Discrete Mathematical Structures
CS 2233 Lecture Five

Prof. William Winsborough
January 27, 2009

Business

- **Recall: Attendance in recitation is not optional!**
- **Recall:** Homework 2 due Thursday January 29
  - Section 1.2: 2, 6, 10
  - Section 1.3: 10d, 10e, 14, 24c, 24d, 32a, 32b, 44
- Return Homework 1
- Practice Quiz
- Questions???

Exercise: In Which Numeric Domains Does each of the Following Hold?

- Domains
  - Z – The integers
  - N – The natural numbers (non-negative integers)
  - R^+ – The positive reals
  - $R^+ \cup \{0\}$ – The non-negative reals
- Formulas (Assume "<" and "≤" have usual interpretation)
  - $\forall x.\exists y.y<x$
  - $\exists x.\forall y.x \leq y$
  - $\forall x.\forall z.(x<z \rightarrow \exists y.(x<y)\wedge(y<z))$

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
    - Sequence of equivalences rewriting one formula into the other
    - 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

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:

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

- Practice problems 14 and 15, p.73

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