Summer 2022

Theory of Computing (CSE 221)

Lecture - 1: Introduction

Course Teacher:
Md. Sadiqur Rahman
Lecturer
Department of Computer Science and Engineering
Daffodil International University

Topic Contents

- ❖ Introduction
  - ❑ Automata
- ❖ Different Forms of Proof
  - ❑ Inductive Proof
  - ❑ If-And-Only-If Proof
  - ❑ Proof by Contradiction
- ❖ The Central Concepts of Automata Theory

Introduction

- Automata = abstract computing devices

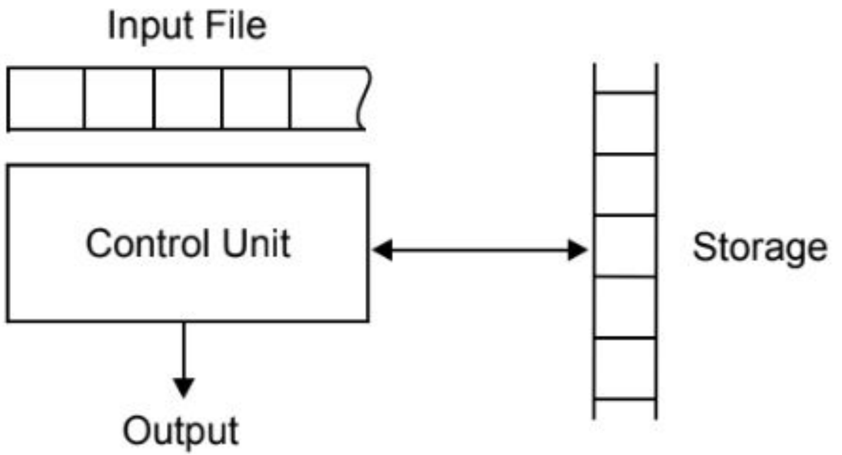


Fig. Automaton

Introduction

- Automata = abstract computing devices
- The word automata comes from the Greek word αὐτόματος, which means **"self-acting, self-willed, self-moving".**
- We will also look at **Finite State Automata** and **Grammars** and **Regular Expressions**.

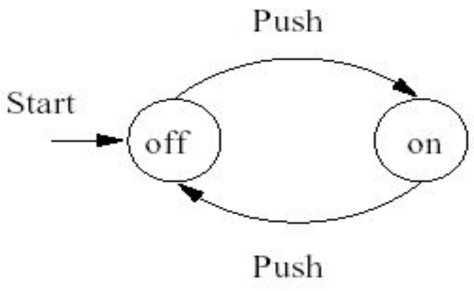
Finite Automata

Finite Automata are used as a model for:

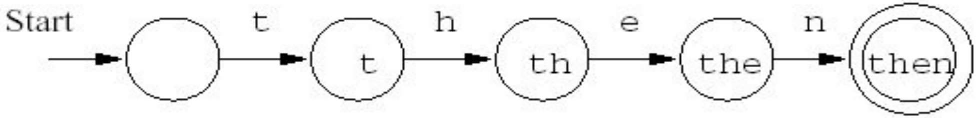
- **Software** for designing digital circuits
- **Lexical analyzer** of a compiler
- **Searching for keywords** in a file or on the web.
- Software for verifying **finite state systems**, such as communication protocols.

Examples

- Example: Finite Automaton modelling an on/off switch



- Example: Finite Automaton recognizing the string then



Inductive Proofs

Prove a statement S(X) about a family of objects X (e.g. integers, trees) in two parts:

1. **Basis**: Prove for one or several small values of X directly.
2. **Inductive Step**: Assume S(Y) for Y "smaller than" X ; prove S(X) using that assumption.

Examples of Inductive Proof

- A complete binary tree with n leaves has $2n$-1 nodes.

  Formally - S(T): if T is a complete binary tree with n leaves, then T has $2n$-1 nodes.

  Induction is on the size = number of nodes of T.

Basis: If T has 1 leaf, it is a one-node tree.

$1 = 2 \times 1 - 1$. (Okay)

Examples of Inductive Proof Cont.

- **Induction**: Assume S(U) for trees with fewer nodes than T. In particular, assume for the subtrees of T.

- T must be a root plus two subtrees U and V.

-If U and V have u and v leaves respectively and T has t leaves, then $u + v = t$.

-By the inductive hypothesis, U and V have $2u$-1 and $2v$-1 nodes respectively.

