BU CS 332 – Theory of Computation

https://forms.gle/7CAfuvEFAgwgbnYT6

Lecture 13:

- Countability
- Diagonalization
- Undecidability?

Reading:

Sipser Ch 4.1, 4.2

Mark Bun

March 18, 2024

Last Time

Church-Turing Thesis

v1: The basic TM (and all equivalent models) capture our intuitive notion of algorithms

v2: Any physically realizable model of computation can be simulated by the basic TM

Decidable languages (from language theory)

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

Encoding of D, w

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: $\mathbb{N} = \{1, 2, 3, \dots\}$

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

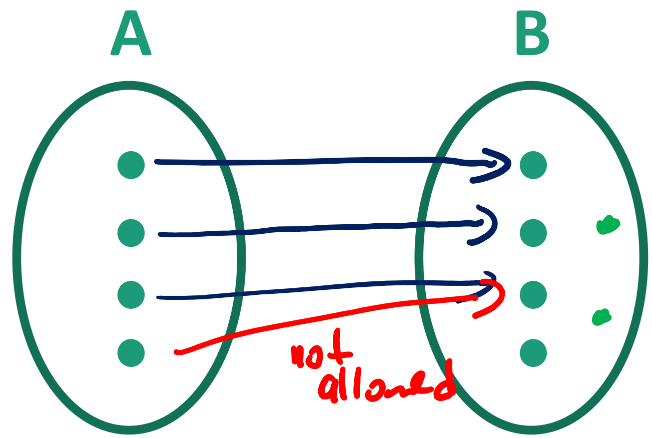
c) The positive powers of 2: $POW2 = \{2, 4, 8, 16, \dots\}$

d) They all have the same size

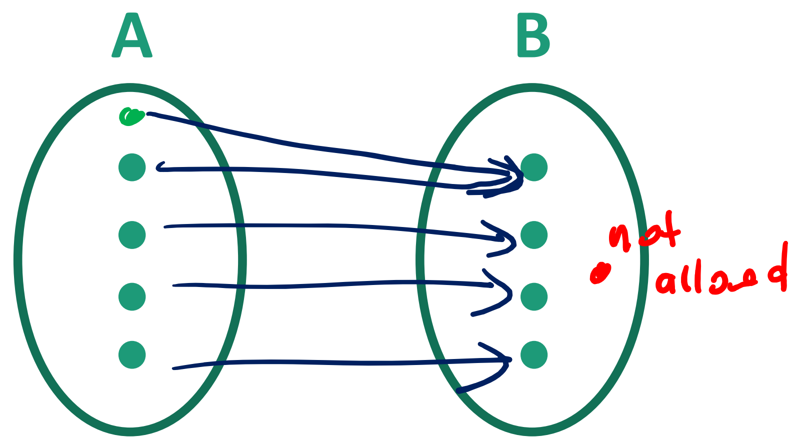
Set Theory Review

A function $f: A \rightarrow B$ is

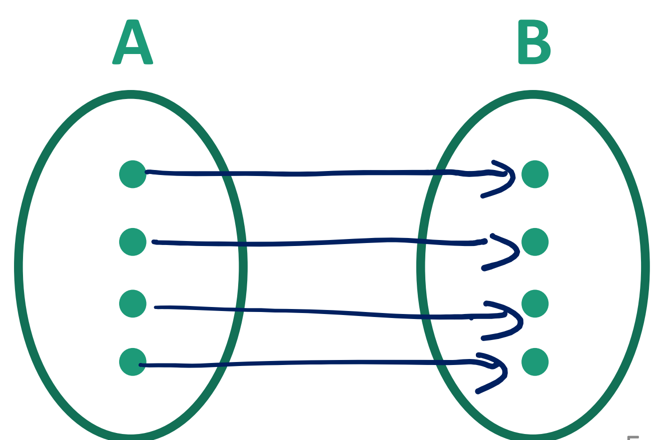
- 1-to-1 (injective) if $f(a) \neq f(a')$ for all $a \neq a'$



