BU CS 332 – Theory of Computation

Lecture 14:

- More on Diagonalization
- Undecidability

Reading:

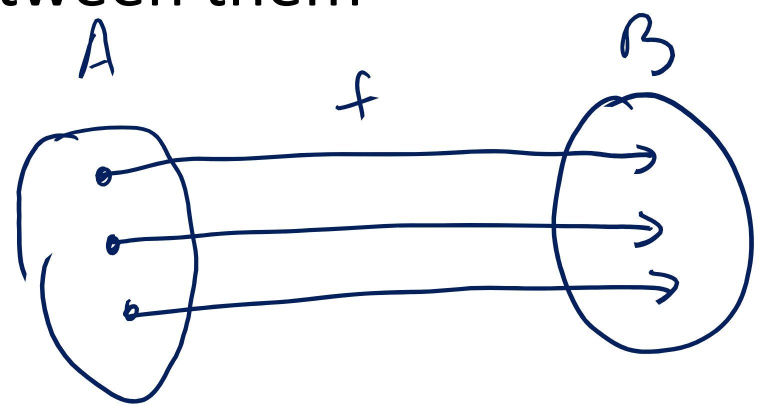
Sipser Ch 4.2

Mark Bun

March 10, 2021

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

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	$0.d_1^1\, d_2^1\, d_3^1\, d_4^1\, d_5^1 \ldots$
2	$0.d_1^2\, d_2^2\, d_3^2\, d_4^2\, d_5^2 \ldots$
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	$0.d_1^5\, d_2^5\, d_3^5\, d_4^5\, d_5^5 \ldots$

$b_1 \neq d_1^1 \Rightarrow b \neq f(1)$

$b_2 \neq d_2^2 \Rightarrow b \neq f(2)$

$b \neq f(n)$ for every n $\Rightarrow$ b is not in the list

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

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

There is no n for which $f(n) = b$, which contradicts the assumption that f is onto

Uncountability of the reals

$b = 0.b_1 b_2 b_3 b_4 \ldots$
$0.9\ 5\ 9\ 5\ 2 \ldots$

A concrete example of the contradiction construction:

$f: \mathbb{N} \to (0,1)$ a bijection

n	$f(n)$
1	$0.8\,6\,7\,5\,3\,0\,9\ldots$
2	$0.1\,4\,1\,5\,9\,2\,6\ldots$
3	$0.7\,1\,8\,2\,8\,1\,8\ldots$
4	$0.4\,4\,4\,4\,4\,4\,4\ldots$
5	$0.1\,3\,3\,7\,1\,3\,3\ldots$

$\forall n,\ b \neq f(n)$
$\Rightarrow$ b is not in the list
$\Rightarrow$ contradiction to f being a bijection

! WARNING ! Just an example for one particular f !

Construct $b \in (0,1)$ which does not appear in this table
$b = 0.b_1 b_2 b_3 \ldots$ 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 $f: \mathbb{N} \to T$
2) "Flip the diagonal" to construct an element $b \in T$ such that $f(n) \neq b$ for every n

Ex: Let $b = 0.b_1b_2b_3...$ 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.

Corollary: If X is countably infinite, then $P(X)$ is uncountable

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

Goal: Construct a set $S \in P(X)$ 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	$x_1 \in f(x)$?	$x_2 \in f(x)$?	$x_3 \in f(x)$?	$x_4 \in f(x)$?	…
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:

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

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

Construct $S =$ a) $\{1\}$ c) $\{2, 3\}$

b) $\{1, 2, 3\}$ d) $\emptyset$

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 $x \in X$:

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

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

"If f is onto, there exists $y \in X$ s.t. $S = f(y)$"

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

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

Case 1: $y \in S \Rightarrow y \notin f(y) \Rightarrow y \notin S$ ✗

Case 2: $y \notin S \Rightarrow y \in f(y) \Rightarrow y \in S$ ✗

$\Rightarrow$ S cannot be $f(y)$ 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: (i.e. some language $L \subseteq \{0,1\}^*$ is undecidable)

$\langle \cdot \rangle$: {TMs over input alphabet $\{0,1\}$} $\to \{0,1\}^*$

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 $\{0,1\}^*$

A language L is a subset of $\{0,1\}^*$ $\Rightarrow$ {languages over $\{0,1\}$} = {subsets of $\{0,1\}^*$} = $P(\{0,1\}^*)$

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 $\{0, 1\}$: $P(\{0, 1\}^*)$

$\{0,1\}^*$ does not have the same size as $P(\{0,1\}^*)$

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 ~~deciders~~ recognizers!

$\Rightarrow$ There must be an unrecognizable language

“Almost all” languages are undecidable

So how about we find one?

