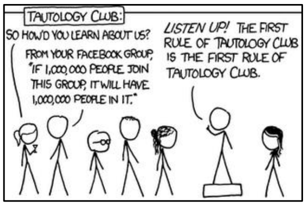
cse 311: foundations of computing

Spring 2015
Lecture 7: Proofs



proofs

Show that $\neg p$ follows from $p \rightarrow r$, $\neg r \vee s$, and $\neg s$.

recall: 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

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

example

Prove: $(p \wedge q) \rightarrow (p \vee q)$

example

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

one 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 to do (1).
3. Write the proof beginning with what you figured out for (2) followed by (1).

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

** 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."

Prime(x): x is an integer > 1 and x is not a multiple of any integer strictly between 1 and x

even and odd

Prove: "The square of every even number is even."

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

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

even and odd

Prove: "The square of every odd number is odd"

English proof of: $\forall x\, (\mathrm{Odd}(x) \rightarrow \mathrm{Odd}(x^2))$

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

even and odd

Prove: "The square of every odd number is odd"

English proof of: $\forall x\, (\mathrm{Odd}(x) \rightarrow \mathrm{Odd}(x^2))$

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. □

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

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