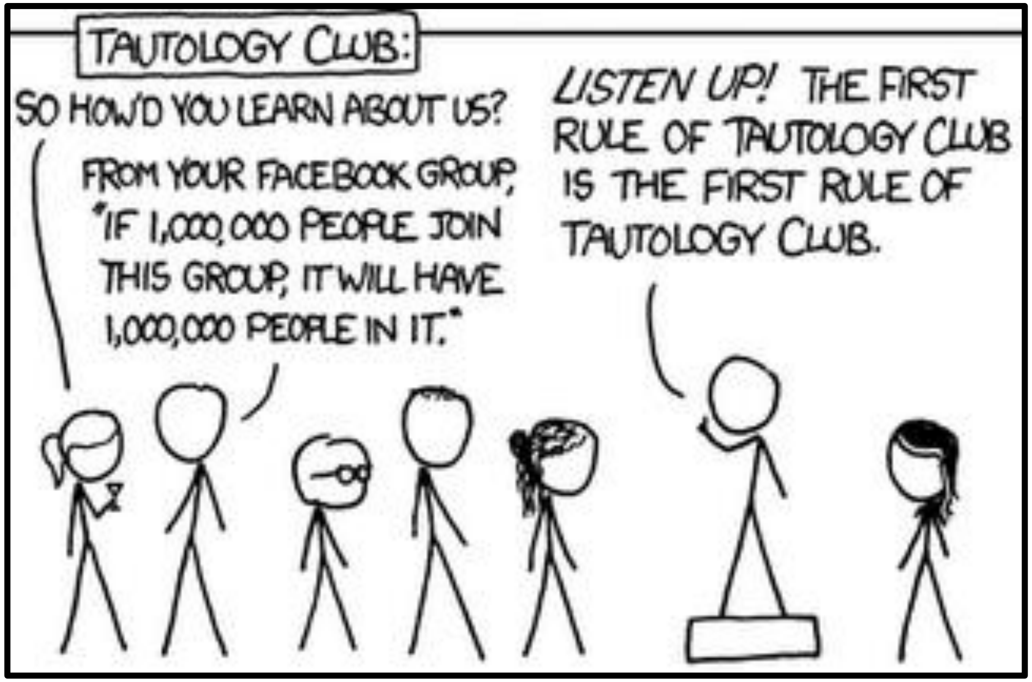
Fall 2015

Lecture 7: Proofs



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 Monday then you have a 311 class today.
  - It is Monday.

- Therefore, by modus ponens:
  - You have a 311 class today.

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

- Each inference rule is written as:

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

...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*

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

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
4.	$\neg p$	modus ponens from 2 and 3

important: applications of inference rules

- You can use equivalences to make substitutions of any sub-formula.

- Inference rules only can be applied to whole formulas (not correct otherwise)

e.g. 1. $p \rightarrow q$ given

2. $(p \vee r) \rightarrow q$ intro $\vee$ from 1.

Does not follow! e.g . p=**F**, q=**F**, r=**T**

simple 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

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

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

1. q given
2. $(p \wedge q) \to r$ 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. $p \to r$ direct proof rule

$$\boxed{(q \wedge ((p \wedge q) \to r)) \to (p \to r)}$$

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

Direct proof:

1. $p \wedge q$ assumption
2. p Elim-$\wedge$
3. $p \vee q$ Intro-$\vee$

By direct proof $(p \wedge q) \rightarrow (p \vee q)$

example

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

Direct proof:

1.	$(p \to q) \wedge (q \to r)$	assumption
2.	$p \to q$	Elim-$\wedge$, 1
3.	$q \to r$	Elim-$\wedge$, 1
4.	p	assumption
5.	q	MP 2, 4
6.	r	MP 3, 5
7.	$p \to r$	DPR
8.	$((p \to q) \wedge (q \to r)) \to (p \to r)$	

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

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

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

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

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

* 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!

"There exists an even prime number."

Even(x)

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

1.	Even(2)	Fact* (math)
2.	Prime(2)	Fact* (math)
3.	Even(2) $\wedge$ Prime(2)	Intro $\wedge$: 1, 2
4.	$\exists$x (Even(x) $\wedge$ 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 $\wedge$: 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 $\wedge$: 3, 4
6.	Even(2) $\wedge$ Prime(2)	Intro $\wedge$: 2, 5
7.	$\exists$x (Even(x) $\wedge$ 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) $\wedge$ **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)

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) for some arbitrary integer a — assumption
2. $\exists y\,(a = 2y)$ — Def of Even(a)
3. $a = 2c$ for some special c — elim-$\exists$
4. $a^2 = 4c^2 = 2\cdot(2c^2)$ — Math fact
5. $\exists b\ a^2 = 2\cdot b$ — intro-$\exists$
6. $\text{Even}(a^2)$ — def of Even
7. $\text{Even}(a) \to \text{Even}(a^2)$ for an arbitrary a
8. $\forall x\,\text{Even}(x) \to \text{Even}(x^2)$ — intro-$\forall$

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

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

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

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

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. $\square$

$\mathrm{Even}(x) \equiv \exists y\ (x=2y)$
$\mathrm{Odd}(x) \equiv \exists y\ (x=2y+1)$
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. $p \rightarrow$ **F** direct Proof rule
5. $\neg p \vee$ **F** equivalence from 4
6. $\neg p$ equivalence from 5