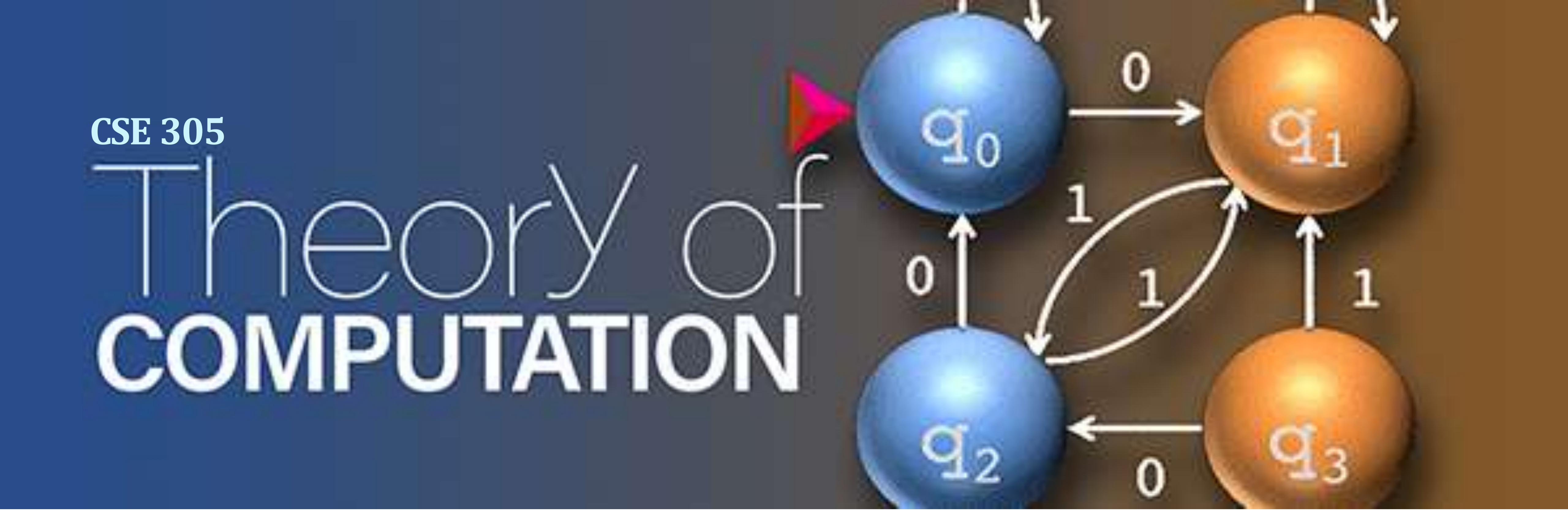


Lecture 12

Problems and Proof Techniques (2)

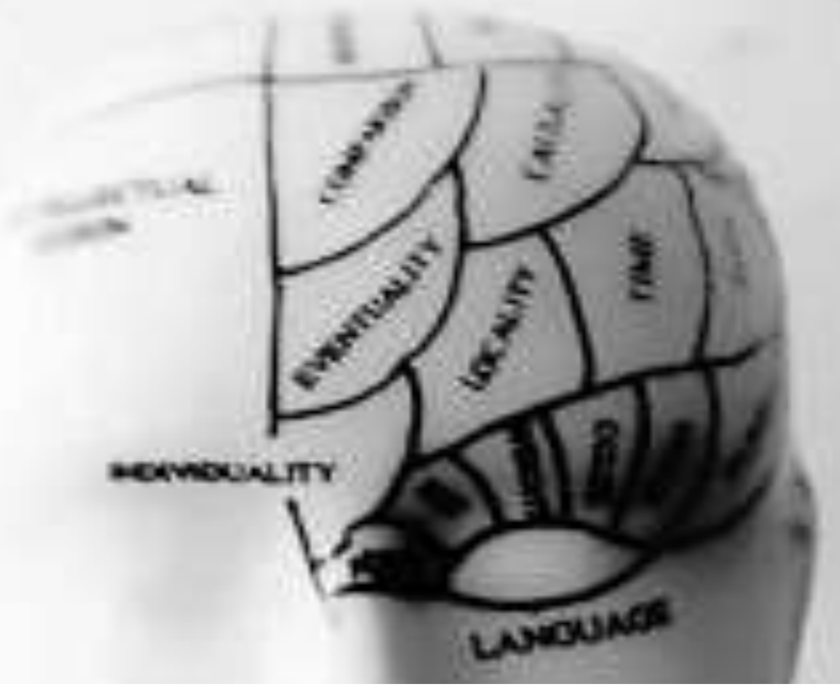
Md. Mijanur Rahman, Prof. Dr.

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

Definitions, Theorems, Proofs

- **Theorems and proofs** are the heart and soul of mathematics and **definitions** are its spirit. These three entities are central to every mathematical subject, including ours.
- ***Definitions: Definitions*** describe the objects and notions that we use. A definition may be simple, as in the definition of *set*, or complex as in the definition of *security* in a cryptographic system. Precision is essential to any mathematical definition.
- When defining some object we must make clear what constitutes that object and what does not. After we have defined various objects and notions, we usually make ***mathematical statements*** about them. Typically a statement expresses that some object has a certain property.
- The statement may or may not be true, but like a definition, it must be precise. There must not be any ambiguity about its meaning.

