cse 311: foundations of computing

Fall 2015

Lecture 27: Infinities and diagonalization

$*54{\cdot}43.\ \vdash :.\ \alpha, \beta \in 1\ .\supset :\ \alpha \cap \beta = \Lambda\ .\equiv.\ \alpha \cup \beta \in 2$

Dem.

$\vdash .\ *54{\cdot}26\ .\supset \vdash :.\ \alpha = \iota\text{‘}x\ .\ \beta = \iota\text{‘}y\ .\supset :\ \alpha \cup \beta \in 2\ .\equiv.\ x \neq y\ .$

$[*51{\cdot}231] \qquad \equiv .\ \iota\text{‘}x \cap \iota\text{‘}y = \Lambda\ .$

$[*13{\cdot}12] \qquad \equiv .\ \alpha \cap \beta = \Lambda \qquad (1)$

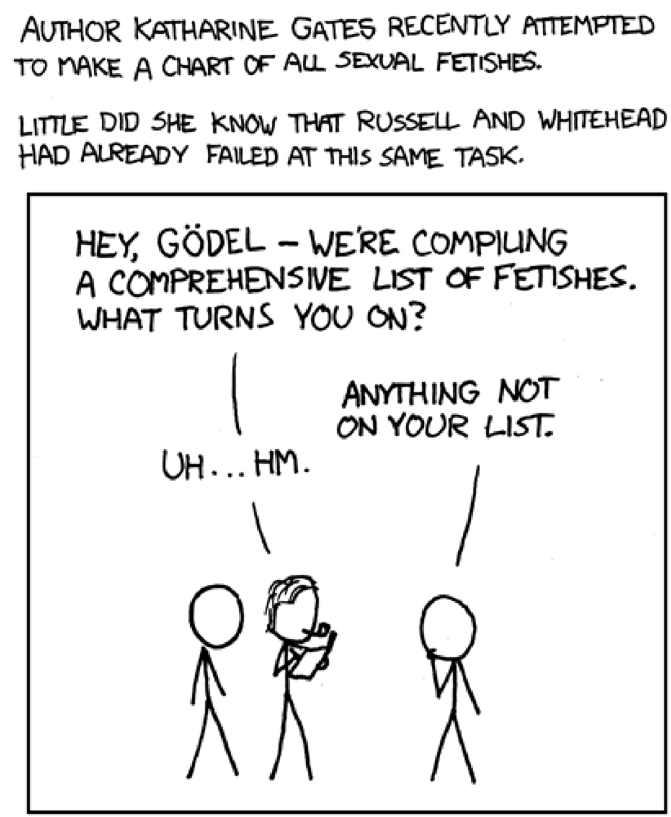
$\vdash .\ (1)\ .\ *11{\cdot}11{\cdot}35\ .\supset$

$\vdash :.\ (\exists x, y)\ .\ \alpha = \iota\text{‘}x\ .\ \beta = \iota\text{‘}y\ .\supset :\ \alpha \cup \beta \in 2\ .\equiv.\ \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash .\ (2)\ .\ *11{\cdot}54\ .\ *52{\cdot}1\ .\supset \vdash .\ \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

[proved on page 86 of Volume II: "The above proposition is occasionally useful."]



Russell's paradox: The set $\mathcal{S}$ of all sets that do not contain themselves.

$$\mathcal{S} \in \mathcal{S} \Rightarrow \mathcal{S} \notin \mathcal{S} \Rightarrow \mathcal{S} \in \mathcal{S}$$

computers from thought

Computers as we know them grew out of a desire to avoid bugs in mathematical reasoning.

Hilbert gave a famous speech at the International Congress of Mathematicians in 1900.

His goal was to mechanize all of mathematics.

In the 1930s, work of Gödel and Turing showed that Hilbert's program is **impossible**.

Gödel's incompleteness theorem
Undecidability of the Halting Problem

Both of these employ an idea we will see today called **diagonalization**.

The ideas are simple but so revolutionary that the inventor Georg Cantor was shunned by the mathematical leaders of the time:

Poincaré referred to them as a "grave disease infecting mathematics."

Kronecker fought to keep Cantor's papers out of his journals.

