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.

Emptiness testing E_{DFA}, Equality testing EQ_{DFA}

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 Diagonalizaiton

What's your intuition?

Which of the following sets is the "biggest"?

a) The natural numbers: $\mathbb{N} = \{1, 2, 3, \ldots\}$

b) The even numbers: $E = \{2, 4, 6, \ldots\}$

c) The positive powers of 2: $POW2 = \{2, 4, 8, 16, \ldots\}$

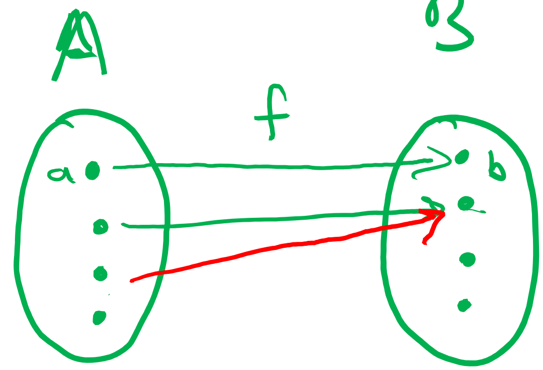
d) They all have the same size

Set Theory Review

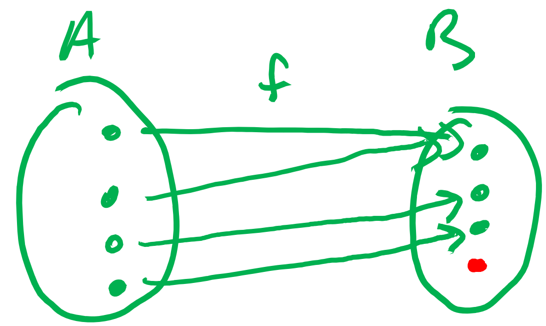
— = not allowed

A function $f: A \to B$ is

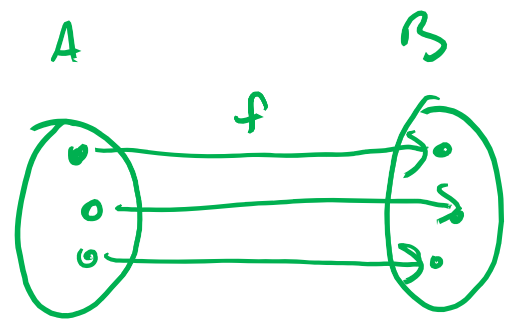
- 1-to-1 (injective) if $f(a) \neq f(a')$ for all $a \neq a'$



- 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 has the same size as B if $\exists$ bijection $f: A \to B$

A set is countable if

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

"countably infinite"

Examples of countable sets

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

finite $\Rightarrow$ countable

all "countably infinite"

- $E = \{2, 4, 6, 8, \ldots\}$ $f: \mathbb{N} \to E$ $f(i) = 2i$
- $SQUARES = \{1, 4, 9, 16, 25, \ldots\}$ $f(i) = i^2$
- $POW2 = \{2, 4, 8, 16, 32, \ldots\}$ $f(i) = 2^i$

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

$= \{(x,y) \mid x, y \in \mathbb{N}\}$

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

$\boxed{1}$ $(1,1)$	$\boxed{2}$ $(2,1)$	$\boxed{4}$ $(3,1)$	$\boxed{7}$ $(4,1)$	$(5,1)$	…
$\boxed{3}$ $(1,2)$	$\boxed{5}$ $(2,2)$	$\boxed{8}$ $(3,2)$	$(4,2)$	$(5,2)$	…
$\boxed{6}$ $(1,3)$	$\boxed{9}$ $(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	…
$\boxed{10}$ $(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	…
$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$\ddots$

stage 1

stage 2

stage 3

$f(i) =$ ith pair enumerated in above sequence

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 $x + y = 2$

(1,1)

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

(1,2) , (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 $x + y - 1$

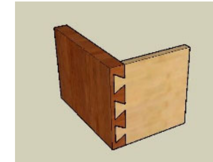
- Define the bijection $f: \mathbb{N} \to S$ by $f(n) =$ the n'th element in this list (ignoring duplicates if needed)

More examples of countable sets

- $\{0,1\}^*$ $\{\epsilon, 0, 1, 00, 01, 10, 11, \ldots\}$
- $\{\langle M \rangle \mid M$ is a Turing machine$\}$ same as above, because $\langle M \rangle$ is just a string
- $\mathbb{Q} = \{$rational numbers$\}$
  Same as $\mathbb{N} \times \mathbb{N}$

- 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



$|L| = 3, \; m(L) = 4$

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

Ex: $L = \{0, 00, 0100\}$ Not finite: $\{0^n \mid n \geq 0\}$

Proof 1: $L = \{x_1, \ldots, x_k\}$ (each $x_i \in \{0,1\}^*$)

