



# Mathematical Foundation of Computer Sciences III

Turing Machine

Guoqiang Li  
School of Software



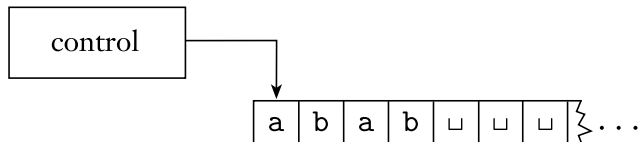
SHANGHAI JIAO TONG  
UNIVERSITY

# Turing Machine

Alan Turing in 1936 proposed Turing machines  $M$ :

- $M$  uses an infinite tape as its unlimited memory, with a tape head reading and writing symbols and moving around on the tape. The tape initially contains only the input string and is blank everywhere else.
- If  $M$  needs to store information, it may write this information on the tape. To read the information that it has written,  $M$  can move its head back over it.
- $M$  continues computing until it decides to produce an output. The outputs accept and reject are obtained by entering designated accepting and rejecting states.
- If  $M$  doesn't enter an accepting or a rejecting state, it will go on forever, never halting.

# Schematic of a Turing machine



# The difference between finite automata and Turing machines



- 1 A Turing machine can both write on the tape and read from it.
- 2 The read-write head can move both to the left and to the right.
- 3 The tape is infinite.
- 4 The special states for rejecting and accepting take effect immediately.



$$B = \{w\#w \mid w \in \{0,1\}^*\}$$

$M_1$  on input string  $w$ :

- 1 Zig-zag across the tape to corresponding positions on either side of the  $\#$  symbol to check whether these positions contain the same symbol. If they do not, or if no  $\#$  is found, reject. Cross off symbols as they are checked to keep track of which symbols correspond.
- 2 When all symbols to the left of the  $\#$  have been crossed off, check for any remaining symbols to the right of the  $\#$ . If any symbols remain, reject; otherwise, accept.

$$B = \{w\#w \mid w \in \{0,1\}^*\}$$



```

      ↓
0 1 1 0 0 0 # 0 1 1 0 0 0 □ ...
      ↓
x 1 1 0 0 0 # 0 1 1 0 0 0 □ ...
      ↓
x 1 1 0 0 0 # x 1 1 0 0 0 □ ...
      ↓
x 1 1 0 0 0 # x 1 1 0 0 0 □ ...
      ↓
x x 1 0 0 0 # x 1 1 0 0 0 □ ...
      ↓
x x x x x x # x x x x x x □ ...
                                ↓
                                accept
  
```

# Formal definition of a Turing machine



## Definition

A **Turing machine** is a 7-tuple,  $(Q, \Sigma, \Gamma, \delta, q_0, q_{accept}, q_{reject})$ , where  $Q, \Sigma, \Gamma$  are all finite and

- $Q$  is set of states,
- $\Sigma$  is the input alphabet **not** containing the **blank symbol**  $\sqcup$ ,
- $\Gamma$  is the tape alphabet, where  $\sqcup \in \Gamma$  and  $\Sigma \subseteq \Gamma$ ,
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$  is the transition function,
- $q_0 \in Q$  is the start state,
- $q_{accept} \in Q$  is the accept state, and
- $q_{reject} \in Q$  is the reject state, where  $q_{reject} \neq q_{accept}$ .





Initially,  $M$  receives its input  $w = w_1w_2 \dots w_n \in \Sigma^*$  on the leftmost  $n$  squares of the tape, and the rest of the tape is blank (i.e., filled  $\sqcup$ ).

The head starts on the leftmost square of the tape.

As  $\Sigma$  does not contain  $\sqcup$ , so the first blank appearing on the tape marks the end of the input.

Once  $M$  has started, the computation proceeds according to the rules described by the transition function.

If  $M$  ever tries to move its head to the left off the left-hand end of the tape, the head stays in the same place for that move, even though the transition function indicates  $L$ .

The computation continues until it enters either the accept or reject states, at which point it halts. If neither occurs,  $M$  goes on forever.

# Configurations



A **configuration** of a Turing machine consists of

- the current **state**,
- the current **tape contents**, and
- the current **head location**.