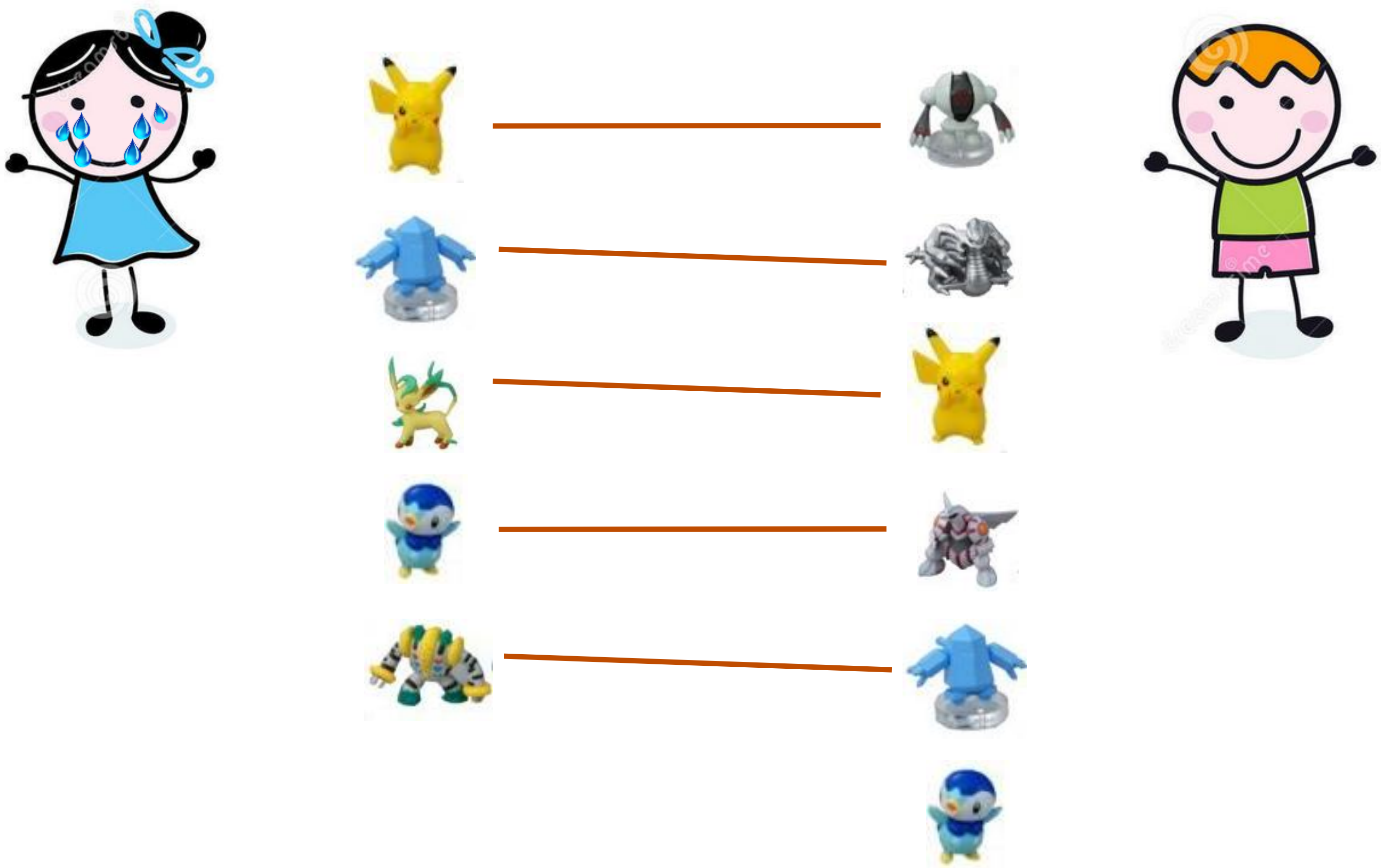
Cantor spent the last 30 years of his life battling depression, living often in "sanatoriums" (psychiatric hospitals).

