15-251: Great Theoretical Ideas in Computer Science

Lecture 6

# To Infinity and Beyond


CARNEGIE
MUSEUM
OF ART
©2009 Google
Google
Report a problem
Image Date: June 2008
C
D

Galileo (1564–1642)

Best known publication:

*Dialogue Concerning the Two Chief World Systems*

His final magnum opus (1638):

*Discourses and Mathematical Demonstrations Relating to Two New Sciences*

# The three characters

Salviati:

Argues for the Copernican system.

The “smart one”.  (Obvious Galileo stand-in.)

Named after one of Galileo’s friends.

Sagredo:

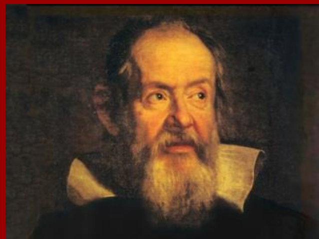
“Intelligent layperson”.  He’s neutral.

Named after one of Galileo’s friends.


Simplicio:

Argues for the Ptolemaic system. The “idiot”.

Modeled after two of Galilelo’s enemies.



Salviati

Simplicio


If I assert that all numbers, including both squares and non-squares, are more than the squares alone, I shall speak the truth, shall I not?

Most certainly.

If I should ask further how many squares there are
one might reply truly that there are
as many as the corresponding number of square-roots,
since every square has its own square-root and every square-root its own square…

Precisely so.

But if I inquire how many square-roots there are,
it cannot be denied that there are as many as the numbers because every number is the square-root of some square. This being granted, we must say that there are as many squares as there are numbers …
Yet at the outset we said that there are many more numbers than squares.

Sagredo: What then must one conclude under these circumstances?

Salviati

… Neither is the number of squares less than the totality of all the numbers, …

… nor the latter greater than the former, …

… and finally, the attributes "equal," "greater," and "less," are not applicable to infinite, but only to finite, quantities.

"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 (1777 – 1855)*

Cantor (1845 – 1918)

# Some of Cantor's contributions

> Explicit definitions comparing the cardinality (size) of (infinite) sets

> There are different levels of infinity.

> There are infinitely many different infinities.

> The diagonalization argument

> Also: $|\mathbb{N}| = |\text{Squares}|$ even though Squares is a proper subset of $\mathbb{N}$.

# 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

**Utter non-sense.**

*- Ludwig Wittgenstein*

# Reaction to Cantor's ideas at the time

Laughable.

*- Ludwig Wittgenstein*

# Reaction to Cantor's ideas at the time

**WRONG.**

*- Ludwig Wittgenstein*

# 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

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

*- David Hilbert*

# Cantor’s Definition

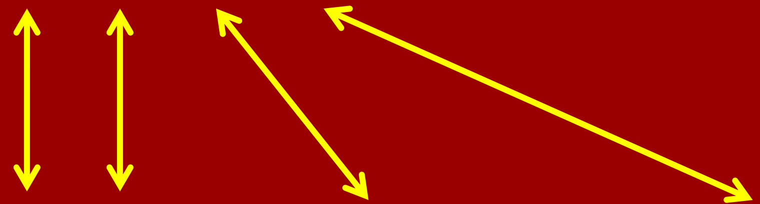
Sets A and B have the same ‘cardinality’ (size), written $|A| = |B|$, if there exists a bijection between them.

Note: This is **not** a definition of “$|A|$”.

This is a definition of the phrase “$|A| = |B|$”.

# In Galileo's case

$\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots \}$



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

There is a **bijection** between $\mathbb{N}$ and S (namely, $f(a)=a^2$)

Thus $|S|=|\mathbb{N}|$ (even though $S \subsetneq \mathbb{N}$).