# Configurations



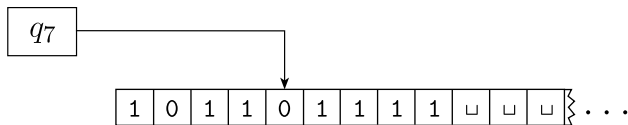
A **configuration** of a Turing machine consists of

- the current **state**,
- the current **tape contents**, and
- the current **head location**.

By  $uqv$  we mean the configuration where

- the current state is  $q$ ,
- the current tape contents is  $uv$ , and
- the current head location is the first symbol of  $v$ .
- The tape contains only blanks following the last symbol of  $v$ .

# Configurations



A Turing machine with configuration  $1011q_701111$

# Formal definition of computation



Let  $a, b, c \in \Gamma$ ,  $u, v \in \Gamma^*$ , and  $q_i, q_j \in Q$ .

① If  $\delta(q_i, b) = (q_j, c, L)$ , then

$ua q_i bv$  yields  $u q_j acv$

.

② If  $\delta(q_i, b) = (q_j, c, R)$ , then

$ua q_i bv$  yields  $uac q_j v$

.

## Formal definition of computation

Let  $a, b, c \in \Gamma$ ,  $u, v \in \Gamma^*$ , and  $q_i, q_j \in Q$ .

- ① If  $\delta(q_i, b) = (q_j, c, L)$ , then

$ua q_i bv$  yields  $u q_j acv$

- ② If  $\delta(q_i, b) = (q_j, c, R)$ , then

$ua q_i bv$  yields  $uac q_j v$

Special cases occur when the head is at one of the ends of the configuration:

- ① For the left-hand end, the configuration  $q_i bv$  yields  $q_j cv$  if the transition is left moving (because we prevent the machine from going off the left-hand end of the tape), and it yields  $c q_j v$  for the right-moving transition.
- ② For the right-hand end, the configuration  $ua q_i$  is equivalent to  $ua q_i \sqcup$  because we assume that blanks follow the part of the tape represented in the configuration.

# Special configurations



The **start configuration** of  $M$  on input  $w$  is the configuration  $q_0 w$ .

In an **accepting configuration**, the state of the configuration is  $q_{accept}$ .

In a **rejecting configuration**, the state of the configuration is  $q_{reject}$ .

Accepting and rejecting configurations are **halting configurations** and do not yield further configurations.

# Formal definition of computation



$M$  accepts  $w$  if there are sequence of configurations  $C_1, C_2, \dots, C_k$  such that

- $C_1$  the **start configuration** of  $M$  on  $w$ .
- Each  $C_i$  yields  $C_{i+1}$ , and
- $C_k$  is an **accepting configuration**.



# Formal definition of computation



$M$  accepts  $w$  if there are sequence of configurations  $C_1, C_2, \dots, C_k$  such that

- $C_1$  the start configuration of  $M$  on  $w$ .
- Each  $C_i$  yields  $C_{i+1}$ , and
- $C_k$  is an accepting configuration.

The collection of strings that  $M$  accepts is the language of  $M$ , or the language recognized by  $M$ , denoted  $L(M)$ .

# Turing-recognizable languages



## Definition

A language is **Turing-recognizable**, if some Turing machine recognizes it.

# Turing-decidable languages

On an input, the machine  $M$  may **accept**, **reject**, or **loop**. By **loop** we mean that the machine simply does not halt.

# Turing-decidable languages

On an input, the machine  $M$  may **accept**, **reject**, or **loop**. By **loop** we mean that the machine simply does not halt.

If  $M$  always halts, then it is a **decider**. A **decider** that recognizes some language is said to decide that language.

# Turing-decidable languages

On an input, the machine  $M$  may **accept**, **reject**, or **loop**. By **loop** we mean that the machine simply does not halt.

If  $M$  always halts, then it is a **decider**. A **decider** that recognizes some language is said to decide that language.

## Definition

A language is Turing-decidable or simply decidable if some Turing machine decides it.

