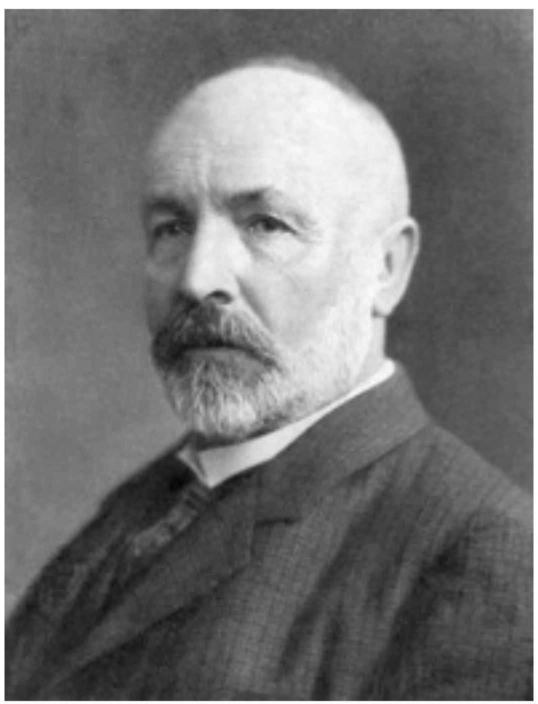
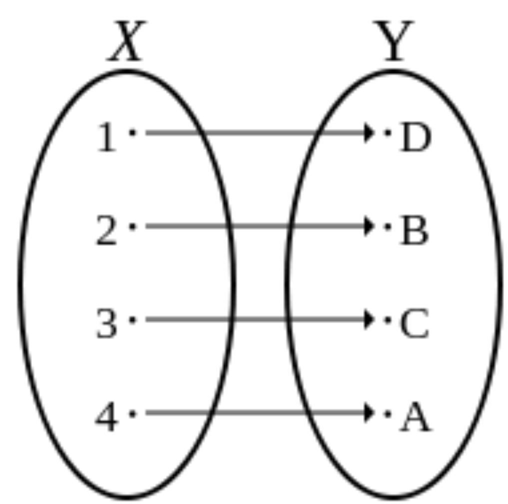
15-251
Great Theoretical Ideas in Computer Science

