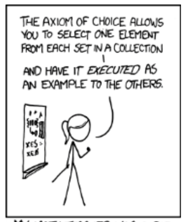
cse 311: foundations of computing

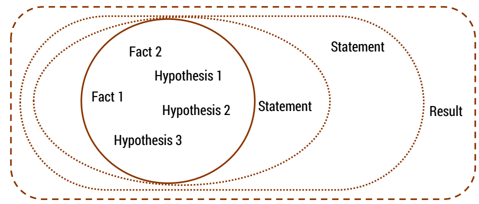
Spring 2015
Lecture 8: More Proofs



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

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

Example:

proof subroutine

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 $p \to r$ follows from q and $(p \land q) \to r$

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

review: 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) $\equiv \exists y\, (x=2y)$

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

English version:
"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) $\equiv \exists y\, (x=2y)$

even and odd

Prove: "The square of every even number is even."
Formal proof of: $\forall x\, (\text{Even}(x) \to \text{Even}(x^2))$

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

even and odd

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 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)$\rightarrow$Even(a^2)	Direct proof rule
8. $\forall x\,(\text{Even}(x)\rightarrow\text{Even}(x^2))$	By intro $\forall$ rule

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

even and odd

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. □

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

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 $\neg q \rightarrow \neg p$, which is the same as $p \rightarrow q$.

1. $\neg q$	Assumption
...	
3. $\neg p$	
4. $\neg q \rightarrow \neg p$	Direct Proof Rule
5. $p \rightarrow q$	Contrapositive

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. $p \rightarrow \mathbf{F}$	direct Proof rule
5. $\neg p \vee \mathbf{F}$	equivalence from 4
6. $\neg p$	equivalence from 5

even and odd

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

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

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

We proceed 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. □

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

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 $x=p/q$.

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

- 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 $x=p/q$.

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

You might try to 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

Domain: Real numbers

proofs summary

- 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)