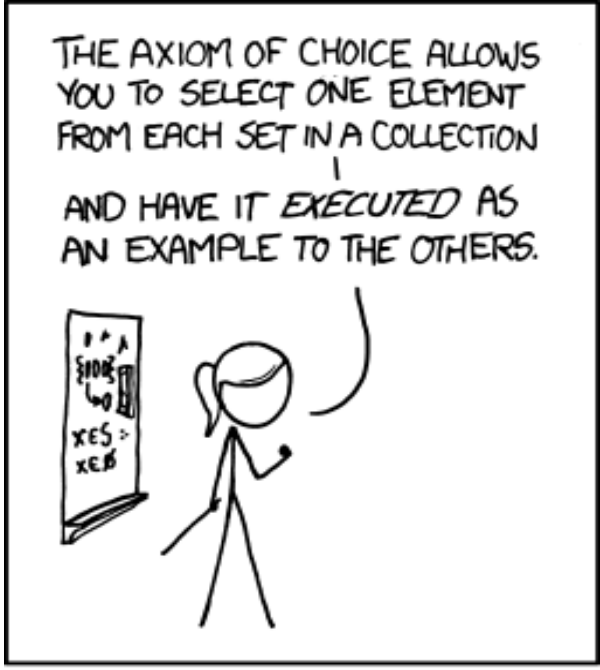
CSE 311



MY MATH TEACHER WAS A BIG BELIEVER IN PROOF BY INTIMIDATION.

Foundations of Computing I

Fall 2014

CSE 311: Foundations of Computing

Fall 2014

Lecture 8: More Proofs

A Bit of Learning Theory

- **Judging Self-Learning**
  - **Nutshell: People are surprisingly bad at being able to judge how much they "learned"**
  - **Papers:**

    The Gap Between Perceived and Actual Learning

    Why People Fail to Recognize Their Own Incompetence (geez…that paper title sounds harsh)

    Many others…

A Bit of Learning Theory

- **Attention Span**
  - ***"I sat in the back of the classroom, observing and taking careful notes as usual. The class had started at one o'clock. The student sitting in front of me took copious notes until 1:20. Then he just nodded off. The student sat motionless, with eyes shut for about a minute and a half, pen still poised. Then he awoke, and continued his rapid note- taking as if he hadn't missed a beat."***
  - **Average time "tuned-in": 10 – 15 Minutes**

    After 30 mins, even if students are re-engaged, it's for

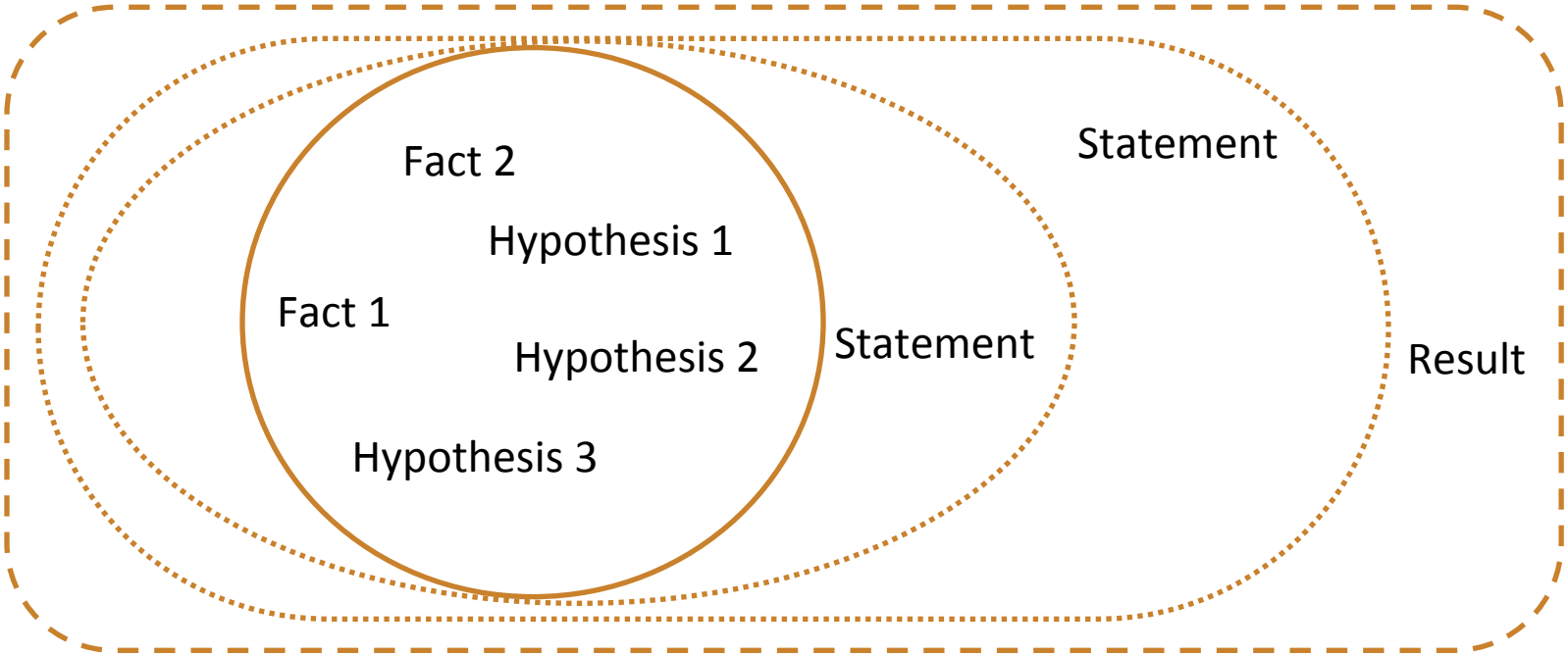
    shorter and

    shorter periods of time…

  - **Paper: *The "Change-Up" in Lectures* & Others**

Review: 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



Aside: Why do we need proofs?