Lecture 5:
Cantor's Legacy





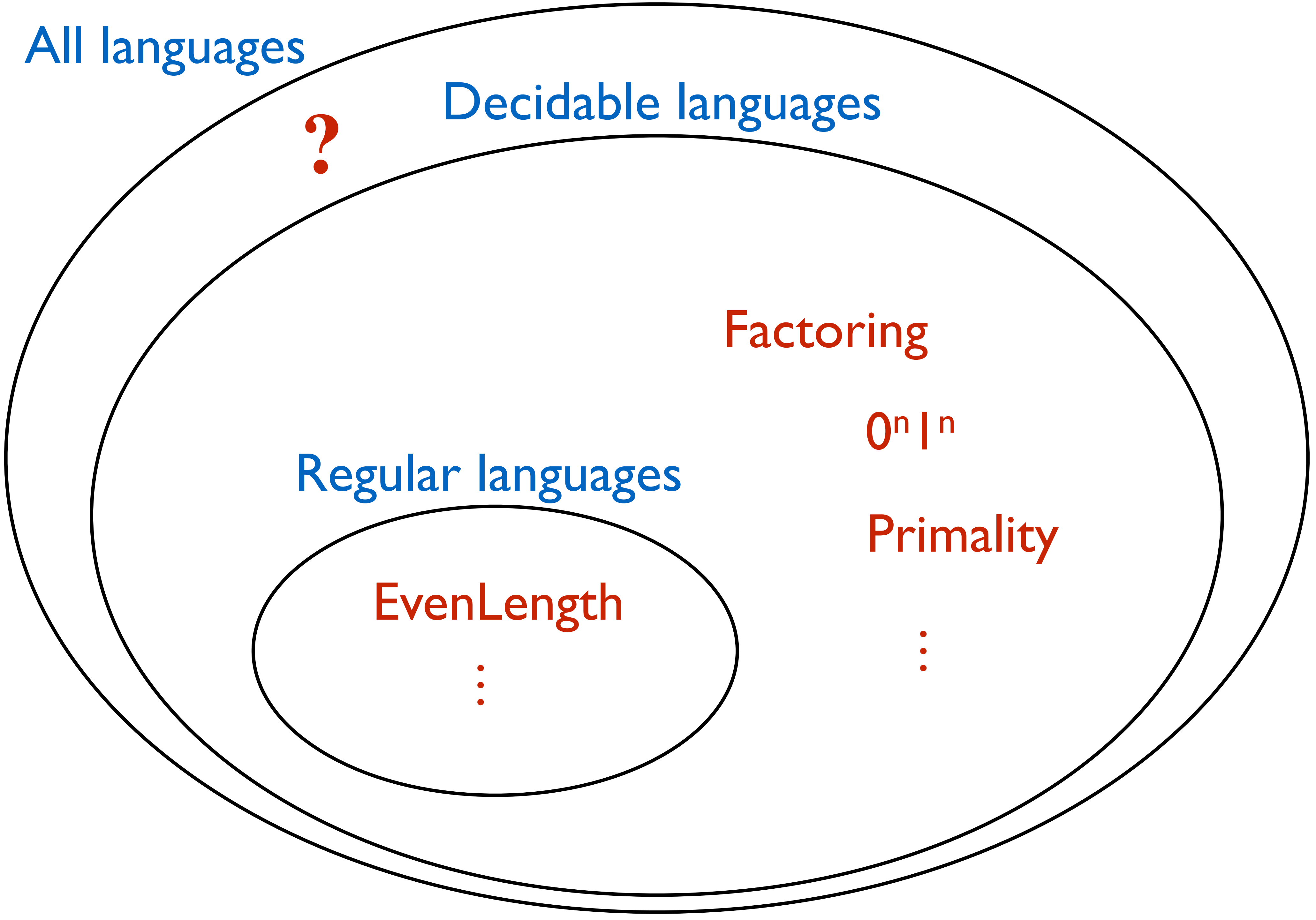
September 15th, 2015

Poll

Select the ones that apply to you:

- I know what an uncountable set means.
- I know Cantor's diagonalization argument.
- I used to know what uncountable meant, I forgot.
- I used to know the diagonalization argument, I forgot.
- I've never learned about uncountable sets.
- I've never learned about the diagonalization argument.

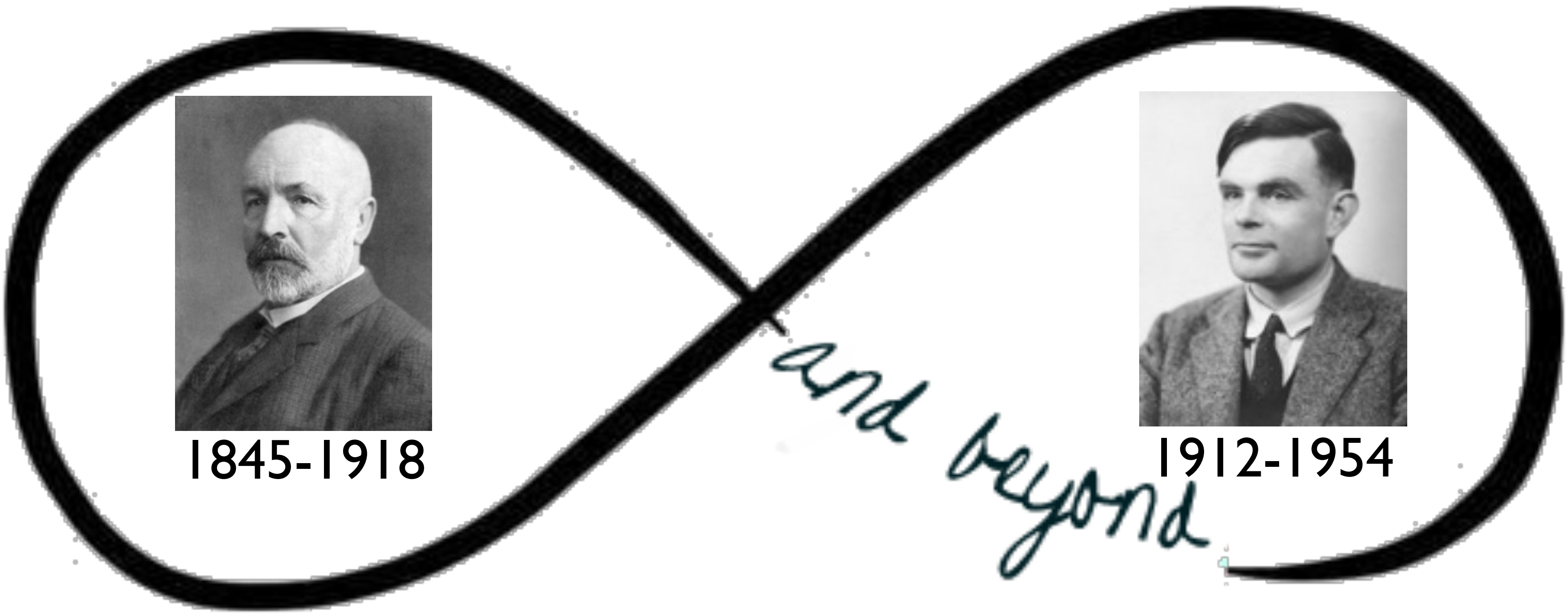
This Week


All languages
Decidable languages
?
Factoring
$0^n 1^n$
Primality
⋮
Regular languages
EvenLength
⋮

Our heroes for this week

father of set theory

father of computer science



Uncountability

Uncomputability

Infinity in mathematics

Pre-Cantor:

"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"

- Carl Friedrich Gauss

Post-Cantor:

Infinite sets are mathematical objects just like finite sets.

