Lec 05: Direct Proofs

Prof. Adam J. Aviv

GW

CSCI 1311 Discrete Structures I
Spring 2020

What is a proof?

Proofs

Definition

A proof is a finite sequence of steps, called logical deduction, which establishes the truth of statement.

A proof is much like programming – you link together (via logical deduction) known true statements and definition to produce a given output (a true of false).

Proofs and Computer Science

What kinds of stuff do we need to *prove* in Computer Science?

- Does a program P properly implement a function f?
- Does a program P halt on every input?
- How much "effort" does it take to compute a result?
- Is this cryptographic protocol secure against a polynomial bound attacker?

Where do we start?

Set of axioms and postulates that we accept as true without proof.

Some assumptions we'll make . . .

- Basic algebraic rules, e.g., communicative, associativity, distributive, additive inverses, multiplicity reciprocal, etc.
  (See Appendix A of Epps)
- Equality properties, such as,
  (1) $A = A$ is true
  (2) if $A = B$ then $B = A$
  (3) and if $A = B$ and $B = C$, then $A = C$
- Closure of integers under addition, subtraction, and multiplication, that is, that the sum, difference and product of integers are integers.
- Most quotients of integers are not necessarily integers, $3 \div 2$ or $3/2$ or $\frac{3}{2}$ is not an integer, but rather a rational, and $3 \div 0$ is *not a number.*

Some Definitions

Even and Oddness

Definition

- An integer n is even if, and only if, n equals twice some integer.
- An integer n is odd if, and only if, n equals twice some integer plus 1.

if $n \in \mathbb{Z}$, then

$$n \text{ is } \textbf{even} \iff (\exists k \in \mathbb{Z})(n = 2k)$$

$$n \text{ is } \textbf{odd} \iff (\exists k \in \mathbb{Z})(n = 2k + 1)$$

How can we use this definition?

If we know an integer n is even, then we can deduce . . . ?

If we know an integer n can be written as 2·(some integer), then we can deduce . . . ?

Recall that $\iff$ is a biconditional, both must be true when one, or the other is true.

Can we show the following?

Definition

- An integer n is even if, and only if, n equals twice some integer.
- An integer n is odd if, and only if, n equals twice some integer plus 1.

0 is even

-19 is odd

202 is even

Prime and Composite Numbers

Definition

- An integer n is prime if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$ then either r or s equals n.
- An integer n is composite if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

if $n \in \mathbb{Z}$ and $n > 1$ then

$$\begin{aligned} n \text{ is } \textbf{prime} &\iff \forall \text{ positive integers } r \text{ and } s \\ &\quad \text{if } n = rs \text{ then} \\ &\quad \text{either } (r = 1 \text{ and } s = n) \text{ or } (r = n \text{ and } s = 1) \\ n \text{ is } \textbf{composite} &\iff \exists \text{ positive integers } n \text{ and } s, \text{ such that} \\ &\quad n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n \end{aligned}$$

Can we show the following?

Definition

- An integer n is prime if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$ then either r or s equals n.
- An integer n is composite if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

1 is not prime

12 is composite

729 is composite

17 is prime

Divisbility

Definition

If n and d are integers and $d \neq 0$ then, n is divisible by d if, and only if, n equals d multiplied by some integer. We can also say that n is a multiple of d, d is a factor of n, d is a divisor of n, or d divides n (written as $d|n$).

If $n, d \in \mathbb{Z}$ and $d \neq 0$

$$d|n \iff \exists \text{ integer } k \text{ such that } n = dk$$

Where "$d|n$" is read as "d divides n"

Can we show the following

Definition

If n and d are integers and $d \neq 0$ then, n is divisible by d if, and only if, n equals d multiplied by some integer. We can also say that n is a multiple of d, d is a factor of n, d is a divisor of n, or d divides n (written as $d|n$).

