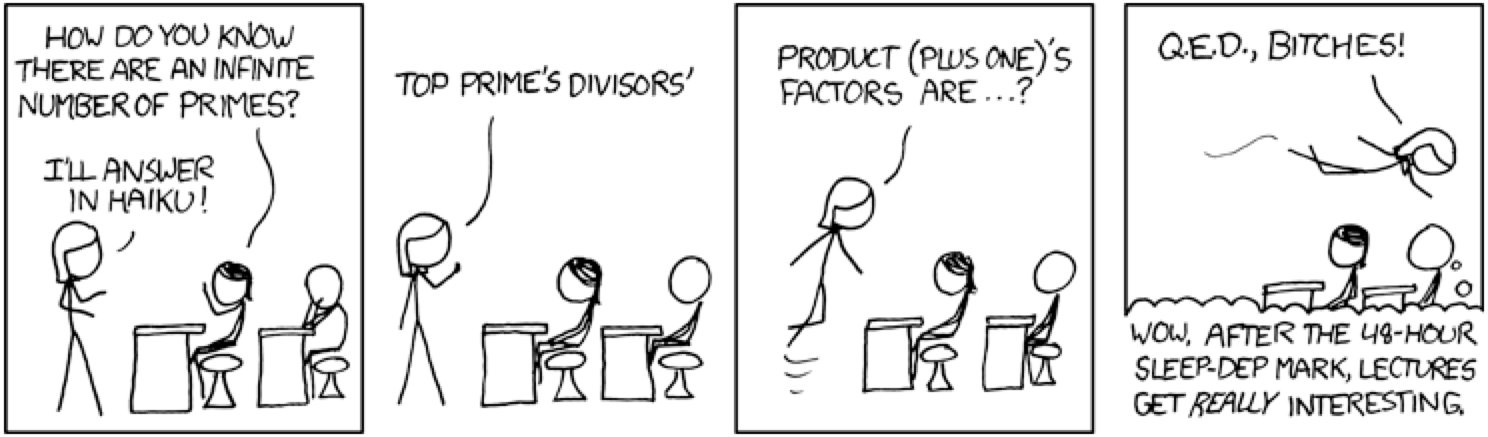
Spring 2015

Proof review session



the notion of proof: establishing truth

Proof: A formal argument establishing the truth of some proposition.

A proof should be **easy to verify**.

But might be (very) hard to generate.

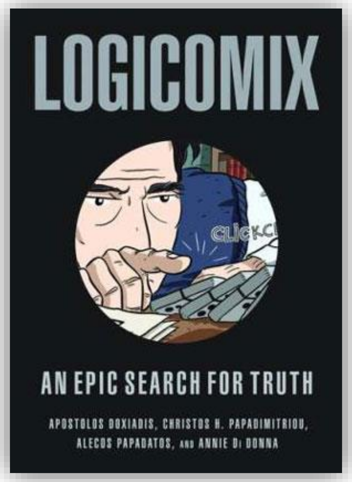
P vs. **NP** question [informal]:

Can computers find proofs efficiently? (see CSE 421, 431)

Proof systems: Start with a basic set of axioms, and use inference rules to devise new theorems.

Which axioms to use is a tricky subject…
see CSE 431.

We will talk about a related issue later:
Undecidability of the halting problem.



inference rules

Modus Ponens	$\dfrac{p,\ p \to q}{\therefore q}$
Direct Proof	$\dfrac{p \Rightarrow q}{\therefore p \to q}$
Elim $\wedge$	$\dfrac{p \wedge q}{\therefore p,\ q}$
Intro $\wedge$	$\dfrac{p,\ q}{\therefore p \wedge q}$
Elim $\vee$	$\dfrac{p \vee q,\ \neg p}{\therefore q}$
Intro $\vee$	$\dfrac{p}{\therefore p \vee q,\ q \vee p}$
Excluded Middle	$\dfrac{}{\therefore p \vee \neg p}$
Elim $\forall$	$\dfrac{\forall x P(x)}{\therefore P(a) \text{ for any } a}$
Intro $\forall$	$\dfrac{\text{Let } a \text{ be an arbitrary} \ldots}{\therefore \forall x P(x)}$
Elim $\exists$	$\dfrac{\exists x P(x)}{\therefore\ P(c) \text{ for some } \textit{special } c}$
Intro $\exists$	$\dfrac{P(c) \text{ for some } c}{\therefore \exists x P(x)}$

$\boxed{(p \wedge q) \to r \;\not\Rightarrow\; p \to r}$

$(\overbrace{\quad}^{p}) \vee (\overbrace{\quad}^{q})$

$\neg(\underbrace{\quad}_{p})$

$\therefore q$

$\neg(p \wedge q) \to r$

$\Rightarrow (\neg p \vee \neg q) \to r$

$p \vee q$

$p \vee \neg\neg q$

$q \equiv \neg\neg q$

Show that $q \to r$ follows from $p \to r$ and $q \to p$.

Direct proof that $q \to r$

1. q Assumption
2. $p \to r$ Given
3. $q \to p$ Given
4. p MP (1), (3)
5. r MP (2), (4)

---

6. $q \to r$

(optional for top-level implication)

1. q

⋮

107. r

$q \to r$

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

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
7. p given
8. r modus ponens from 6 and 7

1. q given
2. p given
3. $p \wedge q$ intro-$\wedge$
4. $(p \wedge q) \rightarrow r$ given
5. r MP 3,4.

