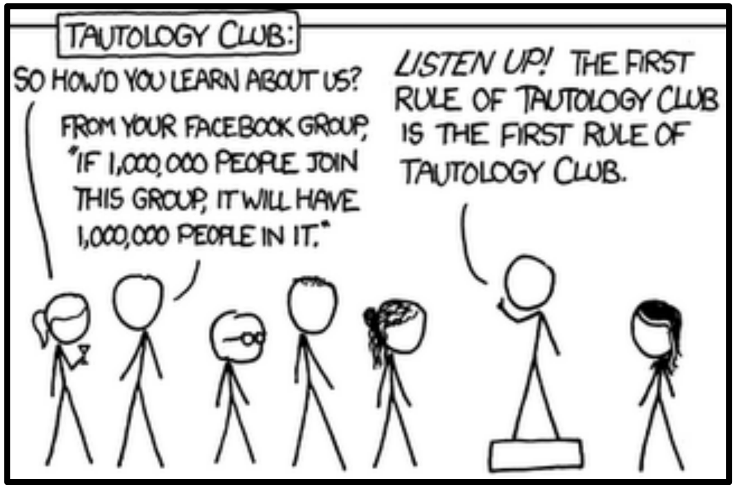


CSE 311

Foundations of Computing I

Fall 2014

Announcements

Homework #2 due today

- Solutions available (paper format) in front
- HW #3 will be posted tonight

Inference Rules

- Each inference rule is written as:
  ...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

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

- Sometimes rules don't need anything to start with. These rules are called axioms:
  - e.g. *Excluded Middle Axiom*

$$\therefore\ p \vee \neg p$$

Simple Propositional Inference Rules

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

	Elim	**Intro**
$\land$	$\dfrac{p \land q}{\therefore\ p,\ q}$	$\dfrac{p,\ q}{\therefore\ p \land q}$
$\lor$	$\dfrac{p \lor q\ ,\ \neg p}{\therefore\ q}$	$\dfrac{p}{\therefore\ p \lor q,\ q \lor p}$
	$\dfrac{p,\ p \rightarrow q}{\therefore\ q}$	$\dfrac{p \Rightarrow q}{\therefore\ p \rightarrow q}$

Direct Proof Rule

Not like other rules

Important: Application 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).**

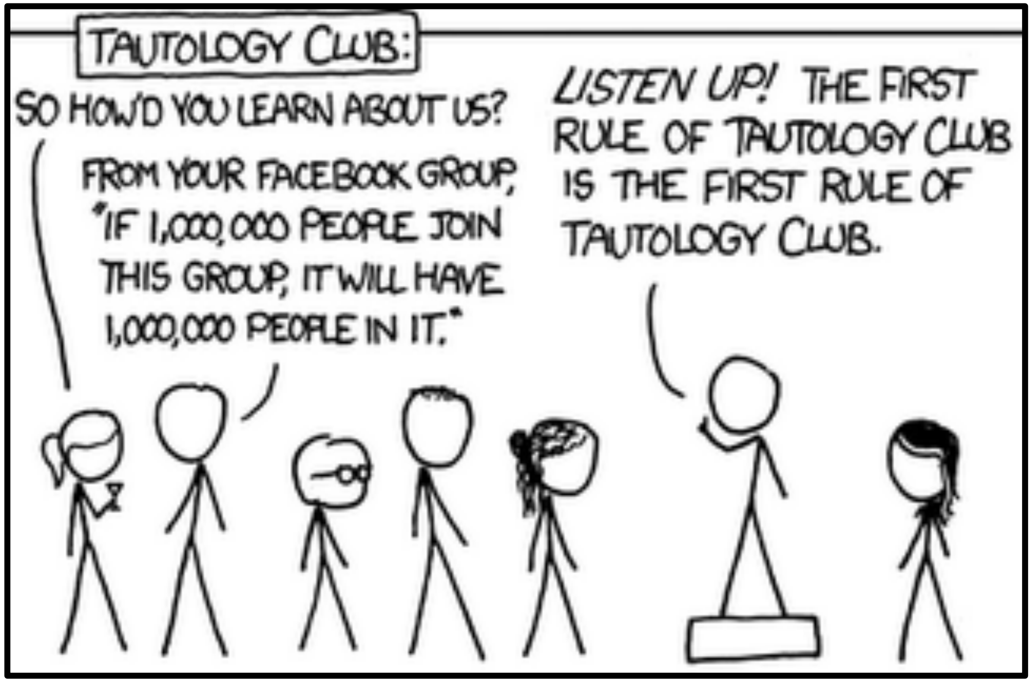
e.g. 1. $p \rightarrow q$ given

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

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

CSE 311: Foundations of Computing

Fall 2013
Lecture 7: Proofs



Proofs

Prove or disprove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $s \vee \neg q$.

If p = T, q = F, s = T, then r can be True or False.

Prove that $\neg r$ follows from $p \wedge s$, $q \rightarrow \neg r$, and $\neg s \vee q$.

1.	$p \wedge s$	Given
2.	$q \rightarrow \neg r$	Given
3.	$\neg s \vee q$	Given
4.	s	Elim $\wedge$: 1
5.	q	Elim $\vee$: 3, 4
6.	$\neg r$	MP: 2, 5

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

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.	$p \wedge q$	Intro $\wedge$: 1, 3
5.	r	MP: 2, 4
6.	$p \rightarrow r$	Direct Proof Rule

Example

Prove: $(p \land q) \rightarrow (p \lor q)$

1.	$p \land q$	Assumption
2.	p	Elim $\land$: 1
3.	$p \lor q$	Intro $\lor$: 2
4.	$(p \land q) \rightarrow (p \lor q)$	Direct Proof Rule

Example

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

1.	$(p \rightarrow q) \wedge (q \rightarrow r)$	Assumption
2.	p	Assumption
3.	$p \rightarrow q$	Elim $\wedge$: 1
4.	q	MP: 2, 3
5.	$q \rightarrow r$	Elim $\wedge$: 1
6.	r	MP: 4, 5
7.	$p \rightarrow q$	Direct Proof Rule
8.	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Direct Proof Rule

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!

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) ∧ Prime(2)	Intro ∧: 1, 2
4.	∃x Even(x) ∧ Prime(x)	Intro ∃: 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 ∃: 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 ∧: 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) ≡ ∃y (x=2y)

Proofs using Quantifiers

1.	2 = 2*1	Definition of Multiplication
2.	Even(2)	Intro ∃: 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 ∧: 3, 4
6.	Even(2) ∧ Prime(2)	Intro ∧: 2, 5
7.	∃x **Even**(x) ∧ **Prime**(x)	Intro ∃: 7

Note that 2 = 2*1 by definition of multiplication. It follows that there is a y such that 2 = 2y; so, two is even. Furthermore, two is an integer, and there are no integers between one and two; so, by definition of a prime number, two is prime. Since two is both even and prime, ∃x **Even**(x) ∧ **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) ≡ ∃y (x=2y)