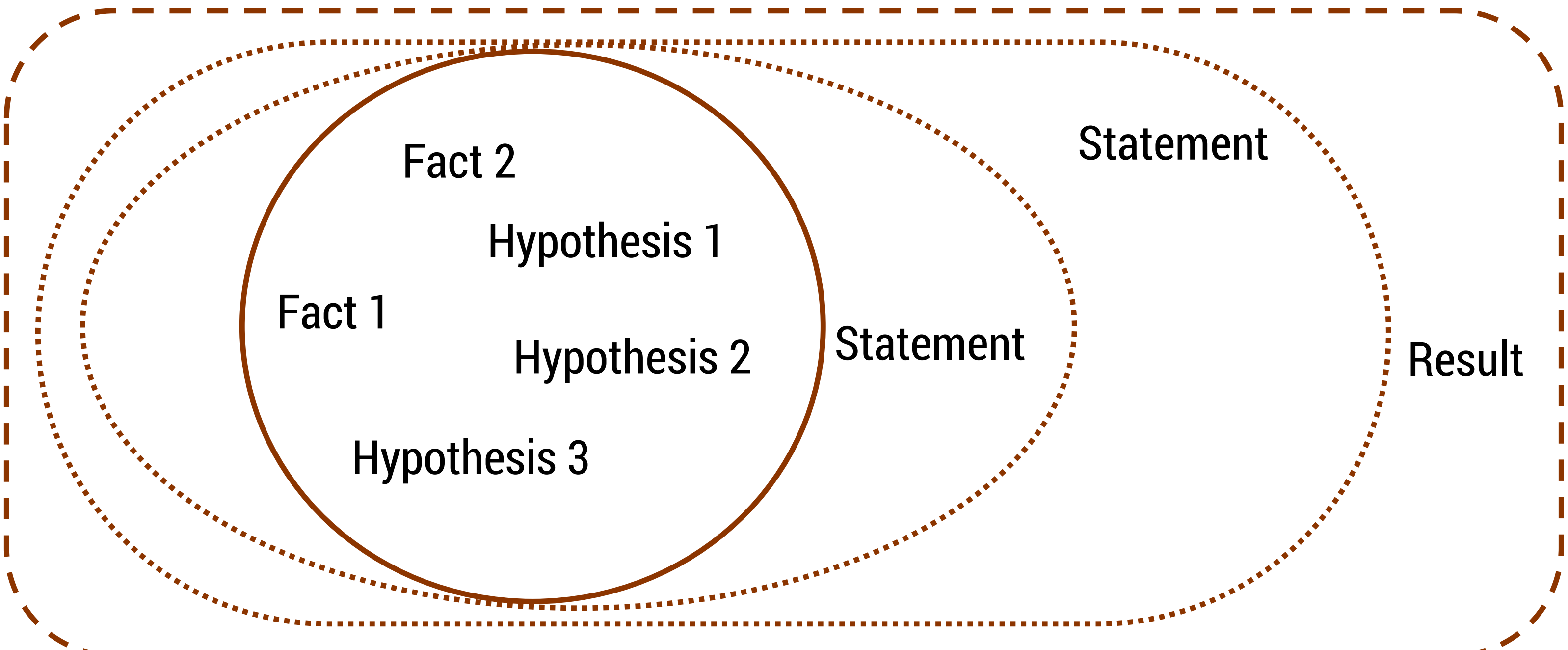
Fall 2015

Lecture 8: More 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: 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."

First, we translate into predicate logic:

$$\exists x\,(\mathrm{Even}(x) \wedge \mathrm{Prime}(x))$$

1.	$\mathrm{Even}(2)$	Fact (math)
2.	$\mathrm{Prime}(2)$	Fact (math)
3.	$\mathrm{Even}(2) \wedge \mathrm{Prime}(2)$	Intro $\wedge$: 1, 2
4.	$\exists x\,(\mathrm{Even}(x) \wedge \mathrm{Prime}(x))$	Intro $\exists$: 3

Prove: “The square of every even number is even.”

Formal 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

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

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

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. $\mathrm{Even}(a^2)$	Definition of Even
7. $\mathrm{Even}(a) \to \mathrm{Even}(a^2)$	Direct proof rule
8. $\forall x\,(\mathrm{Even}(x) \to \mathrm{Even}(x^2))$	By intro $\forall$ rule

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

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

English proof of: $\forall x\ (Odd(x) \rightarrow Odd(x^2))$

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. $\square$

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

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. $\mathbf{F}$

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

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

English proof of: $\neg \exists x\ (Even(x) \wedge Odd(x))$

$\equiv \forall x\ \neg(Even(x) \wedge Odd(x))$

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

- 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

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

Prove: $\forall x\, \forall y\, ((\text{Rational}(x) \wedge \text{Rational}(y)) \rightarrow \text{Rational}(xy))$

Domain: Real numbers

rational numbers

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

Prove: $\forall x\, \forall y\, ((\text{Rational}(x) \wedge \text{Rational}(y)) \rightarrow \text{Rational}(xy))$

Domain: Real numbers

- A real number x is *rational* iff there exist integers p and q with $q \neq 0$ such that x=p/q.

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

You might try to prove:

- If x and y are rational then x+y is rational
- If x and y are rational (and $y \neq 0$) then x/y is rational

Domain: Real numbers

Prove that $\sqrt{2}$ is irrational.

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)

Theorem: There exist two positive irrational numbers x and y such that x^y is rational.

$\pi^{\sqrt{2}}$? e^{π^2} ? φ^{φ} ?