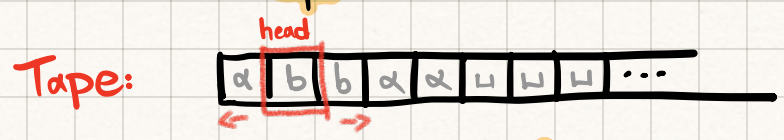


# Lecture 3

## Turing Machines (Sipser, Chapter 3.1)

- So far we have seen two computational models, "Finite Automata" and "Pushdown Automata". Finite automata have no access to memory and Pushdown automata have unlimited memory (in a form of a stack) but usable only in the last in first out manner. They both have limited capabilities which is why we switch to a more powerful model.
- Turing machines(TM) were proposed by Alan Turing in 1936 and they can do everything a real computer can do. Unfortunately, there are certain problems that even TMs cannot solve => problems beyond the theoretical limits of computation.
- The TM model uses a **tape** that has a leftmost end but not a rightmost end.

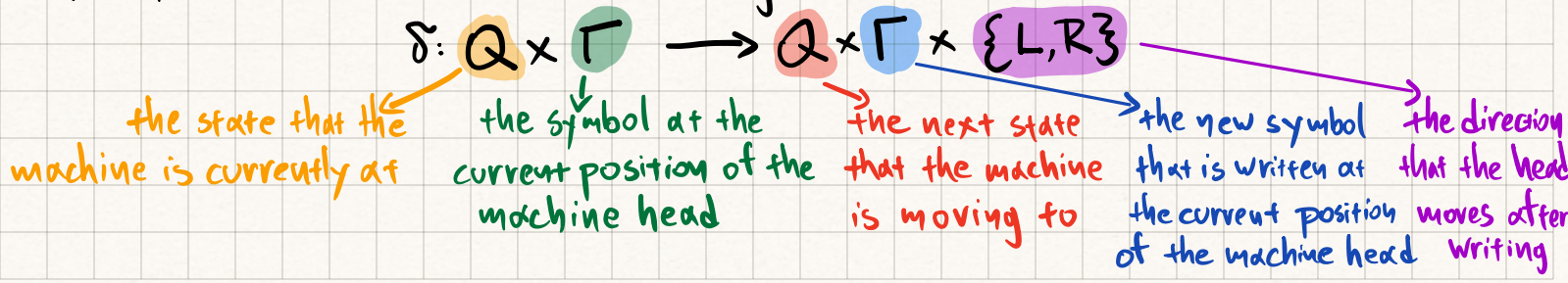


More importantly, we can now **read and write** on **any location** of the tape. To capture this functionality, we have to introduce notation that specifies if the head of the tape is moving to the **left or right**.

- Initially, the tape contains only the input string starting from the leftmost location and the blank character "␣" everywhere else.
- The outputs "accept" and "reject" are obtained by entering the designated accepting and rejecting states. These states are trap states (recall that in Finite and Pushdown automata they are not trap states), and they terminate the execution immediately.

### Formal Definition of a Turing Machine

The transition function  $\delta$  of a Turing machine takes the form:









We say that:  $u \alpha q_i b v$  yields  $u \alpha c q_j v$   
if the transition  $\delta(q_i, b) = (q_j, c, R)$  is part of  $\delta$  definition.

- A Turing machine **accepts** input  $w$  if a sequence of configurations  $C_1, C_2, \dots, C_k$  exists, where:

- ①  $C_1$  is the start state configuration of  $M$  on input  $w$ , i.e.,  $C_1 = q_0 w$ .
- 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 **recognized** by  $M$ , denoted by  $L(M)$ .

Definition 3.5: Call a language Turing-recognizable if some Turing machine recognizes it.

**!** A TM operating on an input  $w$  can have three outcomes, accept, reject, or **loop**.  
Loop means that the machine does not halt. Distinguishing a machine that is looping from one that is taking too long is difficult.

- The TMs that halt on all inputs, i.e., they always make a decision to accept or reject, are called **deciders**.

### Deciding vs. Recognizing:

- Turing machine  $M$  **decides**  $L$  if and only if

- ①  $M$  outputs "accept" for every  $w \in L$
- ②  $M$  outputs "reject" for every  $w \notin L$

- Turing machine  $M$  **recognizes**  $L$  if and only if  $M$  outputs "accept" for all and only the input strings  $w \in L$   $\rightarrow$  this definition allows  $M$  to loop if  $w \notin L$ .

- If  $M$  decides  $L$ , then  $M$  recognizes  $L$  (the other direction is not true).

• Example 3.7: A TM that decides the language consisting of all strings of 0s whose length is a power of two, i.e.,  $L = \{0^{2^n} \mid n \geq 0\}$

Let's think about it: There are some easy corner cases that we can handle fast.

- For example, if the input is the empty string or the input is a symbol from  $\Gamma \setminus \Sigma \rightarrow$  Reject.

$\rightarrow 1$   $\uparrow$  A symbol in the tape alphabet  $\Gamma$  but not input alphabet  $\Sigma$

- If we have an **odd number** of 0s, then the input cannot be in  $L \rightarrow$  Reject

- We need to check if the the number of 0s is a power of 2, e.g.  $w = 0000 = 0^{2^2}$   
Suppose you want to generate  $2^n$  zeros, then most probably you would:



String:  $0 \xrightarrow{\text{double}} 00 \xrightarrow{\text{double}} 0000 \xrightarrow{\text{double}} 00000000 \xrightarrow{\text{double}} \dots \xrightarrow{\text{double}} 00 \dots 00$

# of 0s:  $2^0 \quad 2^1 \quad 2^2 \quad 2^3 \quad 2^n$

- What if instead of doubling to generate a new string, we instead halve the number of 0s.

