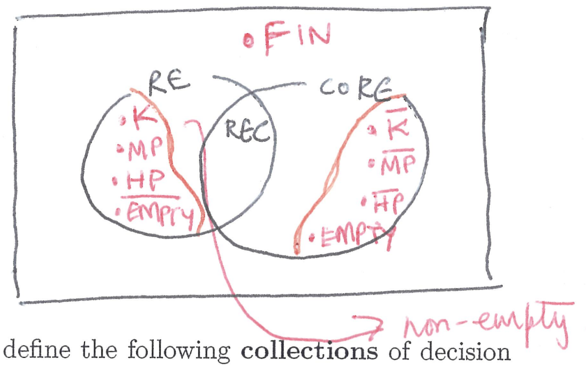
Lecture 11: Hardness, Completeness and Rice's Theorem

Date: September 28, 2023.

Important Decision Problems:



1. $\mathrm{K} = \{\langle M\rangle \mid \langle M\rangle \in \mathbf{L}(M)\}$
2. $\mathrm{MP} = \{\langle M\rangle\#\langle x\rangle \mid x \in \mathbf{L}(M)\}$
3. $\mathrm{HP} = \{\langle M\rangle\#\langle x\rangle \mid M$ halts on $x\}$
4. $\mathrm{EMPTY} = \{\langle M\rangle \mid \mathbf{L}(M) = \emptyset\}$
5. $\mathrm{FIN} = \{\langle M\rangle \mid \mathbf{L}(M)$ is a finite set$\}$

Recursive/Recursively Enumerable Languages: We can define the following **collections** of decision problems.

1. $\mathrm{RE} = \{L \mid \exists M.\ L = \mathbf{L}(M)\}$.
2. $\mathrm{REC} = \{L \mid \exists M.\ M$ decides $L\}$.
3. $\text{co-RE} = \{L \mid \overline{L} \in \mathrm{RE}\}$ $\neq \overline{\mathrm{RE}}$ $\quad \overline{\mathrm{MP}} \in \mathrm{coRE}$

$\mathrm{RE} \cap \mathrm{coRE} = \mathrm{REC}$

equivalent

Proposition 1. *1.* $L \in \mathrm{REC}$ *iff* $\{L, \overline{L}\} \subseteq \mathrm{RE}$.

2. $\overline{\mathrm{K}} \notin \mathrm{RE}$.

3. $\mathrm{MP} \in \mathrm{RE}$.

Computable Functions: A function $f : \Sigma^* \to \Sigma^*$ is **computable** if there is **total** TM M such that on input x, M halts with $f(x)$ written on its tape.

Reductions: For $A, B \subseteq \Sigma^*$, we say A **many-one reduces to** B (denoted $A \leq_m B$) if there is a *computable* function $f : \Sigma^* \to \Sigma^*$ such that

$$x \in A \text{ iff } f(x) \in B.$$

We often drop "many-one" and just say A reduces to B.

Proposition 2. *1. If $A \leq_m B$ and B is recursively enumerable (recursive) then A is recursively enumerable (recursive).*

2. If $A \leq_m B$ then $\overline{A} \leq_m \overline{B}$.

3. If $A \leq_m B$ and $B \leq_m C$ then $A \leq_m C$.

Proposition 3. *1.* $\mathrm{K} \leq_m \mathrm{MP}$

2. $\mathrm{MP} \leq_m \mathrm{HP}$

Problem 1. Prove that $\overline{K} \le_m$ EMPTY.

$$\overline{K} \xrightarrow{f} \text{EMPTY}$$

$\langle M \rangle \rightsquigarrow \langle M' \rangle$ s.t. $\langle M \rangle \notin L(M) \iff \langle M' \rangle \in \text{EMPTY} : L(M') = \phi$

$\langle M \rangle \notin L(M) \Rightarrow L(M') = \phi \Rightarrow \langle M' \rangle \in \text{EMPTY}$

$\langle M \rangle \in L(M) \Rightarrow L(M') = \Sigma^* \Rightarrow \langle M' \rangle \notin \text{EMPTY}$

M': Input x

Run M on $\langle M \rangle$

If M accepts

return accepts

else return rejects

f is computable

EMPTY $\notin$ R.E

$\notin$ REC

$\overline{\text{EMPTY}} \in$ RE

" $\{\langle M \rangle \mid L(M) \neq \phi\}$

FIN $\notin$ RE $\cup$ coRE

Problem 2. Prove that $\overline{K} \le_m$ FIN and $\overline{K} \le_m \overline{\text{FIN}}$.

$\overline{\text{FIN}} \notin$ RE

$\overline{K} \le_m$ FIN because same reduction as $\overline{K} \le$ EMPTY

$$\overline{K} \xrightarrow{f} \overline{\text{FIN}}$$

$\langle M \rangle \rightsquigarrow \langle M' \rangle$ s.t. $\langle M \rangle \in \overline{K}$ iff $\langle M' \rangle \in \overline{\text{FIN}}$

$\langle M \rangle \notin L(M)$ iff $L(M')$ is infinite.

