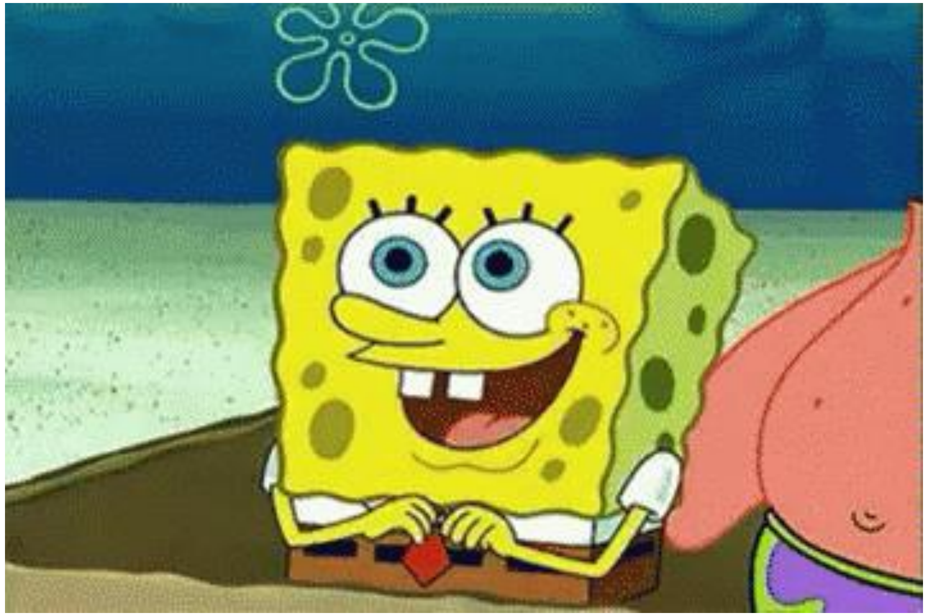

Direct Proof

CSE 311: Foundations of Computing I
Lecture 6

Announcements

- HW1 solutions at the front
- HW2 due Wednesday, 11:59 pm
- Thank you for your feedback!

Review: Predicate Logic

3 Parts

1. Predicate – Function that outputs true or false.
   $\text{Prime}(x) \coloneqq x$ is prime

2. Domain of Discourse – Set of possible inputs to a predicate.
   E.g. Integers

3. Quantifiers – A statement about when a predicate is true
   For all: ∀ There exists: ∃

Theorems and Proofs

Theorems and Proofs

Definition:

A **theorem** is a statement that can be shown to be true.

A **proof** is a valid argument that establishes a statement to be true.

Theorems and Proofs

Examples of theorems include…

- Given a right triangle with side lengths a, b and hypotenuse c, $a^2 + b^2 = c^2$
- There are infinitely many prime numbers.
- There exists a problem that cannot be solved by a program.

Integer

Definition:

An **integer** is a real number with no fractional part.

e.g. $-17, 0, 1, 53$

Odd and Even

Definitions:

An integer x is even iff there exists an integer k such that $x = 2k$.

$\text{Even}(x) \coloneqq \exists k(x = 2k)$

An integer x is odd iff there exists an integer k such that $x = 2k + 1$.

$\text{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

Proof Strategy: Direct Proof

Direct Proof

Direct proof is one strategy for proving statements of the form $\forall x \left(\mathrm{P}(x) \rightarrow \mathrm{Q}(x) \right)$.

Our First Direct Proof

Prove: "For all integers x, if x is even, then x^2 is even."

What's the claim in logic? $\forall x \left(\mathrm{Even}(x) \rightarrow \mathrm{Even}\left(x^2\right)\right)$

How would we prove this claim? Direct Proof!

