Proof Techniques in Mathematics

With Examples, Instructions, and Exercises

SDB

Spring 2025

Outline

Mathematical Statements

- **Definition:** A mathematical statement is a declarative sentence that is either true or false but not both.
- **Types of Statements:**
  1. **Universal Statement:** Claims something is true for all elements in a set.
     - ★ Example: For all integers n, $n^2 \geq 0$.
  2. **Existential Statement:** Asserts the existence of at least one element satisfying a condition.
     - ★ Example: There exists an integer n such that $n^2 = 4$.
  3. **Conditional Statement:** Has the form "If P, then Q" ($P \implies Q$).
     - ★ Example: If n is even, then n^2 is even.
  4. **Biconditional Statement:** Combines two implications: $P \iff Q$.
     - ★ Example: n is even if and only if n^2 is even.

Exercise:

- Write a universal, existential, conditional, and biconditional statement related to numbers or geometry.

Question to Ponder: How do we prove or disprove each type of statement?

Common Mathematical Symbols

- **Logical Symbols:**
  - $\wedge$: Logical AND (e.g., $P \wedge Q$ means both P and Q are true).
  - $\vee$: Logical OR (e.g., $P \vee Q$ means either P, Q, or both are true).
  - $\neg$: NOT (e.g., $\neg P$ means P is false).
  - $\implies$: Implies (e.g., $P \implies Q$ means if P is true, then Q must be true).
  - $\iff$: If and only if (e.g., $P \iff Q$ means P is true if and only if Q is true).
  - $\vdash$: Proves
  - $\models$: Models or Satisfies

Common Mathematical Symbols

- **Set Theory Symbols:**
  - $\in$: Element of (e.g., $x \in A$ means x is an element of set A).
  - $\notin$: Not an element of (e.g., $x \notin A$ means x is not an element of set A).
  - $\subseteq$: Subset of (e.g., $A \subseteq B$ means all elements of A are in B).
  - $\subset$: Proper subset of (e.g., $A \subset B$ means all elements of A are in B and $|A| < |B|$).
  - $\cup$: Union (e.g., $A \cup B$ is the set of all elements in A or B).
  - $\cap$: Intersection (e.g., $A \cap B$ is the set of all elements in both A and B).
  - $\emptyset$: Empty set (e.g., $\emptyset$ is the set with no elements).
  - $\mathbb{N}$: Set of natural numbers
  - $\mathbb{Z}$: Set of integers
  - $\mathbb{Q}$: Set of rational numbers
  - $\mathbb{R}$: Set of real numbers
  - $\mathbb{C}$: Set of complex numbers
  - $\mathcal{P}(A)$: Power set of A, $\mathcal{P}_k(A)$: All k-element subsets of A
  - Open interval: $(a, b) = \{x \in \mathbb{R} : a < x < b\}$.
  - Closed interval: $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$.
  - A sequence is an ordered list of elements: $S = (a_1, a_2, a_3, \dots) = (a_k)_{k=1}^{\infty}$.

Common Mathematical Symbols

- **Quantifiers:**
  - $\forall$: Universal quantifier (e.g., $\forall x \in \mathbb{R}, x^2 \geq 0$ means For all real numbers x, $x^2 \geq 0$).
  - $\exists$: Existential quantifier (e.g., $\exists x \in \mathbb{Z}, x^2 = 4$ means There exists an integer x such that $x^2 = 4$).
  - $\exists!$: There exists exactly one (e.g., $\exists! x \in \mathbb{Z}, x - 2 = 0$ means There exists exatly one integer x such that $x - 2 = 0$).
  - $\nexists$: There does not exist any (e.g., $\nexists x \in \mathbb{Z}, x^4 < 0$ means There does not exist any integer x such that $x^4 < 0$).
- **Common Operations:**
  - $\sum$: Summation (e.g., $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$).
  - $\prod$: Product (e.g., $\prod_{i=1}^{n} i = n!$).
  - $|A|$: Cardinality (e.g., $|A|$ is the number of elements in set A).
  - $|x|$: Absolute value (e.g., $|x|$ is the distance of x from 0).
  - $\bmod$: Modulo operation (e.g., $a \bmod b$ is the remainder when a is divided by b).
  - For a set $A = \{a_1, a_2, \ldots, a_n\}$:
    $\max(A) = \max\{a_i : i \in [1, n]\}, \quad \min(A) = \min\{a_i : i \in [1, n]\}$.

Common Mathematical Symbols - Miscellaneous

- **Relations**
  - $=, \neq$: Equal to, Not equal to
  - $<, >$: Less than, Greater than
  - $\leq, \geq$: Less than or equal to, Greater than or equal to
  - $\equiv$: Equivalent to
  - $\sim$: Similar to
  - $\approx$: Approximately
  - $\propto$: Proportional to
- **Miscellaneous Symbols**
  - $\int$:Integral
  - ∂: Partial derivative
  - ∞: Infinity
  - ∇: Nabla or Del
  - $\mathbb{P}(A)$: Probability of event A
  - $\mathbb{E}$: Expected value
  - $\mathbb{V}$: Variance

Exercises I

- **Translate and rewrite each statement using mathematical symbols:** Beginner Level
  - For every natural number n, n is less than or equal to $n + 1$.
  - There exists a real number x such that $x^2 = 4$.
  - Every element of set A is also an element of set B.
  - If x is greater than 2, then x is also greater than 1.
  - It is not true that all numbers are even.
  - The intersection of sets A and B contains all elements common to both A and B.
  - For every integer x, x is either even or odd.
  - There exists an even integer n such that n is greater than 100.
  - If A is a subset of B, then every element of A is also an element of B.

Exercises II

- **Translate and rewrite each statement using mathematical symbols:** Intermediate Level
  - There exists a subset S of set A such that S is not empty.
  - For all real numbers x and y, if $x \leq y$, then $-y \leq -x$.
  - If A is a subset of B, then the complement of B is a subset of the complement of A.
  - There exists a prime number p such that p is greater than 100.
  - For all integers a and b, if a divides b, then $|a| \leq |b|$.
  - There exists an integer x such that x is both a perfect square and a perfect cube.
  - For every positive integer n, there exists an integer k such that $2^k > n$.
  - If A and B are disjoint sets.