Input: 00000000

00000000  $\xrightarrow{\text{halve}}$  ~~0000~~0000  $\xrightarrow{\text{halve}}$  ~~000000~~00  $\xrightarrow{\text{halve}}$  ~~0000000~~

$2^3 \quad 2^2 \quad 2^1 \quad 2^0$

💡 If we count how many times we halved, we can calculate the "n" in  $2^n$

More importantly, if by halving we reach a point where we have more 0s but we cannot halve anymore, then the input is not a member of L.

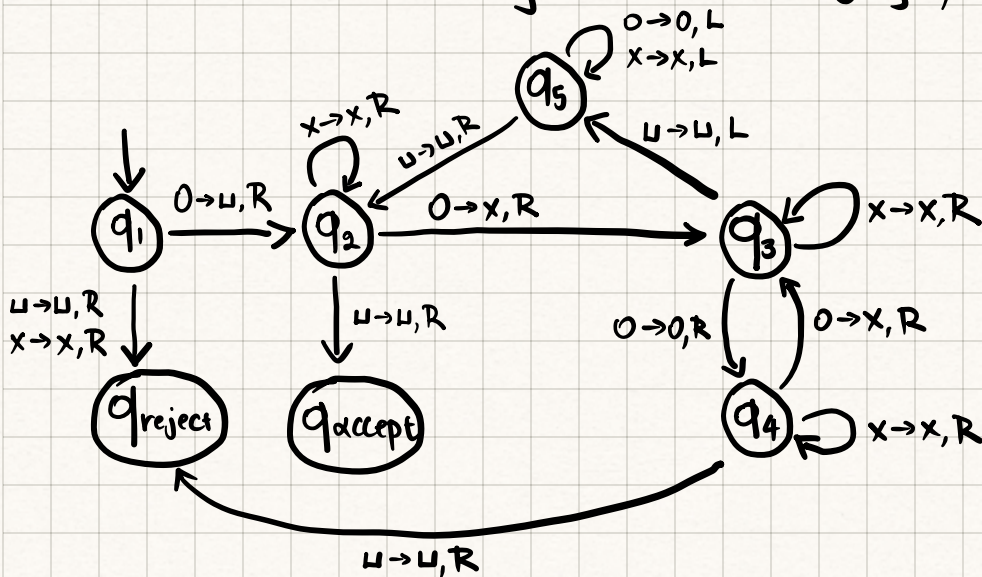
- Notice that when we halved, we crossed out a sequence starting from the leftmost remaining 0. To do that, we need to know the total number of remaining 0s. To perform this in a TM we need to do one pass to count the # of 0s and another pass to cross out the right number of them.

- There is a smarter way that uses only one pass → Cross out every other 0.

$\xrightarrow{\text{halve}}$  ~~00000000~~  $\xrightarrow{\text{halve}}$  ~~00000000~~  $\xrightarrow{\text{halve}}$  ~~00000000~~

- One last thing: Since we need to do a lot of back and forth on the tape, we need to mark the beginning of the tape → Cross out the first 0 using  $\sqcup$

- We define the following TM with  $\Sigma = \{0\}$ ,  $\Gamma = \{\sqcup, 0, x\}$

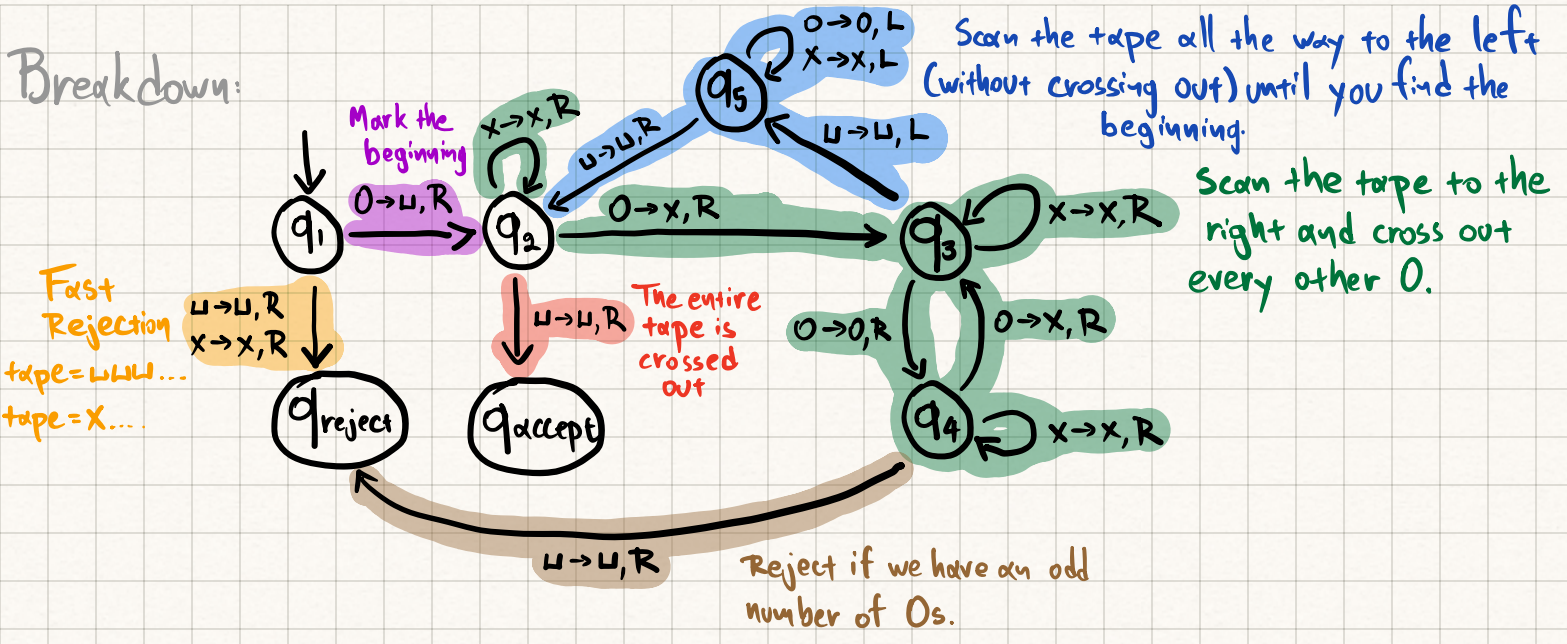


Transition Function:

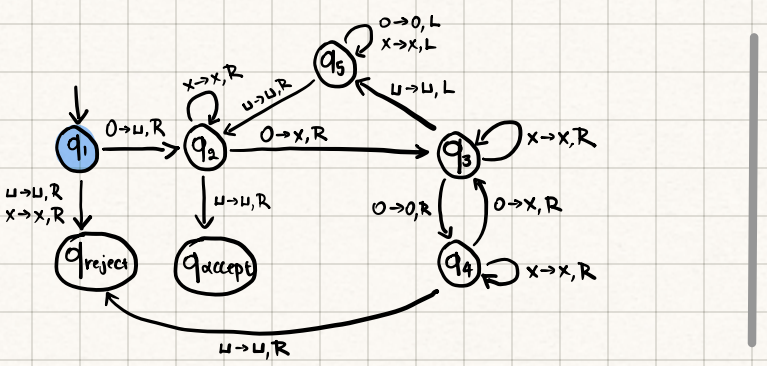
	0	x	$\sqcup$
q <sub>1</sub>	q <sub>2</sub> , $\sqcup$ , R	q <sub>rej</sub> , $\sqcup$ , R	q <sub>rej</sub> , x, R
q <sub>2</sub>	q <sub>3</sub> , x, R	q <sub>2</sub> , x, R	q <sub>acc</sub> , $\sqcup$ , R
q <sub>3</sub>	q <sub>4</sub> , 0, R	q <sub>3</sub> , x, R	q <sub>5</sub> , $\sqcup$ , L
q <sub>4</sub>	q <sub>3</sub> , x, R	q <sub>4</sub> , x, R	q <sub>rej</sub> , $\sqcup$ , R
q <sub>5</sub>	q <sub>5</sub> , 0, L	q <sub>5</sub> , x, L	q <sub>2</sub> , $\sqcup$ , R
q <sub>accept</sub>	$\sqcup$	$\sqcup$	$\sqcup$
q <sub>reject</sub>	$\sqcup$	$\sqcup$	$\sqcup$



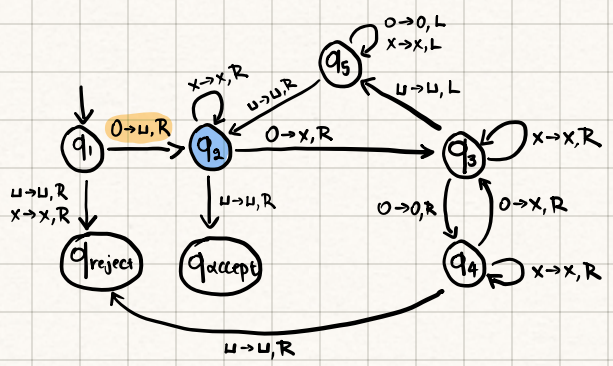
# Breakdown:



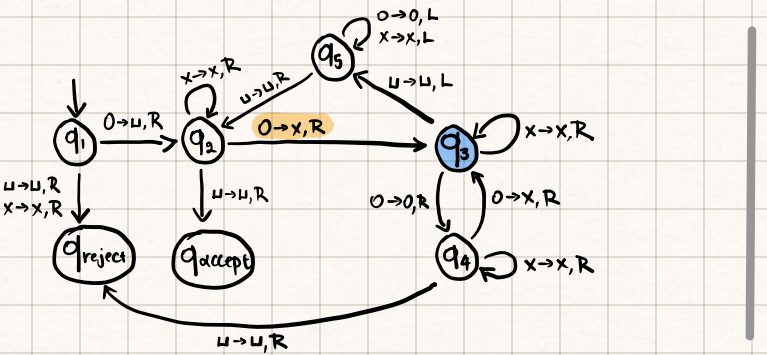
## Example Run $w = 0000$



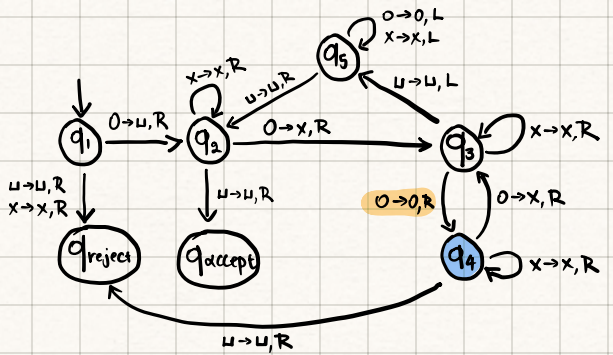
Configuration:  $q_1 0000$  Tape:  $0000$



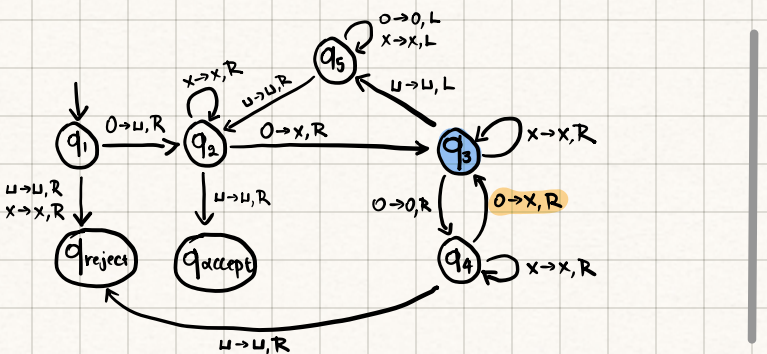
Configuration:  $0q_2000$  Tape:  $0000$