# More examples: Hilbert’s Grand Hotel

# More examples: Hilbert's Grand Hotel

One extra person: $|\mathbb{N}| = |\mathbb{N} \setminus \{0\}|$

(bijection is f(x) = x+1)

$|\mathbb{N} \uplus \{1\}| = |\mathbb{N}|$

Extra bus: $|\mathbb{N}| = |\{2, 4, 6, 8, \ldots\}|$

(bijection is f(x) = 2x)

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

Infinitely many buses: $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$

(injection is f(j,j) = (ith prime)$^j$

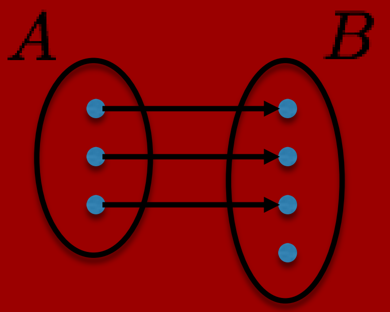
# 3 Important Types of Functions

**injective, 1-to-1**

$f : A \to B$ is injective if

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

$A \hookrightarrow B$

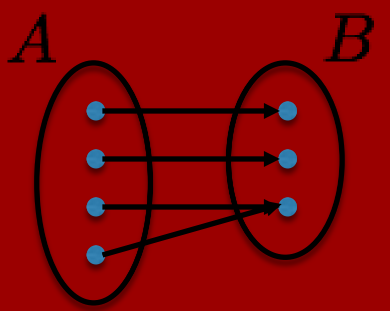



**surjective, onto**

$f : A \to B$ is surjective if

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

$A \twoheadrightarrow B$

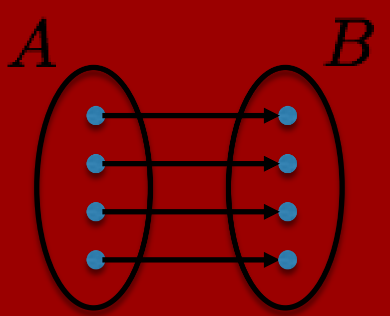



**bijective, 1-to-1 correspondence**

$f : A \to B$ is bijective if

$f$ is injective and surjective

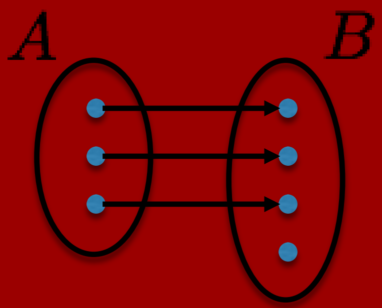
$A \leftrightarrow B$



# Comparing cardinalities

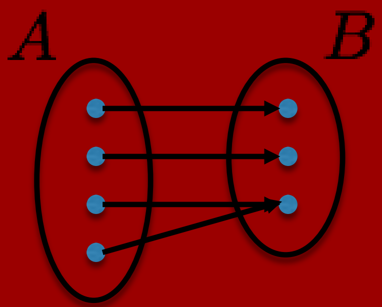
$|A| \leq |B|$

$A \hookrightarrow B$



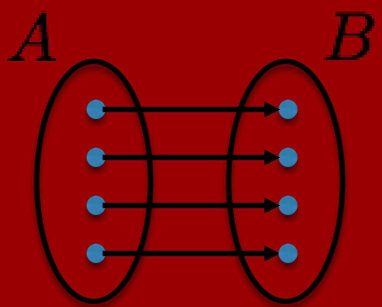

$|A| \geq |B|$

$A \twoheadrightarrow B$




$|A| = |B|$

$A \leftrightarrow B$



# Comparing cardinalities of finite sets

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

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

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

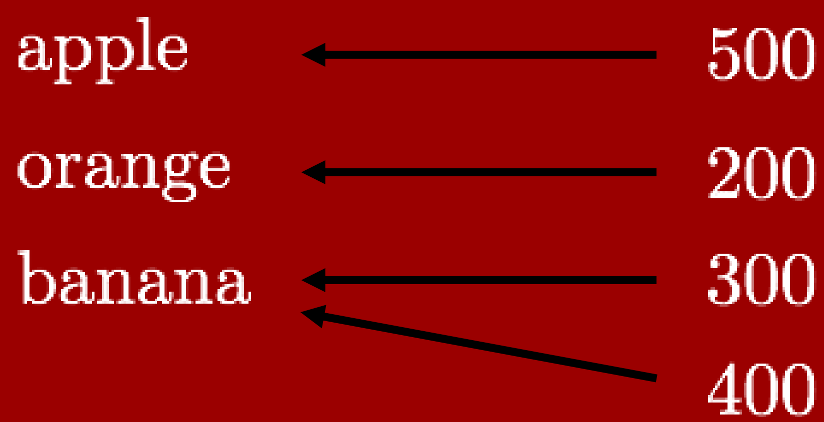

$|A| \leq |B|$ **iff there is an injection from $A$ to $B$.**

# Comparing cardinalities of finite sets

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

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

**What does $|B| \geq |A|$ mean?**




$|B| \geq |A|$ **iff there is an surjection from $B$ to $A$.**

# Sanity checks for infinite sets

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

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

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

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

Transitivity is also true for bijections / equality.