Exercises III

- **Translate and rewrite each statement using mathematical symbols:** Advanced Level
  - For every positive integer n, there exists a prime number p such that $p > n$.
  - For all sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
  - There exists an irrational number x such that x^x is rational.
  - For every $\epsilon > 0$, there exists a $\delta > 0$ such that for all x, if $0 < |x - a| < \delta$, then $|f(x) - L| < \epsilon$.
  - If a sequence (a_n) converges to L, then for every $\epsilon > 0$, there exists an integer N such that for all $n > N$, $|a_n - L| < \epsilon$.
  - There exists a countable set S such that S is dense in $\mathbb{R}$.
  - For all functions f continuous on $[a, b]$, the function f attains a maximum on $[a, b]$.
  - For every infinite sequence of real numbers, there exists a subsequence that converges.

Recurrence Relations

- **Definition:** A recurrence relation defines the nth term of a sequence in terms of previous terms.
- **Example 1: Fibonacci Sequence:**

$$F_n = F_{n-1} + F_{n-2}, \quad F_0 = 0, \quad F_1 = 1.$$

- **Example 2: Tower of Hanoi:**

$$T_n = 2T_{n-1} + 1, \quad T_1 = 1.$$

- **Solution Methods:**
  - **Iteration:** Expand terms to identify a pattern.
  - **Guess and Verify:** Assume a closed-form solution and prove by induction.
  - **Characteristic Equation:** Solve linear recurrences with constant coefficients:

$$T_n - 3T_{n-1} + 2T_{n-2} = 0 \implies \text{roots of characteristic polynomial.}$$

- **Exercise:**
  - Solve the recurrence $T_n = 3T_{n-1} + 4$, with $T_0 = 2$.

Functions

- **Definition:** A function $f : A \to B$ maps each element of A (domain) to a unique element of B (codomain).
- **Types of Functions:**
  - **Injective (One-to-One):** No two distinct elements of A map to the same element of B.
  - **Surjective (Onto):** Every element of B has a pre-image in A.
  - **Bijective:** Both injective and surjective (a perfect pairing between A and B).
- **Examples:**
  - Injective: $f(x) = 2x$ for $f : \mathbb{R} \to \mathbb{R}$.
  - Surjective: $f(x) = x^2$ for $f : \mathbb{R} \to [0, \infty)$.
  - Bijective: $f(x) = x + 1$ for $f : \mathbb{Z} \to \mathbb{Z}$.
- **Exercise:**
  - Prove: The inverse of a bijective function is also a function.

Relations I

- **Definition:** A relation R on a set A is a subset of $A \times A$ (pairs of elements in A).
- **Types of Relations:**
  - **Reflexive:** $(a, a) \in R$ for all $a \in A$.
  - **Symmetric:** $(a, b) \in R \implies (b, a) \in R$.
  - **Transitive:** $(a, b) \in R$ and $(b, c) \in R \implies (a, c) \in R$.
  - **Antisymmetric:** $(a, b) \in R$ and $(b, a) \in R \implies a = b$.
- **Equivalence Relation:**
  - A relation that is reflexive, symmetric, and transitive.
  - Example: "Congruence modulo n" is an equivalence relation.
- **Partial Order:**
  - A relation that is reflexive, antisymmetric, and transitive.
  - Example: Subset relation ($\subseteq$).
- **Exercise:**
  - Prove: The "less than or equal to" relation ($\leq$) on real numbers is a partial order.

Relations II

- **Composition of Relations:**
  - If R is a relation from A to B, and S is a relation from B to C, their composition $S \circ R$ is defined as:

$$(a, c) \in S \circ R \iff \exists b \in B \text{ such that } (a, b) \in R \text{ and } (b, c) \in S.$$

- **Inverse Relation:**
  - For a relation R on A, the inverse R^{-1} is defined as:

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

- **Example:**
  - Let $R = \{(1, 2), (2, 3)\}$ and $S = \{(2, 4), (3, 5)\}$.
  - Then, $S \circ R = \{(1, 4), (2, 5)\}$.
- **Exercise:**
  - Prove that the inverse of an equivalence relation is also an equivalence relation.

Sets I

- **Definition:** A set is a well-defined collection of distinct objects.
- **Basic Operations:**
  - Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.
  - Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
  - Difference: $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$.
  - Complement: $A^c = \{x \mid x \notin A\}$.
- **Power Set:**

$$\mathcal{P}(A) = \text{Set of all subsets of } A.$$

- **Exercise:**
  - Prove: If $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Sets II

- **Definition:** The Cartesian product of two sets A and B is:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

- **Example:**
  - If $A = \{1, 2\}$ and $B = \{x, y\}$, then:

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}.$$

- **Properties:**
  - $|A \times B| = |A| \cdot |B|$.
  - $A \times \emptyset = \emptyset$.
- **Exercise:**
  - Prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Counting and Binomial Coefficients I

- **Counting Principles:**
  - **Addition Principle:** If task A can be done in m ways and task B in n ways (mutually exclusive), total ways $= m + n$.
  - **Multiplication Principle:** If tasks A and B can be done in m and n ways respectively (independently), total ways $= m \cdot n$.
- **Binomial Coefficients:**

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

- **Pascal's Identity:**

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

- **Binomial Theorem:**

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Counting and Binomial Coefficients II

- **Definition:** For two finite sets A and B, the size of their union is given by:
$$|A \cup B| = |A| + |B| - |A \cap B|.$$
- **Three Sets:**

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

- **General Formula:** For n finite sets $A_1, A_2, \ldots, A_n$:
$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\emptyset \neq J \subseteq \{1,\ldots,n\}} (-1)^{|J|+1} \left| \bigcap_{j \in J} A_j \right|$$

Counting and Binomial Coefficients III

- **Example:**
  - Let $|A| = 10$, $|B| = 8$, $|C| = 6$, $|A \cap B| = 4$, $|B \cap C| = 3$, $|C \cap A| = 2$, $|A \cap B \cap C| = 1$.
  - Then:
$$|A \cup B \cup C| = 10 + 8 + 6 - 4 - 3 - 2 + 1 = 16.$$
- **Exercise:**
  - Prove the identity: $\binom{n}{k} = \binom{n}{n-k}$.
  - Use the inclusion-exclusion principle to compute the number of integers from 1 to 100 that are divisible by 2, 3, or 5.
  - Apply the principle to compute the number of surjective functions from a set of size 3 to a set of size 2.

