15-251

Great Theoretical Ideas in Computer Science

Cantor's Legacy: Infinity And Diagonalization

Lecture 24 (April 12, 2007)

∞

The Theoretical Computer:

no bound on amount of memory
no bound on amount of time

Ideal Computer is defined as a computer with infinite RAM

You can run a Java program and never have any overflow, or out of memory errors

An Ideal Computer

It can be programmed to print out:

2: 2.0000000000000000000000…
1/3: 0.33333333333333333333…
ϕ: 1.6180339887498948482045…
e: 2.7182818284559045235336…
π: 3.14159265358979323846264…

Printing Out An Infinite Sequence

A program P prints out the infinite sequence

$s_0, s_1, s_2, \ldots, s_k, \ldots$

if when P is executed on an ideal computer, it outputs a sequence of symbols such that

- The k^{th} symbol that it outputs is s_k
- For every $k \in \mathbb{N}$, P eventually outputs the k^{th} symbol. I.e., the delay between symbol k and symbol k+1 is not infinite

Computable Real Numbers

A real number R is computable if there is a (finite) program that prints out the decimal representation of R from left to right.

Thus, each digit of R will eventually be output.

Are all real numbers computable?

List of questions

Are all real numbers computable?	??

Describable Numbers

A real number R is describable if it can be denoted unambiguously by a finite piece of English text

2: "Two."

π: "The area of a circle of radius one."

Are all real numbers describable?

List of questions

Are all real numbers computable?	??
Are all real numbers describable?	??

Computable r: some program outputs r

Describable r: some sentence denotes r

Is every computable real number, also a describable real number?

And what about the other way?

List of questions

Are all real numbers computable?	??
Are all real numbers describable?	??
Is every computable number describable?	??
Is every describable number computable?	??

Computable $\Rightarrow$ Describable

Theorem:

Every computable real is also describable

Proof:
Let R be a computable real that is output by a program P. The following is an unambiguous description of R:

> "The real number output by the following program:" P

List of questions

Are all real numbers computable?	??
Are all real numbers describable?	??
Is every computable number describable?	Yes
Is every describable number computable?	??

Correspondence Principle

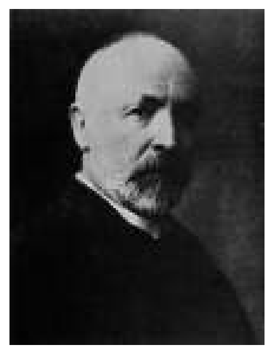
If two finite sets can be placed into bijection, then they have the same size

Correspondence Definition

In fact, we can use the correspondence as the definition:

Two finite sets are defined to have the same size if and only if they can be placed into bijection

Georg Cantor (1845-1918)



Cantor's Definition (1874)

Two sets are defined to have the same size if and only if they can be placed into bijection

Two sets are defined to have the same cardinality if and only if they can be placed into bijection.

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

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

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

The even, natural numbers.

How can E and N have the same cardinality? E is a proper subset of N with plenty left over.

The attempted correspondence
f(x) = x does not take E onto N.

E and N do have the same cardinality!

N = 0, 1, 2, 3, 4, 5, …
E = 0, 2, 4, 6, 8,10, …

f(x) = 2x is a bijection

Lesson:

Cantor's definition only requires that some injective correspondence between the two sets is a bijection, not that all injective correspondences are bijections!

This distinction never arises when the sets are finite

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

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

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

$\mathbb{N}$ and $\mathbb{Z}$ do have the same cardinality!

$\mathbb{N}$ = 0, 1, 2, 3, 4, 5, 6 …
$\mathbb{Z}$ = 0, 1, -1, 2, -2, 3, -3, ….

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

A Useful Transitivity Lemma

Lemma:
If
f: A→B is a bijection, and
g: B→C is a bijection.
Then h(x) = g(f(x)) defines a function
h: A→C that is a bijection

Hence, N, E, and Z all have the same cardinality.

Onto the Rationals!

Do N and Q have the same cardinality?

