CS 365 Models of Computation (Advanced)

Keven Qiu
Instructor: Eric Blais
Winter 2024

Contents

Chapter 1

Introduction

1.1 Two Simplifying Restrictions

Definition: Computational Problem

A task where for each possible input to the problem, there is one or more valid outputs that is to be produced.

This however is too broad, so we impose two simplifying restrictions.

Simplifying Restriction 1

We only consider problems whose inputs are binary strings.

The binary alphabet is $\{0,1\}$ and the set of strings of length n is denoted $\{0,1\}^n$. The unique string in $\{0,1\}^0$ is the empty string, denoted ε.

We write $\{0,1\}^* = \bigcup_{n \geq 0} \{0,1\}^n$ to denote the set of all possible binary strings.

Proposition

For every finite set $\mathcal{X}$ with k elements, there is a one-to-one encoding function $h : \mathcal{X} \to \{0,1\}^{\lceil \log k \rceil}$.

Proof. Fix any ordering $a_1, \ldots, a_k$ of the elements of $\mathcal{X}$. Then define the encoding function h that maps a_i to the string that gives the binary representation of i. $\square$

Simplifying Restriction 2

We only consider decision problems, where there is exactly one valid output for each input, and this output is in $\{0,1\}$.

1.2 Functions and Languages

A decision problem where all inputs are binary strings of length n can be described a Boolean function

$$f : \{0,1\}^n \to \{0,1\}$$

where for each $x \in \{0,1\}^n$, the value $f(x)$ represents the valid output for input x.

We do not want to restrict to just length n binary strings. So problems can be represented by a family of Boolean functions $\{f_n\}_{n\geq 0}$.

Definition: Language

A language is $L \subseteq \{0,1\}^*$.

A language L is equivalent to the family of functions $\{f_n\}$ if for every $x \in \{0,1\}^*$ of length n,

$$x \in L \iff f_n(x) = 1$$

1.3 Cardinality of Languages

Definition: Finite Set

A set S is finite if there is a one-to-one mapping between the elements of S and the elements in the set $\{1, 2, \ldots, n\}$ for some $n \geq 0$.

Definition: Infinite Set

A set not finite.

Definition: Countable Set

A set S is countable if there is a one-to-one mapping between the elements of S and the set of natural numbers $\mathbb{N}$.

Definition: Uncountable Set

A set not countable.

The set of binary strings $\{0,1\}^n$ is finite. The set $\{0,1\}^*$ is infinite.

Proposition

The set $\{0,1\}^*$ is countable.

Proof. Consider the mapping $h : \{0,1\}^* \to \mathbb{N}$ where for each $x \in \{0,1\}^*$, we define $h(x)$ to be the natural number with binary representation $1x$, where we use $1x$ to denote string concatenation. The mapping h is one-to-one. $\square$

Theorem

The set of all languages is uncountable.

Proof. This proof is an example of a diagonalization argument.

Assume for contradiction that the set of all languages is countable. Then we can list the set of languages in some order $L_1, L_2, \ldots$.

We can build a table whose columns are labelled by the strings in $\{0,1\}^*$ in lexicographical order and rows labelled by the languages $L_1, L_2, \ldots$ in the order we defined. For each cell (L_k, x) in the table, enter a 1 in the cell if $x \in L_k$ and 0 otherwise.

Consider now the language D that we obtain by look at the diagonal entries of this table and using their negation to determine if the corresponding string is in D. Namely, if x is the kth string in the lexicographical ordering of $\{0,1\}^*$, then $x \in D$ if and only if $x \notin L_k$.

D is a language so by our assumption, there is a value $n \in \mathbb{N}$ such that $D = L_n$ is the nth language in our list. Let x denote the nth string in the lexicographical order of $\{0,1\}^*$. But then $x \in D$ holds if and only if $x \notin L_n$, so $D \neq L_n$. We have arrived at our contradiction, so the set of all languages must be uncountable. $\square$

1.4 First Uncomputability Result

Proposition

There exist a language L for which there is no program that accepts each input $x \in \{0,1\}^*$ if and only if $x \in L$.

Proof. Assume for contradiction that for every language, there is a program that accepts exactly the set of strings in that language. Then there is a map from the set of all languages to the set of all programs. But every program can be represented as a binary string. So there is a mapping from the set of all languages to $\{0,1\}^*$. But since $\{0,1\}^*$ is countable, there is a mapping from the set of all languages to $\mathbb{N}$, contradicting the previous theorem. $\square$

Chapter 2

Turing Machines

We want a definition of a computer than can capture any computer, no matter how complicated. Our goal is to identify an explicit language that cannot be computed by algorithms over any machine model.

2.1 Definition

Consider an infinite tape split into squares. It has a finite number of states. Each square contains exactly one symbol. There is a tape head that points to over one of the squares. The head is allowed to move left or right and each state has a set of rules.