Modular Arithmetic I

- **Definition:** For integers a and b, and a positive integer n, $a \equiv b \pmod{n}$ means n divides $(a - b)$.
- **Properties:**
  - Addition: $(a + b) \mod n = [(a \mod n) + (b \mod n)] \mod n$.
  - Multiplication: $(a \cdot b) \mod n = [(a \mod n) \cdot (b \mod n)] \mod n$.
- **Examples:**
  - $7 \equiv 2 \pmod{5}$.
  - $12 \equiv 0 \pmod{6}$.
- **Exercise:**
  - Prove: For any integer a, $a^2 \equiv 0$ or $1 \pmod{4}$.

Modular Arithmetic II

- **Chinese Remainder Theorem:**
  - If $n_1, n_2, \ldots, n_k$ are pairwise coprime, then the system:

$$x \equiv a_1 \pmod{n_1},\ x \equiv a_2 \pmod{n_2},\ \ldots,\ x \equiv a_k \pmod{n_k}$$

    has a unique solution modulo $N = n_1 n_2 \ldots n_k$.
- **Example:**
  - Solve: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.
- **Fermat's Little Theorem:**
  - If p is prime and a is an integer not divisible by p:

$$a^{p-1} \equiv 1 \pmod{p}.$$

- **Exercise:**
  - Verify Fermat's Little Theorem for $a = 2$, $p = 7$.

Convolution

- **Definition:** The convolution of two functions f and g over a domain T is defined as:

$$(f * g)(t) = \int_{-\infty}^{\infty} f(\tau)g(t-\tau)\,d\tau \quad \text{(Continuous Case)},$$

or

$$(f * g)[n] = \sum_{k=-\infty}^{\infty} f[k]g[n-k] \quad \text{(Discrete Case)}.$$

- **Applications:**
  - Signal processing.
  - Probability (convolution of distributions).
  - Solving differential equations.
- **Example:**
  - Let $f(t) = e^{-t}$ and $g(t) = u(t)$ (unit step function). Compute $(f * g)(t)$.
- **Exercise:**
  - Compute the convolution of $f[n] = 1$ for $n = 0, 1, 2$ and $g[n] = 1$ for $n = 0, 1$.

Sufficient and Necessary Conditions

- Definitions:
  - A condition P is sufficient for Q if $P \implies Q$. - If P is true, Q must also be true.
  - A condition P is necessary for Q if $Q \implies P$. - If Q is true, P must also be true.
  - A condition can be both necessary and sufficient if $P \iff Q$ (if and only if).
- Examples:
  - Sufficient Condition: If a number is divisible by 4, it is divisible by 2. - Divisibility by 4 is sufficient for divisibility by 2.
  - Necessary Condition: For a number to be divisible by 4, it must be even. - Being even is necessary for divisibility by 4.
  - Necessary and Sufficient Condition: A triangle is equilateral if and only if all its sides are equal.

Exercise:

- Is being a square sufficient, necessary, or both for being a rectangle?
- Provide an example of a condition that is sufficient but not necessary.

Maximal vs. Maximum & Minimal vs. Minimum I

Key Concepts:

- **Maximum/Minimum:** These denote the absolute, global extremum in a set (with respect to a given ordering).
  - Example: In the set $S = \{3, 7, 2, 9\}$ (ordered by $\leq$), $\max(S) = 9$ and $\min(S) = 2$.
- **Maximal/Minimal:** These denote elements that are locally extreme with respect to a partial order, meaning they cannot be extended further, though they may not be unique.
  - Example: In the poset $(\mathcal{P}(\{1, 2\}), \subseteq)$, consider:
    - ⋆ The set $\{1\}$ is **maximal** if there is no set in the collection (other than the maximum) that properly contains it. However, the maximum element (with respect to $\subseteq$) is $\{1, 2\}$.
    - ⋆ In the same poset, the minimal elements are the singletons $\{1\}$ and $\{2\}$ if we restrict our attention to a collection that does not include the empty set; whereas if the empty set is included, $\emptyset$ is the **minimum**.

Maximal vs. Maximum & Minimal vs. Minimum II

Additional Examples:

- **Example 1: Partially Ordered Set (Poset):** Let $S = \{a, b, c\}$ with the relation $a \preceq b$ and $a \preceq c$, but b and c are incomparable.
  - Both b and c are **maximal** elements since there is no element greater than them.
  - There is no unique **maximum** element because b and c are incomparable.
- **Example 2: Set Inclusion:** Consider the collection $\mathcal{F} = \{\{1\}, \{2\}, \{1, 2\}\}$ ordered by inclusion ($\subseteq$).
  - $\{1, 2\}$ is the **maximum** element since it contains every other set.
  - The sets $\{1\}$ and $\{2\}$ are **minimal** elements (they are not contained in any other proper subset in $\mathcal{F}$).

Maximal vs. Maximum & Minimal vs. Minimum III

Key Observations:

- Every maximum is maximal, but a maximal element is not necessarily maximum in a partially ordered set.
- Similarly, every minimum is minimal, but a minimal element may not be the absolute minimum.

Exercise:

- Consider the poset $\{1, 2, 3, 4\}$ with the divisibility relation "$|$". Identify the minimal, maximal, minimum, and maximum elements.
- In the power set $\mathcal{P}(\{a, b, c\})$ ordered by inclusion, list all maximal and minimal elements.

What is "Without Loss of Generality" (WLOG)? I

Definition: "Without Loss of Generality" (WLOG) is a mathematical assumption that simplifies proofs by selecting a specific case while ensuring that all other cases follow by symmetry or similar arguments.

Why is it useful?

- WLOG is useful in logic, computing, business, and everyday reasoning.
- It helps reduce redundant work by focusing on one symmetric case.
- Ensures assumptions do not limit the problem's generality.
- Avoids repetitive arguments.

When Can We Use WLOG? Key Conditions:

- The problem must be symmetric or equivalent across multiple cases.
- The assumption should not restrict the generality of the solution.
- If making an assumption, it must hold for all other possible cases.

Example: When proving a property about numbers a, b, c, we may assume $a \leq b \leq c$ **WLOG**, since the problem is symmetric in a, b, c.