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

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

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

Cantor
Schröder
Bernstein

# Cantor Schröder Bernstein

Theorem: $A \leftrightarrow B \text{ iff } A \hookrightarrow B \text{ and } B \hookrightarrow A$

Proof:

- Draw injections as directed edges between elements in the domain and elements in the range.
- Each element has exactly one outgoing and at most one incoming edge.

→ Get the union of directed cycles and directed paths which are infinite on one or both sides – all alternating between elements in A and B.

- For each such path / cyle take every other edge (starting with the end/beginning for one-sided infinite paths)

This gives a perfect matching / 1-to-1 correspondence.

QED

$\mathbb{N} = \{\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7, \ldots\}$

$E = \{\ 0,\ 2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14, \ldots\}$

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

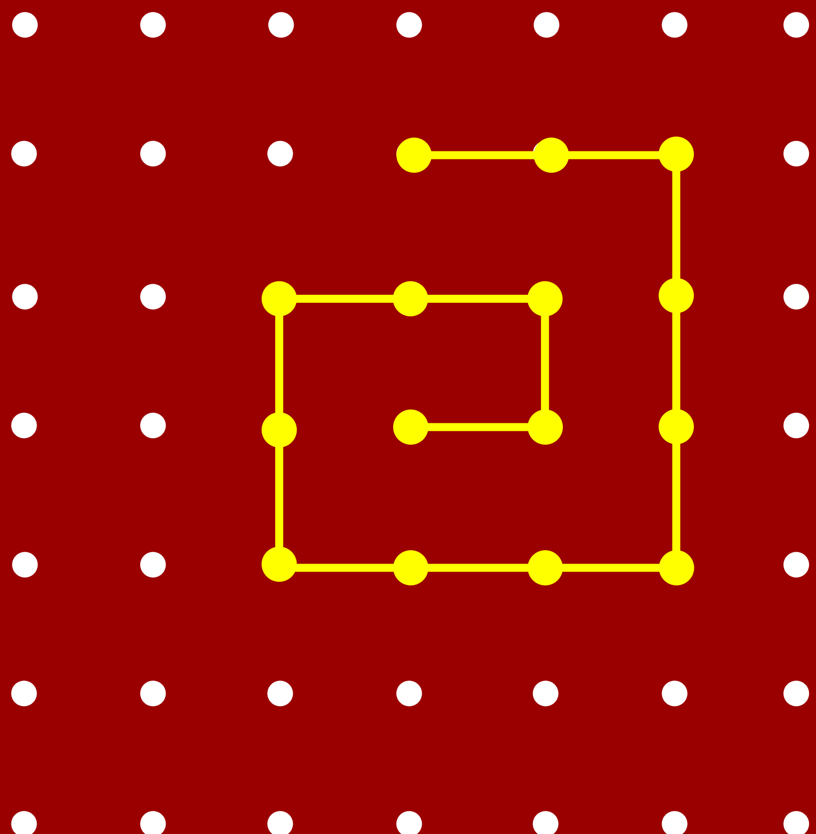
$P = \{\ 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19, \ldots\}$

If S is an infinite set and you can list off its elements as $s_0, s_1, s_2, s_3, \ldots$ uniquely, in a well-defined way, then $|S| = |\mathbb{N}|$.

Any set S with $|S| = |\mathbb{N}|$ is called **countably infinite**.

A set is called **countable** if it is either finite or countably infinite.

So $\mathbb{Z}$ is countable. Is $\mathbb{Z}^2$ countable?



(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)

What about $\mathbb{Q}$, the rationals? Countable?

Come on, no way! Between any two rationals there are infinitely many more.