Then T has $1+(2u-1)+(2v-1)$ nodes.

$$= 2(u+v) - 1$$

$=2t-1$, proving the inductive step.

If-And-Only-If Proof

- X if and only if Y:

1. Prove the **if-part**: Assume Y and prove X.
2. Prove the **only-if part**: Assume X and prove Y.

NOTE:

- The if and only-if parts are converses of each other.
- One part, say “If X then Y” says nothing about whether Y is true when X is false.
- An equivalent form to “if X then Y” is “if not Y then not X”; the latter is the CONTRAPOSITIVE of the former.

Proof by Contradiction Problem

- Prove by contradiction that $\sqrt{2}$ is an irrational number.

Theorem 1.4 : $\sqrt{2}$ *is irrational.*

Proof : Let us assume, to the contrary, that $\sqrt{2}$ is rational.

So, we can find integers r and s ($\neq 0$) such that $\sqrt{2} = \frac{r}{s}$.

Suppose r and s have a common factor other than 1. Then, we divide by the common factor to get $\sqrt{2} = \frac{a}{b}$, where a and b are coprime.

So, $b\sqrt{2} = a$.

Squaring on both sides and rearranging, we get $2b^2 = a^2$. Therefore, 2 divides a^2.

Now, by Theorem 1.3, it follows that 2 divides a.

So, we can write $a = 2c$ for some integer c.

Central Concepts

Alphabet: Finite, nonempty set of symbols

Example: $\Sigma = \{0, 1\}$ binary alphabet

Example: $\Sigma = \{a, b, c, \ldots, z\}$ the set of all lower case letters

Example: The set of all ASCII characters

Strings: Finite sequence of symbols from an alphabet Σ, e.g. 0011001

Empty String: The string with zero occurrences of symbols from Σ

- The empty string is denoted ϵ

Central Concepts

Length of String: Number of positions for symbols in the string.

$|w|$ denotes the length of string w

$|0110| = 4, |\epsilon| = 0$

Powers of an Alphabet: Σ^k = the set of strings of length k with symbols from Σ

Example: $\Sigma = \{0, 1\}$

$\Sigma^1 = \{0, 1\}$

$\Sigma^2 = \{00, 01, 10, 11\}$

$\Sigma^0 = \{\epsilon\}$

Question: How many strings are there in Σ^3

Central Concepts

The set of all strings over Σ is denoted Σ^*

$$\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \cdots$$

Also:

$$\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \Sigma^3 \cup \cdots$$

$$\Sigma^* = \Sigma^+ \cup \{\epsilon\}$$

Concatenation: If x and y are strings, then xy is the string obtained by placing a copy of y immediately after a copy of x

$$x = a_1 a_2 \ldots a_i, y = b_1 b_2 \ldots b_j$$

$$xy = a_1 a_2 \ldots a_i b_1 b_2 \ldots b_j$$

Example: $x = 01101, y = 110, xy = 01101110$

Note: For any string x

$$x\epsilon = \epsilon x = x$$

Type Convention for Symbols and Strings

Commonly, we shall use lower-case letters at the beginning of the alphabet (or digits) to denote symbols, and lower-case letters near the end of the alphabet, typically w, x, y, and z, to denote strings. You should try to get used to this convention, to help remind you of the types of the elements being discussed.

Central Concepts : Language

Languages:

If Σ is an alphabet, and $L \subseteq \Sigma^*$
then L is a language

Examples of languages:

- The set of legal English words
- The set of legal C programs
- The set of strings consisting of n 0's followed by n 1's

$$\{\epsilon, 01, 0011, 000111, \ldots\}$$

Central Concepts

- The set of strings with equal number of 0's and 1's

$$\{\epsilon, 01, 10, 0011, 0101, 1001, \ldots\}$$

- $L_P =$ the set of binary numbers whose value is prime

$$\{10, 11, 101, 111, 1011, \ldots\}$$

- The empty language $\emptyset$

- The language $\{\epsilon\}$ consisting of the empty string

Note: $\emptyset \neq \{\epsilon\}$

Note2: The underlying alphabet Σ is always finite

Problems

Problem: Is a given string w a member of a language L?

Let L_P be a language consisting of all binary strings whose value as a binary number is a prime.

Problems:

Does the string 11101 belong to L_P?
Does the string 10100 belong to L_P?

Thank You