Definitions, Theorems, and Proofs

Intro to Theory of Computation +

Math Review – Part 3

Definitions, theorems, and proofs

"*Theorems and proofs are the heart and soul of mathematics and definitions are its spirit"*….Sipser

- Definitions describe the objects and notions that we use.
- A proof is a *convincing* logical argument that a statement is true
  - Convincing in an absolute sense ("beyond reasonable doubt" is not enough. Mathematics demands proof beyond **any** doubt.)
- A theorem is a mathematical statement proved true.

Theorem and its cousins

- Generally, we reserve the use of the word *theorem* 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

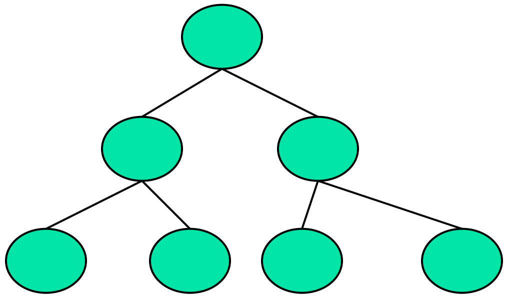
- Occasionally a theorem or its proof may allow us to conclude easily that other, related statements are true.
  - Such statements are called corollaries of the theorem

An example

Theorem: *The height of an n-node binary tree is at least floor(log n)*

Lemma: *Level i of a perfect binary tree has 2^i nodes.*

Corollary: *A perfect binary tree of height h has $2^{h+1}-1$ nodes.*



Quantifiers

"For all" or *"For every"*

- Universal proofs
- Notation: $\forall$

"There exists"

- Used in existential proofs
- Notation: $\exists$

Implication is denoted by =>

- E.g., "IF A THEN B" can also be written as "A=>B"

Finding proofs

- Finding proofs isn't always easy

- Even though no one has a recipe for producing proofs, some helpful general strategies are available
  - Carefully read the statement you want to prove. Rewrite the statement in your own words.
  - Break it down and consider each part separately
    - E.g 1. P if and only if Q statement
    - E.g 2. A = B statement

- Tips for producing a proof:
  - ***Be patient. Come back to it. Be neat. Be concise.***

Proof techniques

- By construction
  - Many theorems state that a particular type of object exists. One way to prove such a theorem is by demonstrating how to construct the object.
  - Example:

    Theorem. For each even number n greater than 2, there exists a 3-regular graph with n nodes

Example of proof by construction

THEOREM 0.22

For each even number n greater than 2, there exists a 3-regular graph with n nodes.

PROOF Let n be an even number greater than 2. Construct graph $G = (V, E)$ with n nodes as follows. The set of nodes of G is $V = \{0, 1, \ldots, n-1\}$, and the set of edges of G is the set

$$\begin{aligned} E = \{\, \{i, i+1\} \mid \text{ for } 0 \leq i \leq n-2\} \cup \{\, \{n-1, 0\}\,\} \\ \cup \{\, \{i, i+n/2\} \mid \text{ for } 0 \leq i \leq n/2 - 1\}. \end{aligned}$$

Picture the nodes of this graph written consecutively around the circumference of a circle. In that case, the edges described in the top line of E go between adjacent pairs around the circle. The edges described in the bottom line of E go between nodes on opposite sides of the circle. This mental picture clearly shows that every node in G has degree 3.

Proof techniques

- By construction
  - Many theorems state that a particular type of object exists. One way to prove such a theorem is by demonstrating how to construct the object.
  - Example:

    Theorem. For each even number n greater than 2, there exists a 3-regular graph with n nodes

- By contradiction
  - Start with the statement contradictory to the given statement
  - Example. Prove that sqrt(2) is irrational.
    - (Start by claiming that sqrt(2) is rational, and so it can be written as a ratio of two integers and arrive at a contradiction.)

Details on proof of sqrt(2) is irrational

- $\sqrt{2} = m/n$
- $n\sqrt{2} = m$
- $2n^2 = m^2$
- $2n^2 = (2k)^2$
- $2n^2 = 4k^2$
- $n^2 = 2k^2$

Proof techniques

- By induction
  - (2 parts) **Basis**, induction hypothesis, **induction step**

The format for writing down a proof by induction is as follows.

Basis: Prove that $\mathcal{P}(1)$ is true.

$$\vdots$$

Induction step: For each $i \geq 1$, assume that $\mathcal{P}(i)$ is true and use this assumption to show that $\mathcal{P}(i+1)$ is true.

$$\vdots$$

Proof techniques

- By induction
  - (2 parts) **Basis**, induction hypothesis, **induction step**
- (By counter-example)
  - Show an example that disproves the claim
- Note: There is no such thing called a "proof by example"!
  - So, when asked to prove a claim, an example that satisfied that claim is *not* a proof

Different ways of saying the same thing

- "*If* H *then* C":
  1. H *implies* C
  2. *H => C*
  3. C *if* H
  4. H *only if* C
  5. *Whenever* H *holds*, C *follows*

"If-and-Only-If" statements

- "A if and only if B"   (A <==> B)
  - *(if part)* if B then A   (<=)
  - *(only if part)* A only if B   (=>)
    (same as "if A then B")
- "If and only if" is abbreviated as "iff"
  - i.e., "A iff B"
- Example:
  - Theorem: *Let x be a real number. Then floor of x = ceiling of x if and only if x is an integer.*
- Proofs for iff have two parts
  - One for the "if part" & another for the "only if part"

Summary (of last three lectures)

- Theory of computation overview
- Mathematical notions and terminology
  - Sets
  - Sequences and tuples
  - Functions and relations
  - Graphs
  - Strings and languages
  - Boolean logic
- Definitions, theorems, and proofs
- Proof techniques
  - By construction
  - By contradiction
  - By induction

HW1 is out

- Due: Fri Jan 28
- Has 6 problems
  - 4 on what we covered so far (look back)
  - 2 on what we will cover next lecture (look forward)
  - 1 involves history of computation
- Submission on Canvas: PDF