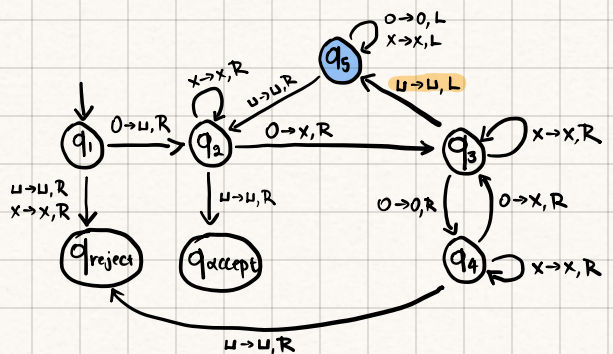
Configuration:  $0xq_300$  Tape:  $0000$



Configuration:  $0x0q_40$  Tape:  $0000$

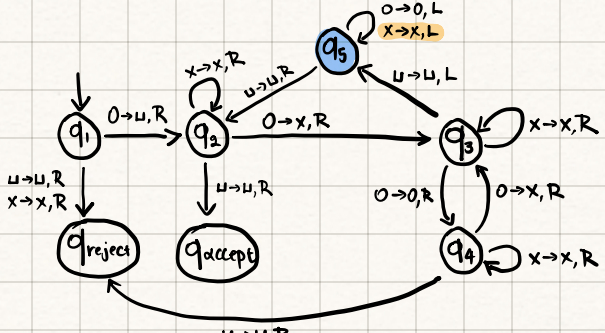


Configuration:  $0x0xq_3$  Tape:  $0000$

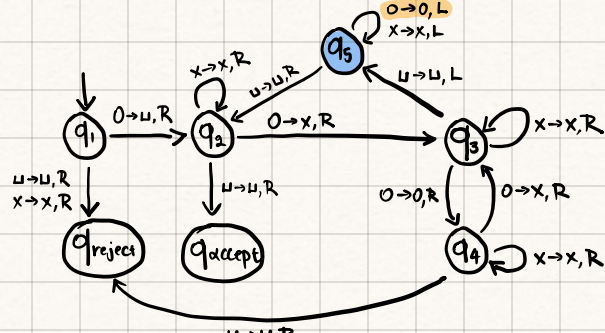


Configuration:  $0x0q_5X$  Tape:  $0000$

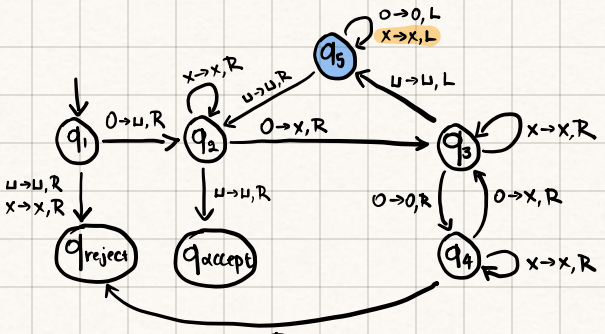




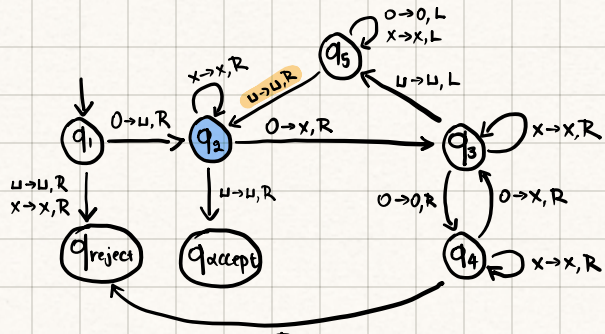
Configuration:  $Uxq_5Ox$  Tape:  $UxOx$



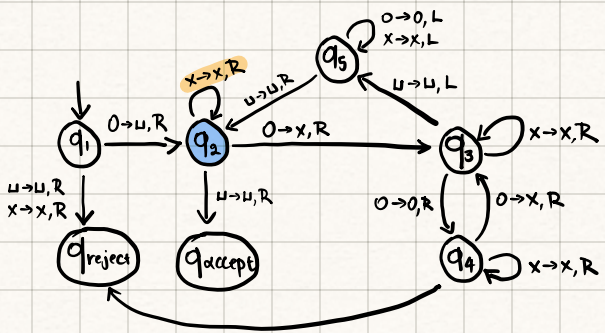
Configuration:  $Uq_5xOx$  Tape:  $UxOx$



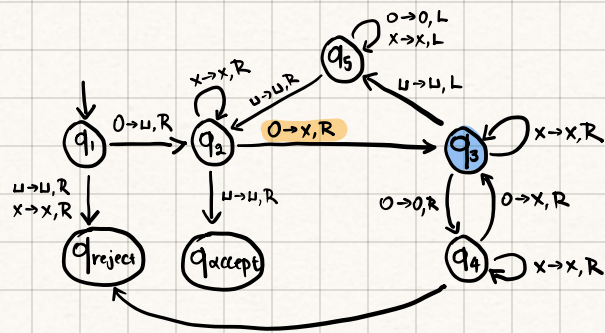
Configuration:  $q_5UxOx$  Tape:  $UxOx$



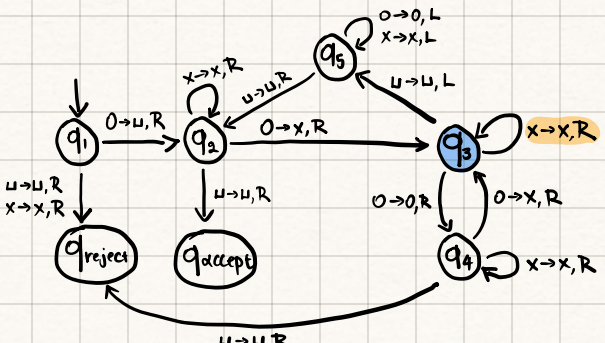
Configuration:  $Uq_2xOx$  Tape:  $UxOx$



