

# COMP30026 Models of Computation

## Reducibility

Harald Søndergaard

Lecture 23

Semester 2, 2020

# This Lecture is Being Recorded



# Undecidable Languages

In the last lecture we saw that

$$A_{TM} = \{ \langle M, w \rangle \mid M \text{ is a TM and } M \text{ accepts } w \}$$

is undecidable.

Tute exercise 100 asks you to prove that it follows that

$$Halt_{TM} = \left\{ \langle M, w \rangle \mid \begin{array}{l} M \text{ is a Turing machine and} \\ M \text{ halts when run on input } w \end{array} \right\}$$

is also undecidable.

# At Least $A_{TM}$ Is Recognisable

Note that

$$A_{TM} = \{ \langle M, w \rangle \mid M \text{ is a TM and } M \text{ accepts } w \}$$

is Turing recognisable.

The reason is that it is possible to construct a **universal** Turing machine  $U$  which is able to simulate any Turing machine.

On input  $\langle M, w \rangle$ ,  $U$  simulates  $M$  on input  $w$ .

If  $M$  enters its accept state,  $U$  accepts.

If  $M$  enters its reject state,  $U$  rejects.

If  $M$  never halts, neither does  $U$ .

# Hilbert's Tenth Problem Revisited

The same goes for the undecidable language

$$\{p \mid p \text{ is a polynomial with integral root}\}$$

This language does have a recogniser.

If the input polynomial  $p$  has  $k$  variables  $x_1, \dots, x_k$  then we can simply enumerate all integer  $k$ -tuples  $(v_1, \dots, v_k)$  and evaluate  $p(v_1, \dots, v_k)$ , one by one. If  $p(v_1, \dots, v_k) = 0$ , accept.

We refer to this type of problem as **semi-decidable**.

# Closure Properties

The set of Turing recognisable languages is closed under the regular operations, and intersection. It is not closed under complement.

The set of decidable languages is closed under the same operations, and also under complement.

Tute exercises 102–105 explore some of these closure results in more detail.

# Relating Decidability and Recognisability

**Theorem:** A language  $L$  is decidable iff both  $L$  and its complement  $L^c$  are Turing recognisable.

**Proof:** If  $L$  is decidable, clearly  $L$  and also  $L^c$  are recognisable.

Assume both  $L$  and  $L^c$  are recognisable. That is, there are recognisers  $M_1$  and  $M_2$  for  $L$  and  $L^c$ , respectively.

A Turing machine  $M$  can then take input  $w$  and run  $M_1$  and  $M_2$  on  $w$  in parallel. If  $M_1$  accepts, so does  $M$ . If  $M_2$  accepts,  $M$  rejects.

Note that at least one of  $M_1$  and  $M_2$  is guaranteed to accept.

Hence  $M$  decides  $L$ .

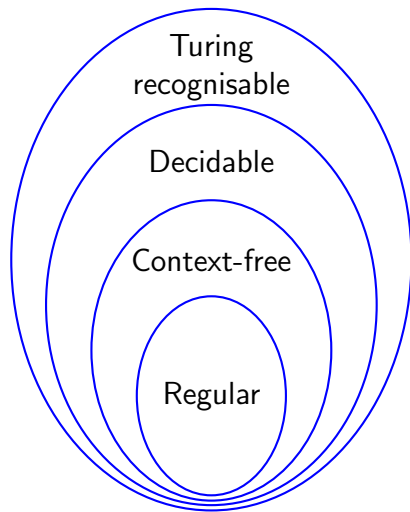
# A Non-Turing Recognisable Language

This gives us an example of a language which is not Turing recognisable:  $(A_{TM})^c$ , that is, the complement of  $A_{TM}$ .

Namely, we know that  $A_{TM}$  is recognisable.

If  $(A_{TM})^c$  was also Turing recognisable,  $A_{TM}$  would be decidable.

But we have shown that it isn't.





# Too Many Languages

As we have seen, the set  $\{0, 1\}^*$  of finite binary strings is a countable set.