5' $\neg(p \wedge q) \vee r$ (4) logical equiv, law of impl.

6' $\neg p \vee \neg q \vee r$ (5') De Morgan

7' $\boxed{\neg p \vee \neg q \vee r \equiv \neg q \vee r}$ not legit

proofs using the direct proof rule

$\neg\neg p \equiv p$ LE

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

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
7. p given
8. r modus ponens from 6 and 7

1. q giv
2. p giv
3. $p \wedge q$ intro-$\wedge$
4. $(p \wedge q) \rightarrow r$ given
5. r MP 3,4.

6.5 $\neg\neg p$ L.E.2

6.6 $\neg p \vee (\neg q \vee r)$ L.E. 6'

6.7 $\neg q \vee r$ Elim-$\vee$ 6.5-6.6

5' $\neg(p \wedge q) \vee r$

6' $(\neg p \vee \neg q) \vee r$

(4') logical equiv, law of impl.

(5') De Morgan

7' $\boxed{\cancel{\neg p \vee \neg q \vee r} \equiv \neg q \vee r}$

not legit

$\vdots$

r

direct proof & logical equivalences

Prove that $p \to q$ follows from r and $\underbrace{\neg(p \to \neg r)}_{(p \wedge r)} \to q$.

cannot use inference rules inside propositions

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

(Incorrect!)

$p \to q$

$(p \vee r) \to q$

$r \to q$

q

universal vs. existential instantiation

Prove that $\exists x\, P(x)$ follows from $\exists x\, Q(x)$ and $\forall x\, (Q(x) \to P(x))$.

1. $\forall x\, (Q(x) \to P(x))$ given
2. $Q(a) \to P(a)$ for a arbitrary $\forall$-inst. (1)
3. $\exists x\, Q(x)$ given
4. $Q(c)$ for some specific c $\exists$-inst (3)

---

1. $\exists x\, Q(x)$ giv
2. $Q(c)$ for some spec. c
3. $\forall x\, ((Q(x) \to P(x))$ ~
4. $Q(c) \to P(c)$ $\forall$-inst, (3)
5. $P(c)$
6. $\exists x\, P(x)$ $\exists$-intro (5)

universal generalization

Prove that $\forall x\big(P(x) \to Q(x)\big)$ and $\forall x\big(Q(x) \to R(x)\big)$ implies $\forall x\,\big(P(x) \to R(x)\big)$.

1.	$\forall x\ (P(x) \to Q(x))$	given
2.	$\forall x\ (Q(x) \to R(x))$	given
3.	$P(a) \to Q(a)$ for some arbitrary a	$\forall$-inst, (1)
4.	$Q(a) \to R(a)$	$\forall$-inst, (2)
5.	$P(a)$	Assump.
6.	$Q(a)$	MP (3), (5)
7.	$R(a)$	MP (6), (4)
8.	$P(a) \to R(a)$	DPR (6)
9.	$\forall x (P(x) \to R(x))$	intro-$\forall$ (8)

example

Prove that given $\forall x\big(P(x) \vee Q(x)\big)$ and

$$\forall x\ \Big(\big(\neg P(x) \wedge Q(x)\big) \rightarrow R(x)\Big),$$

then $\forall x\big(\neg R(x) \rightarrow P(x)\big)$ is also true.

$\neg P(x) \rightarrow R(x)$

1. $\forall x\ (P(x) \vee Q(x))$ — given
2. $\forall x\ ((\neg P(x) \wedge Q(x)) \rightarrow R(x))$ — given
3. $P(a) \vee Q(a)$ for arbitrary a — $\forall$-inst, (1)
4. $(\neg P(a) \wedge Q(a)) \rightarrow R(a)$ — $\forall$-inst, (2)
5. $\neg P(a)$ — Assumption
6. $Q(a)$ — $\vee$-Elim.
7. $\neg P(a) \wedge Q(a)$ — $\wedge$-intro
8. $R(a)$ — MP, (4), (7)
9. $\neg P(a) \rightarrow R(a)$ — DPRC

$\rightarrow$-intro

10. $\neg R(a) \rightarrow P(a)$ — L.E., (9) contrapositive.
11. $\forall x\ (\neg R(x) \rightarrow P(x))$

proof by contradiction: one way to prove $\neg p$

If we assume p and derive False (a contradiction), then we have proved $\neg p$.

If $\neg p$ is given, then p is true.

0. $\neg p$ given

1. p assumption

2... $p \wedge \neg p$ Intro and ..

3. **F**

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

Prove that no whole number is both even and odd.

Pf: Assume f.t.s.o.c. ∃ whole # x

s.t. Even(x) and odd(x).

$\Rightarrow$ ∃ k, j integers s.t.

$x = 2k$

$x = 2j + 1$

$\Rightarrow$ $2k = 2j + 1$

$\Rightarrow$ $k = j + \frac{1}{2}$

which is a contradiction b/c $j + \frac{1}{2}$ is not an int if j is an int

D

English proof

Prove that for all sets A, B, C such that $C \neq \emptyset$, we have

$$A \times C = B \times C \text{ if and ony if } A = B.$$

Prove that if A and B are sets

then $A = B \iff \mathcal{P}(A) = \mathcal{P}(B)$

Let a, b be integers and c, m be positive integers.
Prove that if $ac \equiv bc \pmod{cm}$ then $a \equiv b \pmod{m}$.