Some of Cantor's contributions

- The study of infinite sets
- Explicit definition and use of 1-to-1 correspondence
  - This is the right way to compare the cardinality of sets
- There are different levels of infinity.
  - There are infinitely many infinities.
- $|\mathbb{N}| < |\mathbb{R}|$ even though they are both infinite.
- $|\mathbb{N}| = |\mathbb{Z}|$ even though $\mathbb{N} \subsetneq \mathbb{Z}$.
- The diagonal argument.

Reaction to Cantor's ideas at the time

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

- Henri Poincaré

Reaction to Cantor's ideas at the time

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

- Leopold Kronecker

Reaction to Cantor's ideas at the time

Scientific charlatan.

- Leopold Kronecker

Reaction to Cantor's ideas at the time

Corrupter of youth.

- Leopold Kronecker

Reaction to Cantor's ideas at the time

Wrong.

- Ludwig Wittgenstein

Reaction to Cantor's ideas at the time

Utter non-sense.

- Ludwig Wittgenstein

Reaction to Cantor's ideas at the time

Laughable.

- Ludwig Wittgenstein

Reaction to Cantor's ideas at the time

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

- David Hilbert

Reaction to Cantor's ideas at the time

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

- Ludwig Wittgenstein

First we start with finite sets

How do we count a finite set?

$A = \{\text{apple, orange, banana, melon}\}$

What does $|A| = 4$ mean?

There is a 1-to-1 correspondence (bijection) between

A and $\{1, 2, 3, 4\}$

$$\begin{aligned} \text{apple} &\longleftrightarrow 1 \\ \text{orange} &\longleftrightarrow 2 \\ \text{banana} &\longleftrightarrow 3 \\ \text{melon} &\longleftrightarrow 4 \end{aligned}$$

How do we compare the sizes of finite sets?

$A = \{\text{apple, orange, banana, melon}\}$

$B = \{200, 300, 400, 500\}$

What does $|A| = |B|$ mean?

$$\begin{array}{lcccc}
\text{apple} & \longleftrightarrow & 1 & \longleftrightarrow & 500 \\
\text{orange} & \longleftrightarrow & 2 & \longleftrightarrow & 200 \\
\text{banana} & \longleftrightarrow & 3 & \longleftrightarrow & 300 \\
\text{melon} & \longleftrightarrow & 4 & \longleftrightarrow & 400
\end{array}$$

How do we compare the sizes of finite sets?

$A = \{\text{apple, orange, banana, melon}\}$

$B = \{200, 300, 400, 500\}$

What does $|A| = |B|$ mean?

$$\begin{aligned}
\text{apple} &\longleftrightarrow 500\\
\text{orange} &\longleftrightarrow 200\\
\text{banana} &\longleftrightarrow 300\\
\text{melon} &\longleftrightarrow 400
\end{aligned}$$

$|A| = |B|$ iff there is a 1-to-1 correspondence (bijection) between A and B.

How do we compare the sizes of finite sets?

$A = \{\text{apple, orange, banana}\}$

$B = \{200, 300, 400, 500\}$

What does $|A| \leq |B|$ mean?

$$
\begin{array}{ccccc}
\text{apple} & \longleftrightarrow & 1 & \longleftrightarrow & 500 \\
\text{orange} & \longleftrightarrow & 2 & \longleftrightarrow & 200 \\
\text{banana} & \longleftrightarrow & 3 & \longleftrightarrow & 300 \\
 & & 4 & \longleftrightarrow & 400
\end{array}
$$

How do we compare the sizes of finite sets?

$A = \{\text{apple, orange, banana}\}$

$B = \{200, 300, 400, 500\}$

What does $|A| \leq |B|$ mean?

$$\begin{array}{lcl} \text{apple} & \longrightarrow & 500 \\ \text{orange} & \longrightarrow & 200 \\ \text{banana} & \longrightarrow & 300 \\ & & 400 \end{array}$$

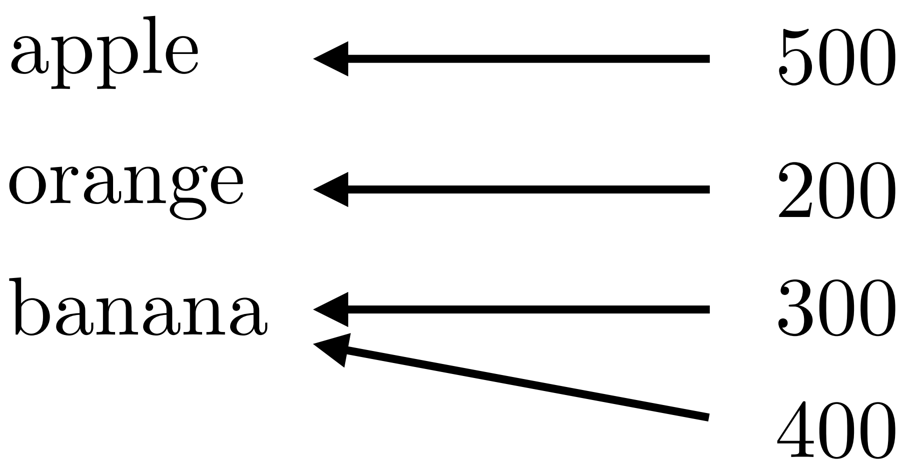
$|A| \leq |B|$ iff there is an injection from A to B .

