Discrete Mathematics

Methods of Proof

Adil M. Khan

Professor of Computer Science

Innopolis University

Proofs

Simply “A Mathematical Proof is a carefully reasoned argument to convince a skeptical listener.

Importance:

- If you have a conjecture, the only way you can safely be sure about its correctness is by presenting a valid proof.

- While trying to prove something, we may

Proofs

More formally

- “A mathematical proof of a statement is a chain of logical deductions leading to the statement from a base set of axioms.

Theorem

Proposition

Axioms:

- Propositions that are simply accepted as true.
- For Example: “There is a straight line segment between every pair of points”

Proofs

Proving theorems can be difficult

Different proof methods

Understanding these methods is a key component of learning how to read and construct mathematical proofs

Once a method is chosen, axioms, definitions, previously proved results, and rules of inference are used to complete the proof

Definitions

• Definitions

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.

Symbolically, if n is an integer, then

$$n \text{ is even} \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k.$$
$$n \text{ is odd} \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

Proofs

- **Proving Implications:**
  - Many theorems are of the form
    - $P \Longrightarrow Q$, P implies Q, or If P then Q.

Proofs

- **Proving Implications:**
  - Many theorems are of the form
    - $P \implies Q$, P implies Q, or If P then Q.

  - If $ax^2 + bx + c = 0$ and $a \neq 0$, then
    - $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
  - If n is an even integer greater than 2, then n is a sum of two primes.

Proofs

- **Proving Implications:**
  - Many theorems are of the form
    - $P \implies Q$, P implies Q, or If P then Q.

- If $ax^2 + bx + c = 0$ and $a \neq 0$, then
  - $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- If n is an even integer greater than 2, then n is a sum of two primes.

- To prove: Method 1:
  - Write , "Assume P"
  - Show that Q logically follows

Proofs

Direct Proof:

Method 1 is an example of "Direct Proof".

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Proofs

Direct Proof:

Lets look at some examples.

Proofs

Theorem: If n is an odd integer, then its square is odd.

Proofs

Theorem: If n is an odd integer, then its square is odd.

Proof: (Use the guidelines that you just learned to prove this theorem using the direct proof method)

Proofs

Another Example: The sum of any two even integers is even.

Proofs

Another Example: For all integers a, b, and c, if a divides b and b divides c, then a divides c.

Proof: (Who will do this on the board?)

Proofs

Direct proofs leads from premises to the conclusion of a theorem.

However, sometimes, attempts at direct proofs lead to dead ends.

For example,

Prove that: If n is an integer and $3n + 2$ is odd, then n is odd.

Attempts at trying to prove this using a direct proof is

Proofs

❑ Proving Implications

Method 2: Prove the contrapositive

P implies Q

Is logically equivalent to

~Q implies ~P

Therefore proving one is as good as proving the other. Proceed as follows

- Write, "We prove the contrapositive"
- Proceed as in method 1

Proofs

Prove by Contrapositive is an example This is a type of **Indirect proofs**

Proofs

Prove by contrapositive is an example This is a type of **Indirect proofs**

Use it to prove : If n is an integer and $3n + 2$ is odd, then n is odd.

Proofs

Example:

If r is irrational, then $\sqrt{r}$ is also irrational

Proofs

Indirect Proofs:

- Proof by contrapositive is an example of indirect proof.
- Another common kind of indirect proof is “proof by contradiction”.
- “You show that if a proposition were false, then same false fact would be true.”

Method:

1. Write, “We use proof by contradiction”
2. Write, “Suppose P is false”
3. Deduce something known to be false (Logical contradiction).
4. Write “This is a contradiction, therefore P

Proofs

Proof by Contradiction:

- **Example:** $\sqrt{2}$ is Irrational.

Proofs

Proof by Contradiction:

- **Example:** $\sqrt{2}$ is Irrational.

  - **Proof:** We use proof by contradiction. Suppose $\sqrt{2}$ is rational. Then there exist integers m and n with no common factors such that.

$$\sqrt{2} = \frac{m}{n}$$

Proofs

Proof by Contradiction:

- **Example:** $\sqrt{2}$ is Irrational.

  - **Proof:** We use proof by contradiction. Suppose $\sqrt{2}$ is rational. Then there exist integers m and n with no common factors such that.

$$\sqrt{2} = \frac{m}{n}$$

Squaring both sides gives

$$2 = \frac{m^2}{n^2} \Rightarrow m^2 = 2n^2$$

Proofs

Proof by Contradiction:

- **Example:** $\sqrt{2}$ is Irrational.