- $(0.5) + (0.2)(0.3) = (0.5 + 0.2)(0.5 + 0.3)$
  $= (0.7)(0.8)$
  $= 0.56$

- Solve for x in the inequality: $|x| + |x-1| < 2$.
  Combining the terms of the left side, we find that the inequality is equivalent to $|2x - 1| < 2$. So, $-1/2 < x < 3/2$.

Inference rules for quantifiers

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

$$\frac{\text{“Let } a \text{ be anything*”} \ldots P(a)}{\therefore \forall x\, P(x)} \qquad \frac{\exists x\, P(x)}{\therefore P(c) \text{ for some } \textit{special}^{**}\ c}$$

* 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:

$$\exists x\ (\text{Even}(x) \wedge \text{Prime}(x))$$

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**

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 (namely, 1); 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, ∃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)

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

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

Formal proof of: $\forall x\ (Even(x) \rightarrow Even(x^2))$

1.	Let y be an arbitrary integer	Define Variable
2.	Even(y)	Assumption
3.	$\exists k\ (y = 2k)$	Definition of Even
4.	$y = 2c$	Elim ∃ (c depends on y)
5.	$y^2 = (2c)^2$	Square both sides
6.	$y^2 = 4c^2$	Algebra
7.	$y^2 = 2(2c^2)$	Algebra
8.	$\exists k\ (y^2 = 2k)$	Intro ∃
9.	$Even(y^2)$	Definition of Even
10.	$Even(y) \rightarrow Even(y^2)$	Direct Proof Rule
11.	$\forall x\ (Even(x) \rightarrow Even(x^2))$	Intro ∀

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

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

Formal proof of: $\forall x\ (Even(x) \rightarrow Even(x^2))$

1.	Even(a)	Assumption: a arbitrary integer
2.	∃y (a = 2y)	Definition of Even
3.	a = 2c	By elim ∃ : c special depends on a
4.	$a^2 = 4c^2 = 2(2c^2)$	Algebra
5.	∃y (a^2 = 2y)	By intro ∃ rule
6.	Even(a^2)	Definition of Even
7.	Even(a)→Even(a^2)	Direct proof rule
8.	∀x (Even(x)→Even(x^2))	By intro ∀ rule

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

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

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

1. Even(a) Assumption: a arbitrary integer
2. ∃y (a = 2y) Definition of Even
3. a = 2c By elim ∃ : c special depends on a
4. $a^2 = 4c^2 = 2(2c^2)$ Algebra
5. ∃y (a^2 = 2y) By intro ∃ rule
6. Even(a^2) Definition of Even
7. Even(a)→Even(a^2) Direct proof rule
8. ∀x (Even(x)→Even(x^2)) By intro ∀ rule

Let a be an arbitrary even integer. Then, a = 2c for some c, by definition of even. Squaring both sides, we see $a^2 = 4c^2 = 2(2c^2)$. **It follows that** a^2 **is even by definition of even. Since a was arbitrary, we've shown the square of every even number is even.**

Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃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 arbitrary 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.

Known vs. Unknown Statements

1. As we prove things, we'll have more and more theorems we know. When you **know** a theorem, start by **using** it.
   - If it's a for all statement, and we want to USE it, then we use Elim ∀
   - If it's an exists statement, and we want to USE it, then we use Elim ∃
2. If we're trying to prove a theorem (with quantifiers), there are four possibilities:
   - It's a "for all" statement (and we think it's **TRUE**)

     Take an arbitrary x, and try to prove it for that x, and use Intro ∀
   - It's an "exists" statement (and we think it's **TRUE**)

     Find some x for which it's true (really; ANY x), and use Intro ∃
   - It's a "for all" statement (and we think it's **FALSE**)

     Negate it, and prove the exists
   - It's an "exists" statement (and we think it's **FALSE**)

     Negate it and prove the "for all"

How do I start a Proof (with quantifiers)?

1. Choose a general strategy. We're building a toolkit.
2. Think about what theorems we know that might help
3. Define variables!!!!!
4. Look at the statements we're trying to prove without quantifiers (the quantifier just tells us which approach: exists -> "find one", forall -> "take arbitrary and prove it")
5. Use algebra, facts, previous theorems, etc. to prove without quantifiers
6. Put the quantifier back on

Counterexamples

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 $\neg \forall x\ P(x)$

Counterexample…example

Every non-negative integer has another number smaller than it.

$$\forall x \, \exists y \, (y < x)$$

We claim $\forall x \, \exists y \, (y < x)$ is false. We want to show $\exists x \, \forall y \, (y \geq x)$.

Consider 0. Let y be a non-negative integer. Since 0 is the smallest non-negative integer, $y \geq 0$. Thus, we've found an x, namely 0, such that $\exists x \, \forall y \, (y \geq x)$.

—or—

We claim $\forall x \, \exists y \, (y < x)$ is false. Consider 0; note that 0 is the smallest non-negative integer. So, 0 is a counter-example and the claim is false.

Proof by Contrapositive: A 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