How do we compare the sizes of finite sets?

$A = \{\text{apple, orange, banana}\}$

$B = \{200, 300, 400, 500\}$

What does $|A| \leq |B|$ mean?



$|A| \leq |B|$ iff there is a surjection from B to A.

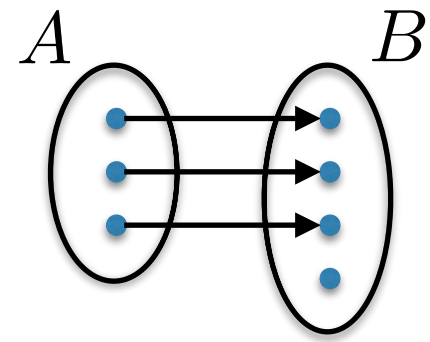
3 important types of functions

injective, 1-to-1

$f : A \to B$ is injective if

$a \neq a' \implies f(a) \neq f(a')$

$\boxed{A \hookrightarrow B}$

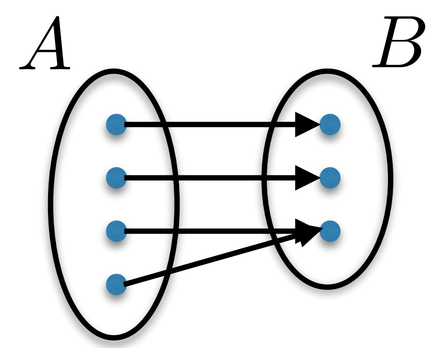


surjective, onto

$f : A \to B$ is surjective if

$\forall b \in B, \exists a \in A \text{ s.t. } f(a) = b$

$\boxed{A \twoheadrightarrow B}$

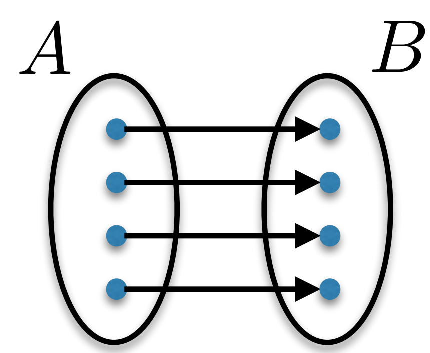


bijective, 1-to-1 correspondence

$f : A \to B$ is bijective if

f is injective and surjective

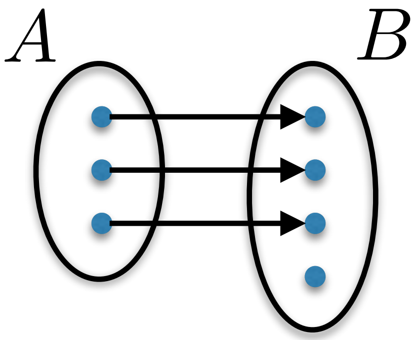
$\boxed{A \leftrightarrow B}$



Comparing the cardinality of finite sets

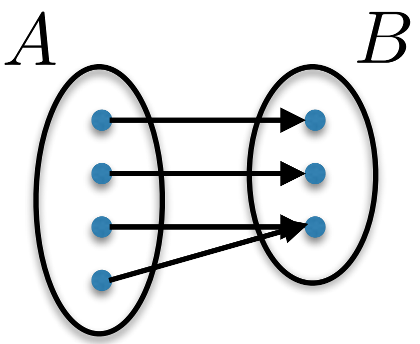
$$|A| \leq |B|$$

$$\boxed{A \hookrightarrow B}$$



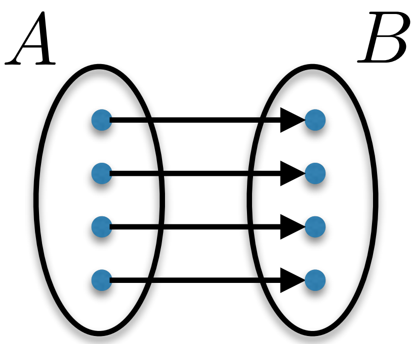
$$|A| \geq |B|$$

$$\boxed{A \twoheadrightarrow B}$$



$$|A| = |B|$$

$$\boxed{A \leftrightarrow B}$$



Sanity checks

$$|A| \leq |B| \text{ iff } |B| \geq |A|$$

$$\boxed{A \hookrightarrow B \text{ iff } B \twoheadrightarrow A}$$

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

$$A \leftrightarrow B \text{ iff } A \hookrightarrow B \text{ and } A \twoheadrightarrow B$$

$$\boxed{A \leftrightarrow B \text{ iff } A \hookrightarrow B \text{ and } B \hookrightarrow A}$$

$$\text{If } |A| \leq |B| \text{ and } |B| \leq |C| \text{ then } |A| \leq |C|$$

$$\boxed{\text{If } A \hookrightarrow B \text{ and } B \hookrightarrow C \text{ then } A \hookrightarrow C}$$

One more definition

$$|A| < |B|$$

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.