Tute exercise 106 asks you to show that the set  $\mathcal{B}$  of all **infinite** binary strings is **uncountable**.

That is interesting, because it follows that the set of all languages over any finite non-empty alphabet  $\Sigma$  is also uncountable.

Namely, the set of all languages over  $\Sigma$  is in a one-to-one correspondence with  $\mathcal{B}$ , as we now show.

# Too Many Languages

Let  $s_1, s_2, s_3, \dots$  be the standard enumeration of  $\Sigma^*$ .

For each language  $A$  over  $\Sigma$ , there is a unique **characteristic sequence**  $\chi_A \in \mathcal{B}$ , whose  $i$ th bit is 1 iff  $s_i \in A$ :

$$\begin{array}{lcl} \Sigma^* : & \{ & \epsilon, a, b, aa, ab, ba, bb, aaa, aab, \dots \} \\ A : & \{ & a, aa, ab, \quad \quad \quad aaa, \quad \quad \dots \} \\ \chi_A : & 0 & 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad \dots \end{array}$$

Hence we cannot put the set of all languages into a one-to-one correspondence with the set of all Turing machines.

That is, we could never hope to have a recogniser for each possible language.

# Reducibility

Let  $P$  and  $P'$  be decision problems with instances  $p_i$  and  $p'_i$ .

$P$  can be **reduced** to  $P'$  iff there is a Turing machine  $M$ :

$$\langle p_i \rangle \longrightarrow \boxed{M} \longrightarrow \langle p'_i \rangle$$

such that  $answer(p_i)$  can be obtained from  $answer(p'_i)$ .

- $P$  reducible to  $P'$  and  $P'$  decidable  $\Rightarrow P$  decidable.
- $P$  reducible to  $P'$  and  $P$  undecidable  $\Rightarrow P'$  undecidable.

So reducibility is useful for proving decidability **and** undecidability results.

# TM Emptiness Is Undecidable

## Theorem:

$$E_{TM} = \{\langle M \rangle \mid M \text{ is a TM and } L(M) = \emptyset\}$$

is undecidable.

**Proof:**  $A_{TM}$  is reducible to  $E_{TM}$ . First notice that, given  $\langle M, w \rangle$ , a Turing machine can modify the encoding of  $M$ , so as to turn  $M$  into  $M'$  which recognises  $L(M) \cap \{w\}$ .

Here is what the new machine  $M'$  does:

- 1 If input  $x$  is not  $w$ , **reject**.
- 2 Otherwise run  $M$  on  $w$  and **accept** if  $M$  does.

# TM Emptiness Is Undecidable

Notice how  $w$  has been “hard-wired” into  $M'$ : This machine is like  $M$ , but it has extra states added to perform the test against  $w$ .

Also note that

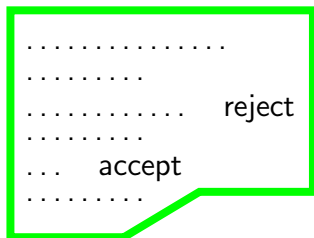
$$L(M') = \begin{cases} \{w\} & \text{if } M \text{ accepts } w \\ \emptyset & \text{otherwise} \end{cases}$$

Here then is a decider for  $A_{TM}$ , using a decider  $R$  for  $E_{TM}$ :

- 1 From input  $\langle M, w \rangle$  construct  $\langle M' \rangle$ .
- 2 Run  $R$  on  $\langle M' \rangle$ .
- 3 If  $R$  rejects, **accept**; if it accepts, **reject**.

