Introduction to Proof in Discrete Mathematics

Dr. Mohammad Salah Uddin

Associate Professor
Dept. of CSE
East West University

November 26, 2024

What is a Proof?

- A **proof** is a logical argument that verifies the truth of a mathematical statement.
- In discrete mathematics, proofs are used to validate statements about numbers, sets, graphs, and algorithms.

Types of Proof Techniques

There are several common techniques used in mathematical proofs:

1. **Direct Proof**
   - Proves a statement by assuming the hypothesis and logically deriving the conclusion.
   - Example: Proving that the sum of two even numbers is even.
2. **Proof by Contradiction**
   - Assumes the negation of the statement and shows that this leads to a contradiction.
   - Example: Proving that $\sqrt{2}$ is irrational.
3. **Proof by Induction**
   - Used to prove statements about integers, typically involving sequences.
   - Two steps: **Base Case** and **Inductive Step**.
4. **Proof by Counterexample**
   - Demonstrates that a statement is false by providing a single example that contradicts it.

Direct Proof

- A **direct proof** demonstrates the truth of a statement by logically deriving the conclusion from the given information.
- It involves assuming the hypothesis is true and using logical steps to arrive at the conclusion.
- Commonly used for statements in the form:

$$\text{If } P, \text{ then } Q.$$

Direct Proof: Example 1

Theorem: The sum of two even numbers is even.

Proof.

Let a and b be even numbers. We can express the even numbers as, there exist integers m and n such that:

$$a = 2m \quad \text{and} \quad b = 2n.$$

Then, the sum is:

$$a + b = 2m + 2n = 2(m + n).$$

Since $m + n$ is an integer, because the sum to two integers is and integer. So, $a + b$ is even. $\square$

Direct Proof: Example 2

Theorem: The product of two odd numbers is odd.

Proof.

Let a and b be odd numbers. By definition of odd numbers, there exist integers m and n such that:

$$a = 2m + 1 \quad \text{and} \quad b = 2n + 1.$$

Then, the product is:

$$a \times b = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1.$$

Since $2mn + m + n$ is an integer, $a \times b$ is odd. $\square$

Direct Proof: Example 3

Theorem: The square of an even number is even.

Proof.

Let n be an even number. By definition, there exists an integer k such that:

$$n = 2k.$$

The square of n is:

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

Since $2k^2$ is an integer, n^2 is even. $\square$

Direct Proof: Example 4

Theorem: The square of an odd number is odd.

Proof.

Let n be an odd number. By definition, there exists an integer k such that:

$$n = 2k + 1.$$

The square of n is:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $2k^2 + 2k$ is an integer, $n^2 = 2m + 1$, where m is an integer. Thus, n^2 is odd. $\square$

Summary of Direct Proof

Direct proof involves starting from known information (hypothesis) and applying logical reasoning to reach a conclusion.

Proof by Contraposition

- In a **proof by contraposition**, we prove a statement of the form:

  $$\text{If } P\text{, then } Q$$

  by proving its contrapositive:

  $$\text{If } \neg Q\text{, then } \neg P.$$

- The contrapositive is logically equivalent to the original statement.
- This method is often easier than direct proof, especially when assuming Q false leads to a clearer argument.

Contraposition: Example 1

Theorem: If n^2 is even, then n is even.

Proof.

We will prove this by contraposition. The contrapositive of the statement is:

If n is odd, then n^2 is odd.

Assume n is odd. Then $n = 2k + 1$ for some integer k.

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $2k^2 + 2k$ is an integer, n^2 is odd. Thus, if n^2 is even, n must be even. $\square$

Contraposition: Example 2

Theorem: If $x + y$ is odd, then one of x or y is odd.

Proof.

We will prove this by contraposition. The contrapositive of the statement is:

If both x and y are even, then $x + y$ is even.

Assume both x and y are even. Then, there exist integers m and n such that:

$$x = 2m \quad \text{and} \quad y = 2n.$$

Therefore:

$$x + y = 2m + 2n = 2(m + n).$$

Since $m + n$ is an integer, $x + y$ is even. Hence, if $x + y$ is odd, at least one of x or y must be odd. $\square$

Contraposition: Example 3

Theorem: If n^2 is not divisible by 3, then n is not divisible by 3.

Proof.

We will prove this by contraposition. The contrapositive of the statement is:

If n is divisible by 3, then n^2 is divisible by 3.

