CS 611: Theory of Computation

Hongmin Li

California State University, East Bay

Part I

Syllabus

Course Overview

The three main computational models/problem classes in the course

Computational Model	Applications
Finite State Machines/ Regular Expressions	text processing, lexical analysis, protocol verification
Pushdown Automata/ Context-free Grammars	compiler parsing, software modeling, natural language processing
Turing machines	undecidability, computational complexity, cryptography

Skills

- Comprehend mathematical definitions
- Write mathematical definitions
- Comprehend mathematical proofs
- Write mathematical proofs

Part II

Math Preliminaries

Sets, functions, relations and sequences

- A set is a collection of items. We use $\in$ to denote the belongs to relation, that is, $a \in A$, denotes that a is an element of A. $A = \{1, 2, 3\}$ is a set whose elements are 1, 2 and 3. $N = \{1, 2, 3, ...\}$ is the set of natural numbers. It is an infinite set. $B = \{1, 2, 3, 2\}$ is NOT a set, it is a multiset, where duplicate matters. C = {n|n is an even number}
- A subset of a set is a set containing zero or more elements of the set. A is a subset of N. Some subsets of A = {1, 2, 3} are {2, 3}, {}, {1}, {1, 2, 3}. Here $1 \in A, 4 \notin A$.

Questions

- How many subsets there exists for a set A that has n elements?

Special Sets

- The empty set $\{\}$: denote, $\emptyset$, a set that has no elements
- Universal set U: either especially stated or implicit, examples: natural numbers $N = 0, 1, 2, 3, ...$, integers $N = \{..., -2, -1, 0, 1, 2, ...\}$

Operations on Sets

- Cartesian Product of Sets: Given two sets A and B, the Cartesian product $A \times B$ is the set consisting of all elements of the form (x, y) where x is an element of A and y is an element of B. $A \times B = \{(x, y)|x \in A, y \in B\}$
- If A = {1, 2}, B = {a, b, c}, what is $A \times B$? $A \times B = \{(1, a), (2, a), (1, b), (2, b), (1, c), (2, c)\}$
- Power Set: Given a set A, a power set of A, is a SET which A consists of all the subsets of A. It is denoted as $Pow(A)$ or 2^A . If $A = \{1, 2\}, 2^A = \{\{\}, \{1\}, \{2\}, \{1, 2\}\}$.
- Union $A \cup B = \{x|x \in A \text{ or } x \in B\}$ Intersection $A \cap B = \{x|x \in A \text{ and } x \in B\}$
- Complement with respect to a Universe U, $\overline{A} = \{x|x \in U, x \notin A\}$.

Sequence

- A sequence is a list of objects in order. Repetition and order both matter in a sequence. $(1, 2, 3) \neq (1, 1, 2, 3) \neq (2, 1, 3)$

Relations

- A k-ary *relation* is a subset of $A_1 \times A_2 \times \cdots \times A_k$.
- For $A = \{1, 2\}$, $B = \{a, b, c\}$, $R = \{(1, a), (1, b), (2, b)\}$ is a relation.
- A binary relation $R \subseteq A \times A$ is a *equivalence relation* if it satisfies:
  - Reflexivity: for every $a \in A$, $(a, a) \in R$
  - Symmetricity: for every $a, b \in A$, if $(a, b) \in R$, then $(b, a) \in R$
  - Transitivity: for every $a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

Functions and Relations

- A *function* F from A to B, denoted $F : A \to B$, is a mapping where for every $a \in A$, there is a unique element $b \in B$ that it is mapped to. We call A the domain and B the range of F.
- $F : A \to B$ is a *one-one* function, if for every $a, a' \in A$, if $a \neq a'$, then $F(a) \neq F(a')$.
- $F : A \to B$ is a *onto* function, if for every $b \in B$, there is an a such that $F(a) = b$.
- A function is bijective if it is both one-one and onto.

Propositional Logic

- Propositions are facts that are true or false.
- Operations on propositions: negation $\neg$, conjunction $\wedge$, disjunction $\vee$, implies $\rightarrow$, iff $\leftrightarrow$

The truth tables are as follows:

P	$\neg P$
T	F
F	T

P	Q	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Proofs

We discussed the following:

- Definition capture objects, notions, concepts
- Mathematical statement
- Proof - logical argument to establish the correctness of a mathematical statement
- Theorem - a mathematical statement which has been proved correct

Example

- Definition ODD: A integer n is odd if $n = 2k + 1$ for some integer k, otherwise, it is even, that is, $n = 2k$ for some integer k.
- Mathematical statement: If n is odd, then n^2 is odd.
- Proof: If n is odd, then $n = 2k + 1$ for some integer k. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since, $k' = 2k^2 + 2k$ is an integer and $n^2 = 2k' + 1$, n^2 is odd from the definition ODD.

Proofs

- For any two sets A and B, $\overline{A \cup B} = \bar{A} \cap \bar{B}$.
- An element x is in $\overline{A \cup B}$ iff it is not in $A \cup B$ (from the definition of complement) iff x is neither in A nor in B (from the definition of union) iff x is in $\bar{A}$ and x is in $\bar{B}$ (from the definition of complement) iff x is in their intersection $\bar{A} \cap \bar{B}$ (from the definition of intersection).

Proofs

- If n is an integer and $3n+2$ is odd, then n is odd.
- (Contrapositive) If n is not odd (even), then $3n+2$ is not odd (even).
- The truth of a statement is equivalent to its contrapositive. So, we can prove a statement, by proving its contrapositive.
- Suppose n is even, then $n = 2k$, $3n+2 = 6k+2 = 2(3k+1)$ is even.

