# CSE 311 Foundations of Computing I

Lecture 8

Proofs and Set Theory

Spring 2013



# Announcements

- Reading assignments
  - Logical Inference
    - 1.6, 1.7 7th Edition
    - 1.5, 1.6 6th Edition
  - Set Theory
    - 2.1-2.3 6th and 7th Editions
- Homework
  - Graded HW 1: If you didn't pick it up yesterday you can get it now. If you did then please return it for recording.
    - Good News: High scores Bad News: No feedback
  - HW 2 due now
  - HW 3 out later today



# Review…Simple Propositional Inference Rules

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

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

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

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

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

Direct Proof Rule

Not like other rules!

See next slide…



# 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

# Important: Applications of Inference Rules

- You can use equivalences to make substitutions of any subformula
- Inference rules only can be applied to whole formulas (not correct otherwise).

e.g. 1. $p \rightarrow q$ Given

~~2. $(p \vee r) \rightarrow q$ Intro $\vee$ from 1.~~

Does not follow! e.g p=**F**, q=**F**, r=**T**



# General Proof Strategy

1. 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**
2. Use the rules for eliminating connectives to **break down the given formulas so that you get the pieces you need** in 1.
3. Write the proof beginning with what you figured out for 2 followed by 1.



# Example

- Prove $\forall x\,(P(y) \rightarrow Q(x))) \rightarrow (P(y) \rightarrow \forall x\, Q(x))$ where x is not a free variable in P(y)



# 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. | $\text{Even}(a)$ | Assumption: a arbitrary |
| 2. | $\exists y\ (a = 2y)$ | Definition of Even |
| 3. | $a = 2c$ | By $\exists$ elimination: c specific depends on a |
| 4. | $a^2 = 4c^2 = 2(2c^2)$ | Algebra |
| 5. | $\exists y\ (a^2 = 2y)$ | By $\exists$ 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 $\forall$ 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
...
3. **F**
4. p→ **F**  Direct Proof rule
5. ¬p ∨ **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: $\neg\ \exists x\ (Even(x) \wedge Odd(x))$

$\equiv \forall x\ \neg(Even(x) \wedge Odd(x))$

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.

Rational(x) ≡ ∃p ∃q ((x=p/q)∧Integer(p) ∧Integer(q) ∧q≠0)

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

$\forall x\ \forall y\ ((Rational(x) \wedge Rational(y)) \rightarrow Rational(xy))$

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.

Rational(x) ≡ ∃p ∃q ((x=p/q)∧Integer(p) ∧Integer(q) ∧q≠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.

Rational(x) ≡ ∃p ∃q ((x=p/q)∧Integer(p) ∧Integer(q) ∧q≠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* ∀x P(x) find a *counterexample*
  - some c such that ¬P(c)
  - works because this implies ∃x ¬P(x) which is equivalent to ¬∀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 $\emptyset$ 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

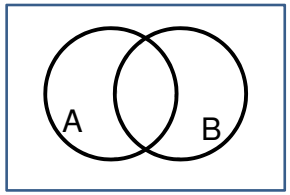
- Definition for $\cup$ based on $\vee$
- Definition for $\cap$ based on $\wedge$
- Complement works like $\neg$



# 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

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