

BU CS 332 – Theory of Computation

<https://forms.gle/eqKpuJzFDYhWfy7eA>



Lecture 13:

- Countability and Diagonalization
- Undecidability

Reading:

Sipser Ch 4.2

Mark Bun

October 21, 2021

Last Time

Decidable languages (from language theory)

$A_{\text{DFA}} = \{\langle D, w \rangle \mid \text{DFA } D \text{ accepts input } w\}$, etc.

Universal Turing machine

A recognizer for $A_{\text{TM}} = \{\langle M, w \rangle \mid \text{TM } M \text{ accepts input } w\}$

...but not a decider

Today: Some languages, including A_{TM} , are *undecidable*

But first, a math interlude...

Countability and Diagonalization

What's your intuition?

Which of the following sets is the “biggest”?



- a) The natural numbers: $\mathbb{N} = \{1, 2, 3, \dots\}$
- b) The even numbers: $E = \{2, 4, 6, \dots\}$
- c) The positive powers of 2: $POW2 = \{2, 4, 8, 16, \dots\}$
- d) They all have the same size

Set Theory Review

A function $f: A \rightarrow B$ is

- **1-to-1 (injective)** if $f(a) \neq f(a')$ for all $a \neq a'$
- **onto (surjective)** if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$
- **a correspondence (bijective)** if it is 1-to-1 and onto, i.e., every $b \in B$ has a unique $a \in A$ with $f(a) = b$

How can we compare sizes of infinite sets?

Definition: Two sets have **the same size** if there is a bijection between them

A set is **countable** if

- it is a finite set, or
- it has the same size as \mathbb{N} , the set of natural numbers

Examples of countable sets

- \emptyset
- $\{0,1\}$
- $\{0, 1, 2, \dots, 8675309\}$

- $E = \{2, 4, 6, 8, \dots\}$
- $SQUARES = \{1, 4, 9, 16, 25, \dots\}$
- $POW2 = \{2, 4, 8, 16, 32, \dots\}$

$$|E| = |SQUARES| = |POW2| = |\mathbb{N}|$$

How to show that $\mathbb{N} \times \mathbb{N}$ is countable?

(1, 1)	(2, 1)	(3, 1)	(4, 1)	(5, 1)	...
(1, 2)	(2, 2)	(3, 2)	(4, 2)	(5, 2)	...
(1, 3)	(2, 3)	(3, 3)	(4, 3)	(5, 3)	...
(1, 4)	(2, 4)	(3, 4)	(4, 4)	(5, 4)	...
(1, 5)	(2, 5)	(3, 5)	(4, 5)	(5, 5)	...

How to argue that a set S is countable

- Describe how to “list” the elements of S , usually in stages:

Ex: Stage 1) List all pairs (x, y) such that $x + y = 2$

Stage 2) List all pairs (x, y) such that $x + y = 3$

...

Stage n) List all pairs (x, y) such that $x + y = n + 1$

...

- Explain why every element of S appears in the list

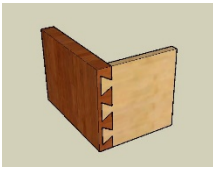
Ex: Any $(x, y) \in \mathbb{N} \times \mathbb{N}$ will be listed in stage $x + y - 1$

- Define the bijection $f: \mathbb{N} \rightarrow S$ by $f(n) =$ the n 'th element in this list (ignoring duplicates if needed)

More examples of countable sets

- $\{0,1\}^*$
 - $\{\langle M \rangle \mid M \text{ is a Turing machine}\}$
 - $\mathbb{Q} = \{\text{rational numbers}\}$
-
- If $A \subseteq B$ and B is countable, then A is countable
 - If A and B are countable, then $A \times B$ is countable

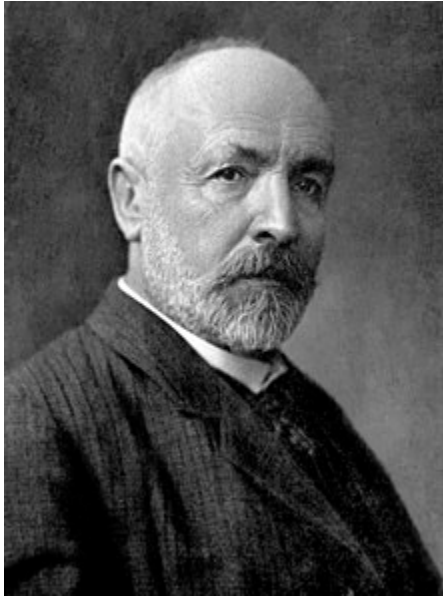
Another version of the dovetailing trick



Ex: Show that $\mathcal{F} = \{L \subseteq \{0, 1\}^* \mid L \text{ is finite}\}$ is countable

So what *isn't* countable?

Cantor's Diagonalization Method



Georg Cantor 1845-1918

- Invented set theory
- Defined countability, uncountability, cardinal and ordinal numbers, ...

