CS 278 – Discrete Mathematics for Computer Science

Chapter 2 - Proofs

Mathematical Definitions:

Even

English "An integer is even if it is divisible by 2."

Math: An integer x is even if there is an integer k such that $x = 2k$.

Odd

English "An integer is odd if it is not divisible by 2."

Math: An integer x is odd if there is an integer k such that $x = 2k + 1$.

Mathematical Definitions:

Parity

The parity of a number is whether the number is even or odd.

Same Parity

Both numbers are even or both numbers are odd.

Opposite Parity

One number is odd and the other is even.

Mathematical Definitions:

Practice

Determine whether 35 is even or odd. Express your answer as a sentence with an equation.

Practice

Do 78 and 34 have the same parity or different parity?

Mathematical Definitions:

Rational

A number r is rational if there exist integers x and y such that r = x / y.

Irrational

If a real number is not rational, then it is irrational.

Mathematical Definitions:

Practice

Show that $0.\overline{27}$ is rational by finding integers x and y.

Mathematical Definitions:

Divides

An integer x divides an integer y if and only if $y = kx$, for some integer k.

The symbol for divides is |. Other ways to express this:

$x \mid y$ "y is a multiple of x" "x is a factor of y"

The symbol for does not divide is $\nmid$

Mathematical Definitions:

Prime

An integer is prime if and only if $n > 1$ and for every positive integer m, if m divides n, then $m = 1$ or $m = n$.

Composite

An integer is composite if and only if $n > 1$ and there is an integer m such that $1 < m < n$ and m divides n.

Mathematical Definitions:

Inequalities

For real numbers x and c, only one can be true:

- $x < c$
- $x = c$
- $x > c$

x and c can also be related by using $\leq$ and $\geq$

Mathematical Definitions:

Inequalities

In proofs, you often must negate an inequality

$\neg (x < c) \equiv x \geq c$

$\neg (x > c) \equiv x \leq c$

Mathematical Definitions:

Positive, Negative, and Zero

positive $x > 0$

zero $x = 0$

negative $x < 0$

non-negative $x \geq 0$

non-positive $x \leq 0$

Mathematical Definitions:

You will need to apply these in proofs.

If $x > 0$, then $x \geq 0$.

If $x < 0$, then $x \leq 0$.

If $x > y$, then $x \geq y$.

If $x < y$, then $x \leq y$.

end of section 2.1

Mathematical Definitions:

Perfect Square

A number n is a perfect square if n = k^2 for some integer k.

Consecutive Integers

Two integers are consecutive if one of the numbers is equal to 1 plus the other number.

end of section 2.1

Introduction to Proofs

Theorem

Statement that can be proven to be true.

Proof

A series of steps, using assumptions or statements that have been shown to be true. The final statement in a proof should be the theorem being proven.

Proof Structure

1) State the theorem to be proven
2) Write the word "Proof:"
3) State assumptions
4) Use complete sentences to express steps in the proof.
5) Put the "end of proof" symbol ■ at the end.

Theorems

Most theorems are universal statements. They may not have the words "for all" or "for every".

Example: The sum of two positive real numbers is strictly greater than the average of the numbers. ("for every" is implied)

In logic, this statement is
$\forall x\ \forall y\ (x > 0 \text{ and } y > 0) \longrightarrow ((x + y) > (x + y) / 2)$

Theorems

Some theorems are existential statements.

Example: There is an integer that is equal to its square.

Logic: $\exists x\ (x = x^2)$ where the domain of x is the set of all integers

Proving universal statements

Proof by exhaustion

Show the statement is true for every value in the domain.

Works well if the domain contains a small number of distinct values.

Proving universal statements

Universal Generalization

If the domain is large or infinite, proof by exhaustion cannot be used.

Use an arbitrary object in the domain. Typically the variable x is used but it can be any variable name.

Proving universal statements

Universal Generalization

The only way to show that a universal statement is true is by a general proof that holds for all objects in the domain.

You can show that a universal statement is false by finding a counterexample (not an easy process).

Counterexamples for conditional statements

One hypothesis:

$\forall x\ (H(x) \longrightarrow C(x))$

A counterexample is a value d that makes H(d) true and C(d) false.

Counterexamples for conditional statements

$\forall x\ ((H_1(x) \wedge H_2(x)) \longrightarrow C(x))$

A counterexample must satisfy all of the hypotheses and contradict the conclusion.

A counterexample is a value d that makes $H_1(d)$ and $H_2(d)$ both true and C(d) false.

Proving existential statements

Existence proof:

A proof that shows an existential statement is true.

Constructive proof of existence:

Gives a specific example or a set of directions to construct an element of the domain with the required properties.

Proving existential statements

Non-constructive proof of existence:

Proves that an element with the required properties exists but does not give a specific example.

Disproving existential statements

To show an existential statement is false, you have to prove that every element of the domain does not have the required properties.

DeMorgan's law again:
To prove $\exists x P(x)$ is false, provide $\forall x \neg P(x)$ is true.

end of section 2.2

Best Practices in Writing Proofs

Consider your audience.