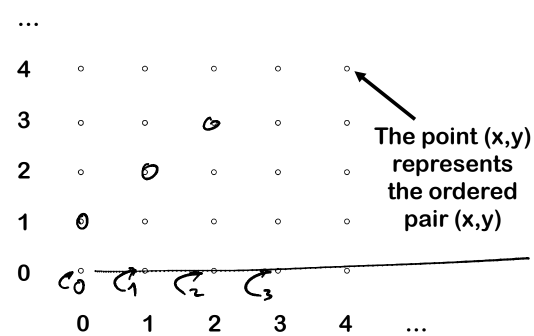
N = { 0, 1, 2, 3, 4, 5, 6, 7, …. }

Q = The Rational Numbers

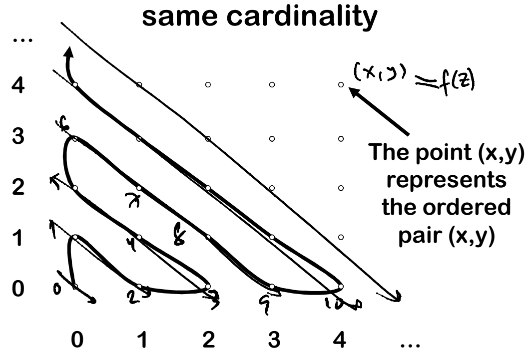
How could it be????

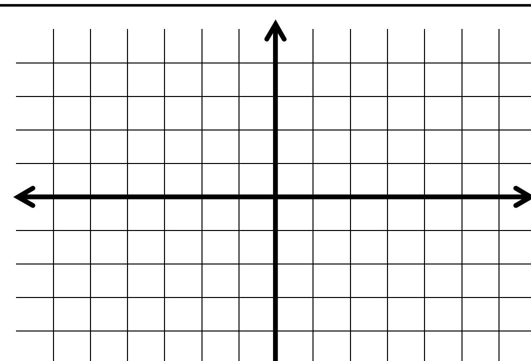
The rationals are dense: between any two there is a third. You can't list them one by one without leaving out an infinite number of them.

How about N and N×N ?

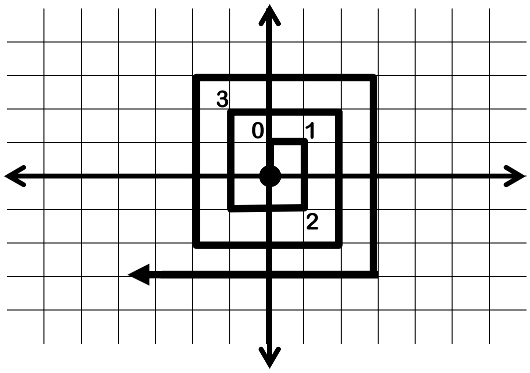


Theorem: N and N×N have the same cardinality





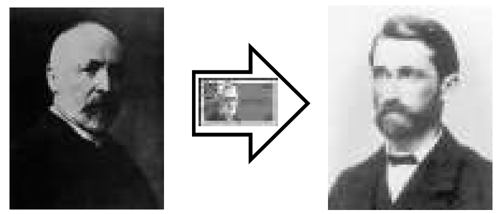
The point at x,y represents x/y



The point at x,y represents x/y

Cantor's 1877 letter to Dedekind:

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



Countable Sets

We call a set countable if it can be placed into a bijection with the natural numbers N

Hence N, E, Z, Q are all countable

Do N and R have the same cardinality? I.e., is R countable?

N = { 0, 1, 2, 3, 4, 5, 6, 7, … }

R = The real numbers

Theorem: The set $R_{[0,1]}$ of reals between 0 and 1 is not countable

Proof: (by contradiction)

Suppose $R_{[0,1]}$ is countable

Let f be a bijection from N to $R_{[0,1]}$

Make a list L as follows:

0: decimal expansion of f(0)
1: decimal expansion of f(1)
…
k: decimal expansion of f(k)
…

Position after decimal point

Index

L	0	1	2	3	4	…
0						
1						
2						
3						
…						

Position after decimal point

	L	0	1	2	3	4	…
f(0)	0	3	3	3	3	3	3
Index	1	3	1	4	1	5	9
	2	1	2	4	8	1	2
	3	4	1	2	2	6	8
	…						

L	0	1	2	3	4	…
0	d_0					
1		d_1				
2			d_2			
3				d_3		
…					d_4	

L	0	1	2	3	4
0	d_0 2				
1		d_1 6			
2			d_2 5		
3				d_3 1	
…					… 3

Confuse = 0.65666…

Define the following real number
$\text{Confuse}_L = 0.C_0C_1C_2C_3C_4C_5 \ldots$

$$C_k = \begin{cases} 5, & \text{if } d_k = 6 \\ 6, & \text{otherwise} \end{cases}$$

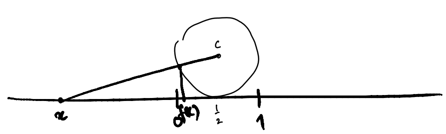
Diagonalized!

