Decidability and Undecidability

Classification of languages/problems

1) Recursively enumerable (R.E.) languages:
   class of languages defined by T.M. (or procedures)
   arbitrary T.M. (that may not halt) = procedure

2) Recursively enumerable (R.E.) languages:
   class of languages defined by T.M. (or procedures)
   arbitrary T.M. (that may not halt) = procedure

3) Non-R.E. languages
   languages/problems for which there is no T.M./procedure

Pictorially:

1) Algorithm (recursively)
   input w → [A] → yes (w ∈ L) → no (w ∉ L)

2) Procedure (R.E.)
   input w → [P] → yes (w ∈ L)

3) Non-R.E.
   input w → ??
The Church-Turing Thesis

We have provided a classification of languages according to TM-acceptance/determination.

However, we are interested in problems and their computability.

Decision problem: is a set of related questions with a yes/no answer.

E.g. the decision problem of determining whether a natural number is prime is the set of questions:

1. Is 0 prime?
2. Is 1 prime?
3. Is 2 prime?

Each question is an instance of the problem. Positive instances, negative instances.

A solution to a decision problem $P$ is an algorithm that determines the correct answer to each question $q$: $e P$.

$P$ is decidable if it has a solution.

What is an algorithm (or effective procedure)?

difficult to define, but we can list some fundamental properties:

- complete: produces correct answer for each instance
- mechanistic: consists of a finite sequence of instructions, each of which can be carried out unambiguously
- deterministic: performs the same computation if executed multiple times on the same input

TM machine computations are mechanistic and deterministic.

If the TM halts on all inputs, then it is an algorithm.
Representation of decision problems:

To provide a TM solution to a decision problem, we need to encode its instances in terms of strings.

- Problem representation $\rightarrow$ TM
- TM computation $\rightarrow$ yes/no

Input $p_i$ $\rightarrow$ $w_i$ $\rightarrow$ yes/no

Note: The choice of the representation may affect the solution. However, it will not affect existence of a TM that is an effective procedure.

Would it make a difference, if we choose a different computation model than the TM?

Several such models have been proposed, based on different paradigms:

- String transformations:
  - Post systems [Emil Post, 1936]
  - Semi-Thue systems [Bekker 1914]
  - Markov systems [Markov, 1961]
  - Unrestricted grammars [Noam Chomsky, 1956]

- Function evaluation:
  - Partial recursive and $\mu$-recursive functions
    [Gödel 1934, Kleene 1936]
  - Lambda calculus [Church 1941]

- Abstract computing machines:
  - Turing Machine
  - Register machines [Stephenson 196]
It has been shown that all of the above algorithmic systems have the same computing power, i.e., they can simulate each other.

It is currently believed that the computing power of any of these systems defines the intrinsic limits of computation. This belief is known as Church–Turing Thesis:

**Church–Turing Thesis for decision problems:**

There is an effective procedure to solve a decision problem if there is a TM that always halts and solves the problem.

A partial solution to a decision problem P is a not necessarily complete but otherwise effective procedure that returns yes for every positive instance p ∈ P.

If p is a negative instance, the procedure may return no or not terminate.

**Church–Turing Thesis for recognition problems:**

A decision problem is partially solvable if there is a TM that accepts the positive instances of the problem.

The most general formulation is in terms of TMs that compute functions (by keeping the result on the tape).

**Church–Turing Thesis for computable functions:**

A function f is effectively computable if there is a TM that computes f.
Note: The Church--Turing thesis cannot be proved, since it relies on the intuitive notion of effective procedure.

It could be disproved by exhibiting an effective procedure not computable by a TM. This is unlikely, given the robustness of the TM model.

We exploit the Church--Turing thesis to simplify proofs of existence of a decision algorithm:

instead of constructing the TM, we describe an intuitively effective procedure to solve the problem.
Closure properties

**Theorem:** \( L \) is recursive \( \implies \overline{L} \) is recursive

*Proof:* Given algorithm \( A \) for \( L \\
\text{construct alg. } \overline{A} \text{ for } \overline{L} \\

Intuitively:

![Diagram](image)

More precisely:

\[ A = (Q, \Sigma, \Gamma, \delta, q_0, \emptyset, F) \]

\[ \overline{A} = (Q \cup \{\overline{f}\}, \Sigma, \Gamma, \delta, q_0, \emptyset, \{f\}) \]

yes \( \rightarrow \) no: We assume that final states of \( F \) are blocking.
So we get that \( \overline{A} \) blocks in a non-final state.

no \( \rightarrow \) yes: If \( \delta(q, k) \) is undefined,
then set \( \overline{\delta}(q, k) = (\overline{f}, k, R) \)

Since \( L \) is recursive, \( A \) always halts (with output yes or no),
hence \( \overline{A} \) also halts always (with output no or yes)
Theorem: Both $L$ and $\overline{L}$ are R.E.