Our First Direct Proof

Definitions
$\text{Even}(x) \coloneqq \exists k(x = 2k)$

Prove: "For all integers x, if x is even, then x^2 is even." $\forall x\left(\text{Even}(x) \rightarrow \text{Even}(x^2)\right)$

Let x be an arbitrary integer. Suppose that x is even. Then by definition of even, there exists some integer k such that $x = 2k$. Squaring both sides, we see that:

$$x^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2$$

Because k is an integer, then $2k^2$ is also an integer. So x^2 is two times an integer. So by definition of even, x^2 is even.

Since x was an arbitrary integer, we can conclude that for all integers x, if x is even then x^2 is even.

Direct Proof Template

Prove: $\forall x \left(\text{Even}(x) \rightarrow \text{Even}(x^2)\right)$

Declare an arbitrary variable for each ∀.	Let x be an arbitrary integer.
Assume the left side of the implication.	Suppose that x is even.
Unroll the predicate definitions.	Then by definition of even, there exists some integer k such that $x = 2k$.
Manipulate towards the goal.	Squaring both sides, we see that: $x^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2$
Reroll definitions into the right side of the implication.	Because k is an integer, then $2k^2$ is also an integer. So x^2 is two times an integer. So by definition of even, x^2 is even.
Conclude that you have proved the claim.	Since x was an arbitrary integer, we can conclude that for all integers x, if x is even then x^2 is even.

Direct Proof Template

- Declare an arbitrary variable for each ∀ quantifier
- Assume the left side of the implication
- Unroll the predicate definitions
- Manipulate towards the goal (using creativity, algebra, etc.)
- Reroll definitions into the right side of the implication
- Conclude that you have proved the claim

Another Direct Proof

Prove: "The product of two odd integers is odd."

What's the claim in logic? $\forall x \forall y \left(\left(\mathrm{Odd}(x) \wedge \mathrm{Odd}(y) \right) \rightarrow \mathrm{Odd}(xy) \right)$

How would we prove this claim?
Direct Proof. In particular, we'll let x, y be arbitrary integers. We'll suppose x, y are odd. We'll show that $x \cdot y$ is odd.

Another Direct Proof

Definitions
$\text{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

Prove: "The product of two odd integers is odd."

$$\forall x \forall y \left(\left(\text{Odd}(x) \wedge \text{Odd}(y) \right) \to \text{Odd}(xy) \right)$$

Let x and y be arbitrary integers. Suppose that x and y are odd. Then by definition of odd, there exists some integer k such that $x = 2k + 1$, and some integer j such that $y = 2j + 1$.

Then multiplying x and y, we can see that:

$$xy = (2k + 1) \cdot (2j + 1) = 4kj + 2j + 2k + 1 = 2(2kj + j + k) + 1$$

Since k, j are integers, $2kj + j + k$ is an integer. So by definition of odd, xy is odd. Since x, y were arbitrary, we have shown that the product of two odd integers is odd.

A note on Domain of Discourse

"The product of two odd integers is odd."

Domain: Integers

Translation:

$\forall x \forall y \left((\mathrm{Odd}(x) \land \mathrm{Odd}(y)) \rightarrow \mathrm{Odd}(xy) \right)$

Proof Outline:

Let x and y be arbitrary integers.

Suppose x and y are odd.

Show xy is odd.

Domain: Odd Integers

Translation:

$\forall x \forall y (\mathrm{Odd}(xy))$

Proof Outline:

Let x and y be arbitrary odd integers.

Show xy is odd.

A note on Translation to Logic

- We first translate the claim to predicate logic because:
  - The translation makes it precise what we are proving
  - The translation hints at the structure of the proof

    e.g. for each ∀, introduce an arbitrary variable
- In practice, computer scientists identify the proof claim and structure without predicate logic translation
- Eventually we'll stop asking you to translate to logic first

Square

Definition:

An integer x is square iff there exists an integer k such that $x = k^2$.

$$\text{Square}(x) \coloneqq \exists k \left(x = k^2\right)$$

Yet Another Direct Proof

<u>Definitions</u>
$\text{Square}(x) \coloneqq \exists k\, (x = k^2)$

Prove: The product of two square integers is square.

