Adam Blank — Spring 2017

CSE 311

Foundations of Computing I

Pre-Lecture Problem

Dooo it!!

Prove: (p ∧ q) → (p ∨ q)

There MUST be an application of the Direct Proof Rule to prove this implication.

Where do we start? We have no givens...

1.1	p ∧ q	Assumption
1.100	p ∨ q	?
100.	(p ∧ q) → (p ∨ q)	DPR

Example

Prove: (p ∧ q) → (p ∨ q)

Given p ∧ q, prove p ∨ q

1.	p ∧ q	given
99.	p	∧ Elim: 1
100.	p ∨ q	∨ Intro: 99

Example

Prove: (p ∧ q) → (p ∨ q)

1.1.	p ∧ q	Assumption (given)
1.2.	p	Elim ∧: 1.1
1.3.	p ∨ q	Intro ∨: 1.2
1.	(p ∧ q) → (p ∨ q)	Direct Proof Rule

Example

Prove: ((p → q) ∧ (q → r)) → (p → r)

1.1	(p → q) ∧ (q → r)	Assumption
1.2	q → r	∧ Elim: 1.1
1.100.1	p	Assumption
1.100.2	p → q	∧ Elim: 1.1
1.100.100	r	?
1.100	p → r	DPR
1.	((p → q) ∧ (q → r)) → (p → r)	DPR

Example

Prove: ((p → q) ∧ (q → r)) → (p → r)

(1.1)	$(p \to q) \land (q \to r)$	Assumption
(1.2)	$p \to q$	∧ Elim: 1.1
(1.3)	$q \to r$	∧ 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)	$(p \to r)$	Direct Proof Rule
(1)	$((p \to q) \land (q \to r)) \to (p \to r)$	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.

$$\frac{?\ ?}{p \wedge q}$$

CSE 311: Foundations of Computing

Lecture 8: More Proofs

Aside: Why do we need proofs? (again!)

- (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
P(c) for some c
∴ ∃x P(x)

∀ Elimination
∀x P(x)
∴ P(a) for any a

Define Q(a)
∃x P(x)
P(a)

∀ Introduction
"Let a be arbitrary*"...P(a)
∴ ∀x P(x)

* in the domain of P

∃ Elimination
∃x P(x)
∴ P(c) for some *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

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

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

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

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

$2 = 2 \cdot 1$
2. Even(2) ∃ intro: 1
3. ∃a (Even(a)) ∃ Intro: 2

Definitions: The Base of All Proofs

Domain of Discourse
Integers

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

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

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** $\exists y\,(2 = 2y)$
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) ≡ $\forall a \forall b\big((a < b \land ab = x) \to (a = 1 \land b = x)\big)$

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.
2.
3.
4.

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) ≡ $\forall a \forall b\big((a < b \land ab = x) \to (a = 1 \land b = x)\big)$

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. $a \le 2 \lor a > 2$ — **Excluded Middle**
4. $b \le 2 \lor b > 2$ — **Excluded Middle**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions

Primeish(x) ≡ $\forall a \forall b\big((a < b \land ab = x) \to (a = 1 \land b = x)\big)$

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

1. Let a be arbitrary — **Defining a**
2. Let b be arbitrary — **Defining b**
3. $a \le 2 \lor a > 2$ — **Excluded Middle**
4. $b \le 2 \lor b > 2$ — **Excluded Middle**
5. $(a \le 2 \lor a > 2) \land (b \le 2 \lor b > 2)$ — **∧ Intro: 3, 4**
6. $(a < b \land ab = 2) \to (a = 1 \land b = 2)$ — **Direct Proof Rule**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions

Primeish(x) ≡ $\forall a \forall b\big((a < b \land ab = x) \to (a = 1 \land b = x)\big)$

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

1. Let a be arbitrary — **Defining a**
2. Let b be arbitrary — **Defining b**
3. $a \le 2 \lor a > 2$ — **Excluded Middle**
4. $b \le 2 \lor b > 2$ — **Excluded Middle**
5. $(a \le 2 \lor a > 2) \land (b \le 2 \lor b > 2)$ — **∧ Intro: 3, 4**
    - 6.1. $a < b \land ab = 2$ — Assumption
    - 6.2. $a < b$ — ∧ Elim: 6.1
    - 6.3. $ab = 2$ — ∧ Elim: 6.1
    - 6.4. $a = 1 \land b = 2$ — Simplifying 5 via 6.2 & 6.3
6. $(a < b \land ab = 2) \to (a = 1 \land b = 2)$ — **Direct Proof Rule**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions

