Proofs

Slides by Christopher M. Bourke
Instructor: Berthe Y. Choueiry

Spring 2006

Computer Science & Engineering 235
Introduction to Discrete Mathematics
Section 1.5 of Rosen
cse235@cse.unl.edu

Notes

Introduction I

> *"A proof is a proof. What kind of a proof? It's a proof. A proof is a proof. And when you have a good proof, it's because it's proven."* –Jean Cocteau

> *"Mathematical proofs, like diamonds, are hard and clear, and will be touched with nothing but strict reasoning."* –John Locke

Mathematical proofs are, in a sense, the only truly absolute knowledge we can have. They provide us with a guarantee as well as an explanation (and hopefully some deep insight).

Notes

Introduction II

Mathematical proofs are necessary in computer science for several reasons.

- An algorithm must always be proven *correct*.
- You may also want to show that its more efficient than other method. This requires a proof.
- Proving certain properties of data structures may lead to new, more efficient or simpler algorithms.
- Arguments may entail assumptions. It may be useful and/or necessary to make sure these assumptions are actually valid.

Notes

Introduction

Terminology

- A *theorem* is a statement that can be shown to be true (via a proof).
- A *proof* is a sequence of statements that form an argument.
- *Axioms* or *postulates* are statements taken to be self-evident, or assumed to be true.
- *Lemmas* and *corollaries* are also (certain types of) theorems. A *proposition* (as opposed to a proposition in logic) is usually used to denote a fact for which a proof has been omitted.
- A *conjecture* is a statement whose truth value is unknown.
- The *rules of inference* are the means used to draw conclusions from other assertions. These form the basis of various methods of proof.

Notes

Theorems

Example

Consider, for example, Fermat's Little Theorem.

Theorem (Fermat's Little Theorem)

If p is a prime which does not divide the integer a, then $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

What is the assumption? Conclusion?

Notes

Proofs: A General How To I

An argument is valid if whenever all the hypotheses are true, the conclusion also holds.

From a sequence of assumptions, $p_1, p_2, \ldots, p_n$, you draw the conclusion p. That is;

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

Notes

Proofs: A General How To II

Usually, a proof involves proving a theorem via intermediate steps.

Example

Consider the theorem "If $x > 0$ and $y > 0$, then $x + y > 0$." What are the assumptions? Conclusion? What steps would you take?

Each step of a proof must be justified.

Notes

Rules of Inference

Recall the handout on the course web page `http://www.cse.unl.edu/~cse235/files/LogicalEquivalences.pdf` of logical equivalences.

Table 2 contains a Cheat Sheet for Inference rules.

Notes

Rules of Inference

Modus Ponens

Intuitively, *modus ponens* (or *law of detachment*) can be described as the inference, "p implies q, p is true, therefore q holds".

In logic terms, modus ponens is the tautology

$$(p \wedge (p \to q)) \to q$$

Notation note: "therefore" is sometimes denoted $\therefore$, so we have, p and $p \to q$, $\therefore q$.

Notes