Great Theoretical Ideas In Computer Science

V. Adamchik CS 15-251

Carnegie Mellon University

Cantor's Legacy

Cantor (1845–1918)

Galileo (1564–1642)

Outline

Cardinality
Diagonalization
Continuum Hypothesis
Cantor's theorem
Cantor's set

Galileo: *Dialogue on Two New Sciences*, 1638

Salviati

I take it for granted that you know which of the numbers are squares and which are not.

Simplicio

I am quite aware that a squared number is one which results from the multiplication of another number by itself.

Very well… 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?

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…

… 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.

Let's review this argument

ℕ = { 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, … }

S = { 0, 1, , , 4, , , , , 9, … }

"All numbers include both squares and non-squares."

S ⊊ ℕ

"Every square has its own square-root and every square-root its own square…"

There is a bijection between ℕ and S.

Cantor's Definition (1873)

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

Reminder: what's a bijection?

It's a perfect matching between A and B.

It's a mapping $f : A \rightarrow B$ which is:

an injection

(i.e., 'one-to-one': if $a \neq b \Rightarrow f(a) \neq f(b)$)

& a surjection

(i.e., 'onto': $\forall b \in B, \exists a \in A$ s.t. $f(a)=b$).

Cantor's Definition

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

E.g.: $|\mathbb{N}| = |\text{Squares}|$
because the function $f : \mathbb{N} \rightarrow$ Squares defined by $f(a)=a^2$ is a bijection.

If A and B are <u>infinite</u> sets
do we always have $|A| = |B|$?

That's exactly what I was wondering in 1873…

Let's try some examples!

Do $\mathbb{N}$ and $\mathbb{E}$ have the same cardinality?

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

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

$f(x) = 2x$ is 1-1 onto.

Do $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality?

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

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

$$f(x) = \begin{cases} (x+1)/2 & \text{if } x \text{ is odd} \\ -x/2 & \text{if } x \text{ is even} \end{cases}$$

The odd numbers in $\mathbb{N}$ map to the positive integers in $\mathbb{Z}$.
The even numbers in $\mathbb{N}$ map to negative integers in $\mathbb{Z}$.

Transitivity Lemma

Lemma: If
$f: A \rightarrow B$ is 1-1 onto, and
$g: B \rightarrow C$ is 1-1 onto.
Then $h(x) = g(f(x))$ defines a function
$h: A \rightarrow C$ that is 1-1 onto

Hence, $\mathbb{N}$, $\mathbb{E}$, and $\mathbb{Z}$ all have the same cardinality.

A Natural Intuition

Intuitively, what does it mean to find a bijection between a set A and ℕ ?

It means to list the elements of A in some order so that if you read down the list, every element will get read.

A Natural Intuition

Let's re-examine the set ℤ. Consider listing them in the following order.

First, list the positive integers (and 0):
Then, list the negative integers:

0, 1, 2, 3, 4, . . ., -1, -2, -3, -4, . . .

What is wrong with this counting?

If you start reading down the list, you will never actually get to the negatives!

A Natural Intuition

How about this list?
0, 1, -1, 2, -2, 3, -3, 4, -4, . . .

For any integer n, at most |2n| integers come before it in the list, so it will definitely get read.

Do ℕ and ℚ have the same cardinality?

ℕ = { 0, 1, 2, 3, 4, 5, 6, 7, ... }

ℚ = The Rational Numbers

No way!

The rationals are dense: between any two there is a third. You can't list them one by one without leaving out an infinite number of them.

Don't jump to conclusions!

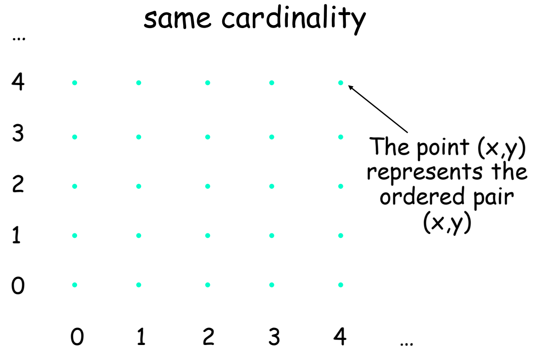
There is a clever way to list the rationals, one at a time, without missing a single one!

