# Theory of Computation Chapter 3 

Guan-Shieng Huang

Mar. 24, 2003

## Universal Turing Machines

- A Turing machine is a special hardware to do computation.
A modern computer can load different programs and do the corresponding computational tasks.
Can a Turing machine act as a universal computational device?
- Universal Turing Machines

The input of a universal TM $U$ is $M ; x$, where $M$ is the description of a TM, $x$ is its input. We can imagine that $U$ interprets $M$ and executes $M$ with the input $x$. Written as

$$
U(M ; x)=M(x)
$$

## Halting Problem

Given the description of a TM $M$ and its input $x$, will $M$ halt on $x$ ?

$$
H=\{M ; x \mid M(x) \neq \nearrow\} .
$$

(Note: A universal TM is implicitly assumed.)

## Proposition 3.1

$H$ is recursively enumerable (R.E.).

1. R.E. $\Rightarrow$ there is a TM $D$ such that

$$
D(M ; x)= \begin{cases}" y e s " & \text { if } M(x) \neq \nearrow \\ \nearrow & \text { otherwise }\end{cases}
$$

2. The universal TM $U$ can serve this task. We only need to modify $U$ s.t. when $M(x)$ halts, $U$ terminates at "yes".

## Theorem 3.1

$H$ is not recursive.

1. recursive $\Rightarrow$ there is a $\mathrm{TM} M_{H}$ such that

$$
M_{H}(M ; x)=\left\{\begin{array}{cl}
" y \mathrm{yes} " & \text { if } M(x) \neq \nearrow \\
" \mathrm{no"} & \text { if } M(x)=\nearrow
\end{array}\right.
$$

2. Proof By Contradiction.

Suppose we have such a TM $M_{H}$. Construct a TM $D(x)$ as
(a) On input $x, D$ first simulates $M_{H}$ on input $x ; x$.
(b) If $M_{H}$ accepts $x ; x, D$ diverges (e.g. moves its cursor to the right of its string forever).
(c) If $M_{H}$ rejects $x ; x, D$ halts.
3. That is,

$$
D(x): \text { if } M_{H}(x ; x)=\text { "yes" then } \nearrow \text { else "yes". }
$$

4. What is $D(D)$ ?
(a) If $D(D)=\nearrow$ :

Step $(\mathrm{b}) \Rightarrow M_{H}(D ; D)=$ "yes" $\Rightarrow D(D) \neq \nearrow$.
(b) If $D(D) \neq \nearrow$ :

Step $(\mathrm{c}) \Rightarrow M_{H}(D ; D)=$ "no" $\Rightarrow D(D)=\nearrow$.

There are countably-many TMs.
There are uncountably-many languages.
Hence, there exists a language that is not recursive.

## Reduction

To show that Problem $A$ is undecidable, we establish that if there were an algorithm for Problem $A$, then there would be an algorithm for Halting $H$, which is absurd.

## Proposition 3.2

The following languages are not recursive.

1. $L_{a}=\{M \mid M$ halts on all inputs $\}$.
2. $L_{d}=\{M ; x ; y \mid M(x)=y\}$.
3. $L_{b}=\{M ; x \mid$ there is a $y$ such that $M(x)=y\}$.
4. $L_{c}=$
$\{M ; x \mid$ the computation $M$ on input $x$ uses all states of $M\}$.
$L_{a}=\{M \mid M$ halts on all inputs $\}$.
Reduce Halting to this problem.
Given $M$; $x$, we construct

$$
M^{\prime}(y): M(x) .
$$

Hence $M^{\prime}$ halts on all inputs if and only if $M$ halts on $x$.

$$
L_{d}=\{M ; x ; y \mid M(x)=y\} .
$$

Given $M ; x$, we construct

$$
M^{\prime}\left(x^{\prime}\right): \text { if ( } M(x) \text { halts), then Output } \epsilon .
$$

Hence $M^{\prime} ; x^{\prime} ; \epsilon \in L_{d}$ if and only if $M$ halts on $x$.

$$
L_{b}=\{M ; x \mid \text { there is a } y \text { such that } M(x)=y\}
$$

The meaning of this problem is not clear.

- $M(x)=\{$ "yes", "no", "halt", $\nearrow\}$.
- Does $M$ halts on $x$ ?
- $\{M ; x \mid M(x)=c\}$ for some constant string $c$.


## Proposition 3.3

If $L$ is recursive, then so is $\bar{L}$.

1. Let $D$ be the TM that decides $L$ :

$$
D(x)= \begin{cases}" y e s " & \text { if } x \in L \\ \text { "no" } & \text { if } x \notin L\end{cases}
$$

2. Construct $D^{\prime}$ such that

$$
D^{\prime}(x)= \begin{cases}" y e s " & \text { if } D(x)=" \text { no" } \\ " \text { no" } & \text { if } D(x)=" y e s "\end{cases}
$$

Then $D^{\prime}$ decides $\bar{L}$.

## Proposition 3.4

$L$ is recursive if and only if both $L$ and $\bar{L}$ are recursively enumerable.

