BU CS 332 – Theory of Computation

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?

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...
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 $x + y = 2$
  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 $f: \mathbb{N} \rightarrow S$ by $f(n) =$ the $n$’th element in this list (ignoring duplicates if needed)
More examples of countable sets

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

• 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 $\mathcal{F} = \{L \subseteq \{0, 1\}^* \mid L \text{ is finite}\}$ is countable
So what 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
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 $b_n \neq d_n^*$ (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>0.8675309...</td>
</tr>
<tr>
<td>2</td>
<td>0.1415926...</td>
</tr>
<tr>
<td>3</td>
<td>0.7182818...</td>
</tr>
<tr>
<td>4</td>
<td>0.4444444...</td>
</tr>
<tr>
<td>5</td>
<td>0.1337133...</td>
</tr>
</tbody>
</table>

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

$b = 0.b_1b_2b_3...$ where $b_n \neq d^n_n$ (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 $f: \mathbb{N} \rightarrow T$

2) “Flip the diagonal” to construct an element $b \in T$ such that $f(n) \neq b$ for every $n$

   Ex: Let $b = 0.b_1b_2b_3\ldots$ where $b_n \neq d_n^m$

   (where $d_n^m$ 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>( x_1 )</th>
<th>( x_2 )</th>
<th>( x_3 )</th>
<th>( x_4 )</th>
<th>( \vdots )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></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>$\vdots$</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>$\vdots$</td>
</tr>
</tbody>
</table>

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

<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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Construct $S =$
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 $y \notin S$
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

**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?
An Explicit Undecidable Language
Last time:

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

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

2) “Flip the diagonal” to construct a set $S \in P(X)$ such that $f(x) \neq S$ for every $x \in X$

3) Conclude that $f$ is not onto, contradicting assumption that $f$ is a bijection
Specializing the proof

**Theorem:** Let $X$ be the set of all TM deciders. Then there exists an undecidable language in $P(\{0, 1\}^*)$

1) Assume, for the sake of contradiction, that $L: X \to P(\{0, 1\}^*)$ is onto

2) “Flip the diagonal” to construct a language $UD \in P(\{0, 1\}^*)$ such that $L(M) \neq UD$ for every $M \in X$

3) Conclude that $L$ is not onto, a contradiction
An explicit undecidable language

<table>
<thead>
<tr>
<th>TM $M$</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$M_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$M_3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$M_4$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\vdots$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Why is it possible to enumerate all TMs like this?

a) The set of all TMs is finite
b) The set of all TMs is countably infinite
c) The set of all TMs is uncountable
An explicit undecidable language

<table>
<thead>
<tr>
<th>TM M</th>
<th>$M(\langle M_1 \rangle)$?</th>
<th>$M(\langle M_2 \rangle)$?</th>
<th>$M(\langle M_3 \rangle)$?</th>
<th>$M(\langle M_4 \rangle)$?</th>
<th>$D(\langle D \rangle)$?</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_1$</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>...</td>
</tr>
<tr>
<td>$M_2$</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>$M_3$</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>$M_4$</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>$D$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Claim: $UD$ is undecidable
An explicit undecidable language

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

**Proof:** Suppose for contradiction, that TM $D$ decides $UD$