cardinality

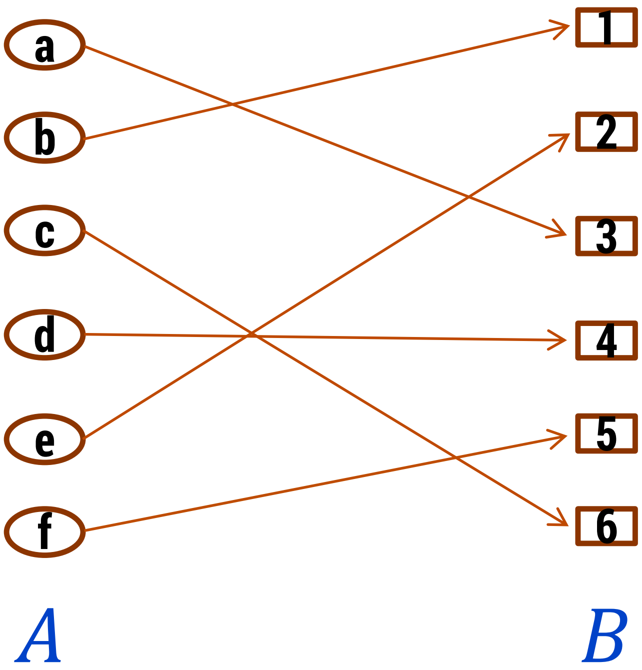
What does it mean that two sets have the same size?

cardinality

What does it mean that two sets have the same size?



Definition: Two sets A and B have the same **cardinality** if there is a one-to-one correspondence between the elements of A and those of B.
More precisely, if there is a 1-1 and onto function $f : A \to B$.



The definition also makes sense for infinite sets!

cardinality

Do the natural numbers and the even natural numbers have the same cardinality?

Yes!

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	2	4	6	8	10	12	14	16	18	20	22	24	26	28

What's the map $f : \mathbb{N} \to 2\mathbb{N}$?

$f(n) = 2n$

Definition: A set is **countable** iff it has the same cardinality as $\mathbb{N}$.

Equivalent: A set S is countable iff there is an 1-1 and onto function $g : \mathbb{N} \to S$

Equivalent: A set S is countable iff we can order the elements $S = \{x_1, x_2, x_3, \ldots\}$ $g(n) = x_{n+1}$

Question:
If $g : \mathbb{N} \to S$ is just **onto**, do we still know that S is countable?

$S = \{0, 1\}$ $g(n) = n \bmod 2$

Definition: A set S is "at most countable" if it is finite or countable.

the set $\mathbb{Z}$ of all integers

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

0	1	2	3	4	5	6	...
0	1	−1	2	−2	3	−3	

$$f(n) = \begin{cases} \frac{n+1}{2} & n \text{ odd} \\ -\frac{n}{2} & n \text{ even} \end{cases}$$

$f: \mathbb{N} \to \mathbb{Z}$

✓

the set $\mathbb{Q}$ of rational numbers

$$\mathbb{Q} = \left\{ \frac{p}{q} : \begin{array}{l} p \in \mathbb{Z} \\ q \in \mathbb{N},\ q \neq 0 \end{array} \right\}$$

We can’t do the same thing we did for the integers.

Between any two rational numbers there are an infinite number of others.

the set of positive rational numbers

0	1	2	3	4	-	-	-	-
1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	...
2/1	2/2	2/3	2/4	2/5	2/6	2/7	2/8	...
3/1	3/2	3/3	3/4	3/5	3/6	3/7	3/8	...
4/1	4/2	4/3	4/4	4/5	4/6	4/7	4/8	...
5/1	5/2	5/3	5/4	5/5	5/6	5/7	...	
6/1	6/2	6/3	6/4	6/5	6/6	...		
7/1	7/2	7/3	7/4	7/5	....			
...	...	...	...	...				

✓

the set of positive rational numbers

The set of all positive rational numbers **is countable.**

$\mathbb{Q}^+ = \{$**1/1, 2/1, 1/2, 3/1, 2/2,1/3, 4/1, 2/3, 3/2, 1/4, 5/1, 4/2, 3/3, 2/4, 1/5, ...**$\}$

List elements in order of numerator+denominator, breaking ties according to denominator.