First, let's warm up with another interesting example:

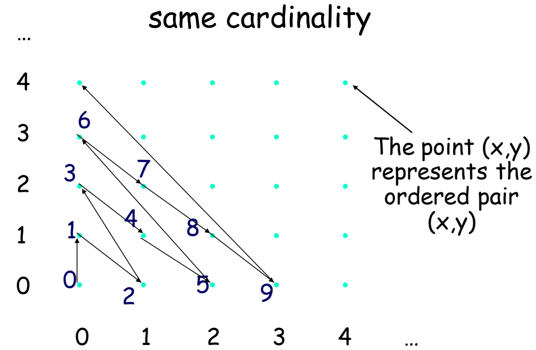
ℕ can be paired with ℕ × ℕ

$|\mathbb{N}| = |\mathbb{N}^2|$

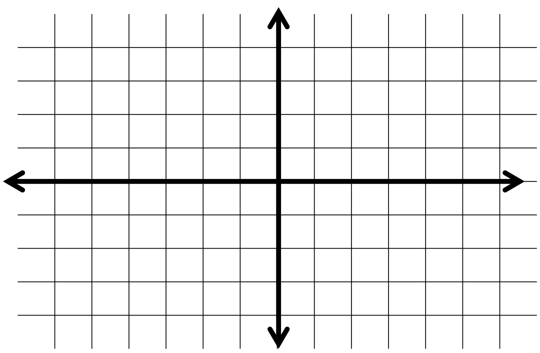
Theorem: ℕ and ℕ × ℕ have the same cardinality



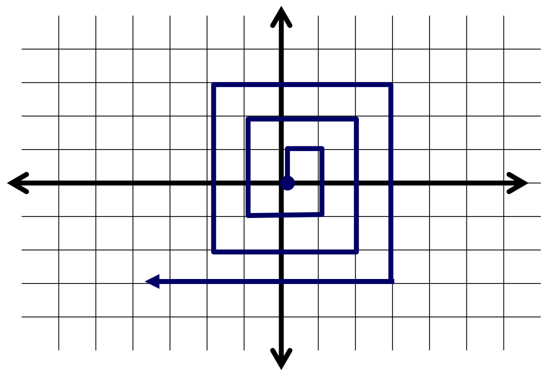
Theorem: ℕ and ℕ × ℕ have the same cardinality



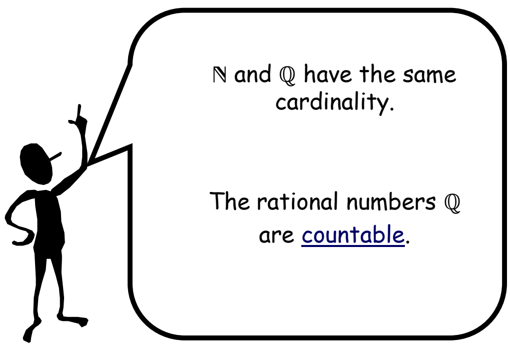
Onto the Rationals!



The point at x,y represents x/y

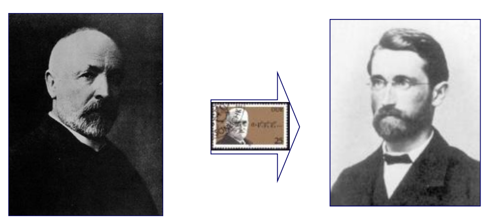


The point at x,y represents x/y



Cantor's 1877 letter to Dedekind:

"I see it, but I don't believe it! "



Let's do one more example.

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

Is $\{0,1\}^*$ countable?

Is $\{0,1\}^*$ countable?

Yes, this is easy. Here is my listing:

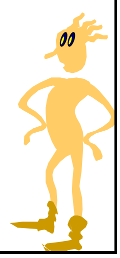
ϵ, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000,…

Length 0 strings	Length 1 strings in binary order	Length 2 strings in binary order	Length 3 strings in binary order

Thus:

The set of all possible Java/C/Py programs is countable.

The set of all possible finite length pieces of English text is countable.



Onto the Reals!

Is $\mathbb{R}$ countable?

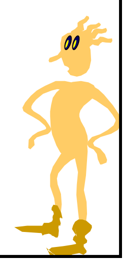
I asked Dedekind this in November, 1873.

$\mathbb{R} = \{ \frac{1}{2}, \sqrt{2}, \pi, \ldots\}$

"…if you could prove that $\mathbb{R}$ is uncountable, it would have an application in number theory: a new proof of Liouville's theorem that there are transcendental numbers!"