**Example:**  $A = \{0^{2^n} \mid n \geq 0\}$

On input string  $w$ :

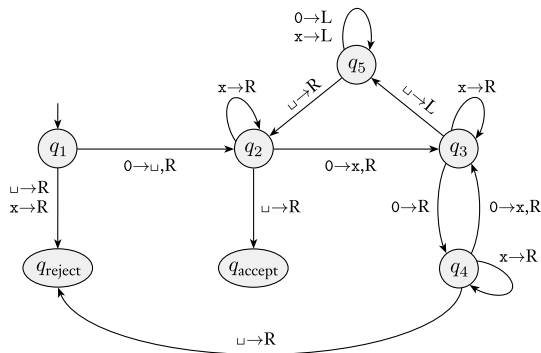
- 1 Sweep left to right across the tape, crossing off every other 0.
- 2 If in stage 1 the tape contained a single 0, accept.
- 3 If in stage 1 the tape contained more than a single 0 and the number of 0s was odd, reject.
- 4 Return the head to the left-hand end of the tape.
- 5 Go to stage 1.

**Example:**  $A = \{0^{2^n} \mid n \geq 0\}$

$Q = \{q_1, q_2, q_3, q_4, q_5, q_{accept}, q_{reject}\}$ , where  $q_1$  is the start state.

$\Sigma = \{0\}$  and  $\Gamma = \{0, x, \sqcup\}$ .

The transition function  $\delta$ :



## Example

 $q_1 0000$  $\sqcup q_2 000$  $\sqcup x q_3 00$  $\sqcup x0q_40$ 
$$\Box x \Box x q_3 \Box$$
$$\Box x \Box q_5 x \Box$$
$$\Box x q_5 0 x \Box$$
$$\sqcup q_5 x 0 x \sqcup$$
$$q_5 \sqcup x 0 x \sqcup$$
$$\sqcup q_2 x 0 x \sqcup$$
$$\Box x q_2 0 x \Box$$
 $\sqcup \mathbf{X} \mathbf{X} q_3 \mathbf{X} \sqcup$  $\sqcup \mathbf{XXX}q_3 \sqcup$  $\sqcup \mathbf{X} \mathbf{X} q_5 \mathbf{X} \sqcup$  $\sqcup x q_5 x x \sqcup$  $\sqcup q_5 \mathbf{XXX} \sqcup$  $q_5 \sqcup \mathbf{XXX} \sqcup$  $\sqcup q_2 \mathbf{xxx} \sqcup$ 
$$\sqcup \mathbf{x} q_2 \mathbf{x} \mathbf{x} \sqcup$$
$$\sqcup \mathbf{X} \mathbf{X} q_2 \mathbf{X} \sqcup$$
 $\sqcup \mathbf{XXX} q_2 \sqcup$  $\sqcup \mathbf{XXX} \sqcup q_{\text{accept}}$



**Example:**  $B = \{w\#w \mid w \in \{0,1\}^*\}$



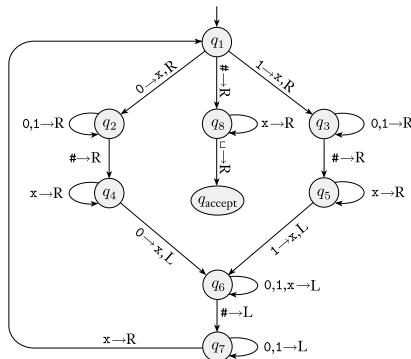


**Example:**  $B = \{w\#w \mid w \in \{0, 1\}^*\}$

$Q = \{q_1, q_2, \dots, q_8, q_{\text{accept}}, q_{\text{reject}}\}$ , where  $q_1$  is the start state.

$\Sigma = \{0, 1, \#\}$  and  $\Gamma = \{0, 1, \#, x, \sqcup\}$ .

The transition function  $\delta$ :



$$B = \{w\#w \mid w \in \{0,1\}^*\}$$



```

      ↓
0 1 1 0 0 0 # 0 1 1 0 0 0 □ ...
      ↓
x 1 1 0 0 0 # 0 1 1 0 0 0 □ ...
      ↓
x 1 1 0 0 0 # x 1 1 0 0 0 □ ...
      ↓
x 1 1 0 0 0 # x 1 1 0 0 0 □ ...
      ↓
x x 1 0 0 0 # x 1 1 0 0 0 □ ...
      ↓
x x x x x x # x x x x x x □ ...
                                ↓
                                accept
  
```

**Example:**  $C = \{a^i b^j c^k \mid i, j, k \geq 1 \text{ and } i \times j = k\}$



**Example:**  $C = \{a^i b^j c^k \mid i, j, k \geq 1 \text{ and } i \times j = k\}$

On input string  $w$ :

- 1 Scan the input from left to right to determine whether it is a member of  $a^+ b^+ c^+$  and reject if it is not.

