CSE 311 Foundations of Computing I

Lecture 8

Proofs

Autumn 2011

Announcements

- Reading assignments
  - Logical Inference
    - 1.6, 1.7 — 7th Edition
    - 1.5, 1.6 — 6th Edition
    - 1.5, 3.1 — 5th Edition

Highlights from last lecture

- Logical Inference
  - Law of excluded middle
  - Introduction and elimination rules for $\wedge$, $\vee$
  - Introduction and elimination rules for $\rightarrow$
    - Modus Ponens and Direct Proof rule
  - Introduction and elimination rules for $\forall$, $\exists$
- Proofs

Simple Propositional Inference Rules

- Excluded middle $\dfrac{\quad}{\therefore\ p \vee \neg p}$
- Two inference rules per binary connective one to eliminate it, one to introduce it.

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

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

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

Direct Proof Rule

Direct Proof of an Implication

- $p \Rightarrow q$ denotes a proof of q given p as an assumption
- The direct proof rule
  - if you have such a proof then you can conclude that $p \rightarrow q$ is true
- E.g.

Proof subroutine

1. p — Assumption
2. $p \vee q$ — Intro for $\vee$ from 1

3. $p \rightarrow (p \vee q)$ — Direct proof rule

General Proof Strategy

A. Look at the rules for introducing connectives to see how you would build up the formula you want to prove from pieces of what is given

B. Use the rules for eliminating connectives to break down the given formulas so that you get the pieces you need to do A.

C. Write the proof beginning with B followed by A.

Example

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

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

Proofs using Quantifiers

- “There exists an even prime number”

Prime(x): x is an integer > 1 and x is not a multiple of any integer strictly between 1 and x

Even and Odd

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

- Prove: “The square of every even number is even”
  Formal proof of: $\forall x\, (\text{Even}(x) \rightarrow \text{Even}(x^2))$

Even and Odd

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

- Prove: “The square of every odd number is odd”
  English proof of: $\forall x\, (\text{Odd}(x) \rightarrow \text{Odd}(x^2))$

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 $\neg p$

- If we assume p and derive False (a contradiction) then we have proved $\neg p$.

1. p Assumption

...

3. **F**
4. $p \rightarrow$ **F** Direct Proof rule
5. $\neg p \vee$ **F** Equivalence from 4
6. $\neg p$ 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: $\neg \exists x\ (\mathrm{Even}(x) \wedge \mathrm{Odd}(x))$

  $\equiv \forall x\ \neg(\mathrm{Even}(x) \wedge \mathrm{Odd}(x))$

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≠0 such that x=p/q.

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

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

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

Domain: Real numbers

Rational Numbers

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

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

- 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≠0 such that x=p/q.

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

- 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)