BU CS 332 – Theory of Computation

https://forms.gle/KujctosE3s84KLHX8

Lecture 14:

- Countability
- Uncountability / diagonalization
- Undecidable languages

Reading:

Sipser Ch 4.2

HW 6 deadline =

Friday 11:59 PM

Mark Bun

October 27, 2022

Last Time

Universal Turing machine

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

…but not a decider

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

But first, a math interlude…

Countability and Diagonalization

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

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

Finite

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

Countably infinite

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

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

numerator / denominator

$f(1)=$ $(1,1)$	$f(3)=$ $(2,1)$	$f(6)=$ $(3,1)$	$(4,1)$	$(5,1)$	…
$f(2)=$ $(1,2)$	$f(5)=$ $(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	…
$f(4)=$ $(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	…
$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	…
$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	

⋱

Construct a bijection $f: \mathbb{N} \to \mathbb{N} \times \mathbb{N}$

How to argue that a set S is countable

E.g. $S = \mathbb{N} \times \mathbb{N}$

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

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

$f(1) = (1,1)$

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

$f(2) = (1,2)$ $f(3) = (2,1)$

…

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

$(1, n)$ $(2, n-1)$ $(3, n-2)$, … $(n, 1)$

…

- 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

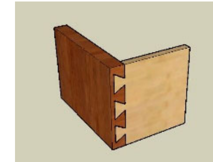
- $\{0,1\}^* = \{\overbrace{\epsilon}^{\text{stage 0}}, \overbrace{0, 1}^{\text{stage 1}}, \overbrace{00, 01, 10, 11}^{\text{stage 2}}, \ldots\}$
- $\{\langle M \rangle \mid M \text{ is a Turing machine}\}$ Choose encoding $\langle \cdot \rangle$ s.t. $\langle M \rangle \in \{0,1\}^*$ for every M
- $\mathbb{Q} = \{\text{rational numbers}\}$

  Same proof as $\mathbb{N} \times \mathbb{N}$ countable

- If $A \subseteq B$ and B is countable, then A is countable
- If A and B are countable, then $\underline{A \times B}$ is countable

- S is countable if and only if there exists a surjection (an onto function) $f : \mathbb{N} \to S$

Another version of the dovetailing trick



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

$L \subseteq \{0,1\}^*$ is finite if it has a finite # of elements

$\{0, 11, 100\}$ is finite $\{0^n \mid n \geq 0\}$ is not finite

$\mathcal{F} = \{\emptyset, \{\varepsilon\}, \{0\}, \{1\}, \dots\}$

Proof 1 Define a function $C : \{0,1,\#\}^* \to \mathcal{F}$

$C(x_1 \# x_2 \# \dots \# x_n) = \{x_1, \dots, x_n\}$

$\exists$ a bijection $f : \mathbb{N} \to \{0,1,\#\}^*$

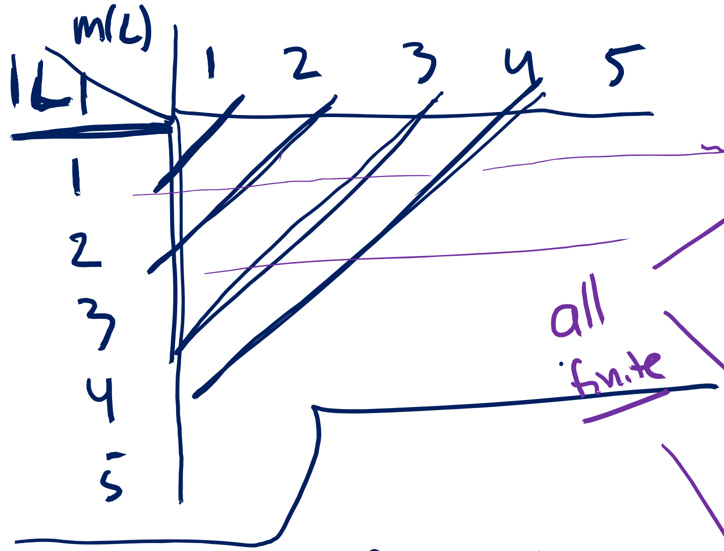
C is a surjection (onto) $\Rightarrow$ $(C \circ f)(n) = C(f(n))$ is a surjection from $\mathbb{N} \to \mathcal{F}$.