**Example:**  $C = \{a^i b^j c^k \mid i, j, k \geq 1 \text{ and } i \times j = k\}$

On input string  $w$ :

- 1 Scan the input from left to right to determine whether it is a member of  $a^+ b^+ c^+$  and reject if it is not.
- 2 Return the head to the left-hand end of the tape.

**Example:**  $C = \{a^i b^j c^k \mid i, j, k \geq 1 \text{ and } i \times j = k\}$

On input string  $w$ :

- 1 Scan the input from left to right to determine whether it is a member of  $a^+ b^+ c^+$  and reject if it is not.
- 2 Return the head to the left-hand end of the tape.
- 3 Cross off an  $a$  and scan to the right until a  $b$  occurs. Shuttle between the  $b$ 's and the  $c$ 's, crossing off one of each until all  $b$ 's are gone. If all  $c$ 's have been crossed off and some  $b$ 's remain, **reject**.

**Example:**  $C = \{a^i b^j c^k \mid i, j, k \geq 1 \text{ and } i \times j = k\}$

On input string  $w$ :

- 1 Scan the input from left to right to determine whether it is a member of  $a^+ b^+ c^+$  and reject if it is not.
- 2 Return the head to the left-hand end of the tape.
- 3 Cross off an  $a$  and scan to the right until a  $b$  occurs. Shuttle between the  $b$ 's and the  $c$ 's, crossing off one of each until all  $b$ 's are gone. If all  $c$ 's have been crossed off and some  $b$ 's remain, **reject**.
- 4 Restore the crossed off  $b$ 's and repeat stage 3 if there is another  $a$  to cross off. If all  $a$ 's have been crossed off, determine whether all  $c$ 's also have been crossed off. If yes, **accept**; otherwise, **reject**.



**Example:**  $E = \{\#x_1\#\dots\#x_\ell \mid \text{each } x_i \in \{0,1\}^* \text{ and } x_i \neq x_j \text{ for each } i \neq j\}$



**Example:**  $E = \{\#x_1\#\dots\#x_\ell \mid \text{each } x_i \in \{0,1\}^* \text{ and } x_i \neq x_j \text{ for each } i \neq j\}$



On input string  $w$ :

- 1 Place a mark on top of the leftmost tape symbol. If that symbol was a blank, **accept**. If that symbol was a  $\#$ , continue with the next stage. Otherwise, **reject**.

**Example:**  $E = \{\#x_1\#\dots\#x_\ell \mid \text{each } x_i \in \{0,1\}^* \text{ and } x_i \neq x_j \text{ for each } i \neq j\}$



On input string  $w$ :

- 1 Place a mark on top of the leftmost tape symbol. If that symbol was a blank, **accept**. If that symbol was a  $\#$ , continue with the next stage. Otherwise, **reject**.
- 2 Scan right to the next  $\#$  and place a second mark on top of it. If no  $\#$  is encountered before a blank symbol, only  $x_1$  was present, so **accept**.

**Example:**  $E = \{\#x_1\#\dots\#x_\ell \mid \text{each } x_i \in \{0,1\}^* \text{ and } x_i \neq x_j \text{ for each } i \neq j\}$



On input string  $w$ :

- 1 Place a mark on top of the leftmost tape symbol. If that symbol was a blank, **accept**. If that symbol was a  $\#$ , continue with the next stage. Otherwise, **reject**.
- 2 Scan right to the next  $\#$  and place a second mark on top of it. If no  $\#$  is encountered before a blank symbol, only  $x_1$  was present, so **accept**.
- 3 By **zig-zagging**, compare the two strings to the right of the marked  $\#$ s. If they are equal, **reject**.



