The Church-Turing Thesis

Huan Long

Shanghai Jiao Tong University

Acknowledgements

Part of the slides comes from a similar course given by Prof. Yijia Chen.

`http://basics.sjtu.edu.cn/~chen/`

Textbook

Introduction to the theory of computation
Michael Sipser, MIT
Third edition, 2012

Outline

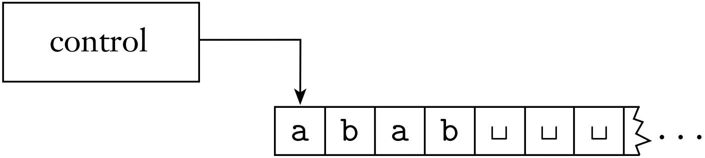
Turing Machines

Turing Machines

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 sting 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.

$B = \{w\#w \mid w \in \{0,1\}^*\}$ (cont'd)

```
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, $(Q, \Sigma, \Gamma, \delta, q_0, q_{\text{accept}})$, where Q, Σ, Γ are all finite and

1. Q is a set of states,
2. Σ is the input alphabet not containing the blank symbol $\sqcup$,
3. Γ is the tape alphabet, where $\sqcup \in \Gamma$ and $\Sigma \subseteq \Gamma$,
4. $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$ is the transition function,
5. $q_0 \in Q$ is the start state,
6. $q_{\text{accept}} \in Q$ is the accept state, and
7. $q_{\text{reject}} \in Q$ is the reject state, where $q_{\text{reject}} \neq q_{\text{accept}}$.

Computation by M

- Initially, M receives its input $w = w_1 w_2 \ldots w_n \in \Sigma^*$ 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 Σ 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

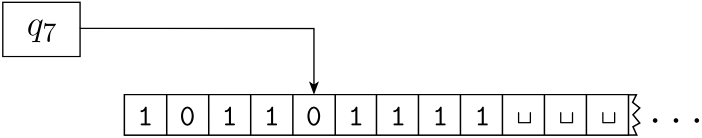
A configuration of a Turing machine consists of

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

by $u\ q\ v$ 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 (cont'd)



A Turing machine with configuration $1011\ q_7\ 01111$

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

$$ua\ q_i\ bv \ \ \text{yields} \ \ u\ q_j\ acv.$$

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

$$ua\ q_i\ bv \ \ \text{yields} \ \ uac\ q_j\ v.$$

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_0w.
- 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 (cont'd)

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

1. C_1 the start configuration of M on w.
2. Each C_i yields C_{i+1}, and
3. 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 $L(M)$.

Definition

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

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 halt, 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.

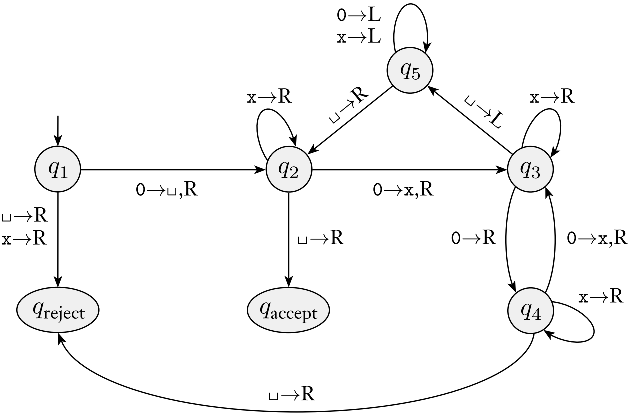
$A = \{0^{2^n} \mid n \geq 0\}$

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.

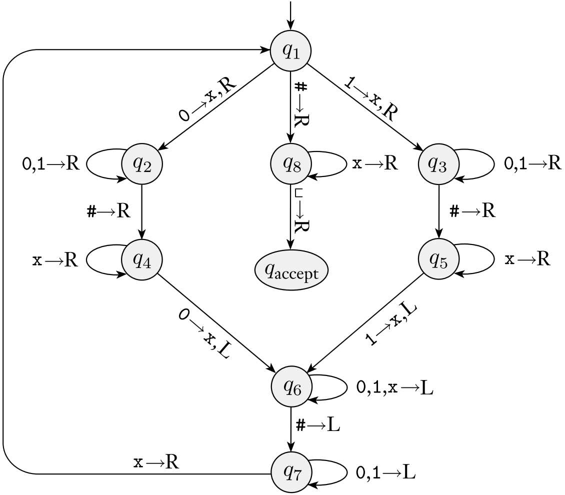
$A = \{0^{2^n} \mid n \geq 0\}$ (cont'd)

- $Q = \{q_1, q_2, q_3, q_4, q_5, q_{\text{accept}}, q_{\text{reject}}\}$, where q_1 is the start state.
- $\Sigma = \{0\}$ and $\Gamma = \{0, x, \sqcup\}$.
- The transition function δ:



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

- $Q = \{q_1, \ldots, q_8, q_{\text{accept}}, q_{\text{reject}}\}$, where q_1 is the start state.
- $\Sigma = \{0, 1, \#\}$, and $\Gamma = \{0, 1, \#, x, \sqcup\}$.
- The transition function δ:



$C = \{a^i b^j c^k \mid i, j, k \geq 1$ 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.

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

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 if 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 two marks to the next $\#$ symbols to the right. If no $\#$ 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.

Variants of Turing Machines

Multitape Turing Machines

A multitape Turing Machine M has several tapes:

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

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

where k is the number of tapes.

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

means that if M is in state q_i and head 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.

