Adam Blank Spring 2016

CSE 311

Foundations of Computing I

Example

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

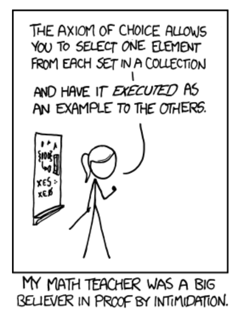
(1.1)	$(p \rightarrow q) \wedge (q \rightarrow r)$	Assumption
(1.2)	$p \rightarrow q$	$\wedge$ Elim: 1.1
(1.3)	$q \rightarrow r$	$\wedge$ Elim: 1.1
(1.4.1)	p	Assumption
(1.4.2)	q	MP: 1.2, 1.4.1
(1.4.3)	r	MP: 1.3, 1.4.2
(1.4)	$(p \rightarrow r)$	Direct Proof Rule
(1)	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	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.

CSE 311: Foundations of Computing

Lecture 8: More Proofs



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

∃ Introduction

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

∀ Elimination

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

∀ Introduction

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

* in the domain of P

∃ Elimination

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

** 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!

Definitions: The Base of All Proofs

Domain of Discourse
Integers

- Before proving anything about a topic, we need to provide definitions.
- A significant part of writing proofs is unrolling and re-rolling definitions.

∃ Introduction
P(c) for some c
∴ ∃x P(x)

Predicate Definitions
Even(x) ≡ ∃y (x = 2y)
Odd(x) ≡ ∃y (x = 2y + 1)

- Prove the statement $\exists a\,(\text{Even}(a))$

1.	$2 = 2 * 1$	Definition of Multiplication
2.	$\text{Even}(2)$	∃ Intro: 1
3.	$\exists x\ \text{Even}(x)$	∃ Intro: 2

Definitions: The Base of All Proofs

Domain of Discourse
Integers

Predicate Definitions
Even(x) ≡ ∃y (x = 2y)
Odd(x) ≡ ∃y (x = 2y + 1)

Prove the statement $\exists a\,(\text{Even}(a))$

1.	$2 = 2 * 1$	Definition of Multiplication
2.	$\text{Even}(2)$	∃ Intro: 1
3.	$\exists x\ \text{Even}(x)$	∃ Intro: 2

Okay, you might say, but now we have "definition of multiplication"! Isn't that cheating?

Well, sort of, but we're going to trust that basic arithmetic operations work the way we'd expect. There's a fine line, and you can always ask if you're allowed to assume something (though the answer will usually be no…).

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Even(x) ≡ $\exists y(x = 2y)$
Odd(x) ≡ $\exists y(x = 2y + 1)$
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\,(\text{Primeish}(a))$

Proof Strategy:

- 2 is going to work.
- Try to prove all the individual facts we need.
- We do this from the inside out…

1.	Let a be arbitrary	Defining a
2.	Let b be arbitrary	Defining b
3.	$a \leq 2 \vee a > 2$	Excluded Middle
4.	$\text{b} \leq 2 \vee b > 2$	Excluded Middle

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\,(\text{Primeish}(a))$

BTW, this justification isn't really good enough…

1.	Let a be arbitrary	Defining a
2.	Let b be arbitrary	Defining b
3.	$a \leq 2 \vee a > 2$	Excluded Middle
4.	$\text{b} \leq 2 \vee b > 2$	Excluded Middle
5.	$(a \leq 2 \vee a > 2) \wedge (\text{b} \leq 2 \vee b > 2)$	∧ Intro: 3, 4
6.1.	$a < b \wedge ab = 2$	Assumption
6.2.	$a < b$	∧ Elim: 6.1
6.3.	$ab = 2$	∧ Elim: 6.1
6.4.	$a = 1 \wedge b = 2$	Simplifying 5 via 4 & 6.2 & 6.3
6.	$(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$	Direct Proof Rule
7.	$\forall b(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$	∀ Intro: 6
8.	$\text{Primeish}(2)$	∀ Intro: 7
9.	$\exists x\ \text{Primeish}(x)$	∃ Intro: 8

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b\left(\left((a < b \wedge ab = x) \rightarrow (a = 1 \wedge b = x)\right)\right)$

Prove the statement $\exists a\,(\text{Primeish}(a))$

Still skipping steps…

1.	Let a be arbitrary	Defining a
2.	Let b be arbitrary	Defining b
3.	$a \leq 2 \vee a > 2$	Excluded Middle
4.	$\text{b} \leq 2 \vee b > 2$	Excluded Middle
5.	$(a \leq 2 \vee a > 2) \wedge (\text{b} \leq 2 \vee b > 2)$	∧ Intro: 3, 4
6.1.	$a < b \wedge ab = 2$	Assumption
6.2.	$a < b$	∧ Elim: 6.1
6.3.	$ab = 2$	∧ Elim: 6.1
6.4.	$(a \leq 2 \wedge b \leq 2) \vee (a \leq 2 \wedge b > 2) \vee (b \leq 2 \wedge a > 2) \vee (a > 2 \wedge b > 2)$	Distributivity on 5
6.5.	$a \leq 2 \wedge b \leq 2$	Combining 6.2, 6.3, 6.4
6.6.	$a = 1 \wedge b = 2$	Simplifying 5 via 4 & 6.2 & 6.3
6.	$(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$	Direct Proof Rule
7.	$\forall b(a < b \wedge ab = 2) \rightarrow (a = 1 \wedge b = 2)$	∀ Intro: 6
8.	$\text{Primeish}(2)$	∀ Intro: 7
9.	$\exists x\ \text{Primeish}(x)$	∃ Intro: 8