- 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 either

- 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

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

finite

natural numbers

$f: \mathbb{N} \to E$ $f(x) = 2x$

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

countably infinite

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

Goal: Construct bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N} = \{ (x,y) \mid x \in \mathbb{N}, y \in \mathbb{N} \}$

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

$f(1) =$ $f(2) =$ $f(4) =$

$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	…
$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	…
$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	…
$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	…
$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	
					⋱

$f(3) =$ $f(5) =$ $f(6) =$

$f(i) = i$'th element enumerated

How to argue that a set S is countable

$S = \mathbb{N} \times \mathbb{N}$

- Describe how to "list" the elements of S, usually in stages: where each stage is finite

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 $x + y = 3$

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

…

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

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

…

- 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

Stage 0: List ε
Stage 1: List all strings of length 1
0, 1
⋮
Stage n: List all strings of length n

- $\{0,1\}^*$ {ε, 0, 1, 00, 01, ...}
- $\{\langle M \rangle \mid M \text{ is a Turing machine}\}$

our input alphabet {0,1}

WLOG, $\langle M \rangle \in \{0,1\}^*$ for every M
$\Rightarrow \{\langle M \rangle \mid M \text{ is a TM}\} \subseteq \{0,1\}^*$

- $\mathbb{Q} = \{\text{rational numbers}\}$

Basically use the proof $\mathbb{N} \times \mathbb{N}$ countable
Interpret (x, y) as $\frac{x}{y}$

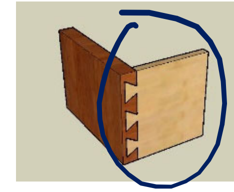
$\frac{1}{2} = \frac{2}{4}$

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

(nonempty) (countably infinite or finite

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

Another version of the dovetailing trick



|L|=3
m(L)=2

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

$L = \{0, 1, 01\}$ is finite $\qquad L' = \{0^n \mid n \geq 0\}$ is not finite

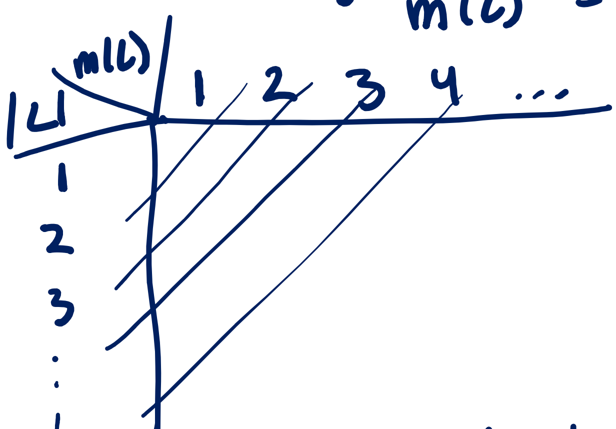
$\mathcal{F} = \{\phi, \{\varepsilon\}, \{0\}, \{1\}, \{\varepsilon, 0\}, \ldots\}$

Solution 1)
- Every finite language is decidable by some TM
- Set of all TMs is countable

$\Rightarrow$ Set of all finite languages is a subset of a countable set, hence countable

Solution 2) Define for every finite language L:
- $|L|$ = # of elements in L
- $m(L)$ = length of longest string in L

both finite for finite languages



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

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

⋮

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

Bijection $f(i)$ = ith distinct language in this enumeration

List of finite languages		i
$\emptyset$	$\xleftarrow{f(1)}$	1
$\{\varepsilon\}$	$\xleftarrow{f(2)}$	2
$\{0\}$	⋮	3
$\{1\}$	⋮	4
$\{\varepsilon, 0\}$	⋮	5
$\{\varepsilon, 1\}$	⋮	6
⋮		

