CSE 311 Foundations of Computing I

Lecture 9

Proofs and Set Theory

Autumn 2012

Announcements

- Reading assignments
  - Today: Inference, Sets and Functions
    - 2.1-2.3 6^{th} and 7^{th} Editions
    - 1.6-1.8 5^{th} Edition
  - Monday:
    - 4.1-4.2 7^{th} Edition
    - 3.4, 3.6 up to p. 227 6^{th} Edition
    - 2.4, 2.5 up to p. 177 5^{th} Edition

Highlights from last lecture

- Formal proofs:
  - simple well-defined rules
  - easy to check
- Inference rules for propositions and quantifiers

Simple Propositional Inference Rules

- Excluded middle plus two inference rules per binary connective, one to eliminate it and one to introduce it

$$\frac{p \wedge q}{\therefore p, q} \qquad \frac{p, q}{\therefore p \wedge q} \qquad \therefore p \vee \neg p$$

$$\frac{p \vee q, \neg p}{\therefore q} \qquad \frac{p}{\therefore p \vee q}$$

$$\frac{p, p \rightarrow q}{\therefore q} \qquad \frac{p \Rightarrow q}{\therefore p \rightarrow q}$$

Direct Proof Rule

Not like other rules!

See next slide…

Reference

Direct Proof of an Implication

- $p \Rightarrow q$ denotes a proof of q given p as an assumption. Don't confuse with $p \rightarrow q$.
- The direct proof rule
  - if you have such a proof then you can conclude that $p \rightarrow q$ is true
- E.g. Let's prove $p \rightarrow (p \vee q)$

  1. p Assumption
  2. $p \vee q$ Intro for $\vee$ from 1
  3. $p \rightarrow (p \vee q)$ Direct proof rule

Proof subroutine for $p \Rightarrow (p \vee q)$

Reference

Example

- Prove $((p \rightarrow q) \wedge (p \rightarrow r)) \rightarrow (p \rightarrow (q \wedge r))$

Inference Rules for Quantifiers

$$\frac{P(c) \text{ for some } c}{\therefore \exists x\, P(x)} \qquad \frac{\forall x\, P(x)}{\therefore P(a) \text{ for any } a}$$

$$\frac{\text{“Let } a \text{ be anything*”} \ldots P(a)}{\therefore \forall x\, P(x)} \qquad \frac{\exists x\, P(x)}{\therefore P(c) \text{ for some special } c}$$

* in the domain of P

Reference

Example

- Prove $(\forall x\ (p \rightarrow q(x))) \rightarrow (p \rightarrow (\forall x\ q(x)))$ where x does not occur in p

Even and Odd

$\text{Even}(x) \equiv \exists y \ (x=2y)$
$\text{Odd}(x) \equiv \exists y \ (x=2y+1)$
Domain: Integers

Prove: "The square of every even number is even"

Formal proof of: $\forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2))$

1.	Assume Even(a)	To prove: $\text{Even}(a) \rightarrow \text{Even}(a^2)$
2.	$\exists y \ (a = 2y)$	Definition of Even
3.	$a = 2b$	By ∃ elimination
4.	$a^2 = 4b^2 = 2(2b^2)$	Algebra
5.	$\exists y \ (a^2 = 2y)$	By ∃ introduction
6.	$\text{Even}(a^2)$	Definition of Even
7.	$\text{Even}(a) \rightarrow \text{Even}(a^2)$	Direct Proof rule
8.	$\forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2))$	By ∀ introduction

Reference

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove: "The square of every odd number is odd"

English proof of: $\forall x\ (Odd(x) \rightarrow Odd(x^2))$

Let x be an odd number.

Then x=2k+1 for some integer k (depending on x)

Therefore $x^2=(2k+1)^2= 4k^2+4k+1=2(2k^2+2k)+1$.

Since $2k^2+2k$ is an integer, x^2 is odd.

"Proof by Contradiction": One way to prove ¬p

If we assume p and derive False (a contradiction) then we have proved ¬p.

1. p Assumption
2. …
3. **F**
4. p → **F** Direct Proof rule
5. ¬p v **F** Equivalence from 4
6. ¬p Equivalence from 5

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove: "No number is both even and odd"

English proof: ¬ ∃x (Even(x)∧Odd(x))

≡∀x ¬(Even(x)∧Odd(x))

Let x be any integer and suppose that it is both even and odd. Then x=2k for some integer k and x=2n+1 for some integer n. Therefore 2k=2n+1 and hence k=n+½.

