Lecture 14:

- Countability
- Uncountability / diagonalization
- Undecidable languages

Reading:
Sipser Ch 4.2

Mark Bun
October 27, 2022
Last Time

Universal Turing machine
A recognizer for  $A_{TM} = \{ \langle M, w \rangle \mid \text{TM } M \text{ accepts input } w \}$ ...but not a decider

Today: Some languages, including $A_{TM}$, are undecidable
     But first, a math interlude...
Countability and 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

- $\emptyset$
- $\{0, 1\}$
- $\{0, 1, 2, \ldots, 8675309\}$
- $E = \{2, 4, 6, 8, \ldots\}$
- $SQUARES = \{1, 4, 9, 16, 25, \ldots\}$
- $POW2 = \{2, 4, 8, 16, 32, \ldots\}$

\[ |E| = |SQUARES| = |POW2| = |\mathbb{N}| \]
How to show that $\mathbb{N} \times \mathbb{N}$ is countable?

Construct a bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$
How to argue that a set $S$ is countable

$\text{Eq. } S = \mathbb{N} \times \mathbb{N}$

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

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

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

... 

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

... 

• 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 \text{ is a Turing machine} \}

• \mathbb{Q} = \{\text{rational numbers}\}

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

• If \( A \subseteq B \) and \( B \) is countable, then \( A \) is countable

• If \( A \) and \( B \) are countable, then \( A \times B \) is countable

• \( S \) is countable if and only if there exists a surjection (an onto function) \( f : \mathbb{N} \rightarrow S \)
Another version of the dovetailing trick

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

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

$\emptyset, 0, 11, 1001$ are finite  $\{0^n | n \geq 3\}$ is not finite

$L = \emptyset, \{0\}, \{0, 3\}, \{0, 2\}, \{3\}, \ldots$

**Proof**: Define a function $C: \{0, 1\}^* \rightarrow \mathbb{F}$

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

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

$C$ is a surjection (onto) $\Rightarrow (C \circ f)(n) = C(f(n))$

is a surjection from $\mathbb{N} \rightarrow \mathbb{F}$. 
Proof 2) $|L| = \# \text{ of elements in } L$

  e.g. $|\emptyset, \epsilon, 0, 011113| = 3$

  $m(L) = \max \text{ length of a string in } L$

  e.g. $m(\emptyset, \epsilon, 0, 011113) = 5$

Claim: Every finite language $L$ appears in this list

Let $n = \max \{ |L|, m(L) \}$

Then $L$ appears in stage $k$ such that $f(i) = i^{th}$ thing enumerated in this list.
So what \textit{isn’t} countable?
Cantor’s Diagonalization Method

• 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

Georg Cantor 1845-1918
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

<table>
<thead>
<tr>
<th>(n)</th>
<th>(f(n))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 . (d_1^1 d_2^1 d_3^1 d_4^1 d_5^1 \ldots)</td>
</tr>
<tr>
<td>2</td>
<td>0 . (d_1^2 d_2^2 d_3^2 d_4^2 d_5^2 \ldots)</td>
</tr>
<tr>
<td>3</td>
<td>0 . (d_1^3 d_2^3 d_3^3 d_4^3 d_5^3 \ldots)</td>
</tr>
<tr>
<td>4</td>
<td>0 . (d_1^4 d_2^4 d_3^4 d_4^4 d_5^4 \ldots)</td>
</tr>
<tr>
<td>5</td>
<td>0 . (d_1^5 d_2^5 d_3^5 d_4^5 d_5^5 \ldots)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>n</th>
<th>( f(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>b ≠ f(1) 0.8675309... ( b = 0.95952... )</td>
</tr>
<tr>
<td>2</td>
<td>b ≠ f(2) 0.1415926...</td>
</tr>
<tr>
<td>3</td>
<td>b ≠ f(3) 0.7182818...</td>
</tr>
<tr>
<td>4</td>
<td>0.4444444444...</td>
</tr>
<tr>
<td>5</td>
<td>0.133371333...</td>
</tr>
</tbody>
</table>

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

\( b = 0.b_1b_2b_3... \) where \( b_n \neq d_n \) (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, 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 $X$.

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

What should we do?

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 $f: X \rightarrow P(X)$

<table>
<thead>
<tr>
<th>$x$</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_2$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_3$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_4$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Diagonalization argument

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

<table>
<thead>
<tr>
<th>( x )</th>
<th>( x_1 \in f(x) )?</th>
<th>( x_2 \in f(x) )?</th>
<th>( x_3 \in f(x) )?</th>
<th>( x_4 \in f(x) )?</th>
<th>( \ldots )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_1 )</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>( x_2 )</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>( x_3 )</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>( x_4 )</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td></td>
</tr>
</tbody>
</table>

Define \( S \) by flipping the diagonal:

\[
\begin{align*}
\forall i &
\quad x_i \in S \iff x_i \notin f(x_i) \\
\forall i &
\quad x_i \notin S \implies x_i \in f(x_i)
\end{align*}
\]
Example

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

Ex. $f(1) = \{1, 2\}$, $f(2) = \emptyset$, $f(3) = \{2\}$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$1 \in f(x)$?</th>
<th>$2 \in f(x)$?</th>
<th>$3 \in f(x)$?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>2</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
<tr>
<td>3</td>
<td>$\times$</td>
<td>$\times$</td>
<td>$\times$</td>
</tr>
</tbody>
</table>

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 \( f: X \rightarrow P(X) \)

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 \( y \notin S \) \( \Rightarrow \) \( S \neq f(y) \) 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) \( \{0, 1\} \)

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

\( \boxed{c)} \) \( P(\{0, 1\}^*) \): 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?