Allowed assumptions:
1) rules of algebra
2) The set of integers is closed under + - and *
3) Every integer is either even or odd.
4) If x is an integer, there is no integer between x and x + 1.
5) Real numbers are ordered
6) The square of a real number is greater than or equal to 0.

Best Practices in Writing Proofs

All steps in a proof must be justified.

Common keywords:

- Thus and therefore
- Let
- Suppose
- Since
- By definition
- By assumption
- In other words
- Gives or yields

Best Practices in Writing Proofs

Read the Proof Tips handout.

Example of a poorly written proof

Theorem to be proven

The product of an even integer and an odd integer is even.

Proof:

Since x is even, x = 2k for some integer k. Since y is odd, y = 2j+1, for some integer j.

Plugging in the expression 2k for x and 2j+1 for y into xy gives: xy=2k(2j+1)=2·k(2j+1)=2(2jk+k).

Since j and k are integers, 2jk+k is also an integer.

The expression xy is equal to two times an integer and is therefore even. ■

Existential instantiation

If an object is known to exist:
- the object can be given a name
  as long as the name is not being used for something else

Example:
If n is odd, then n = 2(some integer) + 1
We can give the object "some integer" the name k.
As long as the k is not being used for something else.

Common mistakes in proofs

- Generalizing from examples

  8 is even and 8^2 is even. Therefore if n is an even integer, then n^2 is an even integer. This is an invalid argument.

- Skipping steps

  If n is odd, n = 2k + 1. Therefore $n^2 = (2k + 1)^2$ and n^2 is odd.

Common mistakes in proofs

- Circular reasoning

  Assuming the theorem to be proven is true.

  For example, show "Every odd integer has an odd square."

  Let $n^2 = 2k + 1$ for some integer k.

- Assuming facts that haven't been proven
  - Suppose r is a rational number. The product of two rational numbers is rational.

end of section 2.3

Writing Direct Proofs

Direct Proof

1. assume the hypothesis is true
2. show that the conclusion is true

Writing Direct Proofs

Example

Show that if x is an even integer and y is an odd integer, then 3x + 2y is even.

- Assume x is even. x = 2m for some integer m
- Assume y is odd. y = 2n + 1 for some integer n

Writing Direct Proofs

Example

$$\begin{aligned} 3x + 2y &= 3(2m) + 2(2n + 1) \\ &= 6m + 4n + 2 \\ &= 2(3m + 2n + 1) \end{aligned}$$

The set of integers is closed under + - and *. Therefore, if m and n are integers, then $3m + 2n + 1$ is an integer.

Writing Direct Proofs

Example

$$3x + 2y = 2(3m + 2n + 1)$$

$3x + 2y$ is 2 times an integer. Therefore $3x + 2y$ is an even integer. ■

Writing Direct Proofs

Example

Show that the negative of an odd integer is also odd.

- Assume x is odd. $x = 2k + 1$ for some integer k.

$$\begin{aligned} -x = -(2k+1) &= -2k - 1 \\ &= -2k - 1 - 1 + 1 \\ &= (-2k - 2) + 1 \\ &= 2(-k - 1) + 1 \end{aligned}$$

Since k is an integer and the set of integers is closed under + - and * , $-k - 1$ is also an integer.

Writing Direct Proofs

Example

$-x = 2(-k - 1) + 1$

Since k is an integer and the set of integers is closed under + - and * , $-k - 1$ is also an integer.

-x is 2 times an integer + 1

Therefore –x is odd. ■

end of section 2.4

Proof by Contrapositive

Theorem to be proven: p ⟶ c

Show it's true by proving the contrapositive ¬c ⟶ ¬p

1. Assume ¬c
2. Show ¬p

Proof by Contrapositive

Example

For every pair of real numbers x and y, if x+y is irrational, then x is irrational or y is irrational.

- Assume ¬c which is ¬(x is irrational or y is irrational).

Applying DeMorgan's law, this becomes
¬x is irrational and ¬y is irrational

Reworded: x is rational and y is rational

Proof by Contrapositive

Let x be rational, then there are integers a and b such that

x $= \frac{a}{b}$ and b != 0

Let y be rational, then there are integers c and d such that

y $= \frac{c}{d}$ and d != 0

Now, we need to show ¬p which is ¬(x+y is irrational).
Reworded this would be x+y is rational.

Proof by Contrapositive

$$x + y = \frac{a}{b} + \frac{c}{d}$$

$$= \frac{ad + bc}{bd}$$

Since a, b, c, and d are integers and the set of integers is closed under + - and *, then ad + bc and bd are integers. Since b != 0 and d != 0, then bd != 0.

$x + y = \frac{m}{n}$ where m and n are integers. Therefore, x + y is rational. ■

end of section 2.5

Proof by Contradiction

Contradiction

1. Assume the theorem is false
2. Show that some logical inconsistency occurs.

This is sometimes called an "indirect proof".