$\Rightarrow$ both $L$ and $\overline{L}$ are recursive

Proof: Let $P, \overline{P}$ be procedures (i.e. TMs) for $L, \overline{L}$.

We run them in parallel, to get an alg. $A$ for $L$.

Intuitively:

\[
\begin{array}{ccc}
\text{Input} & \xrightarrow{P} & \text{yes} \\
A & \xrightarrow{P} & \text{yes} \\
 & \xrightarrow{P} & \text{no}
\end{array}
\]

Note: we assume that $P$ is non-blocking on non-final states.

Note: for every $w$, one of $P, \overline{P}$ will halt and give the
right answer.

More precisely:

For $A$ use 2 tapes, one simulating that of $P$

States of $A$: for each state $q$ of $P$ state $q$ of $\overline{P}$ of $A$

Transitions:

for each pair $(\delta(q, \epsilon), (q', x', d_1))$ in $P$

we have a transition in $A$

$\delta((q, q), \epsilon, x') = ((q', q'), (x', d_1), (q', d_2))$

Final states: every $(q, q)$ s.t. $q$ is final in $P$

Note: if $\overline{P}$ accepts in $q$, then $q$ is final (and we
assume it is halting). Hence, if $A$ reaches

$(q, q)$, $P$ cannot be final, and since $q$

is halting, $A$ rejects.

q.e.d.
The two previous results imply that, for every language $L$, we have that

- either both $L$ and $\overline{L}$ are recursive
- or at least one of $L$, $\overline{L}$ is non-R.E.

<table>
<thead>
<tr>
<th>$L$ rec.</th>
<th>$\overline{L}$ R.E. but not rec.</th>
<th>$\overline{L}$ non-R.E.</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
</tbody>
</table>

(✓ means that this case is not possible)

**Theorem:** $L_1, L_2$ rec. $\implies$ $L_1 \cup L_2$ rec.

(recursive languages are closed under union)

**Proof:** Let $A_1, A_2$ be algorithms for $L_1, L_2$

Output "no" of $A_1$ triggers $A_2$ means:

- if $A_1$ halts in a non-final state $q$ (i.e., $w \notin L_1$),
- then we have a transition from $q$ to the initial state of $A_2$ (to feed $w$ to $A_2$, we can store $w$ on a second tape before running $A_1$)

$q.e.d.$
Theorem: \( L_1, L_2 \text{ R.E.} \Rightarrow L_1 \cup L_2 \text{ R.E.} \)

(R.E. languages are closed under union)

Proof: let \( P_1, P_2 \) be procedures (i.e. TMs) for \( L_1, L_2 \)
we run \( P_1, P_2 \) in parallel

\[
\text{input} \ w \xrightarrow{\text{yes}} \ P_1 \xrightarrow{\text{yes}} \ P_2 \xrightarrow{\text{yes}} \ P_1 \cup P_2
\]

Note: we assume that \( P_1, P_2 \) are non-blocking on non-final states

Note: if \( w \in L_1 \cup L_2 \), one of \( P_1 \) or \( P_2 \) will halt and answer yes

Exercise: work out the details

Exercise: prove/disprove closure under intersection, reversal

Showing languages to be undecidable/non-R.E.

To show languages to be undecidable (non-R.E.) we make use of the basic idea of feeding the encoding of a T.M. as input to a T.M.

\( \text{e.g.} \) Universal T.M. (UTM):

- input: T.M. \( M \)
  \( M \)'s input \( w \) \text{ \textit{encoding \( M \)}} \} \langle M, w \rangle

- output: UTM accepts \( \langle M, w \rangle \Leftrightarrow M \) accepts \( w \)

Diagonalization: consider what happens when certain T.M.'s are fed their own encoding as input.
In both cases we need a suitable way of encoding T.M.'s by means of strings

We consider encoding T.M.'s by means of strings over \{0, 1\}, i.e., as binary integers.