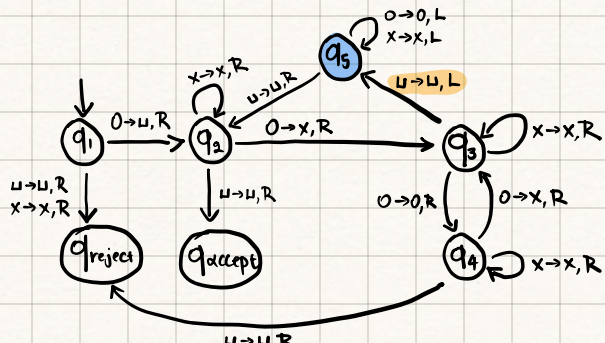
Configuration:  $Uxq_2Ox$  Tape:  $UxOx$



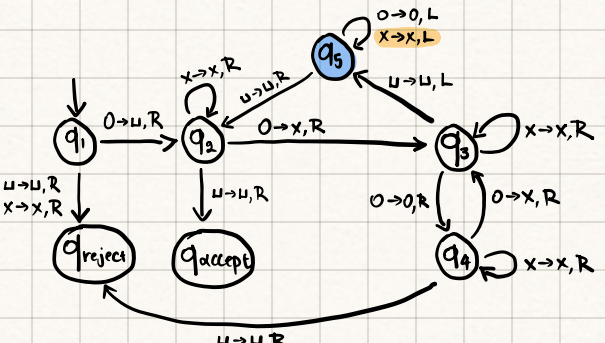
Configuration:  $Uxxq_3x$  Tape:  $UxxX$



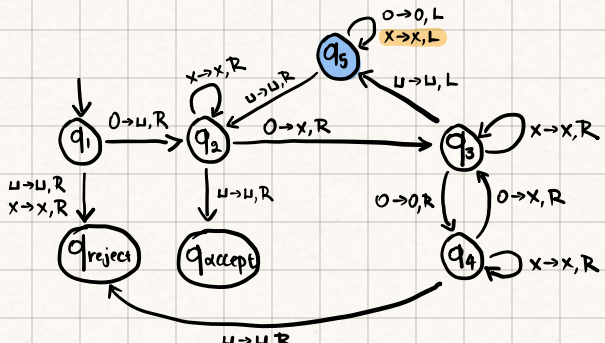
Configuration:  $Uxxxq_3$  Tape:  $UxxxU$



Configuration:  $Uxxq_5x$  Tape:  $UxxxX$

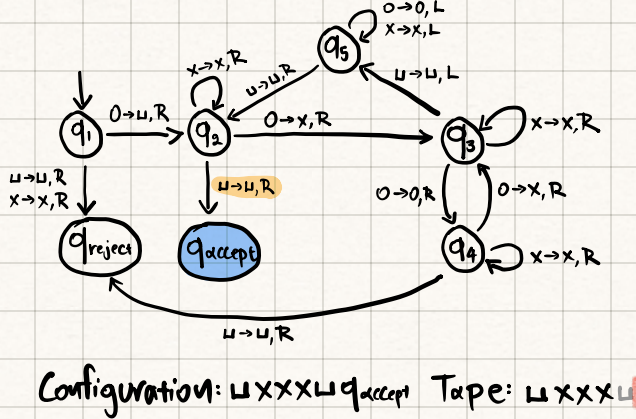
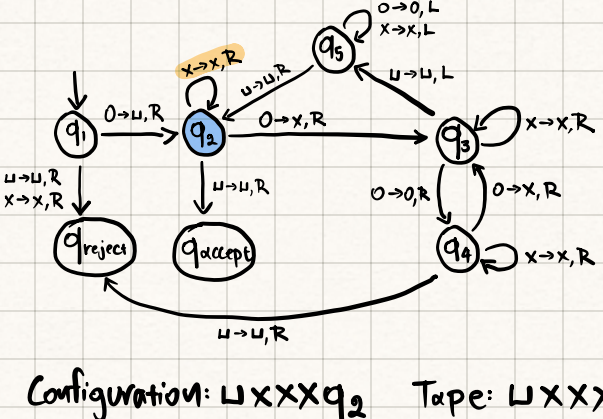
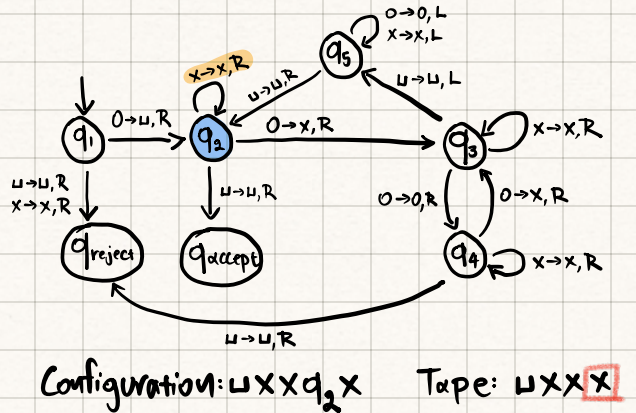
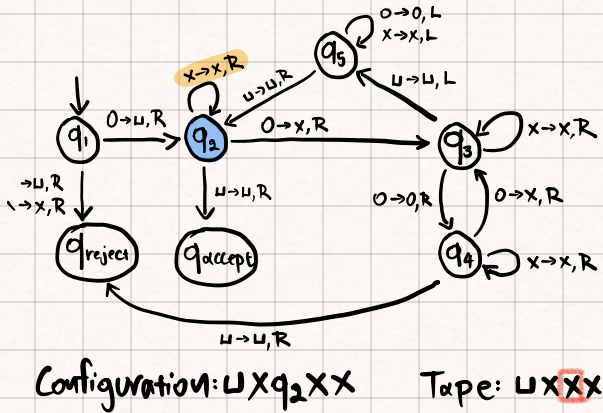
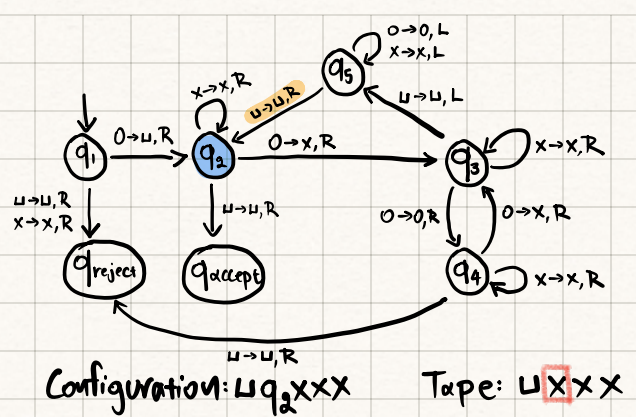
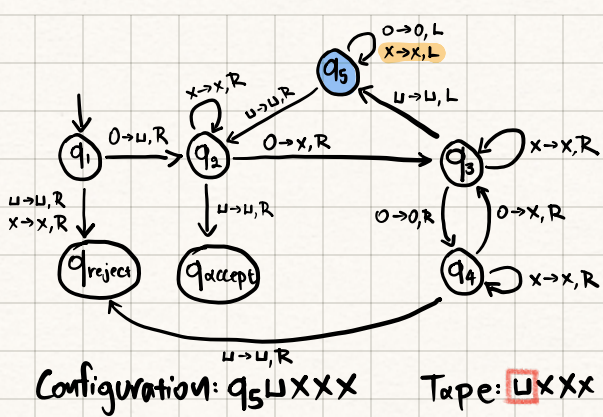


