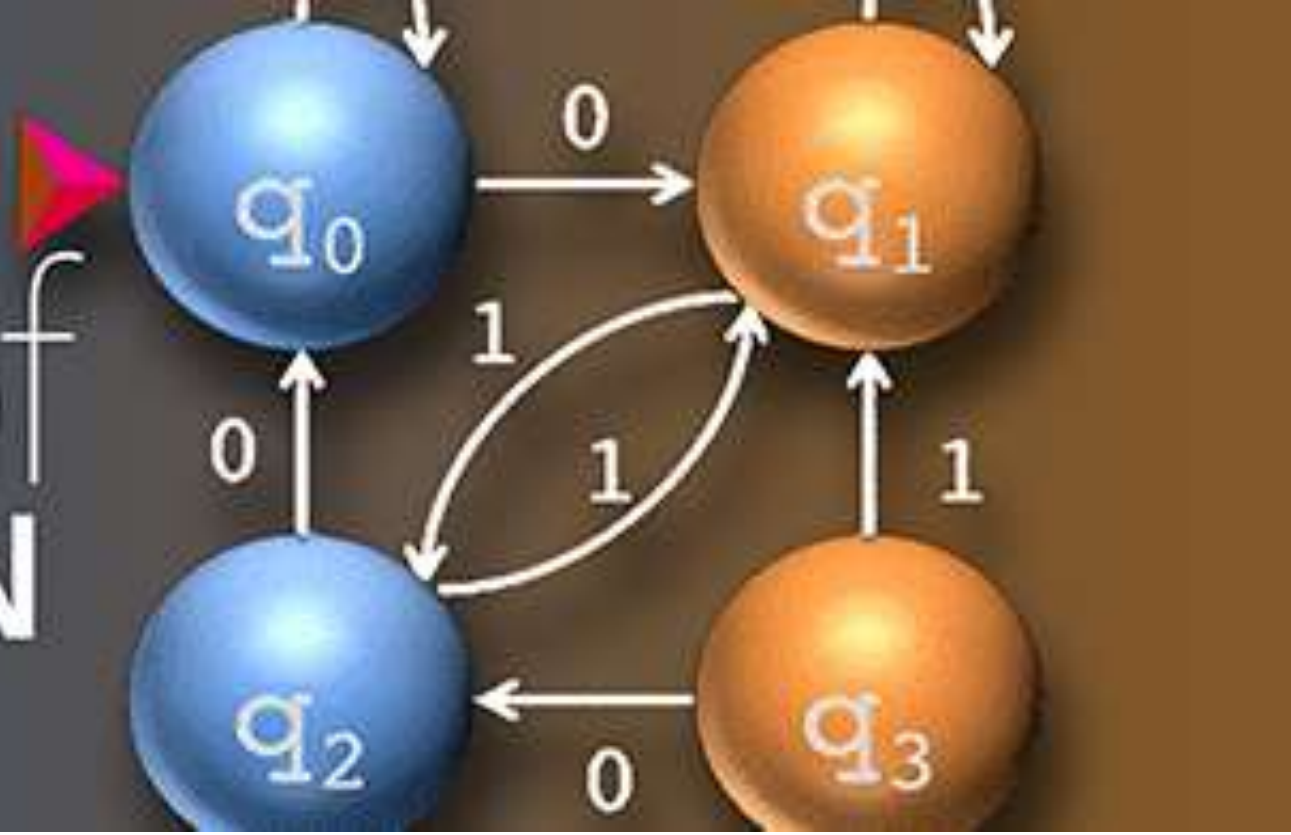
CSE 305

Theory of COMPUTATION



Lecture 13

Problems and Proof Techniques (3)

Md. Mijanur Rahman, Prof. Dr.

Dept. of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Bangladesh.

www.mijanrahman.com

Contents

Problems and Proof Techniques

- ❑ Task and Problem
- ❑ Problem Representations
- ❑ Types of Problems
- ❑ Definitions, Theorems, Proofs
- ❑ Proof Techniques

❑ Proof Techniques:

- Direct proof technique
- Proof by construction
- Proof by contradiction
- Proof by counter example
- Proof by induction
- Proof by using pigeonhole principle
- Proof technique for if and only if statements

Direct Proof Technique

- **A direct proof is a sequence of statements which are either givens or deductions from previous statements, and whose last statement is the conclusion to be proved.**
  - Direct proof technique is used to prove implication statements which have two parts, **an "if-part" known as Premises and a "then part" known as Conclusions.**
  - In this proof technique one starts with the premise and proceeds directly to conclusions with a chain of implications that use known facts, laws and formulas.