But two integers cannot differ by ½ so this is a contradiction.

Rational Numbers

- A real number x is *rational* iff there exist integers p and q with $q \neq 0$ such that $x = p/q$.

$$\text{Rational}(x) \equiv \exists p\, \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0)$$

- Prove:
  - If x and y are rational then xy is rational

$$\forall x\, \forall y\ ((\text{Rational}(x) \wedge \text{Rational}(y)) \rightarrow \text{Rational}(xy))$$

Domain: Real numbers

Rational Numbers

- A real number x is *rational* iff there exist integers p and q with $q \neq 0$ such that $x = p/q$.

$$\text{Rational}(x) \equiv \exists p\, \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0)$$

- Prove:
  - If x and y are rational then xy is rational
  - If x and y are rational then x+y is rational

Rational Numbers

- A real number x is *rational* iff there exist integers p and q with $q \neq 0$ such that $x=p/q$.

$$\text{Rational}(x) \equiv \exists p\, \exists q\ ((x=p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0)$$

- Prove:
  - If x and y are rational then xy is rational
  - If x and y are rational then x+y is rational
  - If x and y are rational then x/y is rational

Counterexamples

- To *disprove* $\forall x\ P(x)$ find a *counterexample*
  - some c such that $\neg P(c)$
  - works because this implies $\exists x\ \neg P(x)$ which is equivalent to $\neg \forall x\ P(x)$

Proofs

- Formal proofs follow simple well-defined rules and should be easy to check
  - In the same way that code should be easy to execute
- English proofs correspond to those rules but are designed to be easier for humans to read
  - Easily checkable in principle
- Simple proof strategies already do a lot
  - Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)

Set Theory

- Formal treatment dates from late 19th century
- Direct ties between set theory and logic
- Important foundational language

Definition: A set is an unordered collection of objects

$x \in A$: "x is an element of A"
"x is a member of A"
"x is in A"

$x \notin A$: $\neg (x \in A)$

Definitions

- A and B are *equal* if they have the same elements

$$A = B \equiv \forall x\,(x \in A \leftrightarrow x \in B)$$

- A is a *subset* of B if every element of A is also in B

$$A \subseteq B \equiv \forall x\,(x \in A \rightarrow x \in B)$$

Empty Set and Power Set

- Empty set $\varnothing$ does not contain any elements

- Power set of a set A = set of all subsets of A

$$\mathcal{P}(A) = \{ B : B \subseteq A \}$$

Cartesian Product : $A \times B$

$$A \times B = \{ (a, b) \mid a \in A \wedge b \in B \}$$

Set operations

$A \cup B = \{ x \mid (x \in A) \vee (x \in B) \}$ union

$A \cap B = \{ x \mid (x \in A) \wedge (x \in B) \}$ intersection

$A - B = \{ x \mid (x \in A) \wedge (x \notin B) \}$ set difference

$A \oplus B = \{ x \mid (x \in A) \oplus (x \in B) \}$ symmetric difference

$\overline{A} = \{ x \mid x \notin A \}$
(with respect to universe U) complement

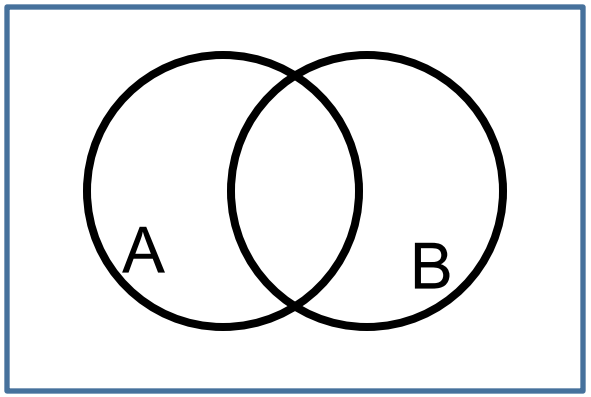
It's Boolean algebra again

- Definition for $\cup$ based on $\vee$
- Definition for $\cap$ based on $\wedge$
- Complement works like $\neg$

De Morgan's Laws

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$



Proof technique:
To show C = D show
$x \in C \rightarrow x \in D$ and
$x \in D \rightarrow x \in C$

Distributive Laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$