Let \( M = (Q, \Sigma, \Gamma, \delta, q_0, q_f, B, F) \) be a T.M.

We assume \( \Sigma = \{0, 1\} \), i.e., we consider only T.M.'s

w.r.t. \( \Gamma = \{0, 1, B\} \) over the binary alphabet

(though no limitation)

- initial state \( q_0 \)
- single final state \( q_f \)

We use the following notation:

- \( \kappa_1 = 0 \), \( \kappa_2 = 1 \), \( \kappa_3 = B \)
- \( d_1 = \text{left} \), \( d_2 = \text{right} \)

Encoding of transitions: \( \delta(q_i, \kappa_j) = (q_k, x, \ell, d_m) \)

with \( i, k \in \{1, \ldots, n\} \)

\( \delta, \ell \in \{1, 2, 3\} \)

\( m \in \{0, 1\} \)

We encode the transition as \( 0^i 10^j 10^k 10^\ell 10^m \)

Encoding \( E(M) \) of entire T.M. \( M \):

Let \( E_1, \ldots, E_m \) be the encodings of the transitions of \( M \).

We encode \( M \) as:

\( E(M) = E_1 11 E_2 11 E_3 11 \ldots 11 E_m 11 \)

Encoding of \( M \) with its input \( w \): \( E(M) 111 w \)

(note: the first 111 indicates that the encoding \( E(M) \) is finished)
- each bit string encodes a unique T.M.
  - either it is a valid encoding and encodes a unique T.M.
  - or it is not a valid encoding according to our rules:
    - in this case we assume that it encodes the particular
      machine $M_0$ with 1 state and no transitions
      ($I(M_0) = \emptyset$)
- each T.M. admits at least 1 encoding (possibly many)

**Enumerating binary strings:**

We define an ordering on binary strings:
- in increasing order of length
- strings of the same length are ordered lexicographically

$\Rightarrow \emptyset, 0, 1, 00, 01, 10, 11, 000, 001, \ldots$

Let $w_n$ be the $n$-th string in this ordering
(starting with $w_1 = \emptyset$)

We define $M_i$ as the T.M. encoded by $w_i$, i.e. $w_i = \mathcal{E}(M_i)$
$\Rightarrow$ we get an ordering of T.M.'s:
- each T.M. appears at least once in the ordering
  - may appear many times

**Note:** each binary string $w_i$ can be viewed:
- as a string fed as input to a T.M.
- as the encoding $w_i = \mathcal{E}(M_i)$ of a T.M. $M_i$
The diagonalization language

Exploiting the ordering enumeration of \( w_i / M_i \), we can consider the infinite table \( T \) st. \( \forall i, j \geq 1 \):

\[
T(i, j) = \begin{cases} 1 & \text{if } w_j \in L(M_i) \\ 0 & \text{if } w_j \notin L(M_i) \end{cases}
\]

<table>
<thead>
<tr>
<th>( w_1 )</th>
<th>( w_2 )</th>
<th>( w_3 )</th>
<th>( w_4 )</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>( M_1 )</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( M_2 )</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( M_3 )</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( M_4 )</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Each row of \( T \) is a characteristic vector of \( L(M_i) \), specifying which strings belong to \( L(M_i) \).

**Definition:** The diagonalization language

\[
L_d = \{ w_i \mid T(i, i) = 0 \} = \{ w_i \mid w_i \notin L(M_i) \}
\]

In other words: \( L_d \) is defined as the language whose characteristic vector is the bit by bit complementation of the diagonal of \( T \).

**Theorem:** \( L_d \) is non-R.E.

**Proof:** By contradiction, assume \( L_d \) is R.E. and has a T.M. that accepts \( L_d \).

Then \( \exists k > 1 \) st. \( L(M_k) = L_d \)
Question: is $w_k \in L_d$

Case 1: $w_k \in L_d \Rightarrow w_k \in L(M_k)$ 
$\Rightarrow T(h, h) = 1$
$\Rightarrow w_k \notin L_d$  contradiction

Case 2: $w_k \notin L_d \Rightarrow w_k \notin L(M_k)$
$\Rightarrow T(h, h) = 0$
$\Rightarrow w_k \in L_d$  contradiction

Intuition: $L_d$ is defined so that it disagrees with each $L(M_i)$ on at least string $w_i$. 
$\Rightarrow \forall M_i$ can have $L_d$ as its language
But all T.M. s appear in the enumeration
$\Rightarrow \forall$ T.M. can accept $L_d$

Universal T.M.