Some praise for his work:

“Scientific charlatan...renegade...corruptor of youth”
–L. Kronecker

“Set theory is wrong...utter nonsense...laughable”
–L. Wittgenstein

Uncountability of the reals

Theorem: The real interval $[0, 1]$ is uncountable.

Proof: Assume for the sake of contradiction it were countable, and let $f: \mathbb{N} \rightarrow [0,1]$ be a bijection

n	$f(n)$
1	$0 . d_1^1 d_2^1 d_3^1 d_4^1 d_5^1 \dots$
2	$0 . d_1^2 d_2^2 d_3^2 d_4^2 d_5^2 \dots$
3	$0 . d_1^3 d_2^3 d_3^3 d_4^3 d_5^3 \dots$
4	$0 . d_1^4 d_2^4 d_3^4 d_4^4 d_5^4 \dots$
5	$0 . d_1^5 d_2^5 d_3^5 d_4^5 d_5^5 \dots$

Construct $b \in [0,1]$ which does not appear in this table
– contradiction!

$b = 0 . b_1 b_2 b_3 \dots$ where $b_i \neq d_i^i$ (digit i of $f(i)$)

Uncountability of the reals

A concrete example of the contradiction construction:

n	$f(n)$
1	0.8675309 ...
2	0.1415926 ...
3	0.7182818 ...
4	0.4444444 ...
5	0.1337133 ...

Construct $b \in [0,1]$ which does not appear in this table
– contradiction!

$b = 0.b_1b_2b_3\dots$ where $b_i \neq d_i^i$ (digit i of $f(i)$)

Diagonalization

This process of constructing a counterexample by “contradicting the diagonal” is called **diagonalization**

Structure of a diagonalization proof

Say you want to show that a set T is uncountable

- 1) Assume, for the sake of contradiction, that T is countable with bijection $f: \mathbb{N} \rightarrow T$
- 2) “Flip the diagonal” to construct an element $b \in T$ such that $f(n) \neq b$ for every n

Ex: Let $b = 0.b_1b_2b_3\dots$ where $b_n \neq d_n^n$
(where d_n^n is digit n of $f(n)$)

- 3) Conclude that f is not onto, contradicting assumption that f is a bijection

A general theorem about set sizes

Theorem: Let X be any set. Then the power set $P(X)$ does **not** have the same size as X .

Proof: Assume for the sake of contradiction that there is a bijection $f: X \rightarrow P(X)$

Goal: Construct a set $S \in P(X)$ (meaning, $S \subseteq X$) that cannot be the output $f(x)$ for any $x \in X$

Diagonalization argument

Assume a correspondence $f: X \rightarrow P(X)$

x					
x_1					
x_2					
x_3					
x_4					
\vdots					

Diagonalization argument

Assume a correspondence $f: X \rightarrow P(X)$

x	$x_1 \in f(x)?$	$x_2 \in f(x)?$	$x_3 \in f(x)?$	$x_4 \in f(x)?$...
x_1	Y	N	Y	Y	
x_2	N	N	Y	Y	
x_3	Y	Y	Y	N	
x_4	N	N	Y	N	
\vdots					\ddots

Define S by flipping the diagonal:

$$\text{Put } x_i \in S \iff x_i \notin f(x_i)$$

Example

Let $X = \{1, 2, 3\}$, $P(X) = \{\emptyset, \{1\}, \{2\}, \{1,2\}, \{2,3\}, \{1,2,3\}\}$

Ex. $f(1) = \{1, 2\}$, $f(2) = \emptyset$, $f(3) = \{2\}$

x	$1 \in f(x)?$	$2 \in f(x)?$	$3 \in f(x)?$
1			
2			
3			

Construct $S =$

A general theorem about set sizes

Theorem: Let X be any set. Then the power set $P(X)$ does **not** have the same size as X .

Proof: Assume for the sake of contradiction that there is a bijection $f: X \rightarrow P(X)$

Construct a set $S \in P(X)$ that cannot be the output $f(x)$ for any $x \in X$:

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

If $S = f(y)$ for some $y \in X$,

then $y \in S$ if and only if $y \notin S$

Undecidable Languages

Undecidability / Unrecognizability

Definition: A language L is undecidable if there is no TM deciding L

Definition: A language L is unrecognizable if there is no TM recognizing L

An existential proof

Theorem: There exists an undecidable language over $\{0, 1\}$

Proof:

Set of all encodings of TM deciders: $X \subseteq \{0, 1\}^*$

Set of all languages over $\{0, 1\}$: $P(\{0, 1\}^*)$

There are more languages than there are TM deciders!

⇒ There must be an undecidable language

An existential proof

Theorem: There exists an **unrecognizable** language over $\{0, 1\}$

Proof:

Set of all encodings of **TMs**: $X \subseteq \{0, 1\}^*$

Set of all languages over $\{0, 1\}$: $P(\{0, 1\}^*)$

There are more languages than there are TM **recognizers!**

\Rightarrow There must be an **unrecognizable** language

“Almost all” languages are undecidable



But how do we actually find one?