CSE 311 Foundations of Computing I

Lecture 8

Proofs

Autumn 2012

Announcements

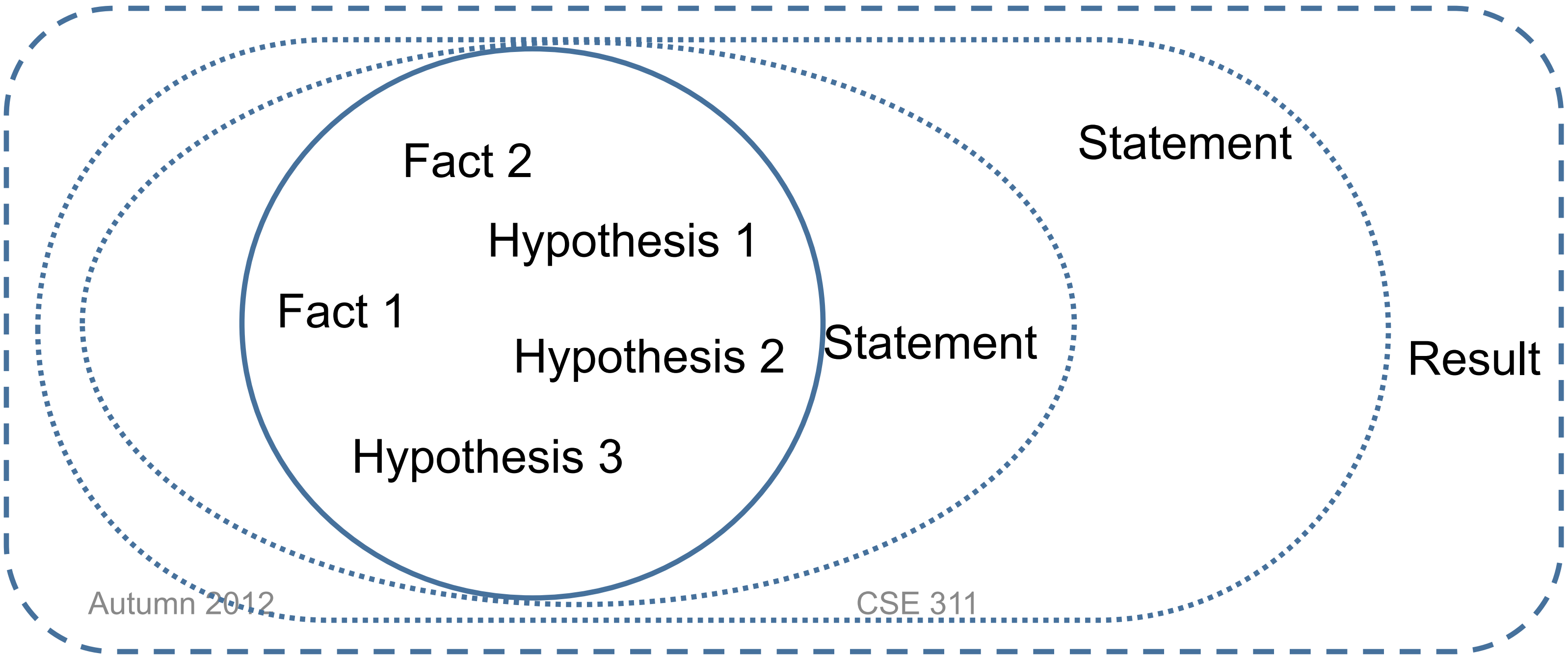
- Reading assignments
  - Logical Inference
    - 1.6, 1.7 7^{th} Edition
    - 1.5, 1.6 6^{th} Edition
    - 1.5, 3.1 5^{th} Edition
- Homework
  - HW 1 returned
  - Turn in HW2 Now!
  - HW3 available

Highlights from last lecture

- Predicate calculus, intricacies of $\forall$, $\exists$
- Introduction to inference

Proofs

- Start with hypotheses and facts
- Use rules of inference to extend set of facts
- Result is proved when it is included in the set



An inference rule: *Modus Ponens*

- If p and $p \rightarrow q$ are both true then q must be true

- Write this rule as

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

- Given:
  - If it is Wednesday then you have 311 homework due today.
  - It is Wednesday.
- Therefore, by Modus Ponens:
  - You have 311 homework due today.

Proofs

- Show that r follows from p , $p \rightarrow q$, and $q \rightarrow r$

1. p Given
2. $p \rightarrow q$ Given
3. $q \rightarrow r$ Given
4. q Modus Ponens from 1 and 2
5. r Modus Ponens from 3 and 4

Inference Rules

- Each *inference rule* is written as which means that if both A and B are true then you can infer C and you can infer D.

$$\frac{A,\ B}{\therefore\ C, D}$$

  - For rule to be correct $(A \land B) \rightarrow C$ and $(A \land B) \rightarrow D$ must be a tautologies
- Sometimes rules don't need anything to start with. These rules are called *axioms*:
  - e.g. *Excluded Middle Axiom*

$$\therefore\ p \lor \neg p$$

Simple Propositional Inference Rules

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

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

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

$$\frac{\quad}{\therefore\ p \lor \neg p}$$

$$\frac{p \lor q\ ,\ \neg p}{\therefore\ q}$$

$$\frac{p}{\therefore\ p \lor q}$$

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

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

Direct Proof Rule

Not like other rules!

See next slide...

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 $p \Rightarrow (p \vee q)$

Example

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

Proofs can use Equivalences too

Show that $\neg p$ follows from $p \rightarrow q$ and $\neg q$

1. $p \rightarrow q$ Given
2. $\neg q$ Given
3. $\neg q \rightarrow \neg p$ Contrapositive of 1 (Equivalence!)
4. $\neg p$ Modus Ponens from 2 and 3

Inference Rules for Quantifiers

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

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

$$\frac{\text{“Let a be anything*”...}P(a)}{\therefore\ \forall x\, P(x)}$$

$$\frac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some special } c}$$

* 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) ≡ ∃y (x=2y)
Odd(x) ≡ ∃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) ≡ $\exists y\ (x=2y)$
Odd(x) ≡ $\exists y\ (x=2y+1)$
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) ≡ $\exists y\ (x=2y)$
Odd(x) ≡ $\exists y\ (x=2y+1)$
Domain: Integers

Prove: "No number is both even and odd"

English proof: $\neg\ \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

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

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 $x=p/q$.

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

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

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

Domain: Real numbers

Rational Numbers

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

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

- 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)