Discrete Mathematical Structures
CS 3233 Lecture Six

Prof. William Winsborough
September 12, 2006

Business

- Read Sections 2.1 and 2.2 for Thursday
- **Homework Three:** due Tuesday September 19
  - Section 1.6: 2 (natural-language proof), 12, 18
  - Section 1.7: 4, 6, 8
  - Section 2.1: 2a, 2b, 6, 8, 18
  - Section 2.2: 2, 6, 10, 20, 26a
- Questions???

Theorems and Proofs

- A *theorem* is a statement (such as a formula) that can be shown to be true in all cases (a tautology)
- 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
  - More general rules of inference

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

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 $\neg p \rightarrow F$

Example Proof by Contradiction

- Example 21, p.66:
  - Def: a real number *r* is *rational* if there exist integers *s* and *t* such that $r = s / t$. Otherwise *r* is called *irrational*
  - Theorem: $\sqrt{2}$ is irrational
  - Proof Strategy: Assume $\sqrt{2}$ is rational and derive a contradiction (a false statement)
    - p is "$\sqrt{2}$ is irrational"
    - Directly prove $\neg p \rightarrow F$

More Important Methods of Proof

- Proof by case analysis
- Proof of equivalence
- Existence proof—Constructive/Non-constructive
  - Constructive example
    - "Prove there are 100 consecutive positive integers that are not perfect squares"
    - Proof sketch: consider the integers between 100^2 and 101^2
  - Non-constructive example
    - Show there exist irrational x and y such that x^y is rational
    - Proof:
      - $x=\sqrt{2}$ and $y=\sqrt{2}$ (if $\sqrt{2}^{\sqrt{2}}$ rational) or
      - $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$ (if $\sqrt{2}^{\sqrt{2}}$ is irrational)

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

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

Rules of Inference for Existentially Quantified Statements

- Existential instantiation

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

  - c must be a new name (constant) that does not appear earlier in the proof
- Existential generalization

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

  - c can be any name

Universal Modus Ponens

- Combines propositional modus ponens with universal instantiation:

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

Using Rules of Inference for Quantified Statements

- Problems 14 and 15, p.73
- We won't always be so meticulous about identifying exactly which rules of inference are being used
  - But it's important to understand the fundamentals of how proofs can be constructed