BU CS 332 – Theory of Computation

Lecture 14:

- More on decidability
- Countable and uncountable sets

Reading:

Sipser Ch 4.2

- HW 5 delayed until 3/25 2 PM
- You may drop 2 lowest HW assignments

Mark Bun

March 18, 2020

Last Time

Machine model $\mathcal{C}$

$A_{\mathcal{C}} = \{\langle M, w\rangle \mid M$ is a machine of type $\mathcal{C}$ and M accepts $w\}$

$E_{\mathcal{C}} = \{\langle M\rangle \mid M$ is a machine of type $\mathcal{C}$ recognizing the empty language $\emptyset\}$

(Not the same as testing $L(M) = \{\varepsilon\}$)

$EQ_{\mathcal{C}} = \{\langle M_1, M_2\rangle \mid M_1, M_2$ are machines of type $\mathcal{C}$ and $L(M_1) = L(M_2)\}$

	$\mathcal{C}$ = DFA	$\mathcal{C}$ = CFG
	A_{DFA} decidable	A_{CFG} decidable
	E_{DFA} decidable	E_{CFG} decidable
	EQ_{DFA} decidable	

A_{NFA}
A_{REX}
A_{PDA}
A_{TM}

One more decidable language (Sipser 4.10)

Theorem: $INFINITE_{\text{DFA}} =$
$\{\langle D \rangle \mid D$ is a DFA that accepts infinitely many strings$\}$
is decidable

D is a DFA recognizing $\{0, 1, 10\}$ $\Rightarrow$ $\langle D \rangle \notin INFINITE_{DFA}$
D is a DFA recognizing $L(0^*1^*)$ $\Rightarrow$ $\langle D \rangle \in INFINITE_{DFA}$

Lemma: Let D be a DFA with n states. Then D accepts infinitely many strings if and only if D accepts some string of length $\geq n$.

$\Rightarrow$ D accepts inf. many strings $\Rightarrow$ D has to accept some string of length $\geq n$

why? contradiction: If D only accepts strings of length $< n$, then D accepts only finitely many strings $\times$

$\Leftarrow$ D accepts some string w of length $\geq n$

Pumping Lemma: Can write $w = xyz$, y nonempty and $xy^iz \in L(D)$ for every $i = 0, 1, 2, \ldots$

$\{xy^iz \mid i \geq 0\}$ is an infinite subset of $L(D)$ $\Rightarrow$ $L(D)$ is infinite

One more decidable language (Sipser 4.10)

Theorem: $INFINITE_{\text{DFA}} = \{\langle D \rangle \mid D \text{ is a DFA that accepts infinitely many strings}\}$ is decidable

Proof: The following TM decides $INFINITE_{\text{DFA}}$:

On input $\langle D \rangle$, where D is a DFA with n states:

1. Let A be a DFA recognizing all strings of length $\geq n$
2. Let B be a DFA recognizing $L(A) \cap L(D)$ using cross-product construction
3. Run the decider for E_{DFA} on input $\langle B \rangle$. Accept if it *rejects*, and reject if it *accepts*.

$L(B) = L(A) \cap L(D) = \phi \iff D$ does <u>not</u> accept any string of length $\geq n$

$L(B) = L(A) \cap L(D) \neq \phi \iff \exists$ a string of length $\geq n$ that D accepts

$\iff D$ recognizes an infinite language (by Lemma)

Problems in Language Theory

$A_{TM} = \{\langle M, w\rangle \mid M$ is a TM accepting input $w\}$

A_{DFA} decidable	A_{CFG} decidable	A_{TM} ?
E_{DFA} decidable	E_{CFG} decidable	E_{TM} ?
EQ_{DFA} decidable	EQ_{CFG} ?	EQ_{TM} ?

Infinite DFA decidable

Undecidability

These natural computational questions about computational models are **undecidable**

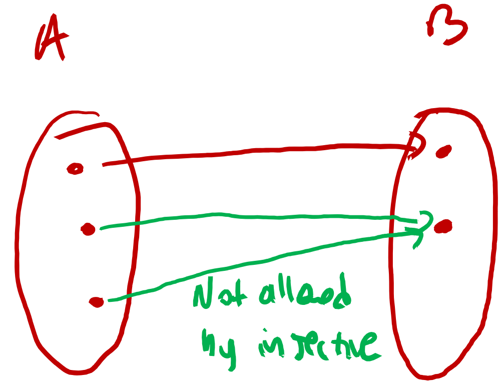
I.e., computers cannot solve these problems no matter how much time they are given

Countability and Diagonalizaiton

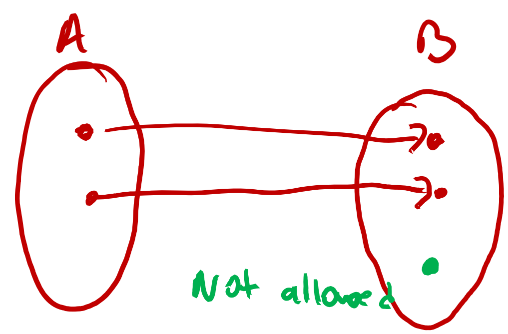
Set Theory Review

A function $f: A \to B$ is

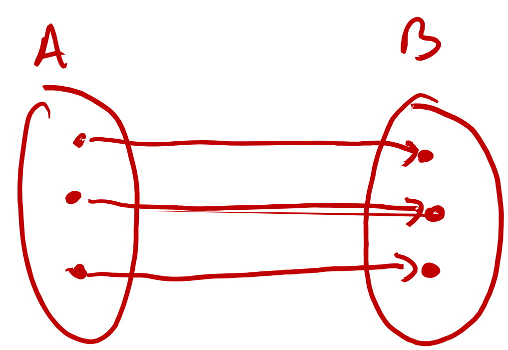
- 1-to-1 (injective) if $f(a) \neq f(a')$ for all $a \neq a'$