Common Misuses of WLOG

Be Careful!

- WLOG is not valid when assuming something that eliminates valid cases.
- Example: Assuming a triangle is isosceles when proving a theorem about **all** triangles.
- Always verify that symmetry or relabeling ensures the assumption does not alter the generality.

Key Takeaways:

- WLOG simplifies proofs by assuming a specific case when all other cases are symmetric.
- It is commonly used in combinatorics, graph theory, algebra, and geometry.
- Misuse occurs when the assumption restricts the generality of the proof.

Final Thought: Always justify why WLOG is valid when using it in a proof.

WLOG Beyond Math Proofs I

- Language & Translation
  - Translating "John and Mary went to the store"
  - WLOG, assume "John" is mentioned first.
  - The meaning remains unchanged regardless of order.

  Why? - Word order choice does not affect the translation logic.
- Computer Science & Algorithms
  - Sorting algorithms often assume input order WLOG.
  - Quicksort: WLOG, choose the first element as the pivot.
  - Any other pivot choice can be transformed into this case.

  Why? - The same logic applies to all pivot choices.
- Legal & Contracts
  - In a contract, two equal partners may be labeled as:
  - "Partner A" and "Partner B" WLOG.
  - The document remains valid regardless of label choice.

  Why? - Their roles are symmetric in the contract.

WLOG Beyond Math Proofs II

- Game Strategy & Decision Making
  - In tic-tac-toe, WLOG assume the first move is in the center.
  - Edge/corner moves can be analyzed similarly.

  Why? - Game symmetry makes this a general case.
- Physics & Engineering
  - Analyzing a charged particle in a uniform field.
  - WLOG assume the field points along the x-axis.
  - Rotations allow extension to other directions.

  Why? - Symmetry in physics simplifies analysis.
- Business & Economics
  - Studying tax policy impact on companies.
  - WLOG assume an average-income company.
  - High/low-income cases can be adjusted similarly.

  Why? - A representative case gives a generalizable conclusion.

WLOG Beyond Math Proofs III

- Psychology & Sociology Surveys
  - Analyzing consumer behavior for a new product.
  - WLOG assume an average-income respondent.
  - Higher/lower income groups follow similar trends.

  Why? - Allows focusing on a typical case without losing generality.

Key Takeaways:

- WLOG is not just for mathematical proofs.
- It simplifies reasoning in logic, computing, business, and science.
- The assumption must be valid for all cases.

Final Thought: Next time you simplify a problem, check if you're using WLOG!

Outline

Proof

Definition: A proof is a logical argument that establishes the truth of a mathematical statement.

- A proof is built using:
  - Axioms: Fundamental truths accepted without proof.
  - Definitions: Precise meanings of mathematical terms.
  - Previously proven theorems and lemmas.
- **Purpose:** To ensure that a statement is universally true in all cases, leaving no room for doubt.

Example:

- Proving that the sum of two even integers is even.

Exercise:

- Why is a proof essential in mathematics and computer science?

Theorem

Definition: A theorem is a significant mathematical statement that has been rigorously proven.

- Theorems are the cornerstone of mathematical reasoning, providing powerful and general results.
- **Example:** The Pythagorean Theorem:

$$a^2 + b^2 = c^2 \quad \text{for a right triangle.}$$

Exercise:

- Identify a theorem from geometry, algebra, or calculus, and explain its significance.

Axioms and Assumptions I

- **Axioms:**
  - Axioms are fundamental truths accepted without proof as the basis for reasoning.
  - They provide the foundational framework for mathematical theories.

  Example: Euclidean Geometry Axiom:

  Through any two distinct points, there exists exactly one line.

- **Assumptions:**
  - Assumptions are conditions or premises accepted as true temporarily for a specific proof or context.
  - They are not universally valid but apply within the scope of a particular argument or model.

  Example: Assume $x > 0$ to prove a property of positive integers.

Axioms and Assumptions II

Comparison:

- Axioms are universal and foundational.
- Assumptions are context-specific and temporary.

Exercise:

- Identify an assumption in a proof or problem-solving context and explain its role in reaching the conclusion.

Lemma, Corollary, and Remark

- **Lemma:** A preliminary result used to prove a larger theorem.
  - Simplifies complex proofs by breaking them into manageable parts.
  - **Example:** The Division Algorithm as a lemma for proving properties of the greatest common divisor (gcd).
- **Corollary:** A result that follows directly from a theorem with little or no additional proof.
  - Often a specific case or direct extension of a theorem.
  - **Example:** The angles of a triangle sum to 180° (corollary of Euclid's parallel postulate).
- **Remark:** An observation or note that provides additional insight, context, or clarification to a result.
  - Explains why certain results hold or how they extend to other contexts.
  - **Example:** A remark on why the quadratic formula works only for equations of degree 2.

Exercise:

- Identify a lemma, corollary, and remark from any textbook and explain how they relate to a theorem.

Proof Structure

- A structured proof typically consists of three parts:
  1. **Given:** State the assumptions or hypotheses.
  2. **To Show:** Clearly define the statement to be proven.
  3. **Proof:** Provide the logical argument, step by step, leading from the assumptions to the conclusion.

Example:

- Prove: If n is even, then n^2 is even.

Proof:

- **Given:** n is even, i.e., $n = 2k$ for some integer k.
- **To Show:** n^2 is even.
- **Proof:** $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which is divisible by 2.

Exercise:

- Write a structured proof for: The product of two odd integers is odd.

Proof Structure (Expanded)

- **Essential Components of a Proof:**
  1. **Hypotheses:** The given assumptions or premises.
  2. **Goal:** The statement or conclusion to be proven.
  3. **Logical Argument:** A sequence of logically valid steps connecting the hypotheses to the conclusion.
- **Best Practices:**
  - Clearly state all assumptions at the beginning.
  - Avoid skipping logical steps, even if they seem obvious.
  - Use appropriate notations and symbols for clarity.
  - Conclude with a formal statement such as "Thus, the theorem is proven."

Exercise:

- Rewrite the following proof with better structure:

  "If n is even, then n^2 is even because $n = 2k$, so $n^2 = 4k^2$."