  - **Proof:** We use proof by contradiction. Suppose $\sqrt{2}$ is rational. Then there exist integers m and n with no common factors such that.

$$\sqrt{2} = \frac{m}{n}$$

Squaring both sides gives

$$2 = \frac{m^2}{n^2} \Rightarrow m^2 = 2n^2$$

This means that m^2 is even, which implies that m is even. That is for some integer k.

$$m = 2k$$

$$m^2 = (2k)^2 = 4k^2 = 2n^2$$

Or equivalently

$$n^2 = 2k^2$$

Proofs

Proof by Contradiction:

- **Example:** $\sqrt{2}$ is Irrational.

- **Proof:** We use proof by contradiction. Suppose $\sqrt{2}$ is rational. Then there exist integers m and n with no common factors such that.

$$\sqrt{2} = \frac{m}{n}$$

Squaring both sides gives

$$2 = \frac{m^2}{n^2} \Rightarrow m^2 = 2n^2$$

This means that m^2 is even, which implies that m is even. That is for some integer k.

$$m = 2k$$

$$m^2 = (2k)^2 = 4k^2 = 2n^2$$

Or equivalently

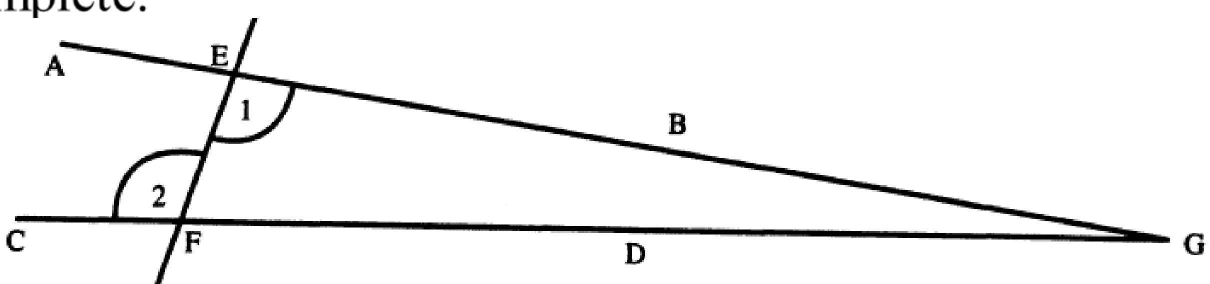
$$n^2 = 2k^2$$

Consequently n^2 is even, and so n is even.

Hence both "m" and "n" have a common factor of 2, which contradicts our supposition. Hence the supposition is false, and the theorem is true.

Proofs

- **Theorem:** **"**If a straight line falling on two straight lines makes the alternate angles equal to one another, the straight lines will be parallel".
- **Proof:** Assume that $\angle 1 = \angle 2$ in the fig, Euclid has to establish that lines AB and CD were parallel– i.e. according to definition one had to prove that these lines can never meet. Adopting an indirect argument, assumed they intersected and sought a contradiction. i.e. suppose AB and CD, if extended far enough, meet at point G. then the fig EFG is long stretched-out triangle. But $\angle 2$ an exterior angle of $\triangle EFG$, equals $\angle 1$, an opposite and interior angle of this same triangle. Again, this is impossible according to exterior angle theorem. Hence we conclude that AB and CD never intersect, no matter how far they are extended. Since this is precisely Euclid's definition of these lines being parallel, the proof is complete.



Proofs

Proof by Division into cases.

- Breaking a proof into cases, and proving each case separately.
- Useful for complicated proofs.

Proofs

Proof by Division into cases.

- Breaking a proof into cases, and proving each case separately.
- Useful for complicated proofs.

Example: Any two consecutive integers have opposite parity.

Proofs

Proof by Division into cases.

- Breaking a proof into cases, and proving each case separately.
- Useful for complicated proofs.

Example: Any two consecutive integers have opposite parity.

Proof: Assume m and m+1 be the two consecutive integers. We break the proof in two cases.

Proofs

Proof by Division into cases.

- Breaking a proof into cases, and proving each case separately.
- Useful for complicated proofs.

Example: Any two consecutive integers have opposite parity.

Proof: Assume m and m+1 be the two consecutive integers. We break the proof in two cases.

Case 1: (m is Even):

Proofs

Proof by Division into cases.

- Breaking a proof into cases, and proving each case separately.
- Useful for complicated proofs.

Example: Any two consecutive integers have opposite parity.

Proof: Assume m and m+1 be the two consecutive integers. We break the proof in two cases.

Case 1: (m is Even): This means m=2k, for some integer k. Thus

$$m+1 = 2k + 1$$

which is odd, by definition of odd numbers. Hence in

Proofs

Proof by Division into cases.

Proof: Case 2: (m is Odd):

Proofs

Proof by Division into cases.

Proof: Case 2: (m is Odd): in this case,

$$m = 2k + 1 \text{ , for some integer } k$$

Proofs

Proof by Division into cases.