By design, Confuse_L can't be on the list L!

Indeed, note that Confuse_L differs from the k^{th} element on the list L in the k^{th} position.

This contradicts the assumption that the list L is complete; i.e., that the map f: N to $R_{[0,1]}$ is onto.

The set of reals is uncountable! (Even the reals between 0 and 1)



Sanity Check

Why can't the same argument be used to show that the set of rationals Q is uncountable?

Note that CONFUSE_L is not necessarily rational. And so there is no contradiction from the fact that it is missing from the list L

Back to the questions we were asking earlier

List of questions

Are all real numbers computable?	??
Are all real numbers describable?	??
Is every computable number describable?	Yes
Is every describable number computable?	??

Standard Notation

Σ = Any finite alphabet
Example: {a,b,c,d,e,…,z}

Σ^* = All finite strings of symbols from Σ including the empty string ε

Theorem: Every infinite subset S of Σ^* is countable

Proof:

Sort S by first by length and then alphabetically

Map the first word to 0, the second to 1, and so on…

Some infinite subsets of Σ^*

Σ = The symbols on a standard keyboard

For example:

The set of all possible Java programs is a subset of Σ^*

The set of all possible finite pieces of English text is a subset of Σ^*

Thus:

The set of all possible Java programs is countable.

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

But look:

There are countably many Java programs and uncountably many reals.

Hence, most reals are not computable!

There are countably many descriptions and uncountably many reals.

Hence:
Most real numbers are not describable!

List of questions

Are all real numbers computable?	No
Are all real numbers describable?	No
Is every computable number describable?	Yes
Is every describable number computable?	??

Next lecture…

To end, here's an important digression about infinity…

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

Are there more?

Definition: Power Set

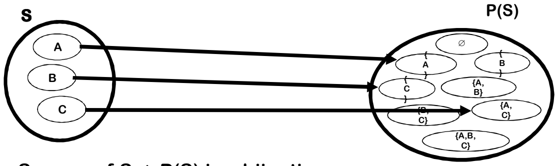
The power set of S is the set of all subsets of S.

The power set is denoted as P(S)

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

How do sizes of S and P(S) relate if S is infinite?

Theorem: S can't be put into bijection with P(S)



Suppose f:S → P(S) is a bijection.

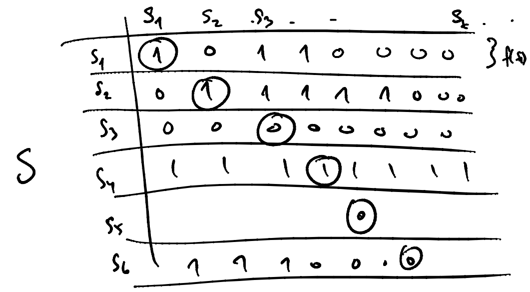
Let $CONFUSE_f = \{ x \mid x \in S, x \notin f(x) \}$

Since f is onto, exists $y \in S$ such that $f(y) = CONFUSE_f$.
Is y in $CONFUSE_f$?

YES: Definition of $CONFUSE_f$ implies no

NO: Definition of $CONFUSE_f$ implies yes

CONFUSE = { s_3, s_5, s_6,



For any set S (finite or infinite),
the cardinality of P(S)
is strictly greater than
the cardinality of S.

This proves that there are at least a countable number of infinities.

Indeed, take any infinite set S.
Then P(S) is also infinite, and its cardinality is a larger infinity than the cardinality of S.

This proves that there are at least a countable number of infinities.

The first infinity is the size of all the countable sets. It is called:

$$\aleph_0$$

$\aleph_0, \aleph_1, \aleph_2, \ldots$

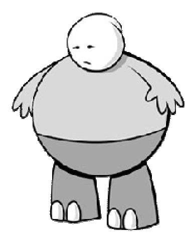
Cantor wanted to show that the number of reals was $\aleph_1$

Cantor called his conjecture that $\aleph_1$ was the number of reals the "Continuum Hypothesis."

However, he was unable to prove it. This helped fuel his depression.

The Continuum Hypothesis can't be proved or disproved from the standard axioms of set theory!

This has been proved!



Here's What You Need to Know…

- Cantor's Definition: Two sets have the same cardinality if there exists a bijection between them.
- E, N, Z and Q all have the same cardinality
- Proof that there is no bijection between N and R
- Definition of Countable versus Uncountable