Definitions, Theorems, Proofs

- **Proof:** Proof is an art of convincing the reader that the given statement is true.
  - A ***proof*** is a convincing logical argument that a statement is true. In mathematics an argument must be airtight, that is, convincing in an absolute sense.
  - In everyday life or in the law, the standard of proof is lower. A murder trial demands proof "beyond any reasonable doubt." The weight of evidence may compel the jury to accept the innocence or guilt of the suspect.
  - However, evidence plays no role in a mathematical proof. A mathematician demands proof beyond *any* doubt.

Definitions, Theorems, Proofs

- **Theorem:**
  - A ***theorem*** is a mathematical statement proved true. Generally we reserve the use of that word for statements of special interest.
  - Occasionally we prove statements that are interesting only because they assist in the proof of another, more significant statement. Such statements are called ***lemmas.***
  - Occasionally a theorem or its proof may allow us to conclude easily that other, related statements are true. These statements are called ***corollaries*** **(*consequences* or *outcomes*)** of the theorem.

Finding Proofs

- The only way to determine the truth or falsity of a mathematical statement is with a mathematical proof. Unfortunately, finding proofs isn't always easy. It can't be reduced to a simple set of rules or processes.
- During this course, you will be asked to present proofs of various statements. Don't despair at the prospect! Even though no one has a recipe for producing proofs, some helpful general strategies are available.

- Finding proofs involves:
    1. First, carefully read the statement you want to prove.
    2. Do you understand all the notation?
    3. Rewrite the statement in your own words.
    4. Break it down and consider each part separately.

Finding Proofs

- Sometimes the parts of a multipart statement are not immediately evident. One frequently occurring type of multipart statement has the form "*P* if and only if Q", where both P and Q are mathematical statements.
  1. This notation is shorthand for a two-part statement. The first part "*P* if and only if Q", which means: If P is true, then Q is true, written as $P \Rightarrow Q$.
  2. The second part is "*P* if Q", which means: If Q is true, then P is true, written as $P \Leftarrow Q$.

- The first of these parts is the forward direction of the original statement, and the second is the reverse direction. We write "*P* if and only if Q" as $P \Leftrightarrow Q$.

Finding Proofs

- **Finally, when you believe that you have found the proof, you must write it up properly.**
  1. A well-written proof is a sequence of statements, wherein each one follows by simple reasoning from previous statements in the sequence.
  2. Carefully writing a proof is important, both to enable a reader to understand it and for you to be sure that it is free from errors.

Few Tips for Producing a Proof

- The following are a few tips for producing a proof:

1. ***Be patient.*** Finding proofs takes time. If you don't see how to do it right away, don't worry. Researchers sometimes work for weeks or even years to find a single proof.
2. ***Come back to it.*** Look over the statement you want to prove, think about it a bit, leave it, and then return a few minutes or hours later. Let the unconscious, intuitive part of your mind have a chance to work.
3. ***Be neat.*** When you are building your intuition for the statement you are trying to prove, use simple, clear pictures and/or text. You are trying to develop your insight into the statement, and sloppiness gets in the way of insight. Furthermore, when you are writing a solution for another person to read, neatness will help that person understand it.
4. ***Be concise.*** Brevity helps you express high-level ideas without getting lost in details. Good mathematical notation is useful for expressing ideas concisely. But be sure to include enough of your reasoning when writing up a proof so that the reader can easily understand what you are trying to say.

Types of Proof Techniques

- **Proof of a mathematical statement is an art of convincing the reader that the given statement is correct.**
- The proof techniques are chosen according to the statement that is to be proved.
  - Some of the proof techniques start with the given statement and some of them start with the opposite of the given statement and some statements are proved by constructing a model.
- There are different methods to prove a statement based on the way the proof starts and proceeds.

Types of Proof Techniques

- **The followings are some important proof techniques used in computation:**
  1. Direct proof technique
  2. Proof by construction
  3. Proof by contradiction
  4. Proof by counter example
  5. Proof by induction
     1. Recursive functions
     2. Principle of mathematical induction
     3. The strong principle of induction
     4. Structural induction
  6. Proof by using pigeonhole principle
  7. 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.**
  1. 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.**
  2. 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:**
  1. Assume n is an even number (n is a universally quantified variable which appears in the statement we are trying to prove).
  2. Because n is even, $n = 2k$ for some k (k is existentially quantified, defined in terms of n, which appears previously).
  3. Now $n^2 = (2k)^2 = 2(2k^2)$ (these algebraic manipulations are examples of modus ponens).
  4. 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:**
  1. Assume *m* and *n* are odd numbers (introducing two universally quantified variables to stand for the quantities mentioned in the statement).
  2. 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).
  3. **Now $m+n=(2j-1)+(2k-1)=2(j+k-1)$ (modus ponens).**
  4. Let $i=j+k-1$ (existentially quantified); **then $m+n=2i$ is even (by definition).**

? THE END