Configuration:  $Uxq_5xx$  Tape:  $UxxxX$



Configuration:  $Uq_5xxx$  Tape:  $UxxxX$





Quiz 3.1: Suppose we compute on the above TM. Which of the following configurations cannot be seen in this TM?

- A)  $q_1 00000000$
- B)  $ux0q_40$
- C)  $uxxxxuq_{accept}$
- D)  $uxxxxxxxuq_{accept}$



2. Effective calculability. Abbreviation of treatment.

A function is said to be 'effectively calculable' if its values can be found by some purely mechanical process. Although it is fairly easy to get an intuitive grasp of this idea it is nevertheless desirable to have some more definite, mathematically expressible definition. Such a definition was first given by Gödel at Princeton in 1934 (Gödel [2], 28) following in part an unpublished suggestion of Herbrand, and has since been developed by Kleene (Kleene [2]). We shall not be concerned much here with this particular definition. Another definition of effective calculability has been given by Church (Church [5], 356-356) who identifies it with  $\lambda$ -definability. The author has recently suggested a definition corresponding more closely to the intuitive idea (Turing [1], see also Post [1]). It was said above "a function is effectively calculable if its values can be found by some purely mechanical process." We may take this statement literally, understanding a purely mechanical process one which could be carried out by a machine. It is possible to give a mathematical description, in a certain normal form, of the structures of these machines. The development of these ideas leads to the author's definition of a computable function, and an identification of computability<sup>5</sup> with effective calculability.

<sup>5</sup> We shall use the expression 'computable function' to mean a function calculable by a machine, and let 'effectively calculable' refer to the intuitive idea without particular identification with any one of these definitions. We do not restrict the values taken by a computable function to be natural numbers; we may for instance have computable propositional functions.

It is not difficult through somewhat laborious, to prove these

Ph.D. Thesis of Alan Turing titled "Systems of Logic Based on Ordinals", 1938

# The Church-Turing Thesis (Sipser, Ch. 3.3)

- No computational procedure will be considered as an algorithm unless it can be represented as a Turing machine

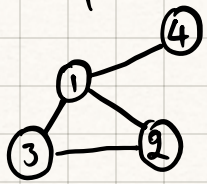
Intuitive notion of algorithms  $\longleftrightarrow$  Turing machine algorithms

What is the right level of detail when describing TM algorithms?

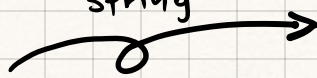
- Formal Description:** Provide a detailed description of TM's states, transition function, etc.
- Implementation Description:** Use text to describe the way that it moves its head and the way it stores data on its tape.
- High-level Description:** Use text to describe the algorithm ignoring implementation details (head movement etc.)

• TMs are powerful. They can handle/solve problems beyond regular languages. They can handle languages that concern all kinds of mathematical objects.

For example:  
Graph G



Encoding as a string



List of nodes      List of edges

$$\langle G \rangle = (1, 2, 3, 4) ((1, 2), (2, 3), (3, 1), (1, 4))$$

Properly formed input strings:

- The list of nodes should contain no repetitions
- List of nodes: decimal numbers, List of edges: pairs of decimal numbers
- Every node on edge list should appear on node list

Thus, we can have a TM that decides language

$$L = \{ \langle G \rangle \mid G \text{ is a connected undirected graph} \}$$



# Decidability (Sipser, Chapters 4.1 and 4.2)

- Let's investigate the power of TM/algorithms to solve problems. We will see that some problems can be solved algorithmically but certain problems cannot.

Explore the limits of algorithmic solvability

## Decidable Languages

We give an algorithm for testing whether a finite automaton accepts a string

[Theorem 4.1: Language  $L = \{ \langle B, w \rangle \mid B \text{ is a DFA that accepts input string } w \}$  is a decidable language

Proof:

→ High-level description

$M =$  "On input  $\langle B, w \rangle$ , where  $B$  is a 5-tuple describing a DFA and  $w$  is a string:

1. Simulate  $B$  on input  $w$
2. If the simulation ends in  $B$ 's accept state, then  $M$  accepts. If it ends in a non-accepting state, then  $M$  rejects."