Proof by induction

- Show that $1 + 2 + \cdots + n = n(n+1)/2$.
- Let $P(n)$ denote $1 + 2 + \cdots + n = n(n+1)/2$. We need to show that $P(1), P(2), P(3), \cdots$ are all true.
- We cannot show each of them individually.

Proof by induction

- Induction is a proof technique that allows us to prove a certain fact $P(n)$ holds for all n, by showing the following two facts:
  - $P(1)$ is true.
  - For every k, if $P(k)$ is true, then $P(k+1)$ is true.
- The first statement is called the base case. The second statement is proved for any generic k. We need to argue that $P(k+1)$ is true using the fact that $P(k)$ is true. Here $P(k)$ is called the induction hypothesis. "For every k, if $P(k)$ is true, then $P(k+1)$ is true." is the induction step.
- Note that if we prove the base case and the induction step, then we have shown that $P(n)$ is true for all n.
- $P(1)$ is true because of base case, $P(2)$ is true by instantiating $k=1$, $P(3)$ is true by taking $k=2$ and so on.

Proof by induction template

- Show that $1 + 2 + \cdots + n = n(n+1)/2$.
- **Step 0:** First, write the statement in the form of: Show that $P(n)$ is true for all n.
- Let $P(n)$ denote $1 + 2 + \cdots + n = n(n+1)/2$. We need to show that $P(n)$ is true for all n.
- **Step 1:** Prove the base case, that is, $P(1)$ is true.
- Base case: Show that $P(1)$ is true. To show $P(1)$ is true, we need to show that $1 = 1(1+1)/2$. Since, both L.H.S and R.H.S are equivalent, we have proved the statement.
- **Step 2:** Write down the induction hypothesis. $P(k) : 1 + 2 + \cdots + k = k(k+1)/2$. This will be assumed to be true.
- **Step 3:** Prove the induction step. That is, assuming $P(k)$ is true, prove that $P(k+1)$ is true.

Proof by induction template

- Show that $1 + 2 + \cdots + n = n(n+1)/2$.
- **Step 3:** Prove the induction step. That is, assuming $P(k)$ is true, prove that $P(k+1)$ is true.
- Need to show that $1 + 2 + \cdots + k + 1 = k(k+1)/2$. Think how you can use the $P(k)$ here. Alternative, how can you reduce the statement involving $k+1$ to one involving k.
- For instance, the L.H.S of $P(k+1)$ can be written $(1 + 2 + 3 + \cdots + k) + k + 1$ where the first part matches with the L.H.S of $P(k)$. Hence, you can replace $(1 + 2 + 3 + \cdots + k)$ with $k(k+1)/2$. Now, L.H.S of $P(k+1)$, namely, $(1 + 2 + 3 + \cdots + k) + k + 1$ is equal to $k(k+1)/2 + k + 1 = (k+1)(k/2+1) = (k+1)(k+2)/2$, which is the required R.H.S for $P(k+1)$.

Proof by induction template

- Show that the number of elements in the power set of A is 2^n, where n is the number of elements in A.
- **Step 0:**First, write the statement in the form of: Show that $P(n)$ is true for all n.
- Let $P(n)$ denote if a set has size n, then the number of elements in its power set is 2^n.
- **Step 1:** Prove the base case, that is, $P(1)$ is true.
- Base case: Show that $P(1)$ is true. To show $P(1)$ is true, we need to show that if a set has size 1, then its power set has size $2^1 = 2$. Consider a set of size 1. It is of the form $A = \{a\}$. Its power set is $\{\{\}, \{a\}\}$, it has size 2.
- **Step 2:** Write down the induction hypothesis. $P(k)$: If a set has size k, then its power set has size 2^k.
- **Step 3:** Prove the induction step. That is, assuming $P(k)$ is true, prove that $P(k+1)$ is true.

Proof by induction template

- Show that the number of elements in the power set of A is 2^n, where n is the number of elements in A.
- **Step 3:** Prove the induction step. That is, assuming $P(k)$ is true, prove that $P(k+1)$ is true.
- Need to show that the power set of any set with $k+1$ elements has size 2^{k+1}. Think how you can use the $P(k)$ here. Alternative, how can you reduce the statement involving $k+1$ to one involving k.
- How is a set of size $k+1$ related to a set of size k? Let A be a set of size $k+1$. Then $A = B \cup \{a\}$, where a is not an element of B, and B is of size k.
- Consider power set of A, it contains subsets of A.
- The subsets of A can be divided into two groups, X be the set of all subset of A, which do not contain a, and Y be the set of all subsets of A which contain a.

Proof by induction template

- How many elements are in X? Every element of X does not contain a, hence, it is a subset of B. And all subsets of B do not contain a, therefore they are elements of X. Therefore, X is exactly the power set of B, and contains 2^k elements.
- How many elements are in Y? Note that every element of Y contains a. That is, an element of Y is of the form $S \cup \{a\}$, where S is a subset of A and does not contain a, that is, S is a subset of B. In fact, a set S belongs to the power set of B exactly when $S \cup \{a\}$ belongs to Y. Therefore the elements of Y are obtained by adding a to every element of the power set of B. Hence, the number of elements of Y and that of power set of B are the same, and Y has 2^k elements. The total number of elements in power set of A is $2^k + 2^k = 2^{k+1}$.

Proof by induction template

- As a concrete example for the statements in the above proof, try the following.
- Take $A = \{1, 2, 3\}$. Write the subsets of A which do not contain 3, called X, and the elements in the power set of A which contain 3, called Y. You will notice that X is the power set of $B = \{1, 2\}$ and the number of elements in X and Y are the same.