Only k numbers have total of sum of $k + 1$, so every positive rational number comes up some point.

Technique is called "dovetailing."

Notice that repeats are OK because we can skip over them.

Formal statement about "skipping":
A set S is **countable** iff S is infinite and there is an onto map $g : \mathbb{N} \to S$.

the set $\mathbb{Q}$ of rational numbers

$g : \mathbb{N} \to \mathbb{Q}^+$ 1-1, onto

$f : \mathbb{N} \to \mathbb{Q}$

$$f(n) = \begin{cases} g\left(\frac{n}{2}\right) & \text{if } n \text{ is even} \\ -g\left(\frac{n+1}{2}\right) & \text{if } n \text{ is odd} \end{cases}$$

✓

Claim: Σ^* is countable for every finite Σ

$|\Sigma| > 0$

$\Sigma = \{0, 1, 2\}$

$\Sigma^* = \{\epsilon, 0, 1, 2, 00, 01, 02, 10, \ldots\}$

$\Sigma^* = \{\epsilon,$
$0, 1, 2,$
$00, 01, 02, 10, 11, 12, 20, 21, 22,$
$000, \ldots\}$

~~ϵ, 0, 00, 000, 0000~~

the set of all Java programs is countable

Let Σ be the alphabet for JAVA.

$\text{JAVA} \subseteq \Sigma^*$

- JAVA is infinite
- Let $g : \mathbb{N} \to \Sigma^*$ be onto

want $f : \mathbb{N} \to \text{JAVA}$ onto

$$f(n) = \begin{cases} g(n) & \text{if } g(n) \in \text{JAVA} \\ P_0 & \text{otherwise} \end{cases}$$

P_0 = some fixed program

ok ok, everything is countable except your mom

“Your mamma so fat she couldn’t be put into one to one correspondence with the natural numbers.”

Burn.

are the real numbers countable?

Theorem [Cantor]:
The set of real numbers between 0 and 1 is **not** countable.

Proof will be by contradiction. Uses a new method called diagonalization.

real numbers between 0 and 1: [0,1)

Every number between 0 and 1 has an infinite decimal expansion:

1/2 = 0.50000000000000000000000...

1/3 = 0.33333333333333333333333...

1/7 = 0.14285714285714285714285...

π-3 = 0.14159265358979323846264...

1/5 = 0.19999999999999999999999...

= 0.20000000000000000000000...

Representation is unique except for the cases that the decimal expansion ends in all 0's or all 9's.

proof that [0,1) is uncountable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4	5	6	7	8	9	...
r_1	0.	5	0	0	0	0	0	0	0	...	...
r_2	0.	3	3	3	3	3	3	3	3	...	...
r_3	0.	1	4	2	8	5	7	1	4	...	...
r_4	0.	1	4	1	5	9	2	6	5	...	...
r_5	0.	1	2	1	2	2	1	2	2	...	...
r_6	0.	2	5	0	0	0	0	0	0	...	...
r_7	0.	7	1	8	2	8	1	8	2	...	...
r_8	0.	6	1	8	0	3	3	9	4	...	...
...	....	...	....	....	...	...	...	...	...	...	

proof that [0,1) is uncountable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4	5	6	7	8	9	...
r_1	0.	5	0	0	0	0	0	0	0	...	...
r_2	0.	3	3	3	3	3	3	3	3	...	...
r_3	0.	1	4	2	8	5	7	1	4	...	...
r_4	0.	1	4	1	5	9	2	6	5	...	...
r_5	0.	1	2	1	2	2	1	2	2	...	...
r_6	0.	2	5	0	0	0	0	0	0	...	...
r_7	0.	7	1	8	2	8	1	8	2	...	...
r_8	0.	6	1	8	0	3	3	9	4	...	...
...	....	...	....	....	...	...	...	...	...	...	

proof that [0,1) is uncountable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5	0	0	0						
r_2	0.	3	3	3	3						
r_3	0.	1	4	2	8	5	7	1	4	...	...
r_4	0.	1	4	1	5	9	2	6	5	...	...
r_5	0.	1	2	1	2	2	1	2	2	...	...
r_6	0.	2	5	0	0	0	0	0	0	...	...
r_7	0.	7	1	8	2	8	1	8	2	...	...
r_8	0.	6	1	8	0	3	3	9	4	...	...
...	....	...	....	....	...	...	...	...	...	...	