Not so fast:

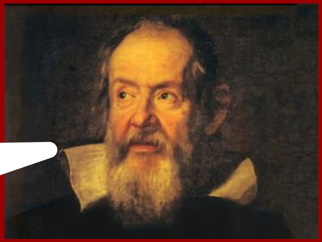
$$f(p,q) = \begin{cases} p/q & \text{if } q \neq 0, \\ 0 & \text{if } q = 0. \end{cases}$$

Is clearly a surjection, so $|\mathbb{Z}^2| \geq |\mathbb{Q}|$.

Let's do one more example.

Let {0,1}* denote the set of all binary strings of any finite length.

Is {0,1}* countable?



Yes, this is easy. Here is my listing:

ϵ, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, …

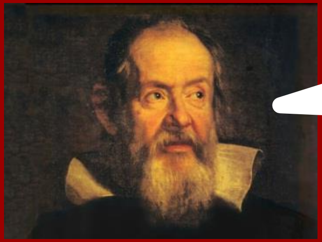
Length 0 strings

Length 1 strings in binary order

Length 2 strings in binary order

Length 3 strings in binary order

Perhaps this definition
just captures the difference
between finite and infinite?



Good question.
If A and B are infinite sets
do we always have $|A| = |B|$?

Yeah, I was thinking about all this in 1873.
The next most obvious question:
Is $\mathbb{R}$ (the reals) countable?

The 1873 proof was specifically tailored to ℝ.

In 1891, I described a much slicker proof of uncountability.

People call it…

**The Diagonal Argument**

I'll use the diagonal argument to prove the set of all **infinite** binary strings, denoted $\{0,1\}^{\mathbb{N}}$, is uncountable.

Examples of infinite binary strings:

x = 00000000000000000000000000000…

y = 01010101010101010101010101010…

z = 10110111011110111110111111 0…

w = 00110101000101000101000101000…

(Here $w_n = 1$ if and only if n is a prime.)

I'll use the diagonal argument to prove **the set of all infinite binary strings**, denoted $\{0,1\}^{\mathbb{N}}$, is **uncountable**.

Interesting! I remember we showed that $\{0,1\}^*$, the set of all **finite** binary strings, is **countable**.

Yep.

What about $\mathbb{R}$?

We'll come back to it. Anyway, strings are more interesting than real numbers, don't you think?

# Theorem: $\{0,1\}^{\mathbb{N}}$ is NOT countable.

Suppose for the sake of contradiction that you *can* make a list of all the infinite binary strings.

For illustration, perhaps the list starts like this:

0: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…
1: 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1…
2: 1 0 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 1 0 1 1…
3: 0 0 1 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 0…
4: 0 1 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1…
5: 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…
… …

# Theorem: $\{0,1\}^{\mathbb{N}}$ is NOT countable.

Consider the string formed by the 'diagonal':

0: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…

1: 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1…

2: 1 0 1 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 1 0 1 1…

3: 0 0 1 1 0 1 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 0…

4: 0 1 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1…

5: 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…

… …

# Theorem: $\{0,1\}^{\mathbb{N}}$ is NOT countable.

Consider the string formed by the ‘diagonal’:

0: **0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…

1: 0 **1** 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1…

2: 1 0 **1** 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 1 0 1 1…

3: 0 0 1 **1** 0 1 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 0…

4: 0 1 0 1 **0** 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1…

5: 1 1 0 0 0 **1** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…

… … ⋱

## Theorem: $\{0,1\}^{\mathbb{N}}$ is NOT countable.

Actually, take the negation of the string on the diagonal:

**1 0 0 0 1 0…**

It can’t be anywhere on the list, since it differs from every string on the list! **Contradiction.** ■

0: **0** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…

1: 0 **1** 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1…

2: 1 0 **1** 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 1 0 1 1…

3: 0 0 1 **1** 0 1 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 0…

4: 0 1 0 1 **0** 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1…

5: 1 1 0 0 0 **1** 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…

… … ⋱

# Theorem: $\{0,1\}^{\mathbb{N}}$ is NOT countable.

Here is the same proof, using words:

Suppose for contradiction's sake that $\{0,1\}^{\mathbb{N}}$ is countable.

Thus $|\mathbb{N}| \geq |\{0,1\}^{\infty}|$;

i.e., there's a surjection $f : \mathbb{N} \rightarrow \{0,1\}^{\infty}$.

Define an infinite binary string $w \in \{0,1\}^{\infty}$ by $w_n = \neg\, f(n)_n$.