Outline

Introduction to Proof Techniques

- Proofs are fundamental to mathematics and computer science for verifying claims and establishing truth.
- Common techniques include:
  1. Direct Proof
  2. Proof by Contradiction
  3. Proof by Contrapositive
  4. Mathematical Induction
  5. Proof by Exhaustion
  6. Proof using Counterexamples
- This slide deck provides instructions, examples, and exercises for each technique.

Direct Proof

- **Definition:** A direct proof establishes the truth of a statement by straightforward logical deductions.
- **Steps:**
  1. Assume the hypothesis is true.
  2. Use logical reasoning to deduce the conclusion.

Example:

- Prove: If n is an even integer, then n^2 is even.

Proof:

- Let $n = 2k$ for some integer k (definition of even numbers).
- Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which is divisible by 2.
- Thus, n^2 is even.

Exercise:

- Prove: The sum of two even integers is even.

Transition: Sometimes, proving a statement directly is not possible. Let's explore indirect techniques.

Proof by Contradiction I

- **Definition:** Assume the negation of the statement is true and derive a contradiction.
- **Steps:**
  1. Assume the statement to be proven is false.
  2. Show this assumption leads to a contradiction.

Example:

- Prove: $\sqrt{2}$ is irrational.

Proof by Contradiction II

Proof:

- Assume $\sqrt{2}$ is rational, i.e., $\sqrt{2} = p/q$, where p and q are coprime integers.
- Then $2 = p^2/q^2$, so $p^2 = 2q^2$.
- Thus, p^2 is even, implying p is even. Let $p = 2k$.
- Substituting: $(2k)^2 = 2q^2 \implies q^2 = 2k^2$, so q is also even.
- This contradicts the assumption that p and q are coprime.
- Therefore, $\sqrt{2}$ is irrational.

Exercise:

- Prove: There are infinitely many prime numbers.

Transition: Let's explore another indirect technique: Proof by Contrapositive.

Proof by Contrapositive I

- **Definition:** Prove the contrapositive of the statement: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.
- **Steps:**
  1. Restate the contrapositive of the original statement.
  2. Prove the contrapositive directly.

Example:

- Prove: If n^2 is odd, then n is odd.

Proof:

- Contrapositive: If n is even, then n^2 is even.
- Let $n = 2k$ (definition of even numbers).
- Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which is even.
- Thus, if n is even, n^2 is even, proving the contrapositive.

Proof by Contrapositive II

Exercise:

- Prove: If $a \cdot b = 0$, then $a = 0$ or $b = 0$ (using contrapositive).

Transition: What if the statement involves iteration? Let's look at Mathematical Induction.

Mathematical Induction I

- **Definition:** A proof technique used to show a statement holds for all natural numbers.
- **Steps:**
  1. **Base Case:** Prove the statement is true for the first value (e.g., $n = 1$).
  2. **Inductive Step:** Assume the statement is true for $n = k$, and prove it holds for $n = k + 1$.

Example:

- Prove: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ for all $n \geq 1$.

Proof:

- Base Case: For $n = 1$, $1 = \frac{1(1+1)}{2} = 1$. True.
- Inductive Hypothesis: Assume $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$.

Mathematical Induction II

- Inductive Step: For $n = k + 1$,

$$1 + 2 + \ldots + k + (k + 1) = \frac{k(k+1)}{2} + (k + 1)$$

$$= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}.$$

  Thus, the statement holds for $n = k + 1$.

Exercise:

- Prove: $2^n > n^2$ for $n \geq 5$ using induction.

Transition: Let's now look at exhaustive methods for finite scenarios.

Proof by Exhaustion I

- **Definition:** A proof method where all possible cases are checked individually to establish the truth of a statement.
- **Steps:**
  1. Divide the problem into finite cases.
  2. Verify the statement for each case.

Example:

- Prove: For integers n, if $n^2 \leq 4$, then $n = -2, -1, 0, 1,$ or 2.

Proof by Exhaustion II

Proof:

- The inequality $n^2 \leq 4$ implies $-2 \leq n \leq 2$.
- The possible integer values for n are $-2, -1, 0, 1, 2$.
- For each n, verify:

$$(-2)^2 = 4, (-1)^2 = 1, 0^2 = 0, 1^2 = 1, 2^2 = 4.$$

  All satisfy $n^2 \leq 4$.
- Thus, the statement holds.

Exercise:

- Prove: A triangle with sides a, b, c is right-angled if $a^2 + b^2 = c^2$, for all permutations of a, b, c when $a, b, c \in \{3, 4, 5\}$.

Transition: Next, we explore how disproving a claim with a single counterexample can be effective.

Proof by Counterexample I

- **Definition:** To disprove a universal statement, it suffices to provide a single example where the statement does not hold.
- **Steps:**
  1. Identify a claim to disprove.
  2. Find a single counterexample that violates the claim.

Example:

- Disprove: All prime numbers are odd.

Proof:

- A counterexample is the prime number 2.
- Since 2 is even, the statement is false.

Proof by Counterexample II

Example:

- Disprove: For all integers n, $n^2 + n + 41$ is prime.

Proof:

- Let $n = 40$. Then:

$$40^2 + 40 + 41 = 1681 = 41 \cdot 41,$$

  which is not prime. Hence, the statement is false.

Exercise:

- Find a counterexample to disprove: For all integers $n > 1$, $2^n - 1$ is prime.

Transition: Let's now summarize the connections between these techniques and how to choose the right one for a given proof.

Existence and Constructive Proofs

- **Existence Proof:**
  - Demonstrates the existence of an object satisfying certain properties.
  - Does not necessarily construct the object.
- **Constructive Proof:**
  - Explicitly constructs an example that satisfies the given conditions.

Example: Prove there exists an even prime number.

- **Existence Proof:** Observe that 2 is an even number and is prime.
- **Constructive Proof:** Construct the number 2 and show it is both even and prime.

Exercise:

- Prove that there exists a real number x such that $x^2 = 2$.

Existential Proof: An Interesting Example I

Theorem: There exist irrational numbers a and b such that a^b is rational.
Proof:

- Consider $a = \sqrt{2}$ and $b = \sqrt{2}$, and Let $x = (\sqrt{2})^{\sqrt{2}}$
- We need to consider two cases:
  - If x is rational, we have found a and b (both $\sqrt{2}$) such that a^b is rational.
  - If x is irrational, we can use this value of x. Let $a = (\sqrt{2})^{\sqrt{2}}$ and $b = \sqrt{2}$. Then:

$$a^b = \left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^{(\sqrt{2}\cdot\sqrt{2})} = (\sqrt{2})^2 = 2$$

- Since 2 is rational, we have found irrational numbers a and b such that a^b is rational.
- Therefore, in either case, there exist irrational numbers a and b such that a^b is rational.