$3|21$

$9|108$

6 is a factor of 54

Direct Proof Techniques

Direct Proofs

If we want to show some statement is true, say $P(x) \implies Q(x)$:

Goal:	To prove $P(x) \implies Q(x)$
Approach:	Assume $P(x)$
	$\vdots$
	Therefore $Q(x)$

The . . . is our logical deduction

Proving an Extensional with an Example

An existential statement, is true when at least one example exists.

$$\exists x \in D \text{ such that } Q(x)$$

A constructive proof of existence is when we can either provide a specific x to show that $Q(x)$ is true, or provide instructions for finding such an x.

Prove the following with an Example

12 is a composite number

3|24

$\exists a, b, c \in Z$, such that $a^2 + b^2 = c^2$

$\exists$ prime p such that $2^p - 1$ is also prime

Disproving Universals Statements with a Counter Example

A universal statement is false when we can show its negation is true.

To prove the following

$$\neg[(\forall x \in D)(P(x) \rightarrow Q(x))]$$

is equivalent to showing

$$(\exists x \in D)(P(x) \wedge \neg Q(x))$$

If there exists an example of x where the hypothesis is true but the conclusion is false, then the universality of the implication is false. Such an example is called a counter example.

Disprove the following with a Counter Example

$(a^2 = b^2) \implies (a = b)$

$\forall k \in \mathbb{Z}$, if $k \geq 1$, then $4k + 3$ is prime

$\forall n \in \mathbb{Z}$, if $n \geq 1$, then $2n^2 + 11$ is prime

Disproving an Existential

An existential statement is false when we can show its negation is true

To prove the following

$$\neg[(\exists x \in D)(P(x))]$$

is equivalent to showing

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

To disprove an existential statement requires showing that predicate is false for all conditions, or there does not exist example to make the statement true. To disprove an existential requires proving a universal statement.

Proving Universal Statements via Exhaustion

We can prove a universal statement via exhaustion

$$(\forall x \in D)(P(x) \to Q(x))$$

The statement is true if, for every x in D, when $P(x)$ is true, $Q(x)$ is true. Trying all x's may be challenging, or impossible, depending on the problem.

Example

Prove that,

$$\forall n \in \mathbb{Z}, \text{ where } n \text{ is even and } 4 \leq n \leq 12,$$
$$\text{then } n \text{ can be written a sum of two primes}$$

Goldbach conjecture states that this is true *for all even positive integers* – it's impossible to prove that via exhaustion, although it's been tested to 4×10^{12}.

Proving Universal Statements by Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, suppose x is a particular but arbitrarily chosen element of the set, and show that x satisfies the property.

"Mentalist" problem

Pick a number (an integer), any number!

- Add 5.
- Multiply by 4.
- Subtract 6.
- Divide by 2.
- Subtract twice the original number.

Your result is 7!

And, we can prove it is always 7 by showing it is so for a particular but arbitrarily chosen x.

Prove the following

The sum of two even integers is even.

Theorem

$\forall a, b \in \mathbb{Z}$, *if a and b are even, then $a + b$ is even.*

Proof.

Let a and b be particular but arbitrary chosen integers. Suppose a and b are even integers, then there exists integers k and j, such that $a = 2k$ and $b = 2j$, by the definition of even. Then,

$$\begin{aligned} a + b &= 2k + 2j && \textit{(alg. substitution)} \\ &= 2(k + j) && \textit{(distributive law)} \end{aligned}$$

Let $i = (k + j)$, then $a + b = 2i$, and thus, $a + b$ must be even. □

Exercises

If a is even and b is odd, then $a + b$ is odd.

Divisibility is transitive: if $a|b$ and $b|c$, then $a|c$.

Every integer greater than 1 is either prime or composite. (tricky!)