Cantor proved $\mathbb{R}$ is uncountable in December 1873.

To do this, he invented a very important technique called "Diagonalization"



Theorem: $|\mathbb{R}| \neq |\mathbb{N}|$

We will instead prove that the set of all infinite binary strings, denoted $\{0,1\}^\infty$, is uncountable.

Suppose $\{0,1\}^\infty$, is countable, thus there is a bijection $f: \mathbb{N} \to \mathbb{R}$

We will show that this is not a surjection.

Theorem: $\{0,1\}^\infty$ is NOT countable.

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

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

Theorem: $\{0,1\}^\infty$ is NOT countable.

Consider the string formed by the 'diagonal': the k-th bit in the (k-1)-st string

0: <u>0</u> 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…
1: 0 <u>1</u> 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 <u>1</u> 1 0 1 1 1 0 1 1 1 1 0 1 1 1 1 1 1 0 1 1…
3: 0 0 1 <u>1</u> 0 1 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 0…
4: 0 1 0 1 <u>0</u> 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1…
5: 1 1 0 0 0 <u>1</u> 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0…

Theorem: $\{0,1\}^\infty$ is NOT countable.

Next, negate each bit of that string
1 0 0 0 1 0…

It can't be anywhere on the list, since it differs from every string on the list!

Contradiction.

$\mathbb{R}$ 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 $\{0,1\}^\infty$.

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

Continuum Hypothesis

The cardinality of natural numbers
$|\mathbb{N}| = \aleph_0$ (aleph zero or naught)

There are no infinite sets with cardinality less $\aleph_0$

Question: Is there a set S with
$|\mathbb{N}| < S < |\mathbb{R}|$?
or
$\aleph_0 < S < 2^{\aleph_0} = \aleph_1$?

$\aleph_1$ is the smallest set larger than $\aleph_0$

This is called the Continuum Hypothesis. Cantor spent a really long time trying to prove $|\mathbb{R}| = \aleph_1$, with no success.

The Continuum Hypothesis cannot be proved or disproved from the standard axioms of set theory!

This has been proved!

Kurt Gödel, 1940

We know there are at least 2 infinities.
(the number of naturals, the number of reals.)

Are there more?

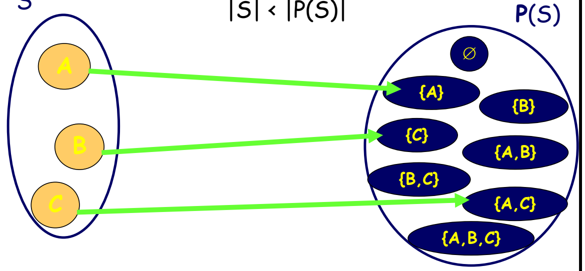
Definition: Power Set

The power set of S is the set of all subsets of S.

The power set is denoted as P(S). For example
$P(\{0,1\}) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$

Proposition:
If S is finite, the power set of S has cardinality $2^{|S|}$

Cantor's Theorem:
The power set of a set has a greater cardinal number than the set itself,
$|S| < |P(S)|$



It follows from this that there is an unending succession of different and greater infinite sets.

Cantor's Theorem

Theorem: There is no a bijection from S onto its power set P(S), and $|S|<|P(S)|$.

Proof:
Clearly, there is an injection, so $|S|\leq|P(S)|$.
Assume, by contradiction, that there is a bijection $f : S \rightarrow P(S)$.

Let $B = \{x \in S \mid x \notin f(x)\}$

Since $B \subset P(S)$, then $\exists\, a \in S$ with $f(a)=B$.
1) if $a \in B$ then $a \notin f(a) = B$ Contradiction!
2) if $a \notin B$ then $a \in f(a) = B$. Contradiction!

The cardinal numbers

$|\mathbb{N}| = \aleph_0 < \aleph_1 < \aleph_2 < \ldots$

$\aleph_k$ is the smallest set larger than $\aleph_{k-1}$

Are there any more infinities?

Let $S = \{\aleph_k \mid k \in \mathbb{N}\}$
P(S) is provably larger than any of them!!

No single infinity is big enough to count the number of infinities!

Generalized Continuum Hypothesis

The cardinal numbers

$\aleph_0 < \aleph_1 < \aleph_2 < \ldots$

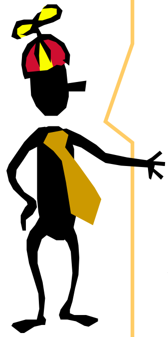
$\aleph_1$ is the smallest set larger than $\aleph_0$

The power sets

$|S| < |P(S)| < |P(P(S))| < \ldots$

Question: $\aleph_1 = |\mathbb{R}|$?

