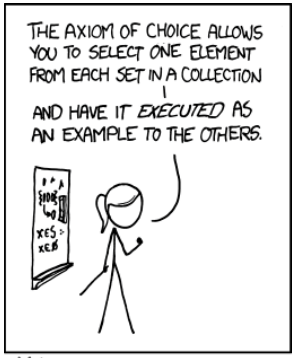
CSE 311: Foundations of Computing

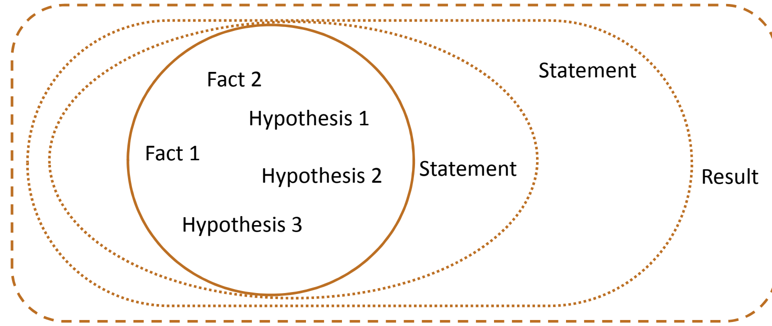
Fall 2013
Lecture 8: More Proofs



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

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: *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: Propositional Inference Rules

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

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

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

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

Direct Proof Rule
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

Inference rules for quantifiers

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

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

* in the domain of P

** By special, we mean that c is a name for a value where P(c) is true. We can't use anything else about that value, so c has to be a NEW variable!

Proofs using Quantifiers

"There exists an even prime number"

First, we translate into predicate logic:

$$\exists x \; \text{Even}(x) \land \text{Prime}(x)$$

1.	Even(2)	Fact (math)
2.	Prime(2)	Fact (math)
3.	Even(2) $\land$ Prime(2)	Intro $\land$: 1, 2
4.	$\exists$x (**Even**(x) $\land$ **Prime**(x))	Intro $\exists$: 3

Proofs using Quantifiers

1.	Even(2)	Fact* (math)
2.	Prime(2)	Fact* (math)
3.	Even(2) $\land$ Prime(2)	Intro $\land$: 1, 2
4.	$\exists$x (Even(x) $\land$ Prime(x))	Intro $\exists$: 3

Those first two lines are sort of cheating; we should prove those "facts".

1.	2 = 2*1	Definition of Multiplication
2.	Even(2)	Intro $\exists$: 1
3.	There are no integers between 1 and 2	Definition of Integers
4.	2 is an integer	Definition of 2
5.	Prime(2)	Intro $\land$: 3, 4

Prime(*x*): x is an integer > 1 and x is not a multiple of any integer strictly between 1 and x
Even(x) ≡ $\exists$y (x=2y)

Proofs using Quantifiers

1.	2 = 2*1	Definition of Multiplication
2.	Even(2)	Intro $\exists$: 1
3.	There are no integers between 1 and 2	Definition of Integers
4.	2 is an integer	Definition of 2
5.	Prime(2)	Intro $\land$: 3, 4
6.	Even(2) $\land$ Prime(2)	Intro $\land$: 2, 5
7.	$\exists$x (Even(x) $\land$ Prime(x))	Intro $\exists$: 7

Note that 2 = 2*1 by definition of multiplication. It follows that there is a y such that 2 = 2y; so, 2 is even. Furthermore, 2 is an integer, and there are no integers between 1 and 2; so, by definition of a prime number, 2 is prime. Since 2 is both even and prime, $\exists$x (**Even**(x) $\land$ **Prime**(x)).

Prime(*x*): x is an integer > 1 and x is not a multiple of any integer strictly between 1 and x
Even(x) ≡ $\exists$y (x=2y)

Even and Odd

Even(x) ≡ $\exists$y (x=2y)
Odd(x) ≡ $\exists$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: $\forall x\,(\text{Even}(x) \to \text{Even}(x^2))$

1. Even(a) — Assumption: a arbitrary integer
2. $\exists y\ (a = 2y)$ — Definition of Even
3. $a = 2c$ — By elim $\exists$: c special 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. Even(a)$\to$Even(a^2) — Direct proof rule
8. $\forall x\,(\text{Even}(x)\to\text{Even}(x^2))$ — 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: $\forall x\,(\text{Odd}(x)\to\text{Odd}(x^2))$

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.

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 $\neg\forall x\ P(x)$

Proof by Contrapositive: another strategy for implications

If we assume $\neg q$ and derive $\neg p$, then we have proven $\neg q \to \neg p$, which is the same as $p \to q$.

1. $\neg q$ — Assumption

...

3. $\neg p$

4. $\neg q \to \neg p$ — Direct Proof Rule

5. $p \to q$ — Contrapositive

Proof by Contradiction: one way to prove $\neg p$

If we assume p and derive F (a contradiction), then we have proven $\neg$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) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Prove: "No integer is both even and odd."

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

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

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

But two integers cannot differ by ½ so this is a contradiction. So, no integer is both even an odd.

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**

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

Domain: Real numbers

Rational Numbers

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

  Rational(x) $\equiv \exists p\, \exists q\ ((x=p/q) \wedge$ Integer(p) $\wedge$ 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

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)