Flipping rule:

Only if the other driver deserves it.

proof that [0,1) is uncountable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5^{1}	0	0	0						
r_2	0.	3	3^{5}	3	3						
r_3	0.	1	4	2^{5}	8	5	7	1	4	...	...
r_4	0.	1	4	1	5^{1}	9	2	6	5	...	...
r_5	0.	1	2	1	2	2^{5}	1	2	2	...	...
r_6	0.	2	5	0	0	0	0^{5}	0	0	...	...
r_7	0.	7	1	8	2	8	1	8^{5}	2	...	...
r_8	0.	6	1	8	0	3	3	9	4^{5}	...	...
...	....	...	....	....	...	...	...	...	...	...	

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

r_{kK}

$\hat{x}_{kk} = \hat{r}_{kk}$

proof that [0,1) is uncountable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5 1	0	0	0						
r_2	0.	3	3 5	3	3						
r_3	0.	1	4	2 5	8	5	7	1	4	...	...
r_4	0.	1	4	1	5 1	9	2	6	5	...	...
r_5	0.	1	2	1	2	2 5	1	2	2	...	...
r_6	0.	2	5	0	0	0	0 5	0	0	...	...
r_7	0.	7	1	8	2	8	1	8 5	2	...	...

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

If diagonal element is $0.x_{11}x_{22}x_{33}x_{44}x_{55}\cdots$ then let's called the flipped number $0.\hat{x}_{11}\hat{x}_{22}\hat{x}_{33}\hat{x}_{44}\underline{\hat{x}_{55}}\cdots$ **It cannot appear anywhere on the list!**

proof that [0,1) is uncountable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5^{1}	0	0	0						
r_2	0.	3	3^{5}	3	3						
r_3	0.	1	4	2^{5}	8	5	7	1	4	...	...
r_4	0.	1	4	1	5^{1}	9	2	6	5	...	...
						2^{5}	1	2	2	...	...
						0	0^{5}	0	0	...	...
						8	1	8^{5}	2	...	...

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

For every $n \geq 1$:

$r_n \neq 0.\hat{x}_{11}\hat{x}_{22}\hat{x}_{33}\hat{x}_{44}\hat{x}_{55}\cdots$

because the numbers differ on the nth digit!

If diagonal element is $0.x_{11}x_{22}x_{33}x_{44}x_{55}\cdots$ then let's called the flipped number $0.\hat{x}_{11}\hat{x}_{22}\hat{x}_{33}\hat{x}_{44}\hat{x}_{55}\cdots$ **It cannot appear anywhere on the list!**

proof that [0,1) is uncountable

Suppose, for the sake of contradiction, that there is a list of them:

		1	2	3	4						
r_1	0.	5^1	0	0	0						
r_2	0.	3	3^5	3	3						
r_3	0.	1	4	2^5	8	5	7	1	4	...	...
r_4	0.	1	4	1	5^1	9	2	6	5	...	...
						2^5	1	2	2	...	...
						0	0^5	0	0	...	...
						8	1	8^5	2	...	...

Flipping rule:

If digit is 5, make it 1.

If digit is not 5, make it 5.

For every $n \geq 1$:

$$r_n \neq 0.\hat{x}_{11}\hat{x}_{22}\hat{x}_{33}\hat{x}_{44}\hat{x}_{55}\cdots$$

because the numbers differ on the nth digit!

So the list is incomplete, which is a contradiction.

Thus the real numbers between 0 and 1 are **uncountable**.

the set of all functions $f : \mathbb{N} \to \{0, \ldots, 9\}$ is uncountable

We have seen that:

- The set of all (Java) programs is countable
- The set of all functions $f : \mathbb{N} \to \{0, \ldots, 9\}$ is not countable

So: There must be some function $f : \mathbb{N} \to \{0, \ldots, 9\}$ that is not computable by any program!

Interesting… maybe.

Can we come up with an explicit function that is uncomputable?

(Next time)