exists a \in A$ s.t. $f(a) = b$

$$f: A \twoheadrightarrow B$$



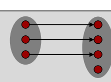
Bijective, 1-1 correspondence:
$f: A \to B$ is bijective if
f is injective and surjective

$$f: A \rightarrowtail\!\!\!\!\twoheadrightarrow B$$

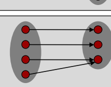


Comparing Cardinality

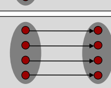
$|A| \leq |B|$ $\quad f: A \rightarrowtail B$



$|A| \geq |B|$ $\quad f: A \twoheadrightarrow B$

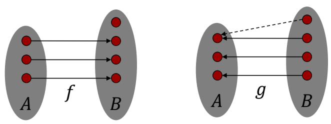


$|A| = |B|$ $\quad f: A \rightarrowtail\!\!\!\!\twoheadrightarrow B$



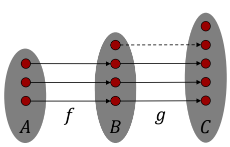
Sanity Checks

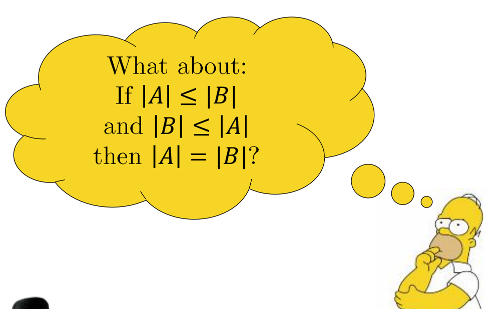
- If $|A| \leq |B|$ then $|B| \geq |A|$
- Indeed, there is an injection $f: A \rightarrowtail B$, so define $g: B \twoheadrightarrow A$ such that
  $\forall b \in \text{range}(f), g(b) = f^{-1}(b)$



Sanity Checks

- If $|A| \leq |B|$ and $|B| \leq |C|$ then $|A| \leq |C|$
- Indeed, there is an injection $f: A \rightarrowtail B$, and an injection $g: B \rightarrowtail C$, so $g \circ f: A \rightarrowtail C$ is an injection





One More Definition

$$|A| < |B|$$
$$\textbf{not } |A| \geq |B|$$

- There is no surjection from A to B
- There is no injection from B to A
- There is an injection from A to B, but there is no bijection between A and B

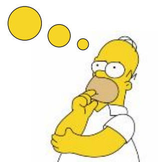
These definitions allow us to compare the cardinality of infinite sets!

Example: $\mathbb{Z}$

- Strangely enough, it holds that $|\mathbb{N}| = |\mathbb{Z}|$
- Indeed, the function $f: \mathbb{N} \rightarrow \mathbb{Z}$ defined by
$$f(n) = (-1)^{n+1} \left\lceil \frac{n}{2} \right\rceil$$
is a bijection

n	0	1	2	3	4	5	6	⋯
$f(n)$	0	1	−1	2	−2	3	−3	⋯

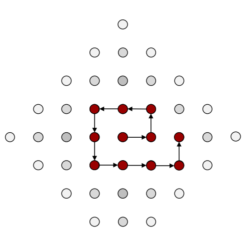
Wouldn't it be more intuitive to conclude that $|\mathbb{N}| < |\mathbb{Z}|$, as $\mathbb{N} \subsetneq \mathbb{Z}$?



Infinity and Beyond

- A set A is called:
  - Countable if $|A| \leq |\mathbb{N}|$
  - Countably infinite if it is countable and infinite
  - Uncountable if $|A| > |\mathbb{N}|$
- Perhaps a better name for countable would be listable: Can list the elements of A so that every element appears eventually

Example: $\mathbb{Z} \times \mathbb{Z}$



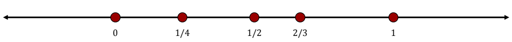
(0,0)
(1,0)
(1,1)
(0,1)
$(-1,1)$
$(-1,0)$
$(-1,-1)$
$(0,-1)$
$(1,-1)$
$(2,-1)$
(2,0)

EXAMPLE: $\mathbb{N} \times \mathbb{N}$

https://youtu.be/Uj3_KqkI9Zo
(2:13)

EXAMPLE: $\mathbb{Q}$

- Idea: list the rational numbers in the order they appear on the line



- Problem: Between any two rational numbers, there is another!
- Better idea: Define a surjection $f: \mathbb{Z} \times \mathbb{Z} \twoheadrightarrow \mathbb{Q}$ via $f(a, b) = a/b$
- $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| \leq |\mathbb{N}|$, and, by transitivity, $\mathbb{Q}$ is countable