**Example:**  $E = \{\#x_1\#\dots\#x_\ell \mid \text{each } x_i \in \{0,1\}^* \text{ and } x_i \neq x_j \text{ for each } i \neq j\}$

On input string  $w$ :

- 1 Place a mark on top of the leftmost tape symbol. If that symbol was a blank, **accept**. If that symbol was a  $\#$ , continue with the next stage. Otherwise, **reject**.
- 2 Scan right to the next  $\#$  and place a second mark on top of it. If no  $\#$  is encountered before a blank symbol, only  $x_1$  was present, so **accept**.
- 3 By **zig-zagging**, compare the two strings to the right of the marked  $\#$ s. If they are equal, **reject**.
- 4 Move the rightmost of the two marks to the next  $\#$  symbol to the right. If no  $\#$  symbol is encountered before a blank symbol, move the leftmost mark to the next  $\#$  to its right and the rightmost mark to the  $\#$  after that. This time, if no  $\#$  is available for the rightmost mark, all the strings have been compared, so **accept**.

**Example:**  $E = \{\#x_1\#\dots\#x_\ell \mid \text{each } x_i \in \{0,1\}^* \text{ and } x_i \neq x_j \text{ for each } i \neq j\}$



On input string  $w$ :

- 1 Place a mark on top of the leftmost tape symbol. If that symbol was a blank, **accept**. If that symbol was a  $\#$ , continue with the next stage. Otherwise, **reject**.
- 2 Scan right to the next  $\#$  and place a second mark on top of it. If no  $\#$  is encountered before a blank symbol, only  $x_1$  was present, so **accept**.
- 3 By **zig-zagging**, compare the two strings to the right of the marked  $\#$ s. If they are equal, **reject**.
- 4 Move the rightmost of the two marks to the next  $\#$  symbol to the right. If no  $\#$  symbol is encountered before a blank symbol, move the leftmost mark to the next  $\#$  to its right and the rightmost mark to the  $\#$  after that. This time, if no  $\#$  is available for the rightmost mark, all the strings have been compared, so **accept**.
- 5 Go to stage 3.

Languages  $A$ ,  $B$ ,  $C$ , and  $E$  are decidable.

All decidable languages are Turing-recognizable, so these languages are also Turing-recognizable.

Demonstrating a language that is Turing-recognizable but undecidable is more difficult.

## Variants of Turing Machines



# Multitape Turing machines



A multitape Turing machine  $M$  has several tapes:

- Each tape has its own head for reading and writing.
- The input is initially on tape 1, with all the other tapes being blank.
- The transition function is

$$\delta : Q \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L, R, S\}^k$$

where  $k$  is the number of tapes.

$$\delta(q_i, a_1, \dots, a_k) = (q_j, b_1, \dots, b_k, L, R, \dots, L)$$

means that if  $M$  is in state  $q_i$  and heads 1 through  $k$  are reading symbols  $a_1$  through  $a_k$ , the machine goes to state  $q_j$ , writes symbols  $b_1$  through  $b_k$ , and directs each head to move left or right, or to stay put, as specified.



## Theorem

*Every multitape Turing machine has an equivalent single-tape Turing machine.*

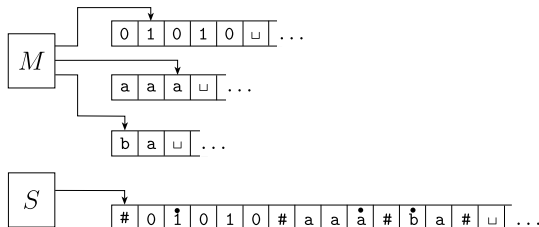
# Proof



We simulate an  $M$  with  $k$  tapes by a single-tape  $S$ .

We simulate an  $M$  with  $k$  tapes by a single-tape  $S$ .

- $S$  uses  $\#$  to separate the contents of the different tapes.
- $S$  keeps track of the locations of the heads by writing a tape symbol with a dot above it to mark the place where the head on that tape would be.