So what is the big deal?

This way of comparing the size of sets
generalizes to infinite sets!

These are the **right** definitions
for infinite sets as well!

Comparing the cardinality of **infinite** sets

$|A| \leq |B|$ $\qquad$ $\boxed{A \hookrightarrow B}$

$|A| \geq |B|$ $\qquad$ $\boxed{A \twoheadrightarrow B}$

$|A| = |B|$ $\qquad$ $\boxed{A \leftrightarrow B}$

Sanity checks for infinite sets

$|A| \leq |B|$ iff $|B| \geq |A|$

$$\boxed{A \hookrightarrow B \text{ iff } B \twoheadrightarrow A}$$

$|A| = |B|$ iff $|A| \leq |B|$ and $|B| \leq |A|$

$$A \leftrightarrow B \text{ iff } A \hookrightarrow B \text{ and } A \twoheadrightarrow B$$

$$\boxed{A \leftrightarrow B \text{ iff } A \hookrightarrow B \text{ and } B \hookrightarrow A}$$

Cantor
Schröder
Bernstein

If $|A| \leq |B|$ and $|B| \leq |C|$ then $|A| \leq |C|$

$$\boxed{\text{If } A \hookrightarrow B \text{ and } B \hookrightarrow C \text{ then } A \hookrightarrow C}$$

So what is the big deal?

Let me show you some interesting consequences.

Examples of equal size sets

$$|\mathbb{N}| = |\mathbb{Z}|$$

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

$$\begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0, & 1, & -1, & 2, & -2, & 3, & -3, & 4, & -4, & \ldots \end{array}$$

$$f(n) = (-1)^{n+1} \left\lceil \frac{n}{2} \right\rceil$$

Examples of equal size sets

$$|\mathbb{N}| = |\mathbb{Z}|$$

Does this make any sense? $\mathbb{N} \subsetneq \mathbb{Z}$

$A \subsetneq B \implies |A| < |B|$? Shouldn't $|\mathbb{N}| < |\mathbb{Z}|$?

Does renaming the elements of a set change its size? No.

Let's rename the elements of $\mathbb{Z}$:

$$\{\ldots, \text{banana}, \text{apple}, \text{melon}, \text{orange}, \text{mango}, \ldots\}$$

Let's call this set F. How can you justify saying $|\mathbb{N}| < |F|$?

Bijection is nothing more than renaming.

Examples of equal size sets

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

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

$$S = \{0, 1, 4, 9, 16, \ldots\}$$

$$f(n) = n^2$$

Examples of equal size sets

$$|\mathbb{N}| = |P|$$

$$\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$$

$$P = \{2, 3, 5, 7, 11, \ldots\}$$

$$f(n) = n\text{'th prime number.}$$

Definition: countable and uncountable sets

Definition:

- A set A is called *countable* if $|A| \leq |\mathbb{N}|$.
- A set A is called *countably infinite* if it is infinite and countable.
- A set A is called *uncountable* if it is **not** countable. (so $|A| > |\mathbb{N}|$)

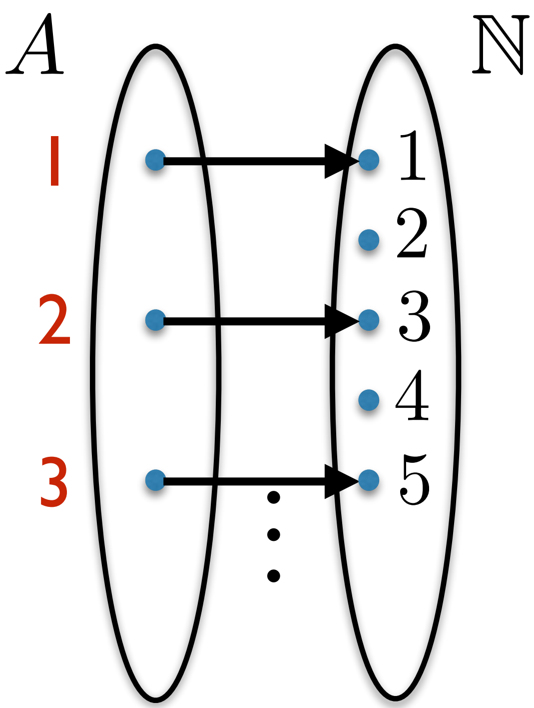
How to think about countable sets

A set A is called *countable* if $|A| \leq |\mathbb{N}|$.

So why is it called "countable"?

$|A| \leq |\mathbb{N}|$ means there is an injection $f : A \to \mathbb{N}$.

you could "count" the elements of *A*
(but could go on forever)



How to think about countable sets

A set A is called *countable* if $|A| \leq |\mathbb{N}|$.

Perhaps a better name would have been *listable*:

can list the elements of A so that
every element appears in the list eventually.