First,  $M$  checks if the input string is a properly formed  $\langle B, w \rangle$  encoding (i.e., a 5-tuple describing a DFA followed by  $w$ ), if not reject.

$M$  carries the simulation directly  $\Rightarrow$  Keeps track of  $B$ 's current state and its position in the input  $w$ .  
by writing on  $M$ 's tape.

Notice that  $B$  is a DFA therefore, it performs a single pass on input  $w$ , which means that it will terminate in  $|w|$  steps.  $\square$

## Undecidability

One of the most philosophically important findings:

"There are problems that are algorithmically unsolvable"

Goal: Learn techniques to prove that a problem is computationally unsolvable.



[Theorem 4.11: The language  $L_{TM} = \{ \langle M, w \rangle \mid M \text{ is a TM and } M \text{ accepts } w \}$  is undecidable.]

Some observations first:

- This theorem shows that **recognizers are more powerful than deciders**.
- Requiring a TM to halt on all inputs restricts the languages that it can process.

For example, the following simple TM recognizes  $L_{TM}$

$U =$  "On input  $\langle M, w \rangle$ , where  $M$  is a TM and  $w$  is a string:

1. Simulate  $M$  on input  $w$ .
2. If  $M$  ever enters its accept state, then  $U$  accepts  
if  $M$  ever enters its reject state, then  $U$  rejects. "

\* It is possible that  $M$  loops on input  $w$ , which is why  $U$  recognizes  $L_{TM}$  but does not decide  $L_{TM}$ .


The above is an example of a **universal Turing machine** that is capable of simulating any other TM  $M$  given its description.

Predecessor of modern computer "one machine that runs arbitrary machines based on the program"

The proof of Thm 4.11 is based on the Diagonalization method discovered by Cantor in 1873. The motivating question was:

"If we have two infinite sets how can we tell if one is larger than the other or whether they are of the same size?"

↳ If we start counting to compare their relative sizes we will never finish.

 Key Observation: For the case of finite sets, two sets have the same size if the elements of one set can be paired with the elements of the other set  $\Rightarrow$  Extend this to infinite sets!

Some definitions before introducing the diagonalization method.

Let  $A, B$  be two sets and  $f$  be a function from  $A$  to  $B$ .

- Function  $f$  is **injective (one-to-one)** if it never maps two different elements to the same place, i.e.,  $\forall a, b \in A, a \neq b \Rightarrow f(a) \neq f(b)$



• Function  $f$  is **surjective (onto)** if it hits every element of  $B$   
 i.e.,  $\forall b \in B, \exists a \in A$  such that  $f(a) = b$

• If function  $f$  that is both one-to-one and onto is called a **correspondence**.

\* We say that  $A$  and  $B$  have the **same size** if there is a correspondence between them.

Example: Let  $N = \{1, 2, 3, \dots\}$  be the set of natural numbers and  
 $E = \{2, 4, 6, \dots\}$  be the set of even natural numbers.

We can prove that these infinite sets have the same size by providing a correspondence from  $N$  to  $E$ .

$f(n) = 2n$       visually  $\rightarrow$

$n$	$f(n)$
1	2
2	4
3	6
4	8
$\vdots$	$\vdots$

\* Counterintuitive example since  $E$  is a proper subset of  $N$ ,  $E \subset N$ .

- A set  $S$  is **countable** if ① either it is finite, or ② it has the same size as  $N$ .

Another Example: The set of positive rational numbers  $Q = \left\{ \frac{m}{n} \mid m, n \in N \right\}$   
 has the same size as  $N$ .

\* Even more counterintuitive!

To prove that they have the same size, we give a correspondence.  
 Create an infinite matrix to list all members of  $Q$

	Increase Denominator $\rightarrow$				
Increase Numerator $\downarrow$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$
	$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$
	$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$
	$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$
	$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$
	$\vdots$				

\* The proposed function must not have the same output for two different inputs. Notice that some numbers are repeated in this infinite matrix  $1 = \frac{1}{1} = \frac{2}{2} = \frac{3}{3} = \frac{4}{4} = \frac{5}{5}$  and  $2 = \frac{2}{1} = \frac{4}{2}$

\* Also we must output every member of set  $Q$ .

Thus, this  $f: N = (1, 2, 3, 4, \dots)$   
 is not a correspondence because it will never reach the second row

$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$
$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$
$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$
$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$
$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$
$\vdots$				

\* List the members on the diagonals

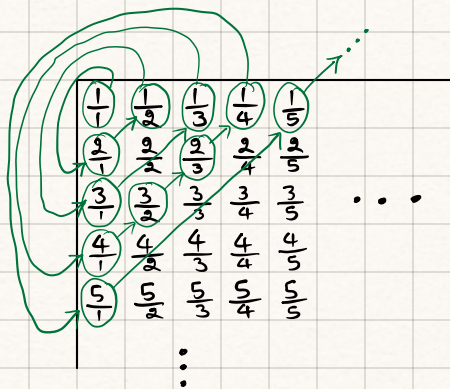
But if we simply list them like that, we create repetitions:

$(\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \dots)$

x not a correspondence

$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$
$\frac{2}{1}$	$\frac{2}{2}$	$\frac{2}{3}$	$\frac{2}{4}$	$\frac{2}{5}$
$\frac{3}{1}$	$\frac{3}{2}$	$\frac{3}{3}$	$\frac{3}{4}$	$\frac{3}{5}$
$\frac{4}{1}$	$\frac{4}{2}$	$\frac{4}{3}$	$\frac{4}{4}$	$\frac{4}{5}$
$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$
$\vdots$				





Skip repeated entries to ensure one-to-one property  
 $\downarrow$   
 Correspondence between  $\mathbb{N}$  and  $\mathbb{Q}$ .