1. $L$ is recursive $\Rightarrow$

$$
D_{L}(x)= \begin{cases}" y e s " & \text { if } x \in L \\ \text { "no" } & \text { if } x \notin L\end{cases}
$$

2. $\bar{L}$ is recursively enumerable

$$
M_{\bar{L}}(x)= \begin{cases}" y e s " & \text { if } x \in \bar{L} \text { or } x \notin L \\ \nearrow & \text { if } x \notin \bar{L} \text { or } x \in L .\end{cases}
$$

3. $L$ is recursively enumerable

$$
M_{L}(x)= \begin{cases}" y \mathrm{yes} " & \text { if } x \in L \\ \nearrow & \text { if } x \notin L\end{cases}
$$

4. Given $D_{L}$, we construct $M_{l}$ and $M_{\bar{L}}$ as follows.

$$
\begin{array}{ll}
M_{L}(x): & \text { if } D_{L}(x)=\text { "yes" then "yes" } \\
& \text { else } \nearrow . \\
M_{\bar{L}}(x): & \text { if } D_{L}(x)=\text { "no" then "yes" } \\
& \text { else } \nearrow .
\end{array}
$$

5. Given $M_{L}$ and $M_{\bar{L}}$, we construct $D_{L}$ as

$$
D_{L}(x)=\left\{\begin{array}{l}
\text { if }\left(M_{L}(x)=" \text { yes" }\right) \text { then "yes" } \\
\text { if }\left(M_{\bar{L}}(x)=" \text { yes" }\right) \text { then "no" }
\end{array}\right.
$$

## Enumerator

$$
E(M)=\left\{x \mid(s, \triangleright, \epsilon) \xrightarrow{M^{*}}(q, y \sqcup x \sqcup \epsilon) \text { for some } q, y\right\}
$$

That is, $E(M)$ is the set of all strings $x$ such that during $M$ 's operation on empty string, there is a time at which $M$ 's string ends with $\sqcup x \sqcup$.

## Proposition 3.5

$L$ is R.E. if and only if there is a machine $M$ such that $L=E(M)$.

1. Suppose $L=E(M)$. We construct a TM $M^{\prime}$ that accepts $L$ as follows.
$M^{\prime}(x)$ : if $x$ appears in the string of $M(\epsilon)$ then "yes" else $\nearrow$.
Then $M^{\prime}(x)=$ "yes" iff $x \in E(M)=L$.
2. Suppose $L$ is R.E. Then we have a TM $M$ s.t.

$$
M(x)= \begin{cases}" y e s " & \text { if } x \in L \\ \nearrow & \text { if } x \notin L .\end{cases}
$$

We need to construct a TM $M^{\prime}$ such that $E\left(M^{\prime}\right)=L$.
$M^{\prime}(\epsilon)$ works as follows.
(a) For $i=1,2,3, \ldots$, simulate $M$ on the $i$ first inputs, one after the other, and each for $i$ steps.
(b) If at any point $M$ would halt with "yes" on one of these $i$ inputs, say $x$, then $M^{\prime}$ write $\sqcup x \sqcup$ at the end of its string before continuing.

## Theorem 3.2: Rice's Theorem

Suppose that $\mathcal{C}$ is a proper, non-empty subset of the set of all R.E. languages. Then
"Given a TM $M$, is $L(M) \in \mathcal{C}$ " is undecidable.

1. A TM is a string, and a string is a TM.
2. WLOG, we assume that $L \in \mathcal{C} \& \emptyset \notin \mathcal{C}$. We reduce Halting to this problem. Given $M ; x$, we construct

$$
M^{\prime}(y): \text { if }(M(x) \text { halts }) \text { then } M_{L}(y)
$$

Then $M ; x \in H$ iff $L\left(M^{\prime}\right)=L$ (and $M ; x \notin H$ iff $L\left(M^{\prime}\right)=\emptyset$. That is, $L\left(M^{\prime}\right) \in \mathcal{C}$ iff $M ; x \in H$.

## Recursive Inseparability

Two disjoint languages $L_{1}$ and $L_{2}$ are recursively inseparable if there is no recursive language $R$ such that $L_{1} \cap R=\emptyset$ and $L_{2} \subset R$. (That is, $\bar{R}$ contains $L_{1}$ and $R$ contains $L_{2}$.)

## Theorem 3.3

Define $L_{1}=\{M \mid M(M)=$ "yes" $\}$ and $L_{2}=\{M \mid M(M)=$ "no" $\}$. Then $L_{1}$ and $L_{2}$ are recursively inseparable.

1. Suppose that recursive language $R$ separates them. Thus, $R \cap L_{1}=\emptyset$ and $L_{2} \subset R$.
2. Consider the $M_{R}$ that decides $R$. "What is $M_{R}\left(M_{R}\right)$ "?
(a) If $M_{R}\left(M_{R}\right)=$ "yes", then $M_{R} \in L_{1}$ and $M_{R} \notin R$, and then $M_{R}\left(M_{R}\right)=$ "no".
(b) If $M_{R}\left(M_{R}\right)=$ "no", then $M_{R} \in L_{2}$ and $M_{R} \in R$, and then $M_{R}\left(M_{R}\right)=$ "yes".

Hence, this $R$ is absurd.

## Corollary

Let $L_{1}^{\prime}=\{M \mid M(\epsilon)=$ "yes" $\}$ and $L_{2}^{\prime}=\{M \mid M(\epsilon)=$ "no" $\}$. Then $L_{1}$ and $L_{2}$ are recursively inseparable.

1. We reduce $L_{1}$ and $L_{2}$ to $L_{1}^{\prime}$ and $L_{2}^{\prime}$. Given any $M$, we construct $M^{\prime}(x)$ simply as $M(M)$. Hence,

$$
M(M)=\text { "yes" iff } M^{\prime}(\epsilon)=\text { "yes" }
$$

and

$$
M(M)=" \mathrm{no"} \text { iff } M^{\prime}(\epsilon)=\text { "no". }
$$

2. If $L_{1}^{\prime}$ and $L_{2}^{\prime}$ are recursively separable, then so do $L_{1}$ and $L_{2}$.