What's the claim in logic?

$$\forall n \forall m \Big(\big(\text{Square}(n) \land \text{Square}(m)\big) \to \text{Square}(nm) \Big)$$

Prove this claim.

Yet Another Direct Proof

Definitions

$\text{Square}(x) \coloneqq \exists k \left(x = k^2\right)$

Prove: "The product of two square integers is square."

$$\forall n \forall m \Big(\big(\text{Square}(n) \land \text{Square}(m)\big) \rightarrow \text{Square}(nm) \Big)$$

Let n and m be arbitrary integers. Suppose that n and m are square. Then by definition of square, $n = k^2$ for some integer k, and $m = j^2$ for some integer j.

Then multiplying n and m, we can see:

$nm = k^2 \cdot j^2 = (kj)^2$

Since k and j are integers, kj is an integer. So by definition of square, nm is square. Since n and m were arbitrary, we have shown that the product of two square integers is square.

Proof Strategy: Contrapositive

A Direct Proof?

Definitions

$\mathrm{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

Prove: For an integer x, if $3x + 2$ is odd, then x is odd.

What's the claim in logic? $\forall x\big(\mathrm{Odd}(3x+2) \rightarrow \mathrm{Odd}(x)\big)$

Prove this claim.

Let x be an arbitrary integer. Suppose that $3x + 2$ is odd. Then $3x + 2 = 2k + 1$ for some integer k. Subtracting both sides by 2, we have $3x = 2k - 1$. Then $x = \frac{2k-1}{3}$…?

Proof by Contrapositive

Proof by contrapositive is another strategy for proving statements of the form $\forall x\big(\mathrm{P}(x) \rightarrow \mathrm{Q}(x)\big)$.

The strategy is to prove the contrapositive, i.e. prove $\forall x\big(\neg\mathrm{Q}(x) \rightarrow \neg\mathrm{P}(x)\big)$

Proof by Contrapositive

Definitions
$\mathrm{Odd}(x) \coloneqq \exists k(x = 2k + 1)$

Prove: For an integer x, if $3x + 2$ is odd, then x is odd.

$$\forall x\big(\mathrm{Odd}(3x+2) \to \mathrm{Odd}(x)\big) \equiv \forall x\big(\mathrm{Even}(x) \to \mathrm{Even}(3x+2)\big)$$

We prove by contrapositive. Let x be an arbitrary integer. Suppose that x is even. Then by definition of even, $x = 2k$ for some integer k. Consider $3x + 2$:

$$3x + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$$

Since k is an integer, $3k + 1$ is an integer. So by definition of even, $3x + 2$ is even. Since x was arbitrary, we have shown that for all integers x, if x is even then $3x + 2$ is even. Thus the contrapositive also holds: for all integers x, if $3x + 2$ is odd, then x is odd.

Another Proof by Contrapositive

Definitions
$\text{Even}(x) \coloneqq \exists k(x = 2k)$

Prove by Contrapositive: For an integer n, if n^3 is even, then n is even.

$$\forall n\left(\text{Even}(n^3) \rightarrow \text{Even}(n)\right) \equiv \forall n\left(\text{Odd}(n) \rightarrow \text{Odd}(n^3)\right)$$

We prove by contrapositive. Let n be an arbitrary integer. Suppose that n is odd. Then by definition of odd, $n = 2k + 1$ for some integer k. Consider n^3:

$$n^3 = (2k+1)^3 = 8k^3 + 8k^2 + 4k + 1 = 2\left(4k^3 + 4k^2 + 2k\right) + 1$$

Since k is an integer, $4k^3 + 4k^2 + 2k$ is an integer. Thus by definition of odd, n^3 is odd. Since n was arbitrary, we have shown that for all integers n, if n is odd then n^3 is odd. Thus the contrapositive also holds: for all integers n, if n^3 is even, then n is even.