M': Input x.

Run M on $\langle M \rangle$ for $|x|$ steps

If M accepts then

return reject

else

return accepts.

$\langle M \rangle \notin L(M)$ —

→ if M halts on $\langle M \rangle$

$L(M') = \Sigma^*$

→ if M doesn't halt on $\langle M \rangle$

$L(M') = \cancel{\phi}\ \Sigma^*$

$\langle M \rangle \in L(M) \Rightarrow M$ halts on $\langle M \rangle$ in k steps

$\Rightarrow L(M') = \{x \mid |x| < k\}$ is finite set

$\Rightarrow \langle M' \rangle \in$ FIN

Definition 1. A language L is **RE-hard** (**co-RE-hard**) if for every $A \in$ RE ($A \in$ co-RE), $A \leq_m L$. A language L is RE-**complete** (co-RE-**complete**) if $L \in$ RE ($L \in$ co-RE) and L is RE-hard (co-RE-hard).

Problem 3. Prove that MP is RE-complete.

MP $\in$ RE because of universal TM.

To prove: $\forall A \in RE$, $A \leq_m MP$.

$A \in RE$, $\exists$ TM M s.t. $A = L(M)$.

$f(x) = \langle M \rangle \# x$ $\quad x \in A \Leftrightarrow x \in L(M) \Leftrightarrow \langle M \rangle \# x \in MP$

Problem 4. Prove that HP is RE-complete.

HP $\in$ RE : On input $\langle M \rangle \# x$, run M on x and accept if M halts.

HP $\in$ RE-hard : $\forall A \in RE$, $A \leq_m HP$.

$MP \leq_m HP$, $\forall A \in RE$, $A \leq_m MP$.

$\Rightarrow \forall A \in RE$ $A \leq_m HP$.

Proposition : If $A \leq_m B$ and A is RE-hard (A is coRE-hard) then B is RE-hard (coRE-hard)

Problem 5. If L is RE-hard then $L \notin$ REC.

L is RE hard. HP is RE-hard. HP $\in$ RE

$HP \leq_m L$, $L \notin REC$ because $HP \notin REC$.

Problem 6. If L is RE-hard then $\overline{L}$ is co-RE-hard.

$\mathbb{P}_{EMPTY} = \{\phi\}$ $\quad$ $\mathbb{P}_{FIN} = \{L \mid L \text{ is finite set}\}$

Definition 2. A **property of languages** is a set of languages. We say a language L satisfies a property $\mathbb{P}$ if $L \in \mathbb{P}$.

- For a property $\mathbb{P}$ of languages, define $L_{\mathbb{P}} = \{\langle M\rangle \mid \mathbf{L}(M) \in \mathbb{P}\}$.

$L_{\mathbb{P}_{EMPTY}} = EMPTY$

$L_{\mathbb{P}_{FIN}} = FIN$

Problem 7. Which of the following languages are "properties of languages"?

1. REG $= \{\langle M\rangle \mid \mathbf{L}(M)$ is regular$\}$.
2. $T_{>32} = \{\langle M\rangle \mid M$ has at least 32 transitions$\}$
3. $L^1_{odd} = \{\langle M\rangle \mid M$ has an odd number of states$\}$
4. $L^2_{odd} = \{\langle M\rangle \mid \exists N.\ N$ has an odd number of states and $\mathbf{L}(M) = \mathbf{L}(N)\}$

Definition 3. A property $\mathbb{P}$ is **trivial** if either $L_{\mathbb{P}} = \emptyset$ or $L_{\mathbb{P}} = \{0,1\}^*$

- If $\mathbb{P}$ is trivial then $L_{\mathbb{P}}$ is decidable.

Theorem 4 (Rice). *If $\mathbb{P}$ is non-trivial then $L_{\mathbb{P}}$ is undecidable.*

$\mathbb{P}$ is non-trivial, $\quad L_{\mathbb{P}} \neq \phi$

$\hookrightarrow \exists M.\ \langle M\rangle \in L_{\mathbb{P}} \Rightarrow L(M) \in \mathbb{P}$

$L_{\mathbb{P}} \neq \{0,1\}^* \Rightarrow \exists M.\ L(M) \notin \mathbb{P}.$

$\phi \in \mathbb{P}$ (WLOG). $\quad \exists N.$ s.t $L(N) \notin \mathbb{P}.$

$\overline{K} \leq_m \underline{L_{\mathbb{P}}}.$ $\quad f(\langle M\rangle)$: Input x

Run M on $\langle M\rangle$

If M accepts

Run N on x

If N accepts

accept

else reject

else

reject.

$\langle M\rangle \notin L(M) \Rightarrow L(f(\langle M\rangle)) = \phi$

$f(\langle M\rangle) \in L_{\mathbb{P}}$

$\langle M\rangle \in L(M) \Rightarrow L(f(\langle M\rangle)) = L(N)$

$\Rightarrow f(\langle M\rangle) \notin L_{\mathbb{P}}.$