Primeish(x) ≡ $\forall a \forall b\big((a < b \land ab = x) \to (a = 1 \land b = x)\big)$

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

1. Let a be arbitrary — **Defining a**
2. Let b be arbitrary — **Defining b**
3. $a \le 2 \lor a > 2$ — **Excluded Middle**
4. $b \le 2 \lor b > 2$ — **Excluded Middle**
5. $(a \le 2 \lor a > 2) \land (b \le 2 \lor b > 2)$ — **∧ Intro: 3, 4**
    - 6.1. $a < b \land ab = 2$ — Assumption
    - 6.2. $a < b$ — ∧ Elim: 6.1
    - 6.3. $ab = 2$ — ∧ Elim: 6.1
    - 6.4. $a = 1 \land b = 2$ — Simplifying 5 via 6.2 & 6.3
6. $(a < b \land ab = 2) \to (a = 1 \land b = 2)$ — **Direct Proof Rule**
7. $\forall b(a < b \land ab = 2) \to (a = 1 \land b = 2)$ — **∀ Intro: 6**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b \big((a < b \land ab = x) \rightarrow (a = 1 \land b = x)\big)$

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

1.	Let a be arbitrary	**Defining a**
2.	Let b be arbitrary	**Defining b**
3.	$a \le 2 \lor a > 2$	**Excluded Middle**
4.	$b \le 2 \lor b > 2$	**Excluded Middle**
5.	$(a \le 2 \lor a > 2) \land (b \le 2 \lor b > 2)$	**$\land$ Intro: 3, 4**
6.1.	$a < b \land ab = 2$	Assumption
6.2.	$a < b$	$\land$ Elim: 6.1
6.3.	$ab = 2$	$\land$ Elim: 6.1
6.4.	$a = 1 \land b = 2$	Simplifying 5 via 6.2 & 6.3
6.	$(a < b \land ab = 2) \rightarrow (a = 1 \land b = 2)$	**Direct Proof Rule**
7.	$\forall b (a < b \land ab = 2) \rightarrow (a = 1 \land b = 2)$	**$\forall$ Intro: 6**
8.	Primeish(2)	**$\forall$ Intro: 7**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b \big((a < b \land ab = x) \rightarrow (a = 1 \land b = x)\big)$

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.	$a \le 2 \lor a > 2$	**Excluded Middle**
4.	$b \le 2 \lor b > 2$	**Excluded Middle**
5.	$(a \le 2 \lor a > 2) \land (b \le 2 \lor b > 2)$	**$\land$ Intro: 3, 4**
6.1.	$a < b \land ab = 2$	Assumption
6.2.	$a < b$	$\land$ Elim: 6.1
6.3.	$ab = 2$	$\land$ Elim: 6.1
6.4.	$a = 1 \land b = 2$	Simplifying 5 via 4 & 6.2 & 6.3
6.	$(a < b \land ab = 2) \rightarrow (a = 1 \land b = 2)$	**Direct Proof Rule**
7.	$\forall b (a < b \land ab = 2) \rightarrow (a = 1 \land b = 2)$	**$\forall$ Intro: 6**
8.	Primeish(2)	**$\forall$ Intro: 7**
9.	$\exists x$ Primeish(x)	**$\exists$ Intro: 8**

Definitions: The Base of All Proofs

Domain of Discourse
Integers >= 1

Predicate Definitions
Primeish(x) ≡ $\forall a \forall b \big((a < b \land ab = x) \rightarrow (a = 1 \land b = x)\big)$