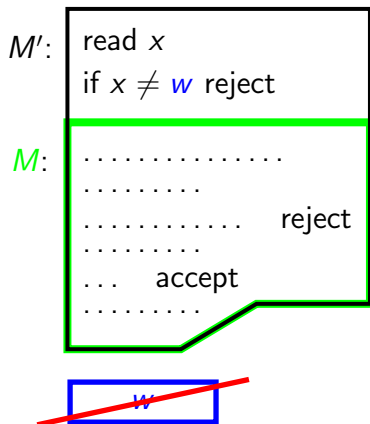
# The Argument in Pictures

$M$ :

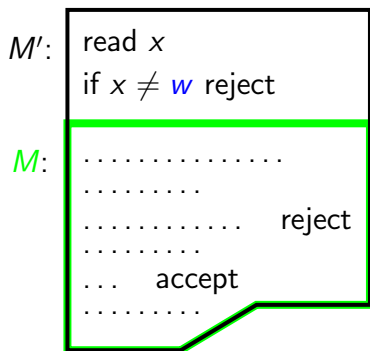


$w$

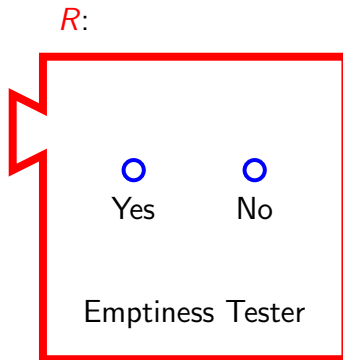
# The Argument in Pictures



# The Argument in Pictures

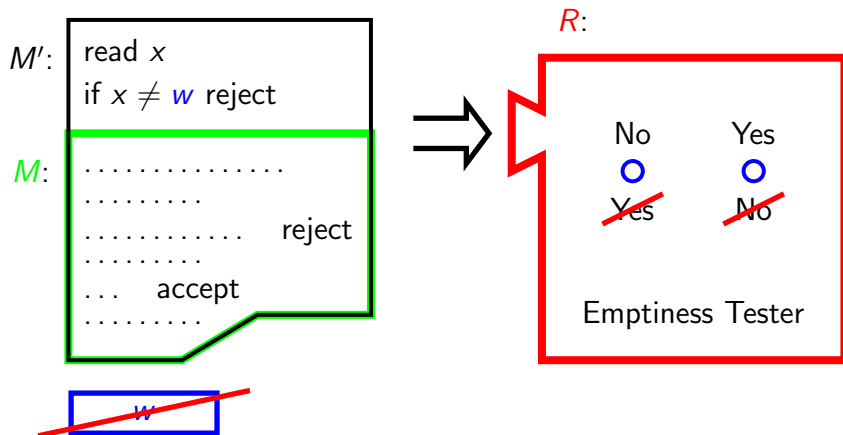


~~$w$~~





# The Argument in Pictures



# TM Equivalence Is Undecidable

## Theorem:

$$EQ_{TM} = \{ \langle M_1, M_2 \rangle \mid M_1, M_2 \text{ are TMs and } L(M_1) = L(M_2) \}$$

is undecidable.

**Proof:**  $E_{TM}$  is reducible to  $EQ_{TM}$ .

Assume that  $S$  decides  $EQ_{TM}$ . Here is a decider for  $E_{TM}$ :

- 1 Input is  $\langle M \rangle$ .
- 2 Construct a Turing machine  $M_\emptyset$  which rejects all input.
- 3 Run  $S$  on  $\langle \langle M \rangle, \langle M_\emptyset \rangle \rangle$ .
- 4 If  $S$  accepts, **accept**; if it rejects, **reject**.

But we know that  $E_{TM}$  is undecidable. So  $EQ_{TM}$  is undecidable.

# Valid and Invalid Computations

Recall how we captured a Turing machine **configuration** as a string (such as  $baq_5bb$ ).

A **valid computation** for Turing machine  $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r \rangle$  (on input  $w$ ) is a string of form

$$C_1 \# C_2 \# \cdots \# C_k \#$$

where

- 1  $C_1$  is  $M$ 's start configuration,
- 2  $C_k$  is an accepting configuration,
- 3 for each **even**  $i \in \{2, \dots, k\}$ ,  $C_{i-1} \Rightarrow C_i^{\mathcal{R}}$
- 4 for each **odd**  $i \in \{2, \dots, k\}$ ,  $(C_{i-1})^{\mathcal{R}} \Rightarrow C_i$

A string (over the same alphabet) which is not a valid computation is an **invalid** computation.