- **Definition:** We say the integer n is **even** if there is an integer k such that $n = 2k$. We say n is **odd** if there is a k such that $n = 2k-1$.

Direct Proof Technique

- **Example:** Prove that "If *n* is an even integer then n^2 is even".

  Given: n is an even integer

  To Prove: n^2 is even

- **Proof:**
  - Assume *n* is an even number (*n* is a universally quantified variable which appears in the statement we are trying to prove).
  - Because *n* is even, $n = 2k$ for some *k* (*k* is existentially quantified, defined in terms of *n*, which appears previously).
  - Now $n^2 = (2k)^2 = 2(2k^2)$ (these algebraic manipulations are examples of modus ponens).
  - Let $j = 2k^2$ (j is existentially quantified, defined in terms of k); **then $n^2 = 2j$, so n^2 is even (by definition).**

Direct Proof Technique

- **Example:** The sum of two odd numbers is even.

  Given: n, m are odd integer

  To Prove: n+m is even

- **Proof:**
  - Assume *m* and *n* are odd numbers (introducing two universally quantified variables to stand for the quantities mentioned in the statement).
  - Because *m* and *n* are odd there are integers *j* and *k;* such that m=2j−1 and n=2k−1 (introducing existentially quantified variables, defined in terms of quantities already mentioned).
  - **Now *m*+*n*=(2j−1)+(2k−1)=2(j+k−1) (modus ponens).**
  - Let i=j+k−1 (existentially quantified); **then m+n=2i is even (by definition).**

Proof by Construction

- **In this method of proof the properties in the statement given are demonstrated with an existing object (or) if such an object does not exist then a method (algorithm with steps) to create the object is provided.**

- **Example:** If a person can add any two numbers then he can add *n* numbers.

  Given: a person can add any two numbers

  To Prove: he can add *n* numbers

Proof by Construction

- **Example:** If a person can add any two numbers then he can add *n* numbers.

  Given: a person can add any two numbers

  To Prove: he can add *n* numbers

- **PROOF:** The statement is proved by proof by construction and the steps are as follows:

To add the n numbers $a_1, a_2, a_3, \ldots, a_n$:

1. Assign Sum = a_1 and $j = 2$.
2. Sum = Sum + a_j.
3. $j = j + 1$, go to Step 2 till $j \leq n$.
4. Sum contains the result of addition of n numbers.

Thus, the statement is proved.

Proof by Contradiction

- Proof by contradiction is a technique which can be used for all the type of statements.
- **In this method it is assumed the statement that is to be proved is false and showed that this assumption leads to contradiction of some well-known fact or contradicts some other assumption made earlier in the proof.**
- **Hence, it is concluded that the statement cannot be false.**

- Example: Prove the statement S= "$\sqrt{2}$ is irrational" using proof by contradiction technique.

  - N.B: A real number r is rational if only if it can be written as $r = a/b$ where a and b are integers and $b!=0$.

Proof by Contradiction

- **Example:** Prove the statement S = "$\sqrt{2}$ is irrational" using proof by contradiction technique.

PROOF First, we assume for the purposes of later obtaining a contradiction that $\sqrt{2}$ is rational. Thus

$$\sqrt{2} = \frac{m}{n},$$

where both m and n are integers. If both m and n are divisible by the same integer greater than 1, divide both by that integer. Doing so doesn't change the value of the fraction. Now, at least one of m and n must be an odd number.