Define $E(L) = x_1 \# x_2 \# \ldots \# x_k$

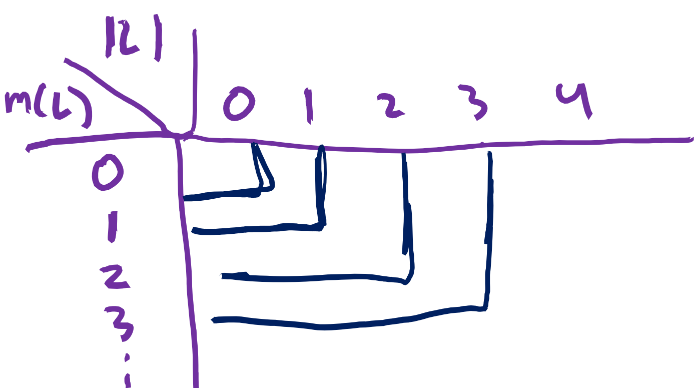
countable

$$\left|\{L \mid L \text{ finite}\}\right| \leq \left|\{E(L) \mid L \text{ finite}\}\right| \leq \left|\{0,1,\#\}^*\right|$$

Proof 2: $|L|$ = number of strings in L

$m(L)$ = length of longest string in L

$f(i)$ = ith new language appearing in list



Stage 0: List all L s.t. $|L| = 0$, $m(L) = 0$

$\boxed{1}$ $\emptyset$

Stage 1: List all L s.t. $|L| \leq 1$, $m(L) \leq 1$

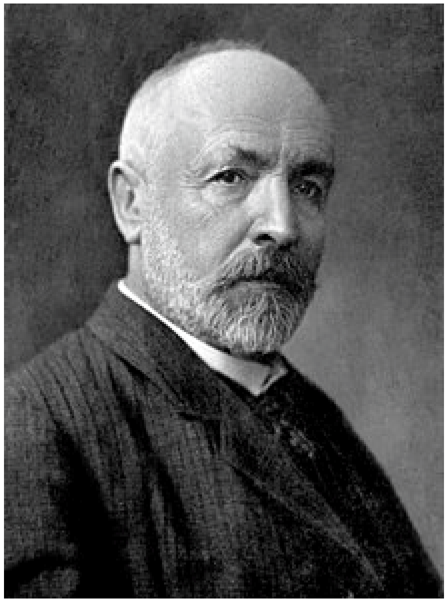
$\emptyset, \{\varepsilon\}, \{0\}, \{1\}$

2 3 4

Stage n: List all L s.t. $|L| \leq n$, $m(L) \leq n$

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	$0.d_1^3\, d_2^3\, d_3^3\, d_4^3\, d_5^3 \ldots$
4	$0.d_1^4\, d_2^4\, d_3^4\, d_4^4\, d_5^4 \ldots$
5	$0.d_1^5\, d_2^5\, d_3^5\, d_4^5\, d_5^5 \ldots$

d_i^n = ith digit of decimal expansion of $f(n)$

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

$b \neq f(i) \;\; \forall i$

$\Rightarrow$ b. does not appear in list

$b = 0.b_1 b_2 b_3 \ldots$ where $b_i \neq d_i^i$ (digit i of $f(i)$) $\Rightarrow$ f is not onto $\times$.

Uncountability of the reals

A concrete example of the contradiction construction:

n	$f(n)$	
1	$0.\boxed{8}6753 09\ldots$	$b_1 \neq d_1^1$ (e.g. $b_1 = 9$)
2	$0.1\boxed{4}15926\ldots$	$b_2 \neq d_2^2$ (e.g. $b_2 = 5$)
3	$0.71\boxed{8}2818\ldots$	$b_3 = 9$
4	$0.444\boxed{4}444\ldots$	$b_4 = 5$
5	$0.1337\boxed{1}33\ldots$	$b_5 = 2$

Construct $b \in [0,1]$ which does not appear in this table – contradiction! $b = 0.95952$

$b = 0.b_1 b_2 b_3 \ldots$ 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 $f: \mathbb{N} \to T$
2) "Flip the diagonal" to construct an element $b \in T$ such that $f(n) \neq b$ for every n

Ex: Let $b = 0.b_1 b_2 b_3 \ldots$ where $b_n \neq d_n^n$

(where d_n^n is digit n of $f(n)$)

3) Conclude that f is not onto, 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. $= \{S \mid S \subseteq X\}$

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

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 $f: X \to P(X)$

x					
x_1					
x_2					
x_3					
x_4					
$\vdots$					

Diagonalization argument

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

	x_1	x_2	x_3	x_4	
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	N	Y	Y	
x_2	N	$\boxed{\text{N}}$ Y	Y	Y	
x_3	Y	Y	Y	N	
x_4	N	N	Y	N	
$\vdots$					$\ddots$

Define S by flipping the diagonal:

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	$\boxed{Y}$ N	Y	N
2	N	$\boxed{N}$ Y	N
3	N	Y	$\boxed{N}$ Y

"Is $x \in f(x)$?"

Construct $S = \{2, 3\}$
$= \{x \in X \mid x \notin f(x)\}$

$S \neq f(1)$
$S \neq f(2)$
$S \neq f(3)$
$\Rightarrow f$ not onto

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 $y \notin S$ $\times$

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) $\{0,1\}$

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

$L \subseteq \{0,1\}^*$

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

Proof:

$|\text{decidable languages}| \leq |X|$

$\Rightarrow$ decidable languages are countable

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

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

$= \{L \mid L \subseteq \{0,1\}^*\} = P(\{0,1\}^*)$ is bigger than $\{0,1\}^*$

There are more languages than there are TM deciders!

$\Rightarrow$ There must be an undecidable language $\Rightarrow P(\{0,1\}^*)$ not countable

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?