UTM: Input $\langle E(M), w \rangle$ with $E(M)$ encoding of a T.M. $M$
$-w$ might string for $M$
Action: UTM simulates $M$ on $w$, and accepts
$\langle E(M), w \rangle$ if and only if $M$ accepts $w$.

Language $L_u$ of UTM

Definition: Universal language

$L_u = \{ \langle E(M), w \rangle \mid w \in L(M) \}$
Theorem: $L_n$ is R.E.

Proof: we construct a T.M. $U$ s.t. $L(U) = L_n$

$U$ has 4 tapes:

- Tape 1: input tape containing $\langle \Sigma(M), w \rangle$ (read-only)
- Tape 2: simulates the tape of $M$
- Tape 3: contains the current state $q_i$ of $M$: $00 \cdots 0$

(Note: the state of $M$ cannot be encoded on the state of $U$, since we have no bound on the number of states that $M$ could have)

- Tape 4: scratch tape

Transitions: $U$ simulates the transitions on tape 1, by modifying tapes 2 and 3

- Initially, copy $w$ to tape 2, and $q_i = 0$ to tape 3 (initial state)

- To simulate each transition of $M$, $U$ uses
  - the current state $q_i = 0^k$ on tape 3
  - the current symbol $x_j$ on tape 2

Looks on tape 1 for transition $0^k10^{i+1}0^k10^{i+2}$, i.e. $\delta(q_i, x_j) = (q_{k}, x_{l}, d_{m})$

and - changes the content of tape 3 to $q_i = 0^k$
- changes the current symbol on tape 2 to $x_l$
- moves the head on tape 2 according to $d_{m}$

$U$ accepts whenever $M$ enters final state $q_f$
To show that $L_1$ is not recursive, we exploit the notion of reduction:

**Reduction**

**Definition:** $L_1$ reduces to $L_2$ (denoted $L_1 \leq L_2$) if there exist a function $R$ (called the reduction from $L_1$ to $L_2$) such that

1. $R$ is computed by some T.M. $M_R$ that takes as input a string $w$ (an instance of $L_1$) and halts leaving a string $R(w)$ on its tape ($M_R$ is an algorithm!)
2. $w \in L_1 \iff R(w) \in L_2$

**Intuitively:**

\[ \Sigma^* \rightarrow L_1 \xrightarrow{R} L_2 \xrightarrow{R} \Sigma^* \]

R maps: all strings in $L_1$ to a subset of all strings in $L_2$

**Theorem:** $L_1 \leq L_2$ and $L_2$ is recursive $\implies$ $L_1$ is recursive

**Proof:** given algorithm $A_2$ for $L_2$

- $M_R$ for $R$

construct algorithm $A_1$ for $L_1$:

\[ w \rightarrow M_R \rightarrow R(w) \xrightarrow{A_2} \equiv \begin{cases} \text{yes} & R(w) \in L_2 \\ \text{no} \end{cases} \]

$q.e.d.$
We can use the same result to show a language to be non-recursive (i.e., undecidable):

**Corollary:** $L_1 \leq L_2$ and $L_1$ is non-recursive

$\Rightarrow L_2$ is non-recursive

The above results apply also to R.E.

**Theorem:** $L_1 \leq L_2$ and $L_2$ is R.E. $\Rightarrow L_1$ is R.E.

$L_1 \leq L_2$ and $L_2$ is non-R.E. $\Rightarrow$ $L_2$ is non-R.E.

Intuitively, $L_1 \leq L_2$ means that $L_2$ is at least as difficult as $L_1$.

**Theorem:** $L_d$ is non-recursive

We show that $L_d \leq L_u$ (i.e., $L_d$ reduces to $L_u$).

The claim follows, since $L_d$ is non-recursive (if $L_d$ were recursive, also $L_d = L_u$ would be recursive, but we know that $L_d$ is non-R.E.)