$\emptyset \quad \{\varepsilon\} \quad \{0\} \quad \{1\} \quad \{00\} \quad \{01\} \quad \{10\} \quad \{11\} \quad \ldots$

Doesn't quite work:

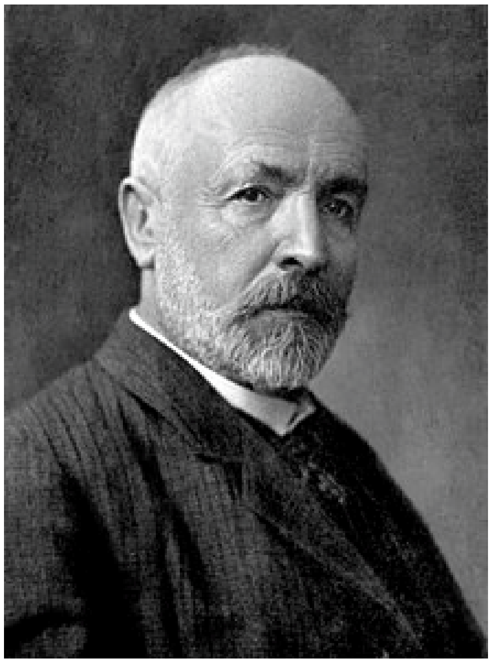
Stage 1: List all languages consisting of ≤ 1 elt

Stage 2: " ≤ 2 elts.

⋮

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 surjection

n	Ex 1	$b_1 \neq d_1^1$ $f(n)$	
1	0.$\boxed{2}$71828...	$0\,.\,\boxed{d_1^1}\, d_2^1\; d_3^1\; d_4^1\; d_5^1\; \ldots$	Decimal expansion of f(1)
2	0.3$\boxed{1}$4159	$0\,.\,d_1^2\; \boxed{d_2^2}\, d_3^2\; d_4^2\; d_5^2\; \ldots$	" of f(2)
3	0.86$\boxed{7}$530	$0\,.\,d_1^3\; d_2^3\; \boxed{d_3^3}\, d_4^3\; d_5^3\; \ldots$ $b_2 \neq d_2^2$	
4	⋮	$0\,.\,d_1^4\; d_2^4\; d_3^4\; \boxed{d_4^4}\, d_5^4\; \ldots$	
5		$0\,.\,d_1^5\; d_2^5\; d_3^5\; d_4^5\; \boxed{d_5^5}\, \ldots$	

b=0.328...

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

$b = 0.\underline{b_1 b_2 b_3}\ldots$ 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 surjection $f: \mathbb{N} \to T$

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 (by contradiction) that f is not a surjection

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 surjection $f: X \to P(X)$

(violating surjectivity $\Rightarrow$ violation of bijectivity)

<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 $x \in X$ violate surjectivity of f.

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 surjection $f: X \to P(X)$

X

x					
x_1					
x_2					
x_3					
x_4					
$\vdots$					

Diagonalization argument

Row corresponds to $f(x_1)$ which is some subset of X

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

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	~~Y~~ N	N	Y	Y	
x_2	N	~~N~~ Y	Y	Y	
x_3	Y	Y	~~Y~~ N	N	
x_4	N	N	Y	N	
⋮					⋱

$x_1 \notin S$ $x_2 \in S$ $x_3 \notin S$

Define S by flipping the diagonal:

Put $x_i \in S \iff x_i \notin f(x_i)$

Example

$, \{1,3\}$

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	~~Y~~ N	Y	N
2	N	~~N~~ Y	N
3	N	Y	~~N~~ Y

depends on

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

$S \subseteq X$, $S \in P(X)$

$\left.\begin{array}{l} S \neq f(1) \\ S \neq f(2) \\ S \neq f(3) \end{array}\right\} \Rightarrow$ S is not in the image of f

contradicts assertion that f is a surjection

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 surjection $f: X \to P(X)$

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 $y \notin S$