EXAMPLE: $\{0,1\}^*$

- $\{0,1\}^* =$ set of finite-length binary strings
- It is countable because we can enumerate them by length:
  $\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, \ldots$
- Similarly for Σ^*, where Σ is a finite alphabet

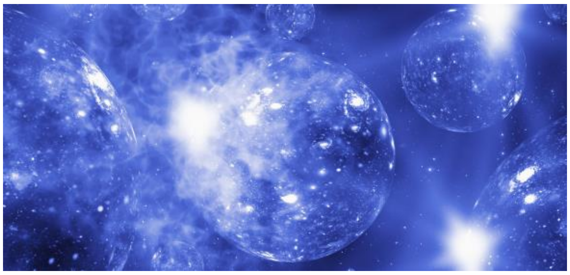
The CS method for showing countability of A: Show that $|A| \leq |\Sigma^*|$ for some alphabet Σ

Example: $\mathbb{Q}[x]$

- $\mathbb{Q}[x]$ is the set of polynomials with rational coefficients, e.g.,
$$x^3 + \frac{1}{4}x^2 + 6x - \frac{22}{7}$$
- Let $\Sigma = \{0, \dots 9, x, +, -, *, /, \wedge\}$
- Every polynomial can be described by a finite string over Σ, e.g.,
$$x\wedge 3 + 1/4x\wedge 2 + 6x - 22/7$$
- Therefore $\mathbb{Q}[x]$ is countable

Cantor's Theorem

- Just when we were starting to think that every set is countable…
- Cantor's Theorem: For any set A,
$$|A| < |\mathcal{P}(A)|$$
- In particular, $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$, that is, $\mathcal{P}(\mathbb{N})$ is uncountable
- More generally,
$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots$$



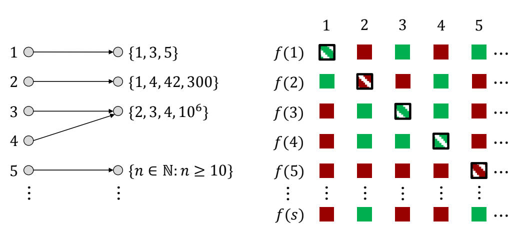
An infinity of infinities!

Proof of Cantor's Theorem

- Assume for contradiction that $|A| \geq |\mathcal{P}(A)|$
- Then there exists $f: A \twoheadrightarrow \mathcal{P}(A)$
- Let $S = \{a \in A: a \notin f(a)\} \in \mathcal{P}(A)$
- Since f is a surjection, there is $s \in A$ such that $f(s) = S$
- But this leads to a contradiction: Is $s \in S$?
  If $s \in S$ then not $s \notin f(s)$, hence $s \notin S$
  If $s \notin S$ then $s \notin f(s)$, hence $s \in S$ ■

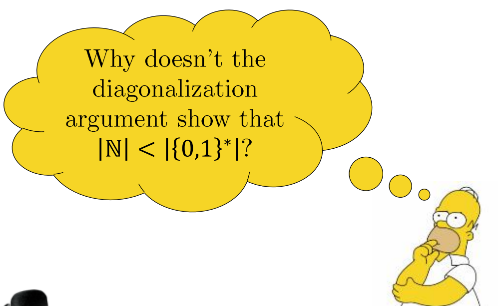
Diagonalization

Example for $f: \mathbb{N} \twoheadrightarrow \mathcal{P}(\mathbb{N})$



Test Your Intuition

- Poll: Which of the following sets is countable?
  1. Infinite-length binary strings
  2. Finite-length strings of natural numbers
  3. Both
  4. Neither



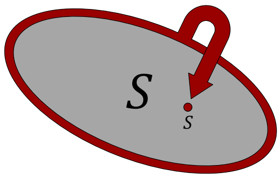
Example: $\mathbb{R}$

- We can now show that $\mathbb{R}$ is uncountable by constructing $f: \mathbb{R} \twoheadrightarrow \{0,1,\ldots,9\}^\infty$
- For each $0.a_1a_2\cdots \in [0,1)$, $f(x) = a_1a_2\cdots$
- Complication:

  $$0.499\cdots = 0.500\cdots$$

  so this would not be a surjection
- But in these cases we can map $1.a_1a_2\cdots$ to the alternative representation

Russell's Paradox



If S is the set of all sets that do not contain themselves, does S contain itself?

Summary

- Terminology:
  - Surjection, injection, bijection
  - Countable and uncountable sets
- Principles:
  - Functions between sets are the right way to compare cardinalities
  - Diagonalization
- Big ideas:
  - Infinity of infinities!