# Proof



On input  $w = w_1 \dots w_n$ :

- 1 First  $S$  puts its tape into the format that represents all  $k$  tapes of  $M$ :

$$\#w_1w_2\dots w_n\#\sqcup\#\sqcup\#\dots\#$$

On input  $w = w_1 \dots w_n$ :

- 1 First  $S$  puts its tape into the format that represents all  $k$  tapes of  $M$ :

$$\#w_1w_2\dots w_n\#\sqcup\#\sqcup\#\dots\#$$

- 2 To determine the symbols under the virtual heads,  $S$  scans its tape from the first  $\#$ , which marks the left-hand end, to the  $k + 1$ st  $\#$ , which marks the right-hand end.

On input  $w = w_1 \dots w_n$ :

- 1 First  $S$  puts its tape into the format that represents all  $k$  tapes of  $M$ :

$$\#w_1w_2\dots w_n\#\sqcup\#\sqcup\#\dots\#$$

- 2 To determine the symbols under the virtual heads,  $S$  scans its tape from the first  $\#$ , which marks the left-hand end, to the  $k + 1$ st  $\#$ , which marks the right-hand end.
- 3 Then  $S$  makes a second pass to update the tapes according to the way that  $M$ s transition function dictates.

On input  $w = w_1 \dots w_n$ :

- 1 First  $S$  puts its tape into the format that represents all  $k$  tapes of  $M$ :

$$\#w_1w_2\dots w_n\#\sqcup\#\sqcup\dots\#$$

- 2 To determine the symbols under the virtual heads,  $S$  scans its tape from the first  $\#$ , which marks the left-hand end, to the  $k + 1$ st  $\#$ , which marks the right-hand end.
- 3 Then  $S$  makes a second pass to update the tapes according to the way that  $M$ 's transition function dictates.
- 4 If  $S$  moves one of the virtual heads to the right onto a  $\#$ , i.e.,  $M$  has moved the corresponding head onto the previously unread blank portion of that tape. So  $S$  writes on this tape cell and shifts the tape contents, from this cell until the rightmost  $\#$ , one unit to the right.



On input  $w = w_1 \dots w_n$ :

- 1 First  $S$  puts its tape into the format that represents all  $k$  tapes of  $M$ :

$$\#w_1w_2\dots w_n\#\sqcup\#\sqcup\dots\#$$

- 2 To determine the symbols under the virtual heads,  $S$  scans its tape from the first  $\#$ , which marks the left-hand end, to the  $k + 1$ st  $\#$ , which marks the right-hand end.
- 3 Then  $S$  makes a second pass to update the tapes according to the way that  $M$ 's transition function dictates.
- 4 If  $S$  moves one of the virtual heads to the right onto a  $\#$ , i.e.,  $M$  has moved the corresponding head onto the previously unread blank portion of that tape. So  $S$  writes on this tape cell and shifts the tape contents, from this cell until the rightmost  $\#$ , one unit to the right.
- 5 Go back to 2.

## Corollary



### Corollary

*A language is Turing-recognizable if and only if some multitape Turing machine recognizes it.*

# Nondeterministic Turing Machines

The **transition function** for a **nondeterministic Turing machine** has the form

$$\delta : Q \times \Gamma \rightarrow \mathcal{P}(Q \times \{L, R\})$$

The **computation** of a nondeterministic Turing machine is a tree whose branches correspond to different possibilities for the machine.

If **some branch of the computation leads to the accept state**, the machine accepts its input.



## Theorem

*Every nondeterministic Turing machine has an equivalent deterministic Turing machine.*

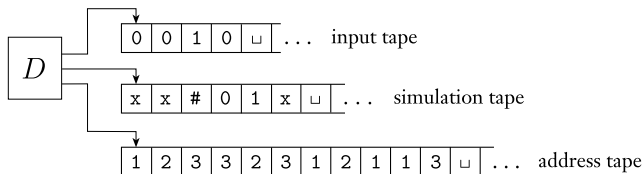
### Proof

SHANGHAI JIAO TONG  
UNIVERSITY

We simulate a nondeterministic  $N$  by a deterministic  $D$ .

We simulate a nondeterministic  $N$  by a deterministic  $D$ .

- $D$  try all possible branches of  $N$ 's nondeterministic computation.
- If  $D$  ever finds the accept state on one of these branches, it accepts.
- Otherwise,  $D$ 's simulation will not terminate.