$a_1 \qquad a_2 \qquad a_3 \qquad a_4 \qquad a_5 \qquad \cdots$

(this is equivalent to being countable)

How to think about countable sets

A set A is called *countable* if $|A| \leq |\mathbb{N}|$.

This seems to imply that if A is infinite, then $|A| = |\mathbb{N}|$.

Is it possible that A is infinite, but $|A| < |\mathbb{N}|$?

Theorem:

A set A is countably infinite if and only if $|A| = |\mathbb{N}|$.

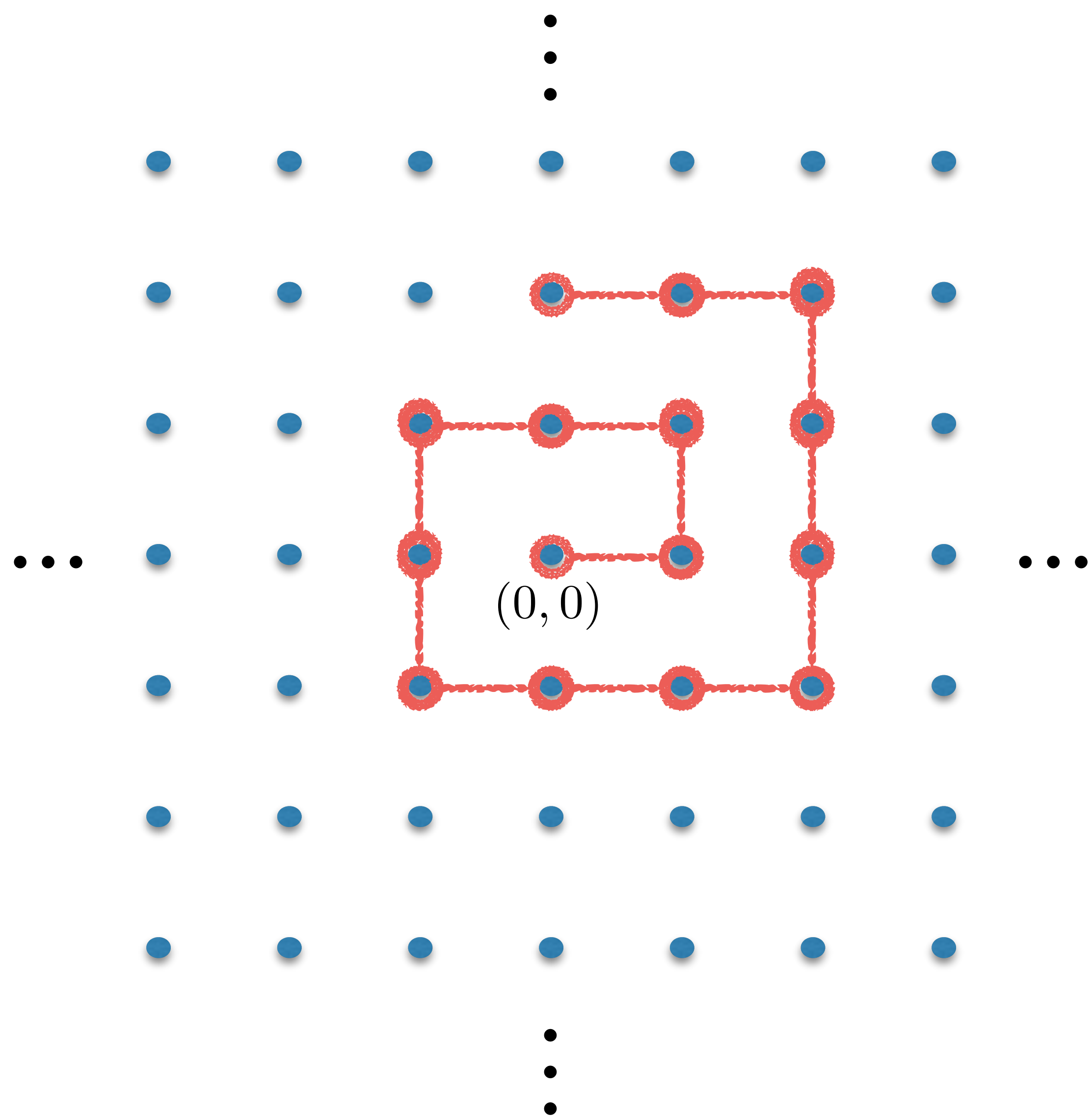
So if A is countable, there are two options:

1. A is finite
2. $|A| = |\mathbb{N}|$

Exercise: prove the theorem

Countable?

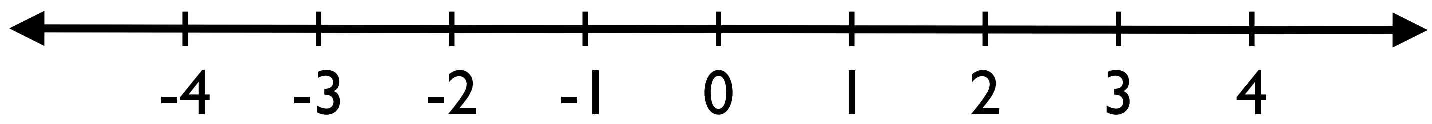
$$|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|?$$



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

Countable?

$$|\mathbb{N}| = |\mathbb{Q}|?$$



Can we list them in the order they appear on the line?