We claim that $w \neq f(m)$ for every $m \in \mathbb{N}$. This is because,

by definition, they disagree in the $m^{th}$ position.

Therefore $f$ is not a surjection onto $\{0,1\}^{\mathbb{N}}$, contradiction.

The same proof also shows:

**Theorem:** For any non-empty set $A$, $|A| < |\mathcal{P}(A)|$.

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

For example: $S = \{1, 2, 3\}$

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

$\mathcal{P}(S) \leftrightarrow \{0,1\}^{|S|}$ $\qquad$ $S = \{1, 2, 3\}$

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

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

The same proof also shows:

**Theorem:** For any non-empty set $A$, $|A| < |\mathcal{P}(A)|$.

Suppose for contradiction's sake that $A \geq \{0,1\}^A$, i.e.,

there's a surjection $f : A \rightarrow \{0,1\}^A$.

Define an string $w \in \{0,1\}^A$ by $w_a = \neg f(a)_a$ for every $a \in A$.

We claim that $w \neq f(b)$ for every $b \in A$. This is because,

by definition, they disagree in the position indexed by $b$.

Therefore $f$ is not a surjection onto $\{0,1\}^A$, contradiction.

Awesome. So not only is $\{0,1\}^{\mathbb{N}}$ uncountable but there is a whole hirarchy of larger and larger infinities:

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

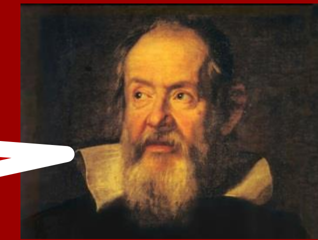
But what about $\mathbb{R}$?

$\mathbb{R}$ is uncountable. Even the set [0,1] of all reals between 0 and 1 is uncountable.

This is because there is a bijection between [0,1] and $\{0,1\}^{\mathbb{N}}$.

Hence $|\mathbb{R}| \geq |[0,1]| = |\{0,1\}^{\mathbb{N}}| > |\mathbb{N}|$.

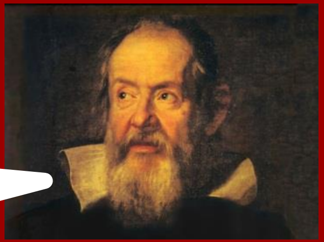
What's the bijection between [0,1] and $\{0,1\}^\infty$?



It's just the function f which maps each real number between 0 and 1 to its binary expansion!

| | | | |
|---|---|---|---|
| E.g.: | 1/2 | $\leftrightarrow$ | .1000000000… |
| | 1/3 | = | 1/4 + 1/16 + 1/64 + … |
| | | $\leftrightarrow$ | .0101010101… |
| | π−3 | = | $.14159265358979323\ldots_{10}$ |
| | | $\leftrightarrow$ | $.0010010000111110\ldots_{2}$ |

Um, technically that's not a surjection.
It misses, e.g., .0111111111111111…



It's just the function f which maps each real number between 0 and 1 to its binary expansion!

E.g.: 1/2 ↔ .1000000000…

1/3 = 1/4 + 1/16 + 1/64 + …
↔ .0101010101…

π−3 = $.14159265358979323\ldots_{10}$
↔ $.0010010000111110\ldots_{2}$

Um, technically that's not a surjection.
It misses, e.g., .0111111111111111…

You're saying because this also equals 1/2?
In the same way that,
in base 10, .499999…
is the same as .500000…?

Yeah.

Sorry.

Ugh. I was hoping you wouldn't notice that. This was all so elegant – and you had to go and bring that up!

There are a variety of easy hacks you can use to get around this issue.

# Summary: cardinalities we've seen so far

| card. | sets with that cardinality |
|---|---|
| 0 | $\emptyset$ |
| 2 | {0,1}, {red,green}, … |
| … | … |
| "$\aleph_0$" "aleph zero" | $\mathbb{N}$, Primes, Squares, $\mathbb{Z}$, $\mathbb{Z}^2$, $\mathbb{N}^2$, $\mathbb{Q}$, $\{0,1\}^*$, … |
| $\mathcal{P}(\mathbb{N})$ = "$\mathfrak{c}$" "the continuum" | $\{0,1\}^{\mathbb{N}}$, [0,1], $\mathbb{R}$… |
| $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ | {S \| S subset of $\mathbb{R}$ } |
| … | |

# Summary: cardinalities we've seen so far

Fact: There are no infinite sets with cardinality less than $|\mathbb{N}|$.