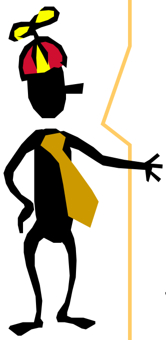
Question: $2^{\aleph_k} = \aleph_{k+1}$



Exercise

Consider all polynomials with integer coefficients.

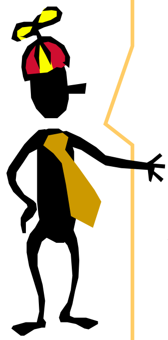
What is the cardinality of this set?



Exercise

Consider the algebraic numbers – roots of the polynomials with integer coefficients

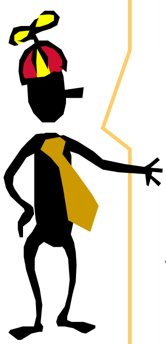
What is the cardinality of this set?



Exercise

Consider all polynomials with rational coefficients.

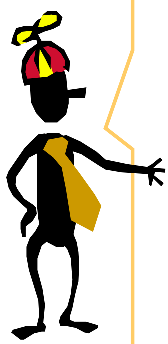
What is the cardinality of this set?



Exercise

Consider the transcendental numbers.

What is the cardinality of this set?



Exercise

Consider $\mathbb{R}^n$.

What is the cardinality of this set?

"I see it, but I don't believe it"

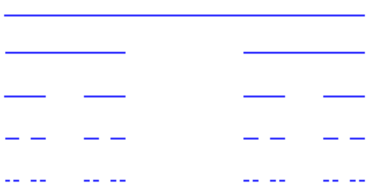
$\mathbb{R}^n$ can be put in
1-1 correspondence with [0,1].

Cantor's set

Tiny sets (measure zero) with uncountably many points

Cantor's set

Cantor Set is formed by repeatedly cutting out the open middle third of a line segment [0,1] (leaving end points) :



Cantor's set

What remains is called the Cantor set
How much did we remove?
What is the size of the Cantor set?

Cantor's set

How much did we remove?

$$\frac{1}{3}+\frac{2}{9}+\frac{4}{27}+\dots=\sum_{k=1}^{\infty}\frac{2^{k-1}}{3^k}=1$$

Cantor's set

Thinking of the size as a length, we removed everything.

Therefore, the Cantor set is very tiny.

Cantor's set

On the other hand, the Cantor set is not empty, since we did not remove the end points

0, 1, 1/3, 2/3,...

Cantor's set

We will show that the Cantor set is <u>uncountable</u>

Cantor's set

Consider the ternary representation of every number in [0,1]

After removing the first middle third remaining numbers are in the form

0.0xxx and 0.2xxx

(no 1s in the first digit)

Note, $0.1_3 = 0.022222..._3$

Cantor's set: second step

Consider the ternary representation of every number in [0,1]

After removing, remaining numbers are in the form

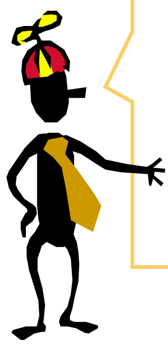
[0.0xxx to 0.01), [0.02xxx to 0.21), [0.22xxx to 1)

(no 1s in the first two digits)

Note, $0.21_3 = 0.2022222..._3$

Cantor's set

The Cantor set is a set of numbers whose ternary decimal representations consist entirely of 0's and 2's.



Problem

Does 1/12 belong to the Cantor set?

$1/12 = 0.0(02)_3$

Cantor's set

Can you find a 1-1 map between [0,1] and the Cantor set?

Cantor's set

The one-to-one map between [0,1] and the Cantor set is called the "Devil's Staircase" .

To see this bijection, take a number from the Cantor set in ternary notation, divide its digits by 2, and you get all coefficients in binary notation.

Here's What You Need to Know…

- Cardinality
- $|\mathbb{N}| = \aleph_0$
- Diagonalization
- $|\mathbb{R}| = c = 2^{\aleph_0}$
- Continuum Hypothesis $\aleph_1=2^{\aleph_0}$
- Cantor's theorem
  - $|S| < |P(S)| < |P(P(S))| < \dots$
- Cantor's set