Between **any** two rational numbers, there is another one.

Any rational number can be written as a fraction $\dfrac{a}{b}$.

$\mathbb{Z} \times \mathbb{Z} \twoheadrightarrow \mathbb{Q}$ (map (a, b) to $\dfrac{a}{b}$)

$$\implies |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$$

Countable?

$$|\mathbb{N}| = |\{0,1\}^*|?$$

$\{0,1\}^*$ = the set of finite length binary strings.

ε

0

1

$00, 01, 10, 11$

$000, 001, 010, 011, 100, 101, 110, 111$

$\ldots$

Countable?

$$|\mathbb{N}| = |\Sigma^*|?$$

Σ^* = the set of finite length words over Σ.

Same idea.

Countable?

$$|\mathbb{N}| = |\mathbb{Q}[x]|?$$

$\mathbb{Q}[x]$ = the set of polynomials with rational coefficients.

e.g. $$x^3 - \frac{1}{4}x^2 + 6x - \frac{22}{7}$$

Take $\Sigma = \{0, 1, \ldots, 9, x, +, -, *, /, \hat{}\}$

Every polynomial can be described by a finite string over Σ.

e.g. $x\hat{}3 - 1/4x\hat{}2 + 6x - 22/7$

So $\Sigma^* \twoheadrightarrow \mathbb{Q}[x]$ i.e. $|\mathbb{Q}[x]| \leq |\Sigma^*|$

The CS method for showing a set is countable

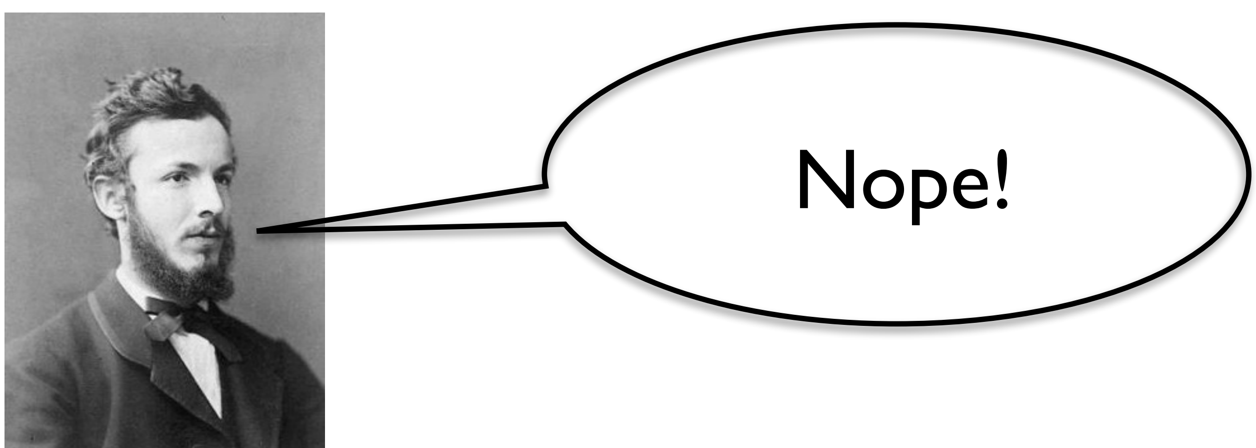
CS method to show a set A is countable $(|A| \leq |\mathbb{N}|)$:

Show $|A| \leq |\Sigma^*|$ for some alphabet Σ.

i.e. $\Sigma^* \twoheadrightarrow A$

i.e. Show that you can encode the elements of A using finite length words over an alphabet Σ.

Seems like every set is countable…



Cantor's Theorem

Theorem: For any non-empty set A,

$$|A| < |\mathcal{P}(A)|.$$

$$S = \{1, 2, 3\}$$

$$\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

$$|\mathcal{P}(S)| = 2^{|S|}$$

$$\mathcal{P}(S) \leftrightarrow \{0,1\}^{|S|}$$

binary strings of length |S|

$$S = \{1, 2, 3\}$$

$$1\ 0\ 1 \quad \longleftrightarrow \quad \{1, 3\}$$

$$0\ 0\ 0 \quad \longleftrightarrow \quad \emptyset$$

Cantor's Theorem

Theorem: For any non-empty set A,

$$|A| < |\mathcal{P}(A)|.$$

So:

$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. I.e. $\mathcal{P}(\mathbb{N})$ is uncountable.

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \cdots$$

(an infinity of infinities)

Cantor's Theorem - Proof by diagonalization

Assume $|\mathcal{P}(A)| \leq |A|$ for some set A.

So $A \twoheadrightarrow \mathcal{P}(A)$. Let f be such a surjection.

