Discrete Mathematical Structures
CS 3233 Lecture Seven

Prof. William Winsborough
September 20, 2007

Business

- Hand in Homework 4
  - Except, as discussed in email, the problems in Section 1.5 will be due next Thursday, 9/27
- Homework 5 due Thursday 9/27:
  - Section 1.5: 4, 8, 16
  - Section 1.6: 2 (natural-language proof), 12, 18
  - Section 1.7: 4, 6, 8
  - Section 2.1: 2a, 2b, 6, 8, 18
- Read for Tuesday 9/25
  - 2.1 and 2.2

Theorems and Proofs

- A *theorem* is a statement (such as a formula) that can be shown to be true in all cases (a tautology)
  - Typically a theorem takes the form of an implication stating that certain *assumptions* entail a certain *conclusion*
- A proof is a demonstration that a statement is a theorem
- Example methods of proof
  - Construction of truth tables
  - Use of equivalences
    - By using these alone, can prove only logical equivalences
  - Use rules of inference to derive the conclusion from the theorem's assumptions

Important Related Terminology

- *Result*: often used to mean a theorem
- *Proposition*: a simple theorem, often presented without proof
- *Lemma*: a theorem whose main utility lies in helping to prove other, more interesting theorems
- *Corollary*: a theorem that follows easily from another more general theorem
- *Conjecture*: a statement that you suspect is true but that you do not yet have a proof for

Rules of Inference for Propositional Logic

- A general, systematic method of proving formulas
- See Table 1 p.66
  - Known equivalences can also be used in proofs
- Use rules of inference to show
  - These hypotheses:
    - If it does not rain or if it is not foggy, the sailing race will be held and the lifesaving demonstration will take place
    - If the race is held, the trophy will be awarded
    - The trophy was not awarded
  - Imply this conclusion:
    - It rained

Some Important Methods of Proof

- Direct proof of $p \rightarrow q$
  - Assume p, derive q
- Proof by Contraposition: directly prove the contrapositive $\neg q \rightarrow \neg p$
  - Assume $\neg q$, derive $\neg p$
- Vacuous and trivial proofs
  - Show that $p \rightarrow q$ holds by showing that p does not hold
- Proof by contradiction
  - Prove p by directly proving $\neg p \rightarrow F$

Rules of Inference for Universally Quantified Statements

- Universal instantiation

$$\frac{\forall x.\ p(x)}{p(c)}$$

  – For any c
- Universal generalization

$$\frac{p(c)}{\forall x.\ p(x)}$$

  – Must show p(c) for *arbitrary* c (meaning c cannot be subject to any assumptions)

Rules of Inference for Existentially Quantified Statements

- Existential instantiation

$$\frac{\exists x.\ p(x)}{p(c)}$$

  – c must be a new name (*i.e.,* a new constant) that does not appear earlier in the proof
- Existential generalization

$$\frac{p(c)}{\exists x.\ p(x)}$$

  – c can be any constant

Universal Modus Ponens

- Combines propositional modus ponens with universal instantiation:

$$\frac{\forall x.\Phi(x)\rightarrow\Psi(x) \quad \Phi(c)}{\Psi(c)}$$

- Practice problems: 14, p73; 1, 11, 17, p85

Constructing Proofs

- Practice problems: 14, p73; 1, 11, 17, p85

Proof Methods for Quantifiers

- Existence proofs (p91)
  – Constructive: find a witness
  – Nonconstructive: Use case analysis and the tautology $p \vee \neg p$
- Practice Problem: 7,p102