- 1 Initially, tape 1 contains the input  $w$ , and tapes 2 and 3 are empty.

# Proof



- 1 Initially, tape 1 contains the input  $w$ , and tapes 2 and 3 are empty.
- 2 Copy tape 1 to tape 2 and initialize the string on tape 3 to be  $\epsilon$ .



- ❶ Initially, tape 1 contains the input  $w$ , and tapes 2 and 3 are empty.
- ❷ Copy tape 1 to tape 2 and initialize the string on tape 3 to be  $\epsilon$ .
- ❸ Use tape 2 to simulate  $N$  with input  $w$  on one branch of its nondeterministic computation.
  - ❶ Before each step of  $N$ , consult the next symbol on tape 3 to determine which choice to make among those allowed by  $N$ 's transition function.
  - ❷ If no more symbols remain on tape 3 or if this nondeterministic choice is invalid, abort this branch by going to stage 4.
  - ❸ Also go to stage 4 if a rejecting configuration is encountered. If an accepting configuration is encountered, accept the input.

- ① Initially, tape 1 contains the input  $w$ , and tapes 2 and 3 are empty.
- ② Copy tape 1 to tape 2 and initialize the string on tape 3 to be  $\epsilon$ .
- ③ Use tape 2 to simulate  $N$  with input  $w$  on one branch of its nondeterministic computation.
  - ① Before each step of  $N$ , consult the next symbol on tape 3 to determine which choice to make among those allowed by  $N$ 's transition function.
  - ② If no more symbols remain on tape 3 or if this nondeterministic choice is invalid, abort this branch by going to stage 4.
  - ③ Also go to stage 4 if a rejecting configuration is encountered. If an accepting configuration is encountered, accept the input.
- ④ Replace the string on tape 3 with the next string in the string ordering. Simulate the next branch of  $N$ 's computation by going to stage 2.

# Corollary



## Corollary

*A language is Turing-recognizable if and only if some nondeterministic Turing machine recognizes it.*

## Corollary

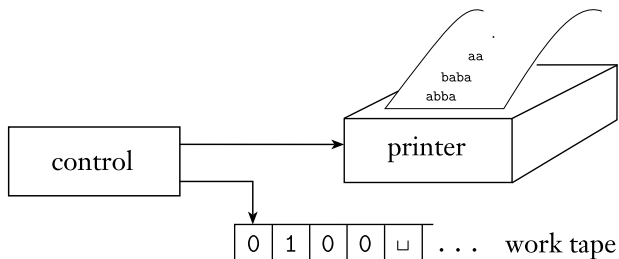
*A language is decidable if and only if some nondeterministic Turing machine decides it.*

An **enumerator** is a Turing machine with an attached printer.

The Turing machine can use that printer as an output device to print strings.

Every time the Turing machine wants to add a string to the list, it sends the string to the printer.

## Schematic of an enumerator





## Theorem

*A language is Turing-recognizable if and only if some enumerator enumerates it.*



Let  $E$  be an enumerator  $E$  that enumerates a language  $A$ . The desired  $M$  on input  $w$ :



Let  $E$  be an enumerator  $E$  that enumerates a language  $A$ . The desired  $M$  on input  $w$ :

- Run  $E$ . Every time that  $E$  outputs a string, compare it with  $w$ .
- If  $w$  ever appears in the output of  $E$ , then accept.





If  $M$  recognizes a language  $A$ , we can construct the following enumerator  $E$  for  $A$ . Let  $s_1, s_2, s_3, \dots$ , be a list of all possible strings in  $\Sigma^*$ .

- ① Repeat the following for  $i = 1, 2, 3, \dots$
- ②     Run  $M$  for  $i$  steps on each input,  $s_1, s_2, \dots, s_i$ .
- ③         If any computations accept, print out the corresponding  $s_j$ .



# Polynomials and their roots



A **polynomial** is a sum of terms, where each term is a product of certain variables and a constant, i.e., **coefficient**. For example,

$$6 \cdot x \cdot x \cdot x \cdot y \cdot z \cdot z = 6x^3yz^2$$

is a term with coefficient 6, and

$$6x^3yz^2 + 3xy^2 - x^3 - 10$$

is a polynomial with four terms, over the variables  $x$ ,  $y$ , and  $z$ .