Existential Proof: An Interesting Example II

Remark: We actually don't know for sure which case is actually true, but we can still conclusively argue that one of them must be.
More such interesting proofs are found in

- Cantor's Diagonal Argument for proving the set of real numbers in the interval $[0, 1)$ is uncountable.
- Infinite Monkey Theorem: A monkey hitting keys at random on a typewriter keyboard for an infinite amount of time will almost surely type a given text, such as the complete works of Shakespeare.

Graphical Representation in Proofs

- **Benefits of Graphical Proofs:**
  - Visualizes complex relationships, making them easier to understand.
  - Highlights patterns or symmetries that aid in logical reasoning.
- **Examples:**
  - **Venn Diagrams:** To prove set identities (e.g., $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$).
  - **Graphs:** To prove connectivity or traversal properties (e.g., Eulerian paths).
  - **Flowcharts:** To represent algorithmic correctness.

Exercise:

- Use a Venn diagram to prove: $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

Pigeonhole Principle

- **Statement:** If n items are placed into m containers, where $n > m$, then at least one container must hold more than one item.
- **Example:** In a group of 13 people, at least two people share the same birth month.

Proof:

- There are 12 months (containers) and 13 people (items).
- By the pigeonhole principle, at least one month must have more than one person.

Exercise:

- Prove that in any set of 27 words, at least two words must start with the same letter.

Choosing the Right Technique

The choice of a proof technique is a critical task, and one can build a sense for this by practice. However, here are some tips to help you get started.

- Use direct proof when the conclusion can be deduced in a straightforward manner.
- Use contradiction or contrapositive for indirect proofs.
- Use induction for statements involving natural numbers or iteration.
- Use counterexamples to disprove universal claims.
- Use exhaustion when the cases are finite and manageable.

Outline

Introduction to Logical Fallacies in Proofs

- **Definition:** Logical fallacies are errors in reasoning that invalidate an argument or proof.
- **Impact:** Even a single fallacy can render a proof incorrect, misleading, or incomplete.
- **Common Types of Fallacies in Proofs:**
  1. Circular Reasoning
  2. Hasty Generalization
  3. Misuse of Assumptions
  4. Overgeneralization
  5. Ignoring Edge Cases
- **Goal:** Learn to identify and avoid logical fallacies to ensure rigorous, valid proofs.

Circular Reasoning

- **Definition:** Assuming the result to be true as part of its proof.
- **Example:**
  - Statement: "This algorithm is correct because it always produces the correct result."
  - Issue: The correctness of the algorithm is assumed rather than proven.
- **Fix:** Provide an independent verification or proof of correctness.

Exercise:

- Identify the flaw in this argument:

  "Triangles have 180° angles because the sum of their angles is 180°."

Hasty Generalization

- **Definition:** Drawing a conclusion based on insufficient evidence.
- **Example:**
  - Statement: "All even numbers are prime because 2 is even and prime."
  - Issue: The conclusion is based on a single example (2) without considering counterexamples (e.g., 4, 6, etc.).
- **Fix:** Use comprehensive testing or proof to ensure the generalization is valid.

Exercise:

- Provide a counterexample to disprove: "All integers greater than 1 are prime."

Misuse of Assumptions

- **Definition:** Applying assumptions outside their intended scope or misinterpreting them.
- **Example:**
  - Statement: "Let $x > 0$. Therefore, $x^2 > x$."
  - Issue: The assumption fails for $x \in (0, 1)$ (e.g., $x = 0.5$).
- **Fix:** Clearly state and adhere to the domain of assumptions.

Exercise:

- Analyze the statement: "If $x > 0$, then $x \geq 1$." Identify the assumption error.

Overgeneralization

- **Definition:** Extending a conclusion beyond its valid scope.
- **Example:**
  - Statement: "Since all polynomials of degree 2 have exactly 2 roots, all polynomials have a number of roots equal to their degree."
  - Issue: Overlooks complex roots, multiplicity, or cases where coefficients are not in an algebraically closed field.
- **Fix:** Specify the scope (e.g., "over the complex numbers") or refine the statement.

Exercise:

- Prove or disprove: "Every even polynomial has only even roots."

Ignoring Edge Cases

- **Definition:** Failing to consider special or boundary cases in a proof.
- **Example:**
  - Statement: "The sum of n positive integers is always greater than n."
  - Issue: Fails for edge cases like $n = 1$ or n integers all equal to 1.
- **Fix:** Analyze edge cases and explicitly account for them in the proof.

Exercise:

- Find an edge case that invalidates the statement: "For all integers n, $n^2 > n$."

False Analogy

- **Definition:** Drawing an invalid conclusion by comparing two unrelated situations.
- **Example:**
  - Statement: "Since a square is a polygon with equal sides, all polygons with equal sides must be squares."
  - Issue: The analogy assumes that all polygons with equal sides have properties exclusive to squares.
- **Fix:** Identify the specific properties being compared and ensure their logical consistency.

Exercise:

- Provide an example where equal sides do not imply a square (e.g., equilateral triangles).

Contradiction Ignored

- **Definition:** Ignoring contradictions in the argument or proof.
- **Example:**
  - Statement: "All integers are both even and odd."
  - Issue: This contradicts the definition of even and odd integers (an integer cannot be both).
- **Fix:** Identify and resolve contradictions before proceeding with the argument.

Exercise:

- Analyze this claim: "A set is both finite and infinite." Explain why it's contradictory.

Ambiguous Definitions

- **Definition:** Using vague or inconsistent definitions in a proof.
- **Example:**
  - Statement: "A number is 'big' if it is greater than 10. Therefore, 11 is very big."
  - Issue: The term 'big' is subjective and not rigorously defined.
- **Fix:** Provide precise definitions for all terms used in the proof.

Exercise:

- Redefine the term "big" to be mathematically precise (e.g., $n > 10^3$).

