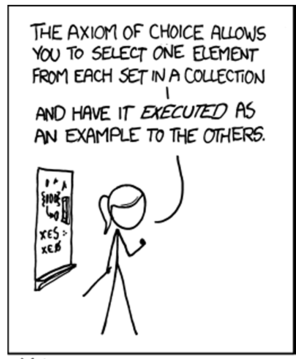
CSE 311: Foundations of Computing

Fall 2013
Lecture 8: Proofs and Set theory



MY MATH TEACHER WAS A BIG BELIEVER IN PROOF BY INTIMIDATION.

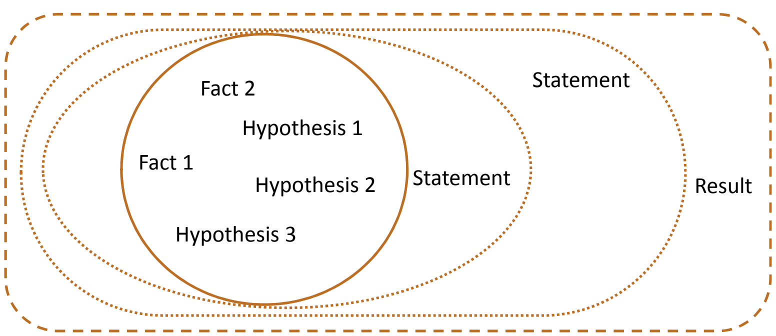
announcements

Reading assignment

- **Logical inference**
  - 1.6-1.7 7th Edition
  - 1.5-1.7 6th Edition
- **Set theory**
  - 2.1-2.3 (both editions)

review: 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



review: an inference rule— *Modus Ponens*

- If p and p $\rightarrow$ q are both true then q must be true
- Write this rule as $\dfrac{p,\ p \rightarrow q}{\therefore\ q}$
- Given:
  - If it is Wednesday then you have a 311 class today.
  - It is Wednesday.
- Therefore, by modus ponens:
  - You have a 311 class today.

review: inference rules

- Each inference rule is written as: $\dfrac{A, B}{\therefore C, D}$
  ...which means that if both A and B are true then you can infer C and you can infer D.
  - For rule to be correct $(A \wedge B) \rightarrow C$ and $(A \wedge B) \rightarrow D$ must be a tautologies
- Sometimes rules don't need anything to start with. These rules are called axioms:
  - e.g. *Excluded Middle Axiom*

$$\dfrac{\quad}{\therefore\ p \vee \neg p}$$

review: simple propositional inference rules

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

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

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

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

Direct Proof Rule
Not like other rules

review: 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

proof subroutine

Example:

1.	p	assumption
2.	$p \vee q$	intro for $\vee$ from 1
3.	$p \rightarrow (p \vee q)$	direct proof rule

review: proofs using the direct proof rule

Show that $p \rightarrow r$ follows from q and $(p \wedge q) \rightarrow r$

1.	q	given
2.	$(p \wedge q) \rightarrow r$	given
3.	p	assumption
4.	$p \wedge q$	from 1 and 3 via Intro $\wedge$ rule
5.	r	modus ponens from 2 and 4
6.	$p \rightarrow r$	direct proof rule

review: inference rules for quantifiers

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

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

$$\frac{\text{"Let } a \text{ be anything*"} \ldots P(a)}{\therefore \forall x\, P(x)}$$

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

* in the domain of P

review: 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 even number is even."

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

1. Even(a) — Assumption: a arbitrary
2. $\exists y\ (a = 2y)$ — Definition of Even
3. $a = 2c$ — By elim $\exists$: c specific depends on a
4. $a^2 = 4c^2 = 2(2c^2)$ — Algebra
5. $\exists y\ (a^2 = 2y)$ — By intro $\exists$ rule
6. 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 intro $\forall$ rule

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: $\forall x\ (\mathrm{Odd}(x) \to \mathrm{Odd}(x^2))$

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.	$p \to F$	direct Proof rule
5.	$\neg p \vee F$	equivalence from 4
6.	$\neg p$	equivalence from 5

even and odd

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
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 $q \neq 0$ 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**

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

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

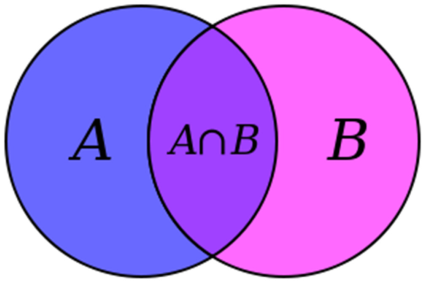
- Formal proofs follow simple well-defined rules and should be easy to check
  – In the same way that code should be easy to execute

- 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"

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

$$A = \{1, 2, 7, \text{cat}, \text{dog}, \varphi, \alpha\}$$

$$\text{cat} \in A$$
$$\text{fish} \notin A$$

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

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

set operations

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

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

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

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

$$\bar{A} = \{ x : x \notin A \}$$ (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

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

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

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

distributive laws

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