Proof by Contradiction

Example:

Prove that $\frac{\sqrt{2}}{2}$ is irrational. (You may use the fact that $\sqrt{2}$ is irrational.)

Assume that $\sqrt{2}/2$ is rational. Then $\sqrt{2}/2 = x/y$, where x and y are integers and $y \neq 0$.

Multiplying both sides of the equation by 2 results in the equality

$\sqrt{2} = 2x/y$. Since x is an integer, 2x is also an integer.

Proof by Contradiction

Example:

$\sqrt{2}$ = 2x/y. Since x is an integer, 2x is also an integer.

Furthermore y is an integer which is not equal to 0.

Since $\sqrt{2}$ is equal to the ratio of two integers in which the denominator is non-zero, then we have shown that $\sqrt{2}$ is rational.

Contradicting the fact proved earlier that $\sqrt{2}$ is irrational.

Therefore the assumption that $\sqrt{2}/2$ is rational is false.

$\sqrt{2}/2$ must be irrational. ■

end of section 2.6

Proof by Cases

Cases

1. Break the domain into separate classes.
2. Show a different proof for each class.

The proof for each class is called a "case".

Number the cases.

Proof by Cases

Many proofs about integers use two cases: even and odd.

Other proofs use 3 cases: > 0 $= 0$ and < 0

Example: For every real number x, $x^2 \geq 0$

Case 1: $x < 0$

Case 2: $x = 0$

Case 3: $x > 0$

Show that the theorem is true for all cases.

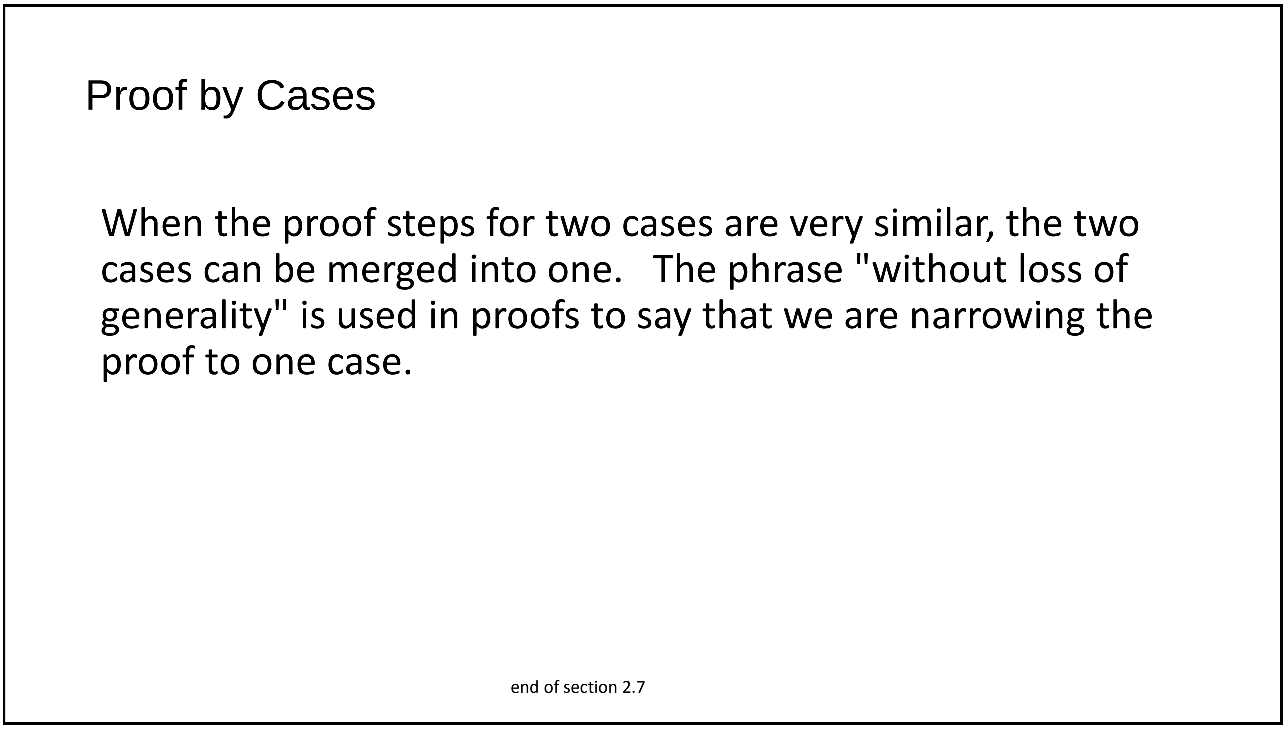
Proof by Cases

Absolute Value Expression

When absolute value appears in the theorem, remember that

$|x| = -x$ if $x \leq 0$

$|x| = x$ if $x \geq 0$



Proof by Cases

When the proof steps for two cases are very similar, the two cases can be merged into one.   The phrase "without loss of generality" is used in proofs to say that we are narrowing the proof to one case.

end of section 2.7