Proof by Intimidation

- **Definition:** Using overly complex language or appealing to authority to assert correctness without actual reasoning.
- **Example:**
  - Statement: "This equation is obviously true because it was proven by a famous mathematician."
  - Issue: The proof lacks any explanation or reasoning.
- **Fix:** Provide clear, step-by-step reasoning accessible to the intended audience.

Exercise:

- Simplify the following statement into clear reasoning: "The Fourier transform is valid here because it's well-known to solve this type of problem."

Overreliance on Specific Cases

- **Definition:** Using specific examples to prove a general statement without rigorous justification.
- **Example:**
  - Statement: "Since $2 + 2 = 4$ and $3 + 3 = 6$, addition always results in an even number."
  - Issue: Fails to consider cases like $1 + 2 = 3$, which disproves the statement.
- **Fix:** Prove the statement for all possible cases using general reasoning.

Exercise:

- Disprove the claim: "The product of two odd numbers is always even."

Misleading Visualization

- **Definition:** Using a diagram or graph that inaccurately represents the problem or misleads the viewer.
- **Example:**
  - Statement: "The area of a circle can be squared because the diagram looks correct."
  - Issue: The diagram may appear convincing but lacks mathematical rigor.
- **Fix:** Verify all visual arguments mathematically.

Exercise:

- Identify the flaw in a misleading Euler diagram where overlapping sets are misrepresented.

Bonus Challenge: Logical Fallacies in Proofs

- Analyze the following flawed proofs and identify the fallacy:
  1. "Since $a^2 + b^2 = c^2$ for $a = 3, b = 4, c = 5$, it holds for all integers."
  2. "Parallel lines meet at infinity because they appear to converge in perspective drawings."
  3. "The function $f(x) = x^2$ is increasing because $1^2 < 2^2$ and $2^2 < 3^2$."

Hint: Look for overgeneralization, misuse of assumptions, or misleading visualizations.

Induction Trap I

Theorem: All horses are the same color.

[False Proof]

We will use induction on the number of horses, n.

- **Base case:** For $n = 1$, there is only one horse, so all horses (the single horse) are trivially the same color.
- **Inductive step:** Assume that for a set of n horses, they are all the same color. We need to show that $n + 1$ horses are also the same color.
  - Take a set of $n + 1$ horses.
  - Divide them into two overlapping subsets: the first subset contains horses $H_1, H_2, \ldots, H_n$ and the second subset contains horses $H_2, H_3, \ldots, H_{n+1}$.
  - By the induction hypothesis, the first subset (horses H_1 to H_n) are all the same color.
  - Similarly, the second subset (horses H_2 to H_{n+1}) are all the same color.
  - Since horses $H_2, H_3, \ldots, H_n$ are common in both subsets and are the same color, it follows that all $n + 1$ horses are the same color.

Induction Trap II

Flaw: This argument fails in the inductive step for $n = 1$ as there is no overlap of H_2 to compare.
Similar mistakes can be easily made for trying to prove the following statements using induction:

- All natural numbers are equal.
- For every positive integer n, the sum of the first n even numbers is $n(n+1)$.
- Prove that for every positive integer n, the sum of the first n cubes is equal to the square of the sum of the first n natural numbers, i.e., $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.
- Prove that for every positive integer n, the sum of the first n Fibonacci numbers is equal to the $(n+2)$-th Fibonacci number minus 1, i.e., $\sum_{i=1}^{n} F_i = F_{n+2} - 1$.

Comprehensive Summary of Logical Fallacies I

- **Common Logical Fallacies in Proofs:**
  1. **Circular Reasoning:** Assuming the conclusion as part of the proof.
  2. **Hasty Generalization:** Drawing conclusions based on insufficient evidence.
  3. **Misuse of Assumptions:** Applying assumptions outside their intended scope.
  4. **Overgeneralization:** Extending conclusions beyond their valid domain.
  5. **Ignoring Edge Cases:** Overlooking special or boundary scenarios.
  6. **False Analogy:** Comparing unrelated scenarios to draw conclusions.
  7. **Ambiguous Definitions:** Using vague or inconsistent terminology.
  8. **Contradiction Ignored:** Proceeding with an argument despite evident contradictions.
  9. **Proof by Intimidation:** Asserting correctness without proper reasoning.
  10. **Misleading Visualizations:** Using diagrams or graphs that inaccurately represent the problem.
  11. **Induction Trap**: Not checking all previous cases

Comprehensive Summary of Logical Fallacies II

- **Key Takeaways:**
  - A rigorous proof requires logical precision, clear reasoning, and attention to detail.
  - Avoid logical fallacies by critically analyzing every step and ensuring consistency.
  - Practice diverse proof techniques to gain confidence in tackling complex problems.

Outline

Substitution Method I

- **Definition:** The substitution method is a proof technique used to verify the correctness of a proposed solution for a recurrence or to establish a bound. - Assume a solution, substitute it into the recurrence, and prove its validity.
- **Steps:**
  1. **Hypothesis:** Assume a solution for the recurrence, typically $T(n) = O(f(n))$ or $T(n) \leq g(n)$.
  2. **Substitution:** Substitute the assumed solution into the recurrence relation.
  3. **Simplification:** Simplify the inequality to verify that it holds.
  4. **Base Case:** Check the solution for the base case(s) of the recurrence.

Substitution Method II

- **Example:** Solve the recurrence:

$$T(n) = 2T(n/2) + n.$$

- **Solution:**
  - **Hypothesis:** Assume $T(n) \leq cn \log n$ for some constant $c > 0$.
  - **Substitute into the recurrence:**

$$T(n) = 2T(n/2) + n \leq 2 \cdot c\frac{n}{2} \log \frac{n}{2} + n.$$

  - **Simplify:**

$$T(n) \leq cn \log n - cn + n = cn \log n - (c-1)n.$$

  - For large n, the inequality holds if $c \geq 1$.
  - **Base Case:** Verify for small values of n (e.g., $T(1) = O(1)$).

Exercise:

- Solve the recurrence $T(n) = T(n-1) + n$ using the substitution method.
- Prove that $T(n) = O(n^2)$ for the recurrence $T(n) = 2T(n/2) + n^2$.