# The Language of Invalid Computations

Rephrasing: A string  $w$  is an **invalid** computation iff one or more of the following properties hold:

- ①  $w$  is **not** of the form  $C_1 \# \cdots \# C_k \#$  with  $C_i$  in  $\Gamma^* Q \Gamma^*$ .
- ②  $C_1$  is **not** a start configuration for  $M$ , that is, not in  $q_0 \Sigma^*$ .
- ③  $C_k$  is **not** accepting, that is, not in  $\Gamma^* q_a \Gamma^*$ .
- ④  $C_{i-1} \not\Rightarrow^{\mathcal{R}} C_i$  for some even  $i$ .
- ⑤  $(C_{i-1})^{\mathcal{R}} \not\Rightarrow C_i$  for some odd  $i$ .

The set of strings satisfying (0)–(2) are regular languages.

We claim the set of strings satisfying (3) is context-free (and so is the set satisfying (4)).

# The Language of Invalid Computations

Here is how to build a PDA  $P$  for the set of strings for which  $C_{i-1} \Rightarrow C_i^{\mathcal{R}}$  is false for some even  $i$ .

- 1  $P$  non-deterministically skips past an even number of  $\#$  symbols.
- 2 While reading through  $C_{i-1}$ ,  $P$  pushes onto its stack the symbols of the configuration  $C$  obtained by  $C_{i-1} \Rightarrow C$ .
- 3 After skipping the next  $\#$ ,  $P$  compares  $C$  (backwards) against the string found until the following  $\#$ ; if they are different,  $P$  scans over the remaining input and accepts.

Conclusion: The language of invalid computations is context-free!

# CFG Exhaustiveness is Undecidable

## Theorem:

$$ALL_{CFG} = \{\langle G \rangle \mid G \text{ is a CFG and } L(G) = \Sigma^*\}$$

is undecidable.

**Proof:** We just saw that, for any Turing machine  $M$ , we can construct a CFG  $G$  that generates all the **invalid computations** for  $M$ .

Clearly  $L(G) = \Sigma^*$  iff  $L(M) = \emptyset$ .

Hence if  $ALL_{CFG}$  is decidable, then so is  $E_{TM}$ .

Since we proved the latter undecidable,  $ALL_{CFG}$  must be undecidable as well.

# CFG Equivalence is Undecidable

Our final language undecidability result is an easy reduction from  $ALL_{CFG}$ .

**Theorem:**

$$EQ_{CFG} = \{\langle G, G' \rangle \mid G, G' \text{ are CFGs and } L(G) = L(G')\}$$

is undecidable.

**Proof:** Assume we have a decider  $E$  for  $EQ_{CFG}$ . Then we can easily build a decider for  $ALL_{CFG}$ . Namely, given input grammar  $G$  over alphabet  $\Sigma$ , construct a CFG  $G_{all}$  for  $\Sigma^*$ . Then run  $E$  on  $\langle G, G_{all} \rangle$ .

# Undecidability in Logic

As we have seen, validity in **propositional** logic is decidable.

Validity in first-order **predicate** logic is undecidable.

However, it is not the quantifiers *per se* that cause that problem. We cross the boundary to the undecidable only when the quantifiers appear together with predicates of arity greater than 1.

**Monadic** logic, that is, the fragment of predicate logic which does not allow predicates of arity 2 and above **is** decidable.



# Rice's Theorem

We have this rather sweeping result:

**Rice's Theorem:** Every interesting semantic Turing machine property is undecidable!

A property  $P$  is **interesting** iff

$$P(M_1) \text{ and not } P(M_2)$$

for some Turing machines  $M_1$  and  $M_2$ .

It is **semantic** iff

$$P(M_1) \text{ iff } P(M_2)$$

for all Turing machines  $M_1$  and  $M_2$  such that  $L(M_1) = L(M_2)$ .