Reduction $R$: given input string $w$ for $L_d$

produce input string $\langle M_i, w \rangle = \varepsilon(M_i) \, \# \, w$ for $L_u$

We define $R(w) = \# \, w \, \# \, w$

Clearly, there exists an algorithm $M_e$ to convert $w$ into $\# \, w \, \# \, w$

We need to show: $w \in L_d \iff R(w) \in L_u$

$\iff w \in L_d \iff w \in \varepsilon(M_i) \iff \langle M_i, w \rangle \in L_u$

$\iff \varepsilon(M_i) \, \# \, w \in L_u \iff w \, \# \, w \in L_u$

$\iff R(w) \in L_u \quad \text{q.e.d.}$
To sum up:

- \( L_d \) is non-R.E.: direct proof via diagonalization
- \( L_d \) is R.E., but non-recursively: exercise
- \( L_n \) is R.E., but non-recursively: R.E. by construction of \( U \)
  non-rec. by \( E_d \leq L_n \)
- \( L_n \) is non-R.E.: by inference from previous line

We can exploit this to show a language \( L \) to be non-rec. or non-R.E.

- \( E_d \leq L \) or \( L_n \leq L \) \( \Rightarrow \) \( L \) is non-recursively
- \( L_d \leq L \) or \( L_n \leq L \) \( \Rightarrow \) \( L \) is non-R.E.

(And hence non-recursively)

Consider the following languages, on \( \Sigma = \{0,1\} \)

- \( L_e = \{ E(M) \mid L(M) = \emptyset \} \)
- \( L_e = \{ E(M) \mid L(M) \neq \emptyset \} \)

Hence: \( L_e \) ... set of all strings that encode T.M.s that accept the empty language

\( L_e \) ... complement of \( L_e \)

We have that: \( L_n \) is R.E. but non-recursively

\( L_e \) is non-R.E.

Proof: see Exercise 10 (10.1, 10.2)
We have shown that a specific property of T.M. languages (namely non-emptyness) is undecidable.

This is just a special case of a much more general result:

All non-trivial properties of R.E. languages are undecidable.

**Property P** of R.E. languages is a set of R.E. languages e.g. the property of being context-free in the set of all CFLs. the empty in the set {∅} consisting of only ∅

A property in trivial if either all or no R.E. language has it.

⇒ P is non-trivial if at least one R.E. language has P and does not have P

Note: e T.M. cannot recognize a property (i.e. a set of languages) by taking as an input string a language, because a language is typically infinite.

⇒ we consider instead a property P on the language of the codes of those T.M.s that accept a language that satisfies P

\[ L_P = \{ E(M) \mid L(M) \text{ has property } P \} \]

**Rice's Theorem:** every non-trivial property of R.E. languages is undecidable.

Proof: let P be a non-trivial property of R.E. languages.

Assume ∅ does not have P (otherwise, we can work with P′)
Since \( L \) is non-trivial, there is some \( L_0 \subseteq \Sigma^* \) with 
\[ L_1 \neq \emptyset. \]
Let \( M_1 \) be s.t. \( L(M_1) = L_1 \Rightarrow \emptyset(M_1) \in L_0 \).

We show that \( L_n < L_\emptyset \):

Reduction \( R \) is an algorithm that:
- takes as input a pair \( \langle M, w \rangle \) considered as instance of \( L_n \).
- produces a code \( E(M_2) \) for \( \emptyset(M) \).
- s.t. \( \langle M, w \rangle \in L_n \Rightarrow E(M_2) \in L_\emptyset \).

Define for \( M_2 \):

- \( M_2 \) ignores first its own input \( x \), and writes \( w \) on step 1.
- simulates \( M \) on \( w \) using an UTM (on step 2).
- if \( M \) accepts \( w \), \( M_2 \) starts simulating \( M_1 \) on \( x \)
  and accepts if \( M_1 \) accepts \( x \).
- if \( M \) rejects \( w \) or does not halt, \( M_2 \) does the same.

Note: since \( R \) takes as input \( \langle E(M), w \rangle \), it can
 handshake \( w \) into \( M_2 \).

We get that:
\[ w \in L(M) \Rightarrow L(M_2) = L(M_1) \Rightarrow \emptyset(M_2) \in L_0 \]
\[ w \notin L(M) \Rightarrow L(M_2) = \emptyset \Rightarrow \emptyset(M_2) \notin L_\emptyset \]
\[ \Rightarrow \langle E(M), w \rangle \in L_n \Rightarrow w \in L(M) \Rightarrow \emptyset(M_2) \in L_\emptyset \]
\[ \Rightarrow R \text{ reduces } L_n \text{ to } L_\emptyset \Rightarrow L_\emptyset \text{ is undecidable} \text{ q.e.d.} \]