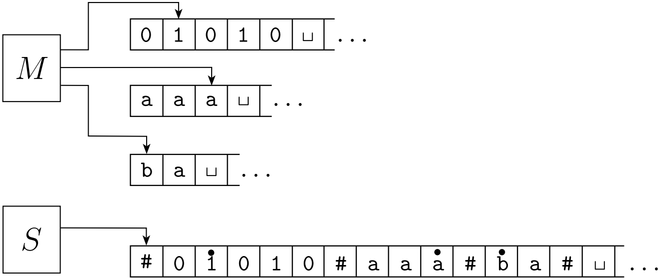
Theorem

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

Proof (1)

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 (2)

On input $w = w_1 \cdots w_n$:

1. first S puts its tape into the format that represents all k tapes of M:

$$\#\dot{w}_1 w_2 \cdots w_n \# \dot{\sqcup} \# \dot{\sqcup} \# \cdots \#.$$

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 $\sqcup$ 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

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

Nondeterministic Turing Machines

1. The transition function for a nondeterministic Turing machine has the form

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

2. The computation of a nondeterministic Turing machine is a tree whose branches correspond to different possibilities for the machine.
3. If some branch of the computation leads to the accept state, the machine accept its input.

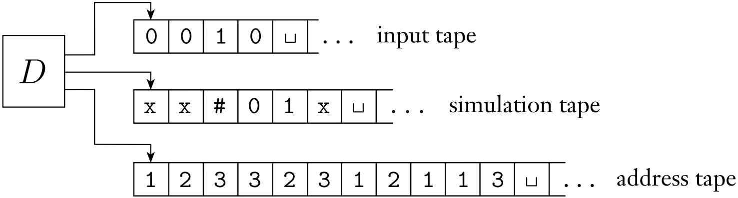
Theorem

Every nondeterministic Turing machine has an equivalent deterministic Turing machine.

Proof (1)

We simulate a nondeterministic N by a deterministic D.

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



Proof (2)

1. Initially, tape 1 contains the input w, and tape 2 and 3 are empty.
2. Copy tape 1 to tape 2 and initialize the string on tape 3 to be ε.
3. Use tape 2 to simulate N with input w on one branch of its nondeterministic computation. 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. If no more symbols remain on tape 3 or if this nondeterministic choice is invalid, abort this branch by going to stage 4. 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

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

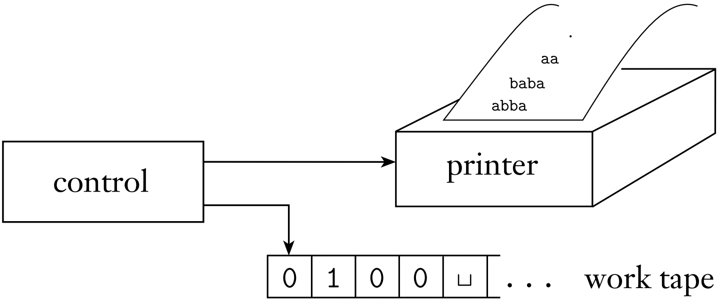
Corollary

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

Enumerators

1. An enumerator is a Turing machine with an attached printer.
2. The Turing machine can use that printer as an output device to print strings.
3. 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.

Proof (1)

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

1. Run E. Every time that E outputs a string, compare it with w.
2. if w ever appears in the output of E, then accept.

Proof (2)

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

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

The Definition of Algorithm

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,

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

is a term with coefficient 6, and

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

is a polynomial with four terms, over the variable 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. The root $(x = 5, y = 3, z = 0)$ is an integral root because all the variables are assigned integer values. Some polynomials have an integral root and some do not.

Hilbet's Problems

Hilbert's tenth problem was to devise an algorithm that test 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:

1. Alonzo Church proposed λ-calculus;
2. Alan Turing proposed Turing machines,
   which were shown to be equivalent.

   So we have the **Church-Turing Thesis**:

$$\begin{array}{c}\text{Intuitive notion of algorithms}\\ \| \\ \text{Turing machine algorithms.}\end{array}$$

Hilbert's Tenth Problem

$D = \{p \mid p$ 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

$D_1 = \{p \mid p$ is a polynomial on a single variable x with integer coefficients and with an integral root$\}$.

Lemma

Both D and D_1 are Turing-recognizable.

Proof.

On input $p(x)$

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

$\square$

A simple variant (con'd)

Lemma

Let

$$p(x) = c_1 x^n + c_2 x^{n-1} + \cdots + c_n x + c_{n+1}$$

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.*