Proof: Case 2: (m is Odd): in this case,

$$m = 2k + 1 \text{ , for some integer } k$$

Thus

$$m + 1 = 2k + 1 + 1$$

$$= 2k + 2$$

$$= 2(k+1)$$

Proofs

Proof by Division into cases.

Proof: Case 2: (m is Odd): in this case,

$$m = 2k + 1 \text{ , for some integer } k$$

Thus

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

But k+1 is integer, as it is a sum of two integers.

Proofs

Proof by Division into cases.

Proof: Case 2: (m is Odd): in this case,

$$m = 2k + 1 \text{ , for some integer } k$$

Thus

$$m + 1 = 2k + 1 + 1$$

$$= 2k + 2$$

$$= 2(k+1)$$

But k+1 is integer, as it is a sum of two integers.

Thus m+1 is twice some integers, hence m+1 is even.

Proofs

Proof by Division into cases.

- Lets look at another example.

Theorem: “If a and b are any integers not both zero, and if q and r are any integers such that.

$$a = b*q + r$$

Then

$$\gcd(a,b) = \gcd(b,r)$$

(gcd= Greatest Common Divisor)

Theorem: “If a and b are any integers not both zero, and if q and r are any integers such that. $a = b*q + r$, Then $\gcd(a,b) = \gcd(b,r)$.

Proof: The proof is divided into two cases:

(I) $\gcd(a,b) \leq \gcd(b,r)$

(II) $\gcd(b,r) \leq \gcd(a,b)$

(I) $\gcd(a,b) \leq \gcd(b,r)$

We will first show that any common divisor of a and b is also a common divisor of b and r.

(I) $\gcd(a,b) \le \gcd(b,r)$

We will first show that any common divisor of a and b is also a common divisor of b and r.

Let a and b be integers not both zero, and let c be a common divisor of a and b. Then $c|a$ and $c|b$ and so, by definition of divisibility, $a=nc$ and $b=mc$, for some integers n and m.

(I) $\gcd(a,b) \le \gcd(b,r)$

We will first show that any common divisor of a and b is also a common divisor of b and r.

Let a and b be integers not both zero, and let c be a common divisor of a and b. Then $c|a$ and $c|b$ and so, by definition of divisibility, $a=nc$ and $b=mc$, for some integers n and m.

Now substitute into the equation

$a = bq + r$ to obtain $nc = mc(q) + r$

(I) $\gcd(a,b) \le \gcd(b,r)$

We will first show that any common divisor of a and b is also a common divisor of b and r.

Let a and b be integers not both zero, and let c be a common divisor of a and b. Then $c|a$ and $c|b$ and so, by definition of divisibility, $a=nc$ and $b=mc$, for some integers n and m.

Now substitute into the equation

$a = bq + r$ to obtain $nc = mc(q) + r$

Then

(I) $\gcd(a,b) \le \gcd(b,r)$

We will first show that any common divisor of a and b is also a common divisor of b and r.

Let a and b be integers not both zero, and let c be a common divisor of a and b. Then c|a and c|b and so, by definition of divisibility, a=nc and b=mc, for some integers n and m.

Now substitute into the equation

$a = bq + r$ to obtain $nc = mc(q) + r$

Then

So every common divisor of a and b is a common divisor of b and r.

So every common divisor of a and b is a common divisor of b and r.

It follows that the greatest common divisor of a and b is defined because a and b are not both zero, and it is a common divisor of b and r.

So every common divisor of a and b is a common divisor of b and r.

It follows that the greatest common divisor of a and b is defined because a and b are not both zero, and it is a common divisor of b and r.

but then gcd(a,b) – (being one of the common divisors of b and r) is less than or equal to the greatest common divisor of b and r,

$$\gcd(a,b) \le \gcd(b,r)$$

So every common divisor of a and b is a common divisor of b and r.

It follows that the greatest common divisor of a and b is defined because a and b are not both zero, and it is a common divisor of b and r.

but then gcd(a,b) – (being one of the common divisors of b and r) is less than or equal to the greatest common divisor of b and r,

$$\gcd(a,b) \le \gcd(b,r)$$

Similarly solve part (II).

Proving Universal Statements

- **Direct Proof**

- **Proof by Contrapositive**

- **Proof by Contradiction**

- **Proof by Counterexample**

- **Proof by C**

Proving Existential Statements

We have known that a statement in the form

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

is true if, and only if,

$Q(x)$ is true for at least one x in D.

One way to prove this is to find an x *(called a witness)* in D that makes $Q(x)$ true.

called **constructive proofs of existence**.

- Prove the following: ∃ an even integer n that can be written in two ways as a sum of two prime numbers.

Solution:

Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and 3, 5, and 7 are all prime numbers.