- 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

(correspondence)

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 sets are countable

Bijection $f: \mathbb{N} \to E$

- $E = \{2, 4, 6, 8, \ldots\}$ $f(x) = 2x$ $f(1)=2,\ f(2)=4,\ f(3)=6, \ldots$
- $SQUARES = \{1, 4, 9, 16, 25, \ldots\}$ $f(x) = x^2$
- $POW2 = \{1, 2, 4, 8, 16, 32, \ldots\}$ $f(x) = 2^x$

Countably infinite

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

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

$f(1)=$ $(1,1)$	$f(2)=$ $(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	...
$f(3)=$ $(1,2)$	$f(5)=$ $(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	...
$f(4)=$ $(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	...
$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	...
$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	
					$\ddots$

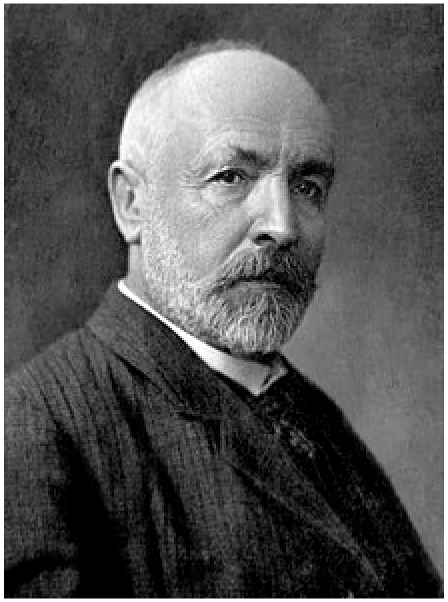
Define a bijection $f: \mathbb{N} \to \mathbb{N} \times \mathbb{N}$

More examples of countable sets

- $\{0,1\}^*$
- $\{\langle M \rangle \mid M \text{ is a Turing machine}\}$ $\subseteq \{0,1\}^*$
- $\mathbb{Q} = \{\text{rational numbers}\}$

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

Sylvester Medal, Royal Society, 1904

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 correspondence

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	$0\,.\,d_1^5\;d_2^5\;d_3^5\;d_4^5\boxed{d_5^5}\ldots$

$f(1) = 0.7359205..$

d_m^n = mth digit of $f(n)$

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

violates $f: \mathbb{N} \to (0,1)$ being onto

$b = 0.d_1 d_2 d_3 \ldots$ where $d_i \neq$ digit i of $f(i)$

$d_1 \neq d_1^1,\; d_2 \neq d_2^2, \ldots$

Uncountability of the reals

A concrete example:

$b = 0.959952$ $\in (0,1)$

n	$f(n)$
1	$0.\boxed{8}6753 09\ldots$
2	$0.1\boxed{4}15926\ldots$
3	$0.71\boxed{8}2818\ldots$
4	$0.444\boxed{4}444\ldots$
5	$0.1337\boxed{1}33\ldots$

b differs from f(1) in position 1
$\Rightarrow b \neq f(1)$
b differs from f(2) in pos. 2
$\Rightarrow b \neq f(2)$

b cannot be f(n) for any n

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

$b = 0.d_1d_2d_3\ldots$ where $d_i \neq$ digit i of $f(i)$

Diagonalization

This process of constructing a counterexample by "contradicting the diagonal" is called diagonalization

What if we try to do this with the rationals?

What happens if we try to use this argument to show that $\mathbb{Q} \cap (0,1)$ [rational numbers in $(0,1)$] is uncountable?

Let $f: \mathbb{N} \rightarrow \mathbb{Q} \cap (0,1)$ be a correspondence

$b = 0.95952\ldots$

might not be rational

n	$f(n)$
1	0 . 8 6 7 8 6 7 8 ...
2	0 . 1 4 1 4 1 4 1 ...
3	0 . 7 1 8 2 7 1 8 ...
4	0 . 4 4 4 4 4 4 4 ...
5	0 . 1 3 3 7 1 3 3 ...

Construct $b \in (0,1)$ which does not appear in this table

$b = 0.d_1 d_2 d_3 \ldots$ where $d_i \neq$ digit i of $f(i)$

A general theorem about set sizes

Theorem: Let X be a set. Then the power set $P(X)$ does **not** have the same size as X. $P(X) = \{\text{subsets } S \text{ of } X\}$

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

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

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 $f: X \to P(X)$ = Power set of X

$f(x)$

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	N	Y	Y	
x_2	N	N → Y	Y	Y	
x_3	Y	Y	Y → N	N	
x_4	N	N	Y	N → Y	
$\vdots$					$\ddots$

Define S by flipping the diagonal: $S = \{x_2, x_4, \ldots\}$.

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

For every $x \in X$:
$x \in S \iff x \notin f(x)$

Example

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

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	
⋮				⋱

Construct $S = \{2,3\} \neq f(x)$ for any x

A general theorem about set sizes

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

If $y \in S$: - By def'n of S, $y \notin f(y)$
- $S = f(y) \Rightarrow y \notin S$

If $y \notin S$: - By def'n of S, $y \in f(y)$
- $S = f(y) \Rightarrow y \in S$

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

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

$x \in S \Leftrightarrow x \notin f(x)$

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

$\Downarrow$

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

$y \in S \Leftrightarrow y \notin S$

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

$\times$