We multiply both sides of the equation by n and obtain

$$n\sqrt{2} = m.$$

We square both sides and obtain

$$2n^2 = m^2.$$

Because m^2 is 2 times the integer n^2, we know that m^2 is even. Therefore m, too, is even, as the square of an odd number always is odd. So we can write $m = 2k$ for some integer k. Then, substituting $2k$ for m, we get

$$\begin{aligned} 2n^2 &= (2k)^2 \\ &= 4k^2. \end{aligned}$$

Dividing both sides by 2 we obtain

$$n^2 = 2k^2.$$

But this result shows that n^2 is even and hence that n is even. Thus we have established that both m and n are even. But we had earlier reduced m and n so that they were *not* both even, a contradiction.

Proof by Counter Example

- This is different from the proving methods, **this method of proof is used to prove that the given statement is false.**
- Using this method it is easy to prove that generalized statements are false. It is sufficient to choose one sample and say the statement does not hold good.
- **Example:** Consider the following statement “All primes are odd” and prove it is false.
- **PROOF:**
  - The statement given above is a generalized statement and it generalizes that the set of all prime numbers are odd.
  - It can be proved false by considering one prime and show that the prime number is even.
  - **The number 2 is considered, 2 is a prime number but it is even hence the given statement is false.**

Proof by Induction

- Induction is the technique by which the truth of a general statement can be inferred from the truth of a few specific instances.
- **Therefore, the process of reasoning from general observations to specific truth is called induction**. The method of proof by induction is discussed as follows:
- ***Method of proof by induction***
  - Consider *P(n)* to be a proposition (or statement) where *n* is a positive integer.
  - To prove the statement we need to follow the three steps listed below.
    - ***i.*** ***Basic step:*** Show that the proposition (or statement) *P(n)* is true for *n* = 0 or 1.
    - ***ii.*** ***Induction hypothesis:*** Assume that the statement or the proposition *P(n)* is true for *n* = *k*.
    - ***iii.*** ***Induction step:*** Show that the statement or the proposition *P(n)* is also true when n = *k+1*.

Proof by Induction

- **Example: Proof by mathematical induction**

Example Prove $1^3 + 2^3 + 3^3 + 4^3 + \ldots + n^3 = \{n(n+1)/2\}^2$ using mathematical induction.

Solution

Basic step: For $n = 1$, $P(1) = 1^3 = \{1(1+1)/2\}^2 = 1^2 = 1$; therefore, the statement is true for $n = 1$.

Induction hypothesis: Let $P(n)$ be true for $n = k$, i.e., $1^3 + 2^3 + 3^3 + 4^3 + \ldots + k^3 = \{k(k+1)/2\}^2$

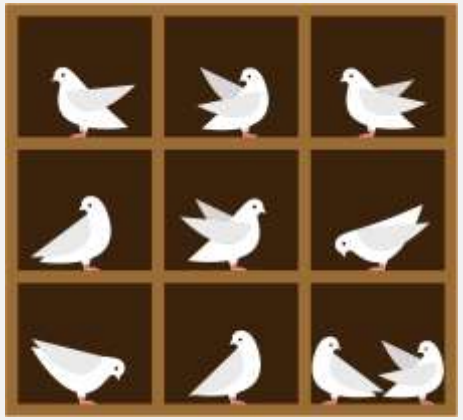
Induction step: Adding $(k+1)^3$ on both sides of the above equation, we obtain

$$\begin{aligned} 1^3 + 2^3 + 3^3 + 4^3 + \ldots + k^3 + (k+1)^3 &= \{k(k+1)/2\}^2 + (k+1)^3 \\ &= [k^2(k+1)^2 + 4(k+1)(k+1)^2]/4 \\ &= \{(k+1)^2[k^2 + 4(k+1)]\}/4 \\ &= [(k+1)^2(k+2)^2]/4 \\ &= \{(k+1)(k+2)/2\}^2 \end{aligned}$$

- Therefore, the statement holds true for k+1 also. Hence, by induction, it holds true for all values of n.

Proof by Using Pigeonhole Principle

- The pigeonhole principle states that "**if there are *n* boxes and *m* items (or pigeons) where the number of items is greater than the number of boxes, i.e., *m* > n, there will be at least one box which contains more than one items or pigeons**".
- **The formal statement of the principle is given as:**
  - There does not exist an injective function on finite sets whose co-domain is smaller than its domain.
  - Thus, some two elements of the domain have the same image.