Assume n is divisible by 3. Then $n = 3k$ for some integer k.

$$n^2 = (3k)^2 = 9k^2 = 3(3k^2).$$

Since $3k^2$ is an integer, n^2 is divisible by 3. Thus, if n^2 is not divisible by 3, then n is not divisible by 3. $\square$

Proof by Contradiction

Method: In a proof by contradiction, we assume the negation of the statement we want to prove and show that this assumption leads to a contradiction. This contradiction implies that our original assumption must be false, and therefore the statement we wanted to prove is true.

General Steps:

1. Assume that the statement to be proved is false.
2. Show that this assumption leads to a contradiction.
3. Conclude that the assumption must be false, and thus the original statement is true.

Contradiction: Example 1

Theorem: The sum of two odd numbers is even.

Proof:

- Assume, for the sake of contradiction, that the sum of two odd numbers is odd.
- Let the two odd numbers be $2m+1$ and $2n+1$, where m and n are integers.
- The sum of these two numbers is:

$$(2m+1)+(2n+1)=2(m+n+1).$$

This expression is clearly even, which contradicts the assumption that the sum is odd. Therefore, the sum of two odd numbers must be even.

Contradiction: Example 2

Theorem: The product of two even numbers is even.
Proof:

- Assume, for the sake of contradiction, that the product of two even numbers is odd.
- Let the two even numbers be $2m$ and $2n$, where m and n are integers.

The product of these two numbers is:

$$(2m)(2n) = 4mn.$$

Clearly, this is even because it is divisible by 2. This contradicts the assumption that the product is odd. Therefore, the product of two even numbers must be even.

Contradiction: Example 3

Theorem: The sum of an even number and an odd number is odd.
Proof:

- Assume, for the sake of contradiction, that the sum of an even number $2m$ and an odd number $2n + 1$ is even.

The sum is:

$$(2m) + (2n + 1) = 2(m + n) + 1.$$

This is clearly odd, not even. Therefore, our assumption is false. Hence, the sum of an even number and an odd number is odd.

Contradiction: Example 4

Theorem: There is no integer x such that $x^2 = 3$.

Proof:

- Assume, for the sake of contradiction, that there is an integer x such that $x^2 = 3$.

Then $x^2 = 3$, and we need to check if any integer satisfies this equation.

Checking the possible integer values of x, we find:

$$x = \pm 1 \quad \Rightarrow \quad x^2 = 1 \quad \text{(not 3)}.$$

$$x = \pm 2 \quad \Rightarrow \quad x^2 = 4 \quad \text{(not 3)}.$$

$$x = \pm 3 \quad \Rightarrow \quad x^2 = 9 \quad \text{(not 3)}.$$

Clearly, no integer satisfies $x^2 = 3$.

Therefore, there is no integer x such that $x^2 = 3$.

Proof by Cases

Definition: Proof by cases is a technique where we divide a proof into different cases and prove the statement separately for each case. It is used when a statement can be true in several different ways, each of which needs to be verified.

Procedure:

- Identify all possible cases.
- Prove the statement for each case.
- Conclude the proof after all cases are covered.

When to Use Proof by Cases

Use proof by cases when:

- There are multiple possible scenarios for the statement.
- The conditions for the statement change depending on different situations.
- A direct proof is complicated or infeasible.

Cases: Example 1

Theorem: Any integer n is either even or odd.
Proof: We will prove this by considering two cases.
Case 1: n is even.
By definition, if n is even, then there exists an integer k such that:

$$n = 2k.$$

Since $n = 2k$, n is even by definition.
Case 2: n is odd.
If n is odd, then there exists an integer k such that:

$$n = 2k + 1.$$

Since $n = 2k + 1$, n is odd by definition.
Since every integer n is either even or odd, the statement is proved.

Cases: Example 2

Theorem: The sum of two integers is even if and only if both integers have the same parity (both even or both odd).

Proof: We will prove this by considering all possible cases for the parity of the integers.

Case 1: Both integers are even.

Let $a = 2m$ and $b = 2n$, where m and n are integers. The sum is:

$$a + b = 2m + 2n = 2(m + n),$$

which is even.

Case 2: Both integers are odd.

Let $a = 2m + 1$ and $b = 2n + 1$, where m and n are integers. The sum is:

$$a + b = (2m + 1) + (2n + 1) = 2(m + n + 1),$$

which is also even.

Cases: Example 3

Case 3: One integer is even and the other is odd.
Let $a = 2m$ and $b = 2n + 1$, where m and n are integers. The sum is:

$$a + b = 2m + (2n + 1) = 2(m + n) + 1,$$

which is odd.
Conclusion: The sum of two integers is even if and only if both integers have the same parity.

