Theory of Computer Science – SCJ 3203

Introduction

Mohd Soperi Mohd Zahid
Sazali Abd Manaf

Outline

- Overview of:
  - Automata Theory
  - Complexity Theory, and
  - Computability Theory
- Mathematical Preliminaries

Automata Theory

- deals with the definitions and properties of mathematical models of computation.
  - Finite Automata (FA) used in text processing, compilers and hardware design.
  - Context-free Grammar (CFG) used in programming languages and artificial intelligence.

Complexity Theory

- Computer problems :
  - easy ⇨ sorting
  - hard ⇨ scheduling
- What makes some problems computationally hard and others easy ?
- We don’t know what make them easy and hard but we know how to classify each problems with an elegant scheme.
  - Cryptography is supposed to be a hard problem.

Computability Theory

- There are some problems which can't be solved by computers, e.g., determining whether a mathematical statement is true or false.
- The object of the Computability Theory is to classify the problems whether they are solvable by computers or not.

Mathematical Notions and Terminology Used

- Sets
- Functions and Relations
- Sequences and Tuples
- Trees
- Strings and Languages
- Boolean Logic
- Proof Techniques

Sets

- Importance: languages are sets
- A set is a collection of "things," called the elements or members of the set. It is essential to have a criterion for determining, for any given thing, whether it is or is not a member of the given set. This criterion is called the membership criterion of the set.

Sets

- There are two common ways of indicating the members of a set:
  - List all the elements, e.g. {a, e, i, o, u}
  - Provide some sort of an algorithm or rule, such as a grammar

Sets

- Notation:
  - To indicate that x is a member of set S, we write **$x \in S$**
  - We denote the empty set (the set with no members) as **{} or $\varnothing$**
  - If every element of set A is also an element of set B, we say that A is a subset of B, and write **$A \subseteq B$**
  - If every element of set A is also an element of set B, but B also has some elements not contained in A, we say that A is a proper subset of B, and write $A \subset B$

Operations on Sets

- The union of sets A and B, written **$A \cup B$**, is a set that contains everything that is in A, or in B, or in both.
- The intersection of sets A and B, written **$A \cap B$**, is a set that contains exactly those elements that are in both A and B.

Operations on Sets

- The set difference of set A and set B, written A - B, is a set that contains everything that is in A but not in B.
- The complement of a set A, written as -A or (better) A with a bar drawn over it, is the set containing everything that is not in A. This is almost always used in the context of some universal set U that contains "everything" (meaning "everything we are interested in at the moment"). Then -A is shorthand for U - A.

Additional terminology

- The cardinality of a set A, written |A|, is the number of elements in a set A.
- The powerset of a set Q, written 2Q, is the set of all subsets of Q. The notation suggests the fact that a set containing n elements has a powerset containing 2n elements, including empty set.
- Two sets are disjoint if they have no elements in common, that is, if $A \cap B = \varnothing$.

Sequences and Tuples

- A sequence of objects is a list of those objects in some order.
- Usually designate by writing the list within parenthesis, e.g. (3,2,5).
- may be finite or infinite.
- finite sequences called tuples.
- sequence with k elements is a k-tuple, e.g., (3,2,5) is a 3-tuple.

Cartesian product (Cross product)

- If A and B are two sets, the Cartesian product of A and B, written A x B, is the set of all pairs wherein the first element is a member of A and the second element is a member of B.

Relations and Functions

- Importance: need basic familiarity with the terminology
- A relation on sets S and T is a set of ordered pairs (s, t), where
  - $s \in S$ (s is a member of S),
  - $t \in T$,
  - S and T need not be different,
  - The set of all first elements (s) is the domain of the relation, and
  - The set of all second elements is the range of the relation.

Trees

- Importance: Trees are used in some algorithms.
- A tree is a kind of digraph:
  - It has one distinguished vertex called the root;
  - There is exactly one path from the root to each vertex; and
  - The level of a vertex is the length of the path to it from the root.

Trees

- Terminology:
  - if there is an edge from A to B, then A is the parent of B, and B is the child of A.
  - A leaf is a node with no children.
  - The height of a tree is the largest level number of any vertex.

Boolean Logic

- AND (conjunction) $\wedge$
- OR (disjunction) $\vee$
- NOT (negation) $\neg$
- XOR (exclusive or) $\oplus$
- Equality $\leftrightarrow$: 1 if both of its operands have the same value.
- Implication $\rightarrow$: 0 if its first operand is 1 and the second operand is 0; otherwise 1.

Proof techniques

- Construction
  - Prove a "there exists" statement by finding the object that exists
- Contradiction
  - Assume the opposite and find a contradiction
- Induction
  - Show true for a base case and show that if the property holds for the value k, then it must also hold for the value $k + 1$

Proof by Construction - Example

- A graph is k-regular if all vertices has degree k
- Proof the following theorem:
  - For all even numbers $n > 2$, there exists a 3-regular graph with n nodes.
- Strategy:
  - Find such graph, G by providing formal description of it:
  - $V = \{0, 1, ..., n-1\}$
  - $E = \{\{i, i+1\} \mid \text{for } 0 \le i \le n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i + n/2\} \mid 0 \le i \le n/2 - 1\}$

UTM

Proof by Contradiction - Example

- A number is rational if it is a fraction m/n where m and n are integers (e.g. 2/3 is a rational number, 4/6 is irrational)
- Proof that $\sqrt{2}$ is irrational.
- Strategy:
  - Assume that $\sqrt{2}$ is rational: $\sqrt{2} = m/n$
  - When m/n is rational, both m and n cannot be even numbers
  - $n\sqrt{2} = m$, $2n^2 = m^2$ by squaring both sides
  - so m^2 is an even number and can be written as 2k, proceed!

Proof by induction - Example

- **Theorem**: A binary tree with n leaves has 2n – 1 nodes
- Proving the theorem by induction:
  - Basis: Compute number of nodes for a binary tree with one leave.
  - Induction step:
    - Assume the theorem is true for binary trees with number of leaves, $n \geq 1$
    - Compute the number of nodes for case of $n + 1$

References