Reductions, Halting Problem

Peter Mayr

Computability Theory, September 20, 2023

Recall

- $[M]$ denotes the encoding of the DTM M.
- The **self acceptance problem**

  $$\mathrm{SAP} := \{[M] \ : \ M \text{ is a DTM that accepts } [M]\}$$

  is c.e. but its complement $\overline{\mathrm{SAP}}$ is not c.e. by a diagonalization argument.
- Hence SAP is not computable.

Question

The **acceptance problem**

$$\mathsf{AP} := \{([M], x) \ : \ M \text{ is a DTM}, x \in \Sigma^*, M \text{ accepts } x\}$$

is c.e. Is it computable?

Piggy-backing

Using that SAP is not computable, we can show that AP is neither.

Theorem

AP is not computable.

Proof.

Seeking a contradiction, suppose U is a **halting** DTM with $L(U) = \mathrm{AP}$. Note

$$[M] \in \mathrm{SAP} \quad \text{iff} \quad ([M],[M]) \in \mathrm{AP}.$$

Hence SAP is computable by the following DTM U':

- On input x run U on (x, x).
- If U accepts (x, x), then U' accepts.
- If U rejects (x, x), then U' rejects (in particular if x is not TM-code).

Since U is halting, so is U'. Contradiction. $\square$

Many-one reductions

Definition

Let $A, B \subseteq \Sigma^*$. A **many-one*** **reduction** from A to B is a computable function $f : \Sigma^* \to \Sigma^*$ such that

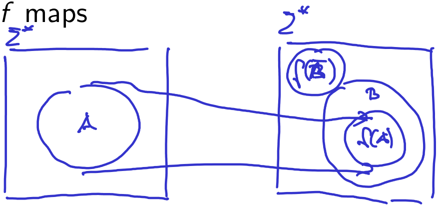
* not necessarily injective

$$\forall x \in \Sigma^* :\ x \in A \text{ iff } f(x) \in B.$$

If a many-one reduction from A to B exists, A is **many-one reducible** to B (short $A \leq_m B$).

A many-one reduction f maps

- A to B and
- $\bar{A}$ to $\bar{B}$.



Example

$\mathrm{SAP} \leq_m \mathrm{AP}$ via $x \mapsto (x, x)$

Hard problems don't reduce to easy ones

Theorem

Assume $A \leq_m B$.
If B is computable, c.e., co-c.e., respectively, then so is A.

(Often used in its contrapositive form.)

Proof.

HW $\square$

Note

- $A \leq_m B$ iff $\overline{A} \leq_m \overline{B}$.
- $\leq_m$ is transitive.
- Outlook: Polytime-, logspace- ... reductions are many-one reductions computable with restricted resources.

Halting Problem

The **halting problem** is

$$\mathrm{HP} := \{([M], x) \ : \ M \text{ is a DTM}, x \in \Sigma^*, M \text{ halts on } x\}.$$

Theorem

HP is c.e. but not computable.

Proof.

Show $\mathrm{HP} \leq_m \mathrm{AP}$ and $\mathrm{AP} \leq_m \mathrm{HP}$ (HW). $\square$

Properties of c.e. languages

- A **property** S of c.e. languages is a set of c.e. languages.

  Ex. property finite = set of finite languages
- S is **trivial** if $S = \emptyset$ (*satisfied by no language*) or

  $S =$ set of all c.e. languages.

Rice's Theorem (1951)

Let S be a non-trivial property of c.e. languages. Then

$$P_S := \{[M] \ : \ M \text{ is a DTM with } L(M) \in S\}$$

is not computable.

In short: No nontrivial property is computable.

Proof.

Wlog

- $\emptyset \notin S$ (else consider $\bar{S}$).
- Fix DTM N such that $L(N) \in S$ (possible since $S \neq \emptyset$).

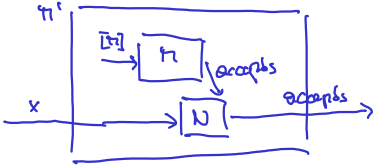
Claim: $\mathrm{SAP} \leq_m P_S$

$\{0,1\}^* \to \{0,1\}^*$

- Need computable $f : [M] \mapsto [M']$ such that

$$[M] \in L(M) \text{ iff } L(M') \in S \qquad (\dagger)$$

  (and non-TM codes are mapped to, say, 0).
- M' does the following on input x:
  1. Run M on input $[M]$. If M rejects, then M' rejects.
  2. Else if M accepts, run N on x. If N accepts x, then M' accepts.



- Then
$$L(M') = \begin{cases} \overset{\in S}{L(N)} & \text{if } [M] \in L(M), \\ \underset{\notin S}{\emptyset} & \text{else.} \end{cases}$$
  Hence (†) holds.
- Note that $[M']$ is computable from $[M], [N]$ and $[U]$ for a universal DTM U. $\square$

Note

The proof of Rice's Theorem for a non-trivial property S yields:

- if $\emptyset \notin S$, then $\overline{P_S}$ is not c.e;
- if $\emptyset \in S$, then P_S is not c.e.

Nothing can be decided

By Rice's Theorem no non-trivial property of c.e. languages (DTMs) is computable, in particular:

- Emptiness: Is $L(M) = \emptyset$?
- Universality: Is $L(M) = \Sigma^*$?
- Finiteness: Is $L(M)$ finite?
- Regularity: Is $L(M)$ regular?
- Computabilty: Is $L(M)$ computable?
- Equality: Is $L(M_1) = L(M_2)$? even for fixed M_2
- Inclusion: Is $L(M_1) \subseteq L(M_2)$?

Question

Which of these (or their complements) are c.e?