# Polynomials and their roots

A **polynomial** is a sum of terms, where each term is a product of certain variables and a constant, i.e., **coefficient**. For example,

$$6 \cdot x \cdot x \cdot x \cdot y \cdot z \cdot z = 6x^3yz^2$$

is a term with coefficient 6, and

$$6x^3yz^2 + 3xy^2 - x^3 - 10$$

is a polynomial with four terms, over the variables  $x$ ,  $y$ , and  $z$ .

A **root** of a polynomial is an assignment of values to its variables so that the value of the polynomial is 0.

This root is an **integral root** because all the variables are assigned integer values. Some polynomials have an integral root and some do not.

Hilbert's tenth problem was to devise an algorithm that tests whether a polynomial has an integral root. He did not use the term algorithm but rather

*a process according to which it can be determined by a finite number of operations.*

# Church-Turing Thesis



In 1936 to formalize the definition of an algorithm:

- Alonzo Church proposed  $\lambda$ -calculus;
- Alan Turing proposed Turing machines,

which were shown to be equivalent.

In 1936 to formalize the definition of an algorithm:

- Alonzo Church proposed  $\lambda$ -calculus;
- Alan Turing proposed Turing machines,

which were shown to be equivalent.

So we have the Church-Turing Thesis:

Intuitive notion of algorithms = Turing machine algorithms

# Hilbert's Tenth Problem

$$D = \{p \mid p \text{ is a polynomial with integer coefficients and with an integral root}\}$$



# Hilbert's Tenth Problem

$$D = \{p \mid p \text{ is a polynomial with integer coefficients and with an integral root}\}$$

## Theorem

*(Yuri Matijasevič, Martin Davis, Hilary Putnam, and Julia Robinson, 1970)*

*$D$  is not decidable.*

## A simple variant



$$D_1 = \left\{ p \left| \begin{array}{l} p \text{ is a polynomial on a single variable } x \text{ with integer} \\ \text{coefficients and with an integral root} \end{array} \right. \right\}$$

## A simple variant



$$D_1 = \left\{ p \mid \begin{array}{l} p \text{ is a polynomial on a single variable } x \text{ with integer} \\ \text{coefficients and with an integral root} \end{array} \right\}$$

### Lemma

Both  $D$  and  $D_1$  are Turing-recognizable.

## A simple variant

$$D_1 = \left\{ p \left| \begin{array}{l} p \text{ is a polynomial on a single variable } x \text{ with integer} \\ \text{coefficients and with an integral root} \end{array} \right. \right\}$$

### Lemma

Both  $D$  and  $D_1$  are Turing-recognizable.

*Proof.*

## A simple variant



$$D_1 = \left\{ p \left| \begin{array}{l} p \text{ is a polynomial on a single variable } x \text{ with integer} \\ \text{coefficients and with an integral root} \end{array} \right. \right\}$$

### Lemma

Both  $D$  and  $D_1$  are Turing-recognizable.

*Proof.*

On input  $p(x)$

Evaluate  $p$  with  $x$  set successively to the values  $0, 1, -1, 2, -2, 3, -3, \dots$ . If at any point the polynomial evaluates to  $0$ , then accept.

## A simple variant



### Lemma

Let

$$p(x) = c_1x^n + c_2x^{n-1} + \dots + c_nx + c_{n+1}$$

with  $c_1 \neq 0$  and  $p(x_0) = 0$ . Define

$$c_{\max} = \max\{|c_i|\}_{i \in [n+1]}$$

Then

$$|x_0| < \frac{c_{\max} \cdot (n+1)}{|c_1|}$$

## A simple variant

## Lemma

Let

$$p(x) = c_1x^n + c_2x^{n-1} + \dots + c_nx + c_{n+1}$$

with  $c_1 \neq 0$  and  $p(x_0) = 0$ . Define

$$c_{max} = \max\{|c_i|\}_{i \in [n+1]}$$

*Then*

$$|x_0| < \frac{c_{max} \cdot (n + 1)}{|c_1|}$$

## Corollary

$D_1$  is decidable.

# Relationship among classes of languages