An explicit undecidable language

TM M					
M_1					
M_2					
M_3					
M_4					
$\vdots$					

Why is it possible to enumerate all TMs like this?

a) The set of all TM deciders is finite
b) The set of all TM deciders is countably infinite
c) The set of all TM deciders is uncountable

An explicit undecidable language

{Y if M_1 accepts on input $\langle M_3\rangle$; N if M_1 loops or rejects input $\langle M_3\rangle$}

TM M	$M(\langle M_1\rangle)$?	$M(\langle M_2\rangle)$?	$M(\langle M_3\rangle)$?	$M(\langle M_4\rangle)$?		$D(\langle D\rangle)$?
M_1	~~Y~~ N	N	Y	Y	…	
M_2	N	~~N~~ Y	Y	Y		
M_3	Y	Y	~~Y~~ N	N		
M_4	N	N	Y	~~N~~ Y		
⋮					⋱	
D						~~N~~ ~~Y~~ N Y

$UD = \{\langle M\rangle \mid M$ is a TM that does not accept on input $\langle M\rangle\}$

Suppose D decides UD

Claim: UD is undecidable

- Case 1: If D does not accept input $\langle D\rangle \Rightarrow \langle D\rangle \in UD \Rightarrow$ D does the wrong thing on input $\langle D\rangle$ ✗ (i.e. D rejects $\langle D\rangle$, since D a decider)
- Case 2: If D does accept input $\langle D\rangle \Rightarrow \langle D\rangle \notin UD \Rightarrow$ " ✗

An explicit undecidable language

Theorem: $UD = \{\langle M \rangle \mid M \text{ is a TM that does } \textbf{not} \text{ accept on input } \langle M \rangle\}$ is undecidable

Proof: Suppose for contradiction, that TM D decides UD

Either:

Case 1: D does not accept $\langle D \rangle \Rightarrow$ ✗

Case 2: D accepts $\langle D \rangle \Rightarrow$ ✗

$\Rightarrow$ D does not decide UD

D was arbitrary, so UD is undecidable

Ex: M = the TM:
"On input w:
If $w = \langle M \rangle$:
Reject
If $w \neq \langle M \rangle$:
Accept."
$M(\langle M \rangle)$: Rejects

A more useful undecidable language

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

Recognized by universal TM

Theorem: A_{TM} is undecidable

Proof: Assume for the sake of contradiction that TM H decides A_{TM}:

$$H(\langle M, w \rangle) = \begin{cases} \text{accept} & \text{if } M \text{ accepts } w \\ \text{reject} & \text{if } M \text{ does not accept } w \end{cases}$$

(if M loops or rejects on w)

Idea: Show that H can be used to decide the (undecidable) language UD -- a contradiction.

"Reduction"

A more useful undecidable language

$A_{\mathrm{TM}} = \{\langle M, w\rangle \mid M \text{ is a TM that accepts input } w\}$

Proof (continued):

Suppose, for contradiction, that H decides A_{TM}

Consider the following TM D:

"On input $\langle M\rangle$ where M is a TM:

1. Run H on input $\langle M, \langle M\rangle\rangle$
2. If H accepts, reject. If H rejects, accept."

Claim: D decides $UD = \{\langle M\rangle \mid \text{TM } M \text{ does not accept } \langle M\rangle\}$

1) $\langle M\rangle \in UD \Rightarrow M$ does not accept $\langle M\rangle \Rightarrow \langle M, \langle M\rangle\rangle \notin A_{TM} \Rightarrow H(\langle M, \langle M\rangle\rangle)$ reject $\Rightarrow D$ accepts

2) $\langle M\rangle \notin UD \Rightarrow M$ accepts $\langle M\rangle \Rightarrow \langle M, \langle M\rangle\rangle \in A_{TM} \Rightarrow H(\langle M, \langle M\rangle\rangle)$ accepts $\Rightarrow D$ rejects

...but this language is undecidable ⨯

Unrecognizable Languages

Theorem: A language L is decidable if and only if L and $\bar{L}$ are both Turing-recognizable.

Proof: $\Rightarrow$

L is decidable $\Rightarrow$ L is recognizable

L is decidable $\Rightarrow$ $\bar{L}$ is decidable

$\Rightarrow$ $\bar{L}$ is recognizable

Unrecognizable Languages

Theorem: A language L is decidable if and only if L and $\bar{L}$ are both Turing-recognizable.

Proof: $\Leftarrow$

Suppose L is recognizable by TM M_1
$\bar{L}$ is recognizable by TM M_2

Construct TM M:
"On input w:
1) Repeat forever:
2) Run M_1 for one step on w. If accepts, accept.
3) Run M_2 for one step on w. If accepts, reject."

Analysis: 1) $w \in L \Rightarrow M_1$ accepts on $w \Rightarrow M$ accepts w
2) $w \notin L \Rightarrow w \in \bar{L} \Rightarrow M_2$ accepts on $w \Rightarrow M$ reject w.

Application:
- A_{TM} is recognizable
- A_{TM} is undecidable

+ Theorem $\Rightarrow$ $\overline{A_{TM}}$ unrecognizable.

Classes of Languages