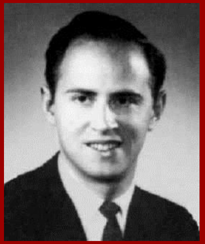
Question: Is there any set S with

$$|\mathbb{N}| < S < |\mathbb{R}|?$$

I didn't think so, and called this the Continuum Hypothesis. I spent a really long time trying to prove it, with no success. ☹

# Summary: cardinalities we've seen so far

There's a reason you failed…
And it's not because the
Continuum Hypothesis is false…



Question: Is there any set S with

$|\mathbb{N}| < S < |\mathbb{R}|$?

I didn't think so, and called this the Continuum Hypothesis. I spent a really long time trying to prove it, with no success. ☹

# Proving sets countable:
# the computer scientist's method

We showed $|\{0,1\}^*| = |\mathbb{N}|$.

Actually, if $\Sigma$ is any finite "alphabet" (set)
then $\Sigma^*$ = {all finite strings over alphabet $\Sigma$}
is countably infinite.

E.g., if $\Sigma$ = {0, 1, …, 9, a, b, …, z, +, −, *, /, ^}:

ϵ, 0, 1, …, a, …, /, ^, 00, 01, …, 0a, 0/, 0^, 10, …, ^/, ^^, 000, 001, …

# Proving sets countable:
# the computer scientist's method

Suppose we want to show that a set
S={all mathematical objects of type-T} is countable.

First specify a way to encode any such object X
with strings over some finite alphabet Σ.
(recall, we write $\langle X \rangle$ for this encoding).

If $\langle \cdot \rangle : \Sigma^* \rightarrow S$ is a surjection, i.e.,
has at least one encoding for any X in S,
then $|\mathbb{N}| = |\Sigma^*| \geq S$.

# Proving sets countable:
# the computer scientist's method:

Encodable = Countable

If a set of mathematical objects is encodable
then it is countable.

# Proving sets countable:
# the computer scientist's method

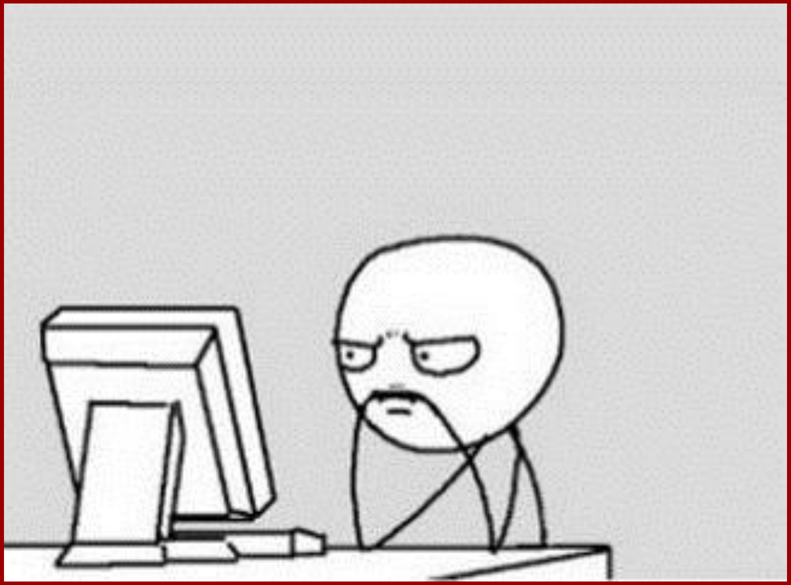
Ex. problem: Prove that $\mathbb{Q}[x]$ is countable.

Valid solution:

Any polynomial in $\mathbb{Q}[x]$ can be described by a finite string over the alphabet

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

(For example: x^3−1/4x^2+6x−22/7.)



Study Guide

Definitions:

Cardinality

Countable

Theorem/proof:

Countability of various sets.

Cantor-Bernstein Thm.

Diagonalization:

Uncountability of $\{0,1\}^{\infty}$.