- For some infinite sets there exists no correspondence with  $\mathbb{N}$ . Such a set is called **uncountable**. ( $\Rightarrow$  Some infinite sets are larger than other infinite sets)

Example: The set of real numbers  $\mathbb{R}$  is uncountable.

Proof: We proceed with a proof by contradiction. Suppose for the sake of contradiction that exists a correspondence  $f$  between  $\mathbb{N}$  and  $\mathbb{R}$ . We will provide a number  $r \in \mathbb{R}$  that does not appear as an output of  $f$ .

An illustration:

$n$	$f(n)$ <small><math>\leftarrow</math> Hypothetical correspondence</small>
1	3.14159...
2	55.55...
3	0.1234...
4	0.5000...
$\vdots$	

define  $r$  such that, the  $i$ -th decimal of  $r$  is different from the  $i$ -th decimal of  $f(i)$ .  
 $r = 0.2415\dots$

Diagram showing  $r$  vs  $f(i)$  comparisons:  
 $r$  vs  $f(1)$ :  $2 \neq 1$   
 $r$  vs  $f(2)$ :  $4 \neq 5$   
 $r$  vs  $f(3)$ :  $1 \neq 3$   
 $r$  vs  $f(4)$ :  $5 \neq 0$

If we construct an  $r$  such that the  $i$ -th decimal is different from the  $i$ -th decimal of  $f(i)$ , then we know that  $r$  is not equal to  $f(n)$  for any value of  $n$ .  $\blacksquare$

Before we see the proof for Theorem 4.11, let's first prove that there are languages that are not Turing-recognizable.

Theorem  
~~Corollary~~ 4.18: Some languages are not Turing-recognizable.

Lemma-A: For any alphabet  $\Sigma$ , the set of strings  $\Sigma^*$  is countable

Proof for Lemma-A: Make a list that covers all the members of the infinite set  $\Sigma^*$ .

Let  $\Sigma = \{a, b, c\}$

List  $LS_{\Sigma^*}$ :  $a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, \dots$

all strings with characters from  $\Sigma$  with length 1.      all strings with characters from  $\Sigma$  with length 2



It is easy to see that the index of its entry of  $LS_{\Sigma^*}$  can be used as a  $\mathbb{N}$  value towards building a correspondence with  $LS_{\Sigma^*}$ . Thus, the set of strings  $\Sigma^*$  is countable.  $\square$

**Corollary - A:** We know that every Turing machine  $M$  can be encoded as a finite string  $\langle M \rangle$ . If we omit from  $\Sigma^*$  the strings that do not encode a TM, then what is left is a subset of  $\Sigma^*$  which we know is countable. Thus, the set of all TM is countable.

An infinite binary sequence is an unending sequence of 0s and 1s.

**Lemma - B:** The set of infinite binary sequences  $\mathbb{B}$  is uncountable.

**Proof for Lemma - B:** By diagonalization. Suppose for the sake of contradiction that  $\mathbb{B}$  is countable. Then, there exists a correspondence with  $\mathbb{N}$ . We can create an infinite binary sequence  $r$  that does not appear as an output of  $f \Rightarrow f$  is not onto  $\Rightarrow f$  is not a correspondence. Iterate through the list implied by  $f$ , for the  $i$ -th entry of the list, check the  $i$ -th bit of  $f(i)$  and assign the opposite to the  $i$ -th bit of  $r$ .

$$\begin{array}{l} f(1) = 10110\dots \\ f(2) = 10011\dots \\ f(3) = 01101\dots \end{array} \quad \begin{array}{l} r = 0\dots\dots \\ r = 01\dots\dots \\ r = 010\dots\dots \end{array}$$

\* Choose the  $i$ -th bit of  $r$  by flipping the  $i$ -th bit of  $f(i)$ .

**Lemma - C:** The set of all languages  $\mathcal{L}$  is uncountable.

**Proof for Lemma - C:** To prove this, we have to build a correspondence between  $\mathbb{B}$  and  $\mathcal{L}$ , i.e., the two sets have the same size.

Recall that a language is a collection of strings from set  $\Sigma^*$ . We can represent the strings that are members of language  $A \in \mathcal{L}$  as an infinite binary sequence  $X_A$  (also called characteristic sequence of  $A$ ) where its  $i$ -th bit takes value 1 if the  $i$ -th string of  $LS_{\Sigma^*}$  is in language  $A$  and value 0 if  $i$ -th string of  $LS_{\Sigma^*}$  is not in language  $A$ .

$LS_{\Sigma^*}$ :	$a$	$b$	$c$	$aa$	$ab$	$ac$	$ba$	$bb$	$bc$	$ca$	$cb$	$cc$	$\dots$
$A = \{$	$\vdots$	$b$	$\vdots$	$\vdots$	$ab$	$\vdots$	$\vdots$	$bb$	$bc$	$\vdots$	$\vdots$	$\vdots$	$\dots\}$
$X_A =$	0	1	0	0	1	0	0	1	1	0	0	0	



Given a fixed  $\Sigma^*$ , each language in  $\mathcal{L}$  has a unique characteristic sequence of  $A$ .

The function  $f: \mathcal{L} \rightarrow \mathbb{B}$ , where  $f(A)$  is the characteristic sequence of  $A$  is one-to-one and onto, and hence is a correspondence.

Thus, since  $\mathbb{B}$  is uncountable,  $\mathcal{L}$  is uncountable as well.

Proof for 4.18: Each Turing machine can recognize a single language.

From Lemma-C the set of all languages is uncountable, while from Corollary-A, the set of all Turing machines is countable.

Since there are uncountably many languages and countably many TMs, we conclude that some languages are not recognized by any TM.  $\blacksquare$

\*The key idea is that the description of a TM must be a finite string whereas the content of a language can be represented by an infinite sequence. This asymmetry is the reason that there are languages not recognized by a TM.