Proof by Using Pigeonhole Principle

- **Proposition PHP1:**
  - (The Pigeonhole Principle, simple version.): **If k+1 or more pigeons are distributed among k pigeonholes, then at least one pigeonhole contains two or more pigeons.**

- **Proof:**
  - The contrapositive of the statement is: If each pigeonhole contains at most one pigeon, then there are at most k pigeons. This is easily seen to be true.

Proof by Using Pigeonhole Principle

- **Proposition PHP2:**

Proposition PHP2. (The Pigeonhole Principle.) If n or more pigeons are distributed among $k > 0$ pigeonholes, then at least one pigeonhole contains at least $\lceil \frac{n}{k} \rceil$ pigeons.

Proof.

Suppose each pigeonhole contains at most $\lceil \frac{n}{k} \rceil - 1$ pigeons. Then, the total number of pigeons is at most $k(\lceil \frac{n}{k} \rceil - 1) < k(\frac{n}{k}) = n$ pigeons (because $\lceil \frac{n}{k} \rceil - 1 < \frac{n}{k} \leq \lceil \frac{n}{k} \rceil$). ∎

Proof by Using Pigeonhole Principle

- **Example PHP1:** Prove that if seven distinct numbers are selected from {1, 2,..., 11}, then some two of these numbers sum to 12.
- **Proof:** Let the pigeons be the numbers selected. Define six pigeonholes corresponding to the six sets: {1, 11}, {2, 10}, {3, 9}, {4, 8}, {5, 7}, {6}. When a number is selected, it gets placed into the pigeonhole corresponding to the set that contains it. Since seven numbers are selected and placed in six pigeonholes, some pigeonhole contains two numbers. By the way the pigeonholes were defined, these two numbers sum to 12.
- Another way to write up the above proof is: Since seven numbers are selected, the Pigeonhole Principle guarantees that two of them are selected from one of the six sets {1, 11}, {2, 10}, {3, 9}, {4, 8}, {5, 7}, {6}. These two numbers sum to 12.
- In Example PHP1, the quantity seven is the best possible in the sense that it is possible to select six numbers from {1, 2,..., 11} so that no two of the numbers selected sum to 12. One example of six such numbers is 1, 2, 3, 4, 5, 6.

Proof Technique for If and Only If Statements

- If and only If statements are special type of if statements which implies that **when the premise is true the conclusion is true and when the conclusion is true premise is also true.** These types of statements are special type of implication statements similar to English statements that have ‘vice versa’ as part of their statements. ‘If and only If’ statements may be shortly referred using ‘iff’.
- To prove ‘iff’ statements the statement is divided into two implication statements and both the statements are proved using any of the proof techniques seen above.
- The two statements obtained after splitting the ‘if and only if’ statements are called ‘if-part’ and ‘only-if part’. Consider a ‘iff’ statement ‘*A* if and only if *B*’, this statement is splitted as follows
  1. **If-part:** if *B* then *A*.
  2. **Only-if part:** if *A* then *B*.

Proof Technique for If and Only If Statements

- **Example:** Prove the statement 'a mod b is equal to b mod a if and only if a is equal to b where a and b are positive integers'.

PROOF: The first step in proving "iff" statements is to split the given statement into two parts if-part and only-if part. The given statement is split into "if-part" and "only-if part" as given below:

If-part: if $a = b$ then $a \bmod b = b \bmod a$

Only-if part: if $a \bmod b = b \bmod a$ then $a = b$.

Proof for "If-part"

This part is proved using direct proof technique. By the definition of modulus, $x \bmod x = 0$. Therefore, when $a = b$, $a \bmod b = b \bmod a = 0$.

Proof for "Only-if part"

This part of the statement is proved using proof by contradiction. Therefore, it is assumed that "a mod b is equal to b mod a", and "a is not equal to b".

When 'a' is not equal to 'b', either $a > b$ or $a < b$.

Let $r = a \bmod b$ and $r_1 = b \bmod a$

When $a > b$, $r < b$, as per the definition a mod b returns only values from 0 to $b - 1$, and $r_1 = b$.

The assumption "a mod b is equal to b mod a" leads to conclude that b is less than itself. By mathematical theory, a number cannot be less than itself hence the assumption made earlier has led to a contradiction.

?

THE END