Example

$\mathbb{N} \twoheadrightarrow \mathcal{P}(\mathbb{N})$

$1 \to \{3, 7, 9\}$
$2 \to \{2, 5\}$
$3 \to \{1, 2, 3\}$
$4 \to \{1, 2, 3\}$
$\vdots$
$s \to S$

$S = \{1, 4, \ldots\}$

Define $S = \{a \in A : a \notin f(a)\} \in \mathcal{P}(A)$.

Since f is a surjection, $\exists s \in A$ s.t. $f(s) = S$.

But this leads to a contradiction: Is $s \in S$?

if $s \in S$ then $s \notin f(s) = S$

if $s \notin S$ then $s \in f(s) = S$

Why is this called a diagonalization argument?

$\square$

Cantor's Theorem - Proof by diagonalization

Example

$$\mathbb{N} \twoheadrightarrow \mathcal{P}(\mathbb{N})$$

$$\begin{array}{l}
1 \longrightarrow \{3,7,9\} \\
2 \longrightarrow \{2,5\} \\
3 \longrightarrow \{1,2,3\} \\
4 \nearrow \\
\vdots
\end{array}$$

$$S = \{1, 4, \ldots\}$$

	1	2	3	4	5	$\cdots$
f(1)	$\boxed{0}$	0	1	0	0	
f(2)	0	$\boxed{1}$	0	0	1	
f(3)	1	1	$\boxed{1}$	0	0	$\cdots$
f(4)	1	1	1	$\boxed{0}$	0	
f(5)	0	0	0	1	$\boxed{1}$	
$\vdots$			$\vdots$			
f(s)= S	1	0	0	1	0	$\cdots$

S is defined so that
S cannot equal any f(i)

Uncountable sets

Let $\{0,1\}^\infty$ be the set of binary strings of infinite length.

{0,1,2,3,4,5,6,7,8,9, … }

0000000000 … $\longleftrightarrow \emptyset$

1111111111 … $\longleftrightarrow \mathbb{N}$

1010101010 … $\longleftrightarrow \{\text{even natural numbers}\}$

⋮

$\{0,1\}^\infty$ is uncountable, i.e. $|\{0,1\}^\infty| > |\mathbb{N}|$

because $\{0,1\}^\infty \leftrightarrow \mathcal{P}(\mathbb{N})$. (just like $\{0,1\}^{|S|} \leftrightarrow \mathcal{P}(S)$)

(Recall $\{0,1\}^*$ *is* countable.)

Uncountable sets

Let $\{0,1\}^\infty$ be the set of binary strings of infinite length.

$\{0,1\}^\infty$ is uncountable, i.e. $|\{0,1\}^\infty| > |\mathbb{N}|$

<u>**Direct diagonal proof:**</u> Suppose $|\{0,1\}^\infty| \leq |\mathbb{N}|$

$$\mathbb{N} \twoheadrightarrow \{0,1\}^\infty$$

1	$\boxed{0}$	0	1	0	0	$\cdots$
2	0	$\boxed{1}$	0	0	1	$\cdots$
3	1	1	$\boxed{1}$	0	0	$\cdots$
4	1	1	1	$\boxed{0}$	0	$\cdots$
5	0	0	0	1	$\boxed{1}$	$\cdots$
$\vdots$			$\vdots$			

1 0 0 1 0 $\cdots$ —> cannot appear in the list

Uncountable sets

$\mathbb{R}$ is uncountable. In fact $(0, 1)$ is uncountable.

exercise

Be careful:

0.4999999999… = 0.500000000…

Appreciating the diagonalization argument

If you want to appreciate something,
try to break it…

Exercise:

Why doesn't the diagonalization argument work for

$\mathbb{N}$, $\{0,1\}^*$, a countable subset of $\{0,1\}^\infty$?

Uncountable sets

Let B be the set of bijections from $\mathbb{N}$ to $\mathbb{N}$.

B is uncountable.

CS method to show a set A is uncountable $(|A| > |\mathbb{N}|)$:

Show $|A| \geq |\{0,1\}^\infty|$

i.e. $A \twoheadrightarrow \{0,1\}^\infty$

i.e. Show that the elements of A
"encode" all the elements of $\{0,1\}^\infty$.

One slide guide to countability questions

You are given a set A .

Is it countable or uncountable?

$|A| \leq |\mathbb{N}|$ or $|A| > |\mathbb{N}|$?

$|A| \leq |\mathbb{N}|$:

- show directly that $A \hookrightarrow \mathbb{N}$ or $\mathbb{N} \twoheadrightarrow A$

- show $|A| \leq |B|$, where

$$B \in \{\mathbb{Z}, \quad \mathbb{Z} \times \mathbb{Z}, \quad \mathbb{Q}, \quad \boxed{\Sigma^*}, \quad \mathbb{Q}[x]\}$$

$|A| > |\mathbb{N}|$:

- show directly using a diagonalization argument

- show $|A| \geq |\{0,1\}^\infty|$

An Interesting Question

Is there a set S such that

$$|\mathbb{N}| < |S| < |\mathcal{P}(\mathbb{N})|?$$

Continuum Hypothesis:

No such set exists.

(Hilbert's 1st problem)

The story continues next lecture…