Proof by Cases: $|xy| = |x| \cdot |y|$

Theorem: Prove that for all real numbers x and y, we have the identity:

$$|xy| = |x| \cdot |y|.$$

Proof by Cases:

- **Case 1:** $x \geq 0$ **and** $y \geq 0$
  - $|x| = x$ and $|y| = y$
  - $|xy| = x \cdot y$
  - $|x| \cdot |y| = x \cdot y$
- **Case 2:** $x \geq 0$ **and** $y < 0$
  - $|x| = x$ and $|y| = -y$
  - $|xy| = |x \cdot (-y)| = -x \cdot y$
  - $|x| \cdot |y| = x \cdot (-y) = -x \cdot y$

Proof by Cases: $|xy| = |x| \cdot |y|$

- **Case 3:** $x < 0$ **and** $y \geq 0$
  - $|x| = -x$ and $|y| = y$
  - $|xy| = |-x \cdot y| = -x \cdot y$
  - $|x| \cdot |y| = (-x) \cdot y = -x \cdot y$
- **Case 4:** $x < 0$ **and** $y < 0$
  - $|x| = -x$ and $|y| = -y$
  - $|xy| = |-x \cdot (-y)| = x \cdot y$
  - $|x| \cdot |y| = (-x) \cdot (-y) = x \cdot y$
- **Case 5:** $x = 0$ **or** $y = 0$
  - If $x = 0$, then $|xy| = 0$ and $|x| \cdot |y| = 0$.
  - If $y = 0$, then $|xy| = 0$ and $|x| \cdot |y| = 0$.

Conclusion: In all cases, $|xy| = |x| \cdot |y|$. Therefore, the proof is complete.

Summary of Proof by Cases

- Proof by cases is used when there are multiple scenarios to consider.
- We divide the problem into separate cases and prove each one.
- Once all cases are proven, the overall statement is concluded.

Remember: Each case must cover all possible outcomes, and no case can be overlooked.

Proof of Equivalences

We want to prove $p \iff q$

- **Statements:** p if and only if q
- **Equivalence:** $p \iff q$ is equivalent to $(p \to q) \wedge (q \to p)$
- **Note:** Both implications must hold.

Example: Proof of Equivalences

Integer is Odd if and Only if n^2 is Odd

Proof of $p \to q$:

- **Statement:** If n is odd, then n^2 is odd.
- **Direct Proof:**
- Suppose n is odd. Then $n = 2k + 1$, where k is an integer.
- Compute n^2:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

- Therefore, n^2 is odd.

Example: Proof of Equivalences

Integer is Odd if and Only if n^2 is Odd

$\boxed{\textbf{Proof of } q \to p\textbf{:}}$

- **Statement:** If n^2 is odd, then n is odd.
- **Indirect Proof:** Use the contrapositive.
- **Contrapositive:** If n is even, then n^2 is even.

Proof:

- Suppose n is even. Then $n = 2k$, where k is an integer.
- Compute n^2:

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

- Therefore, n^2 is even.

Since the contrapositive holds, the implication $q \to p$ is true.

Conclusion: Proof of Equivalences

- **Statement:** Integer is Odd if and Only if n^2 is Odd
- Since both $p \to q$ and $q \to p$ have been proven true, the equivalence is true:

$$n \text{ is odd} \iff n^2 \text{ is odd.}$$

Example: Divisibility by 6

Statement: A number is divisible by 6 if and only if it is divisible by both 2 and 3.

- **(1) Direct Proof of $p \to q$:** If a number is divisible by 6, then it is divisible by both 2 and 3.
- **(2) Direct Proof of $q \to p$:** If a number is divisible by both 2 and 3, then it is divisible by 6.

Proof of $p \to q$

Assume the number is divisible by 6.

- If a number is divisible by 6, it can be written as $n = 6k$, where k is an integer.
- Since $6 = 2 \times 3$, the number is divisible by both 2 and 3.

Hence, the number is divisible by both 2 and 3, proving $p \to q$.

Proof of $q \rightarrow p$

Assume the number is divisible by both 2 and 3.

- If a number is divisible by 2, it can be written as $n = 2m$.
- If a number is divisible by 3, it can be written as $n = 3m$.
- Since both 2 and 3 divide n, their least common multiple (LCM) is 6. Thus, n is divisible by 6.

Hence, the number is divisible by 6.
Since both $p \rightarrow q$ and $q \rightarrow p$ have been proven, the equivalence holds:

$$\text{A number is divisible by 6} \iff \text{It is divisible by both 2 and 3.}$$

Next Slide

Mathematical Induction