Definition: Deterministic 1-Tape Turing Machine

An abstract machine described by the triple

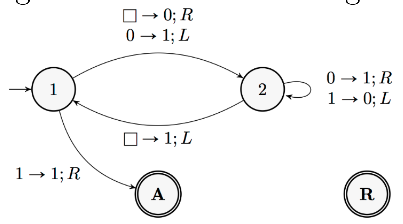
$$M = (m, k, \delta)$$

with $m, k \geq 1$ where

- $Q = \{1, 2, \ldots, m\}$ is the set of internal states,
- $\Gamma = \{\square, 0, 1, 2, \ldots, k\}$ is the tape alphabet, and
- $\delta \colon \mathbf{Q} \times \Gamma \to (\mathbf{Q} \cup \{\mathbf{A}, \mathbf{R}\}) \times \Gamma \times \{L, R\}$ is the transition function.

The state **1** is the initial state of the Turing machine M. **A** and **R** are the accept and reject states, respectively.

Figure 2.1: Transition Diagram



Definition: Configuration

A string $w\mathbf{q}y$ where

- $\mathbf{q} \in \mathbf{Q} \cup \{\mathbf{A}, \mathbf{R}\}$ represents the current state of the machine,
- $wy \in \Gamma^*$ is the current string on the tape, and
- the position of the tape head is on the first symbol of y.

Two configurations are equivalent when they are identical up to blank symbols at the beginning of w or at the end of y. In other words,

$$w\mathbf{q}y = \square w\mathbf{q}y = w\mathbf{q}y\square$$

Definition: Yields

For any strings $w, y \in \Gamma^*$, symbols $a, b, c \in \Gamma$, and states $\mathbf{q} \in \Sigma$ and $\mathbf{r} \in \Sigma \cup \{\mathbf{A}, \mathbf{R}\}$, the configuration $wa\mathbf{q}by$ of the Turing machine M yields the configuration $w\mathbf{r}acy$, denoted

$$wa\mathbf{q}by \vdash w\mathbf{r}acy$$

when $\delta(\mathbf{q}, b) = (\mathbf{r}, c, L)$. Similarly,

$$wa\mathbf{q}by \vdash wac\mathbf{r}y$$

when $\delta(\mathbf{q}, b) = (\mathbf{r}, c, R)$.

A configuration can *derive* another configuration in 0, 1, or more steps.

Definition: Accepts

A Turing machine M accepts $x \in \{0, 1\}^*$ if $\mathbf{1}x$ derives an accepting configuration $w\mathbf{A}y$.

Definition: Rejects

A Turing machine M rejects $x \in \{0, 1\}^*$ if $\mathbf{1}x$ derives a rejecting configuration $w\mathbf{R}y$.

Definition: Halts

A Turing machine M halts on x if it accepts or rejects x.

Definition: Decides

A Turing machine M decides the language $L \subseteq \{0,1\}^*$ if it accepts every $x \in L$ and rejects every $x \notin L$.

Definition: Recognize

A Turing machine M recognizes L if M accepts every $x \in L$ and M rejects or does not halt on $x \notin L$.

Definition: Decidable

A language $L \subseteq \{0,1\}^*$ if and only if there is a Turing machine that decides L.

2.2 Universal Turing Machine

Proposition

There is an encoding that maps each Turing machine M to a binary string $\langle M \rangle \in \{0,1\}^*$.

Proof. Consider the Turing machine $M = (m, k, \delta)$. We find a mapping $\{0, 1, +\}$ to the string $\langle m \rangle + \langle k \rangle + \langle \delta(1,0) \rangle + \cdots$. The positive integers m and k can be encoded by taking their binary representation. The transition function δ can be represented as a table of $m \cdot (k+2)$ entries (one for each internal state-tape symbol pair). Each of these entries can be encoded as a binary string. We can combine all these elements into a single binary representation to obtain the encoding of M. □

Theorem

There is a Universal Turing Machine U such that for every Turing machine M and every input $x \in \{0,1\}^n$, when the input to U is the string $\langle M \rangle x$, then U simulates the execution of M on input x.

Proof. First, U turns x into the initial configuration of M by having the string $\mathbf{1}x$. Then

- Read the current state $\mathbf{q}$ and the symbol a at the tap head in M's current configuration.
- Go back to the encoding $\langle M \rangle$ of M to read the entry $\delta(\mathbf{q}, a)$ of its transition table.
- Update the configuration appropriately by overwriting the symbol a at the tap head position, moving the tape head left or right, and updating the current state of the machine.

□

2.3 Church-Turing Thesis

Church-Turing Thesis

Any decision problem that can be solved by any computer that respects the laws of physics corresponds to a language that can be decided by a Turing machine.

Proposition

Every language $L \subseteq \{0,1\}^*$ that can be computed using counter machines can also be decided by a Turing machine.