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.	$a \le 2 \lor a > 2$	**Excluded Middle**
4.	$b \le 2 \lor b > 2$	**Excluded Middle**
5.	$(a \le 2 \lor a > 2) \land (b \le 2 \lor b > 2)$	**$\land$ Intro: 3, 4**
6.1.	$a < b \land ab = 2$	Assumption
6.2.	$a < b$	$\land$ Elim: 6.1
6.3.	$ab = 2$	$\land$ Elim: 6.1
6.4.	$(a \le 2 \land b \le 2) \lor (a \le 2 \land b > 2) \lor (b \le 2 \land a > 2) \lor (a > 2 \land b > 2)$	Distributivity on 5
6.5.	$a \le 2 \land b \le 2$	Combining 6.2, 6.3, 6.4
6.6.	$a = 1 \land b = 2$	Simplifying 5 via 4 & 6.2 & 6.3
6.	$(a < b \land ab = 2) \rightarrow (a = 1 \land b = 2)$	**Direct Proof Rule**
7.	$\forall b (a < b \land ab = 2) \rightarrow (a = 1 \land b = 2)$	**$\forall$ Intro: 6**
8.	Primeish(2)	**$\forall$ Intro: 7**
9.	$\exists x$ Primeish(x)	**$\exists$ Intro: 8**

Proofs using Quantifiers

"There exists an even primeish number"

First, we translate into predicate logic:

$\exists$x Even(x) $\land$ Primeish(x)

We've already proven Even(2) **and** Primeish(2)**; so, we can use them as givens...**

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

Ugh...so much work

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

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

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."

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 (Even(x) → Even(x^2))

1.	Let a be arbitrary	**Defining a**
2.1.	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** Cheater!!!
2.5.	$\exists y\ (a^2 = 2y)$	**∃ Intro: 2.4**
2.6.	Even(a^2)	**Definition of Even by 2.5**
2.	$\forall x$ (Even(x) → 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. Even(a)

Since a is even, there is a c s.t. $a = 2c$. Then $a^2 = (2c)^2 = 4c^2 = 2(2c^2)$ — 2.2. $\exists y\ (a = 2y)$ 2.3. $a = 2c$ 2.4. $a^2 = 4c^2 = 2(2c^2)$

2.5. $\exists y\ (a^2 = 2y)$ 2.6. Even(a^2)

2. $\cancel{\forall x}$ (Even(x) → 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 arbitrary.	1. Let a be arbitrary
Suppose a is even.	2.1. 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. Even(a^2)
Since a was arbitrary, we've shown the square of every even number is even.	2. $\forall x$ (Even(x) → 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. ← Let a be arbitrary. / Suppose a is even.

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.

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."

WTS: $(\forall x)\,(\mathrm{Odd}(x) \to \mathrm{Odd}(x^2))$

Let a be an arb. odd num.

~~Suppose x is odd.~~ Then, by def. of odd,

$x = 2q+1$ for some q.

note $a^2 = (2q+1)^2 =$

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.

"How can I USE a statement?"

Known Statements

Domain of Discourse
Integers

$\forall x\ (\mathrm{Even}(x) \lor \mathrm{Odd}(x))$

Choose a particular x we care about.

$\exists y\ (16 = 4y)$

*Assert that one exists. *We can't assert any other properties though!!!!**

"How can I USE a statement?"

Known Statements

Domain of Discourse
Integers

$\forall x\ (\mathrm{Even}(x) \lor \mathrm{Odd}(x))$

Choose a particular x we care about.

"Since every integer is either even or odd, it follows that 5 is even or odd…"

$\exists y\ (16 = 4y)$

*Assert that one exists. *We can't assert any other properties though!!!!**

"Choose z such that 16 = 4z…"

"How can I PROVE a statement?"

Unknown Statements

Domain of Discourse
Integers

$(\exists y\ (16 = 4y)) \to (\exists y\ (16 = 2y))$

Suppose the left side and prove the right side.

$\forall x\ \big((\exists y\ (x = 4y)) \to (\exists y\ (x = 2y))\big)$

Define an "arbitrary x" and prove it for that x.

"How can I PROVE a statement?"

Unknown Statements

Domain of Discourse
Integers

$(\exists y\ (16 = 4y)) \to (\exists y\ (16 = 2y))$

Suppose the left side and prove the right side.

"Suppose 16 = 4y for some y. Then, note that 16 = 2(2y). Thus, there is an x such that 16 = 2x (namely, 2y)."

$\forall x\ \big((\exists y\ (x = 4y)) \to (\exists y\ (x = 2y))\big)$

Define an "arbitrary x" and prove it for that x.

"Let x be arbitrary. Suppose x = 4y for some y. Then, note that x = 2(2y). Thus, there is a z such that x = 2z (namely, 2y)."

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 ∃ Intro.

Use ∀ Intro.

Prove the ∀ statement.

Conclude the proof.

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 ∃ Intro. — Consider x = 0.

Use ∀ Intro. — 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.