Proof 2) • $|L|$ = # of elements in L

e.g. $|\{\epsilon, 0, 01111\}| = 3$

• $m(L)$ = max length of a string in L

e.g. $m(\{\epsilon, 0, 01111\}) = 5$



Stage 1: List all sets L s.t. $|L| \le 1$ and $m(L) \le 1$

Stage 2: List all sets L s.t. $|L| \le 2$ and $m(L) \le 2$

⋮

Stage n: List all L s.t. $|L| \le n$ and $m(L) \le n$

Claim: every finite language L appears in this list

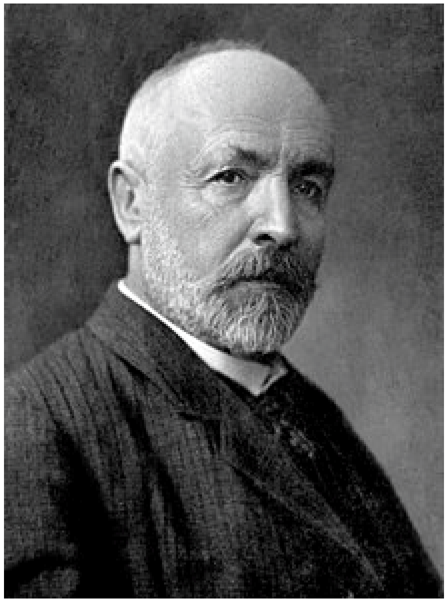
let $k = \max\{|L|, m(L)\}$

Then L appears in stage k

$f(i)$ = i'th thing enumerated in this list.

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 $f: \mathbb{N} \to [0,1]$ be a bijection

n	$f(n)$
1	$0.\boxed{d_1^1}\, d_2^1\, d_3^1\, d_4^1\, d_5^1 \ldots$
2	$0.d_1^2\, \boxed{d_2^2}\, d_3^2\, d_4^2\, d_5^2 \ldots$
3	$0.d_1^3\, d_2^3\, \boxed{d_3^3}\, d_4^3\, d_5^3 \ldots$
4	$0.d_1^4\, d_2^4\, d_3^4\, \boxed{d_4^4}\, d_5^4 \ldots$
5	$0.d_1^5\, d_2^5\, d_3^5\, d_4^5\, \boxed{d_5^5} \ldots$

decimal expansion of $f(n)$

d_i^n = i'th digit of $f(n)$

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

$b = 0.b_1 b_2 b_3 \ldots$ where $b_n \neq d_n^n$ (digit n of $f(n)$)

Uncountability of the reals

A concrete example of the contradiction construction:

n	$f(n)$
1	$b \neq f(1)$ $0.\boxed{8}675309\ldots$ $b = 0.95952\ldots$
2	$b \neq f(2)$ $0.1\boxed{4}15926\ldots$
3	$b \neq f(3)$ $0.71\boxed{8}2818\ldots$
4	$0.444\boxed{4}444\ldots$
5	$0.1337\boxed{1}33\ldots$

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

$b = 0.b_1 b_2 b_3 \ldots$ where $b_n \neq d_n^n$ (digit n of $f(n)$)

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 $b = 0.b_1b_2b_3\ldots$ where $b_n \neq d_n^n$
(where d_n^n is digit n of $f(n)$)

3) Conclude that f is not onto, which contradicts our 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.

$\{S \mid S \subseteq X\}$

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

<u>What should we do?</u>

a) Show that for every $S \in P(X)$, there exists $x \in X$ such that $f(x) = S$

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

c) Construct a set $S \in P(X)$ and two distinct $x, x' \in X$ such that $f(x) = f(x') = S$

Diagonalization argument

Assume a bijection $f: X \to P(X)$

x					
x_1					
x_2					
x_3					
x_4					
$\vdots$					

Diagonalization argument

Assume a bijection $f: X \to P(X)$

Is $x_1 \in f(x_1)$? Is $x_2 \in f(x_1)$?

x	$x_1 \in f(x)$?	$x_2 \in f(x)$?	$x_3 \in f(x)$?	$x_4 \in f(x)$?	…
x_1	$\boxed{\text{Y}}$	N	Y	Y	
x_2	N	$\boxed{\text{N}}$	Y	Y	
x_3	Y	Y	Y	N	
x_4	N	N	Y	N	
$\vdots$					$\ddots$

Define S by flipping the diagonal:

Put $\quad x_i \in S \quad \Leftrightarrow \quad x_i \notin f(x_i)$

$x_1 \in f(x_1) \to x_1 \notin S$

$x_2 \notin f(x_2) \to x_2 \in S$

…

Example

Let $X = \{1, 2, 3\}$, $P(X) = \{\emptyset, \{1\}, \{2\}, \{1,2\}, \{2,3\}, \{1,2,3\}\}$ {3} {1, 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	$\boxed{\text{Y} \quad \text{N}}$	Y	N
2	N	$\boxed{\text{N} \quad \text{Y}}$	N
3	N	Y	$\boxed{\text{N} \quad \text{Y}}$

Construct $S = \{2, 3\}$

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 $f: X \to P(X)$

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 $y \notin S$ $\ast$ $\Rightarrow S \neq f(y)$ for any y

$\Rightarrow f$ not a bijection

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 $\{0,1\}$:

a) $\{0,1\}$ $= \{L \mid L \subseteq \{0,1\}^*\}$

b) $\{0,1\}^*$

c) $P(\{0,1\}^*)$: The set of all subsets of $\{0,1\}^*$

d) $P(P(\{0,1\}^*))$: The set of all subsets of the set of all subsets of $\{0,1\}^*$

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!

$\Rightarrow$ 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?