Discrete Mathematical Structures

CS 2233 Lecture Six

Prof. William Winsborough

January 29, 2009

Business

- Homework 3 due Thursday 2/5:
  - Section 1.4: 2a, 2c, 4c-f, 10 (except h), 24a, 24d, 46
    - Work 4a, 4b, 10h together
    - In 46, ***explain your answers*** and assume the usual interpretation for arithmetic and relational operators
  - Section 1.5: 4, 8, 16
  - Section 1.6: 2 (natural-language proof), 12, 18
  - Section 1.7: 4, 6, 8
- Read for Tuesday 9/18
  - 1.4, 1.5 and 1.6
  - 1.7 through example 14 (p.95)
- Turn in Homework 2
- Further discussion of Homework 1?
- Final question from Practice Quiz 1
- 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:

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

- 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

Proof by Case Analysis

- Suppose we want to prove $p \rightarrow q$
  – Further suppose that $p \equiv p_1 \vee p_2 \vee \ldots \vee p_n$
- Note the following:
  $p_1 \vee p_2 \vee \ldots \vee p_n \rightarrow q \equiv$
  $p_1 \rightarrow q \wedge p_2 \rightarrow q \wedge \ldots \wedge p_n \rightarrow q$
- Putting these together, we see that to prove $p \rightarrow q$, it is sufficient to prove $p_1 \rightarrow q \wedge p_2 \rightarrow q \wedge \ldots \wedge p_n \rightarrow q$
  – Special case:
    When $p_1 \vee p_2 \vee \ldots \vee p_n \equiv T$, this is a way of proving q

Example Proof by Case Analysis

- Problem: give a natural-language proof of the following: $1+2+3+\ldots+n = n(n+1)/2$ for all $n \in \mathbb{N}$
  – Proof structure: consider 2 cases
    - Case 1) n is even:

$$\begin{aligned} &1+2+3+\ldots+n \\ &= 1 + 2 + \ldots + (n/2) + \\ &\quad n + (n-1) + \ldots + ((n/2)+1) \\ &= \underbrace{(n+1) + (n+1) + \ldots + (n+1)}_{n/2} \end{aligned}$$

    - Case 2) n is odd:

$$\begin{aligned} &1+2+3+\ldots+n \\ &= 0 + 1 + \ldots + (n-1)/2 + \\ &\quad n + (n-1) + \ldots + (n+1)/2 \\ &= \underbrace{n + n + \ldots + n}_{(n+1)/2} \end{aligned}$$

Sets

- $s \in S$ means s is an *element* of set S
- Given sets A and B,
  - $A \subseteq B$ means A is a *subset* of B
    - This means $x \in A$ implies $x \in B$
  - $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$
  - $A \subset B$ means A is a *proper subset* of B
    - $A \neq B$
  - $A = \{ a_1, a_2, \ldots \}$ means that A is enumerated by the sequence $a_1, a_2, \ldots$
- *Set comprehension:* the set of values that satisfy a given property
  - *E.g.,* $\text{EvenInts} = \{ x \mid \exists z \in Z . x=2z \}$

Basic Operators

- Empty set
  - $\emptyset = \{ \}$
- Union
  - $A \cup B = \{ x \mid x \in A \lor x \in B \}$
- Intersection
  - $A \cap B = \{ x \mid x \in A \land x \in B \}$
- Cartesian product:
  - $A x B = \{ (a,b) \mid a \in A \land b \in B \}$

Identities and Notation: Big Unions and Intersections

- Set Identities
  - Review Table 1, page 124
  - Review Example 11, page 125
- Notation:
  given a collection of sets $A_1, A_2, \cdots, A_n$

  $\bigcup_{1 \le i \le n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$

  $\bigcap_{1 \le i \le n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$