Quotients and Remainders

Theorem (Quotient-Remainder Theorem)

Given any integer n and positive integer d, there exists unique integers q and r such that

$$n = dq + r \quad \textit{and} \quad 0 \leq r < d$$

(see book for proof)

Another way to understand this theorem is based on modulo and divisor:

$$\begin{aligned} n \text{ div } d &= q && \text{(integer division)} \\ n \text{ mod } d &= r && \text{(integer modulo)} \end{aligned}$$

Where q is the "quotient" and r is the "remainder."

Application of Quotient-Remainder Theorem

Using the quotient-remainder theorem, we can find the definition of even/odd when the divisor $d = 2$. That is,

$$n = 2q + r \quad \text{and } 0 \leq r < 2$$

The only integers that satisfy r is 0 and 1.

$$n = 2q + 0 \quad \text{or } n = 2q + 1$$

These are again the definitions of even/odd. The parity (value of r) is 0 if n is even, and 1 if n is odd.

Corollaries of Theorems

Corollary

Every integer is either even or odd.

Proof.

Following the Quotient-Remainder Theorem, if we fix $d = 2$, and then for every n there must exists a unique q and r, of the form $n = 2q + r$ where $0 \leq r < 2$. The only allowed values of r can either be 0 or 1.

$$n = 2q + 0 \quad \text{or} \quad n = 2q + 1$$

Thus every integer is either even or odd. □

A corollary is a result that follows directly from another proven theorem with minimal proof required.

Proof by cases

Corollary

Any two successive integers have opposite parity

Another way to write this statement is, if m is the successor of n, that is $m = n + 1$, if n is odd, then m is even, and if n is even, then m is odd.

This can be proven using case analysis as we already showed that all integers are either even or odd (i.e., have parity). The result is two cases to prove:

- **(Case 1)** $\text{Even}(n) \implies \text{Odd}(m)$
- **(Case 2)** $\text{Odd}(n) \implies \text{Even}(m)$

Proof by cases

Corollary

Any two successive integers have opposite parity

Proof.

Let n be an integer, and let $m = n + 1$ be the consecutive integer form n. By cases analysis of the parity of n

- **(Case 1: n is even)** We can write $n = 2q$ for some integer q. Substitution for n in $m = n + 1$ gives $m = 2q + 1$, and thus m must be odd.
- **(Case 2: n is odd)** We can write $n = 2q + 1$ for some integer q. Substitution for n in $m = n + q$ gives $m = 2q + 2 = 2(q + 1)$, and thus m must be even.

□

Exercise

For all positive $n \geq 5$, if n is odd, it can ncan either be written as $n = 4q + 1$ or $n = 4q + 3$. *Hint: Consider that the quotient remainder theorem says that for all integers n and divisors d, we can write $n = dq + r$ for some q and $0 \leq r < d$.*

This slide was changed since lecture

How to think about writing proofs

You should think of writing proofs like programming. Constructing a poof and writing it down should be a similar process as describing an algorithm in a given programming language,.

Style for writing proofs

Proofs

Copy the statement of the theorem to be proved to the page

Programming

Make sure your files, functions are properly named so that it is clear what you are doing.

Proofs

Clearly mark the beginning of your proof with the word **Proof**

Programming

You need a main() function to indicate where your program begins.

Style for writing proofs

Proofs

Make your proof self-contained by ensuring that each variable used in the body of your proof is well defined and show how they are derived.

Programming

Declare your variables and their types at the top of your program and functions.

Proofs

Write your proof in complete, grammatically correct sentences and syntactically correct mathematical formulations.

Programming

Your program is meaningless if it doesn't compile, so you use the correct syntax.

Style for writing proofs

Proofs

Keep your reader informed about the status of each statement in your proof, such as stating "Suppose" or "Assume" or "we must show that...", and phrases like "Therefore" or "Consequently" or "It follows that" to show how your logic connects.

Programming

Comment your code!

Proofs

Given a reason for each assertion in your proof.

Programming

Comment your code even more!

Style for writing proofs

Proofs

Display equations and inequalities on separate lines to increase readability and make it easier to check.

Programming

Use white space!