Proofs using Quantifiers

"There exists an even primeish number"

First, we translate into predicate logic:

∃x Even(x) ∧ Primeish(x)

We've already proven $\text{Even}(2)$ and $\text{Primeish}(2)$; so, we can use them as givens…

1.	$\text{Even}(2)$	Prev. Slide
2.	$\text{Primeish}(2)$	Prev. Slide
3.	$\text{Even}(2) \wedge \text{Primeish}(2)$	∧ Intro: 1, 2
4.	$\exists x\,(\text{Even}(x) \wedge \text{Primeish}(x))$	∃ Intro: 3

Ugh…so much work

Predicate Definitions
Even(x) ≡ $\exists y (x = 2y)$
Primeish(x) ≡ $\forall a \forall b \big(((a < b \land ab = x) \to (a = 1 \land b = x)) \big)$

Note that 2 = 2*1 by definition of multiplication. It follows that there is a y such that 2 = 2y; so, two is even.

Consider two arbitrary non-negative integers a, b.
Suppose a < b and ab = 2. Note that when b > 2, the product is always greater than 2. Furthermore, a < b. So, the only solution to the equation is a = 1 and b = 2. So, a = 1 and b = 2.

Since a and b were arbitrary, it follows that 2 is primeish.

Since 2 is even and prime, there exists a number that is even and primeish.

This is the same proof, but infinitely easier to read and write….

Even and Odd

Predicate Definitions
Even(x) ≡ $\exists y \ (x = 2y)$
Odd(x) ≡ $\exists y \ (x = 2y + 1)$

Domain of Discourse
Integers

Prove: "The square of every even number is even."
Formal proof of: $\forall x (\text{Even}(x) \to \text{Even}(x^2))$

1.	Let a be arbitrary	Defining a
2.1.	$\text{Even}(a)$	Assumption
2.2.	$\exists y \ (a = 2y)$	Definition of Even by 2.1
2.3.	$a = 2c$	∃ Elim: 2.2
2.4.	$a^2 = 4c^2 = 2(2c^2)$	Algebra
2.5.	$\exists y \ (a^2 = 2y)$	∃ Intro: 2.4
2.6.	$\text{Even}(a^2)$	Definition of Even by 2.5
2.	$\forall x \ (\text{Even}(x) \to \text{Even}(x^2))$	Direct Proof Rule

Even and Odd

Predicate Definitions
Even(x) ≡ $\exists y \ (x = 2y)$
Odd(x) ≡ $\exists y \ (x = 2y + 1)$

Domain of Discourse
Integers

Let a be arbitrary.	1. Let a be arbitrary
Suppose a is even.	2.1. $\text{Even}(a)$
Then, a = 2c for some c, by definition of even. Squaring both sides, we see $a^2 = 4c^2 = 2(2c^2)$.	2.2. $\exists y \ (a = 2y)$ 2.3. $a = 2c$ 2.4. $a^2 = 4c^2 = 2(2c^2)$
It follows that a^2 is even by definition of even.	2.5. $\exists y \ (a^2 = 2y)$ 2.6. $\text{Even}(a^2)$
Since a was arbitrary, we've shown the square of every even number is even.	2. $\forall x \ (\text{Even}(x) \to \text{Even}(x^2))$

Even and Odd

Predicate Definitions
Even(x) ≡ $\exists y \ (x = 2y)$
Odd(x) ≡ $\exists y \ (x = 2y + 1)$

Domain of Discourse
Integers

Let a be an arbitrary even number. $\left\{ \begin{array}{l} \text{Let a be arbitrary.} \\ \text{Suppose a is even.} \end{array} \right.$

Since this is english, we can combine lines like this as long as we use key words.

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

Predicate Definitions
Even(x) ≡ $\exists y \ (x = 2y)$
Odd(x) ≡ $\exists y \ (x = 2y + 1)$

Domain of Discourse
Integers

Initialize variables. [Header/Intro of the proof]	Let a be an arbitrary even number.
Explain why a^2 is even. [Body of the proof]	Then, a = 2c for some c, by definition of even. Squaring both sides, we see $a^2 = 4c^2 = 2(2c^2)$.
Conclude the sub-proof ["Return" "Inner Result"]	It follows that a^2 is even by definition of even.
Conclude the proof ["What have we shown?"	Since a was arbitrary, we've shown the square of every even number is even.

Now, Prove "The square of every odd number is odd."

Even and Odd

Predicate Definitions
Even(x) ≡ $\exists y \ (x = 2y)$
Odd(x) ≡ $\exists y \ (x = 2y + 1)$

Domain of Discourse
Integers

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

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* ∀x P(x) prove ¬∀x P(x) :

– $\neg\forall x\, P(x) \equiv \exists x \neg P(x)$
– **To prove the existential, find an x for which P(x) is false**
– **This example is called a counterexample.**

Counterexample…example

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

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

Tell the reader that we're about to use a "counterexample".	We claim $\forall x\, \exists y\, (y < x)$ is false. So, we show the negation, $\exists x\, \forall y\, (y \geq x)$, is true.
Use ∃ Elim.	Consider x = 0.
Use ∀ Elim.	Let y be arbitrary.
Prove the ∀ statement.	Since y is non-negative, $y \geq 0$. So, the claim is true.
Conclude the proof.	Thus, the original claim is false.