Additional Examples Using Substitution Method I

- **Example 1:** Recurrence with Quadratic Growth Solve $T(n) = T(n/2) + n^2$.
  - **Hypothesis:** Assume $T(n) \leq cn^2$.
  - **Substitute:**
$$T(n) = T(n/2) + n^2 \leq c\frac{n^2}{4} + n^2.$$
  - **Simplify:**
$$T(n) \leq \frac{cn^2}{4} + n^2.$$
  - Choose $c \geq 4$ to ensure the inequality holds.
  - **Base Case:** Verify for small n (e.g., $T(1)$).
  - **Solution:** $T(n) = O(n^2)$.

Additional Examples Using Substitution Method II

- **Example 2:** Recurrence with Logarithmic Growth Prove that $T(n) = T(n/2) + 1$ satisfies $T(n) = O(\log n)$.
  - **Hypothesis:** Assume $T(n) \leq c \log n$.
  - **Substitute:**
$$T(n) = T(n/2) + 1 \leq c \log \frac{n}{2} + 1.$$
  - **Simplify:**
$$T(n) \leq c(\log n - \log 2) + 1 = c \log n - c + 1.$$
  - The inequality holds if c is appropriately chosen (e.g., $c \geq 1$).

Exercise:

- Solve $T(n) = 2T(n/2) + \sqrt{n}$ using the substitution method.
- Determine both upper and lower bounds for $T(n) = T(n/2) + n \log n$.

Real-World Applications of the Substitution Method I

- **Use in Algorithm Analysis:** The substitution method is widely used to analyze the runtime of recursive algorithms by solving recurrence relations.
- **Examples from Real-World Algorithms:**
  1. **Merge Sort:**
     - ⋆ Recurrence: $T(n) = 2T(n/2) + n$.
     - ⋆ Solution: Assume $T(n) = cn \log n$.
     - ⋆ Application: Proves that Merge Sort runs in $O(n \log n)$ time.
  2. **Binary Search:**
     - ⋆ Recurrence: $T(n) = T(n/2) + O(1)$.
     - ⋆ Solution: Assume $T(n) = c \log n$.
     - ⋆ Application: Confirms logarithmic search time for sorted data.
  3. **Karatsuba Multiplication:**
     - ⋆ Recurrence: $T(n) = 3T(n/2) + O(n)$.
     - ⋆ Solution: Assume $T(n) = cn^{\log_2 3}$.
     - ⋆ Application: Optimized multiplication for large integers with $O(n^{1.585})$ complexity.

Real-World Applications of the Substitution Method II

4. **Divide and Conquer in Image Processing:**
   - ★ Recurrence: $T(n) = 4T(n/2) + n^2$ (e.g., quadtree compression).
   - ★ Solution: $T(n) = O(n^2 \log n)$.

- **Other Applications:**
  - Quick Sort Analysis: Prove that the average-case complexity is $O(n \log n)$.
  - FFT (Fast Fourier Transform): Solve $T(n) = 2T(n/2) + O(n)$ to confirm $O(n \log n)$ performance.

Exercise:

- Solve $T(n) = 3T(n/3) + n$ to analyze the runtime of a recursive search in a ternary tree.
- Prove the recurrence for the Strassen matrix multiplication algorithm: $T(n) = 7T(n/2) + O(n^2)$.

Hybrid Method: Substitution + Induction I

- **Overview:** The hybrid method combines the substitution method (for hypothesis and simplification) with induction (to rigorously prove correctness).
- **Steps:**
  1. **Hypothesize a Solution:** Assume a solution of the form $T(n) \leq f(n)$.
  2. Substitute into the Recurrence: Substitute the hypothesis into the recurrence relation to simplify it.
  3. **Prove by Induction:**
     - ⋆ **Base Case:** Verify the hypothesis holds for the smallest input (e.g., $T(1)$).
     - ⋆ **Inductive Step:** Assume the hypothesis holds for smaller inputs and prove it for n.

Hybrid Method: Substitution + Induction II

- **Example:** Solve $T(n) = 2T(n/2) + n$.
  - Step 1: **Hypothesis:** Assume $T(n) \leq cn \log n$.
  - Step 2: **Substitute:**

$$T(n) = 2T(n/2) + n \leq 2c\frac{n}{2}\log\frac{n}{2} + n.$$

  - Step 3: **Simplify:**

$$T(n) \leq cn \log n - cn + n.$$

  - Step 4: **Induction:**
    - ⋆ **Base Case:** Verify $T(1) = O(1)$.
    - ⋆ **Inductive Step:** Prove that $T(n) \leq cn \log n$ for all n.

Exercise:

- Use the hybrid method to solve $T(n) = 3T(n/3) + n$.
- Prove that $T(n) = T(n-1) + n$ satisfies $T(n) = O(n^2)$.

Advantages of the Hybrid Method I

- **Combines Strengths:**
  - Substitution simplifies the recurrence and generates a hypothesis.
  - Induction rigorously proves correctness.
- **Flexible Approach:**
  - Handles both upper and lower bounds effectively.
  - Useful for complex recurrences where one method alone may fail.
- **Examples:**
  - **Divide-and-Conquer Algorithms:**
    - ⋆ Merge Sort, Quick Sort, Binary Search.
  - **Dynamic Programming:**
    - ⋆ Optimal substructure recurrences.

Exercise:

- Solve $T(n) = 4T(n/2) + n^2$ using the hybrid method.
- Verify that $T(n) = T(n/2) + T(n/4) + n$ satisfies $T(n) = O(n)$.

Combinatorial Proofs

- **Definition:** Prove an identity by counting the same set in two different ways.
- **Example: Binomial Coefficient Identity:**

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

- **Proof:**
  - LHS: Number of ways to choose r items from n.
  - RHS: Split into cases:
    - ★ Case 1: Include a specific item ($\binom{n-1}{r-1}$).
    - ★ Case 2: Exclude the item ($\binom{n-1}{r}$).
- **Exercise:**
  - Prove: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ using a combinatorial argument.

Interactive Proofs I

- **Definition:** An interactive proof is a mathematical process where a **Prover** (P) tries to convince a **Verifier** (V) that a certain statement is true through a sequence of interactions.
- **Key Features:**
  - **Completeness:** If the statement is true, an honest Prover can convince the Verifier.
  - **Soundness:** If the statement is false, no dishonest Prover can convince the Verifier with high probability.

Interactive Proofs II

- **Applications:**
  - Cryptography (e.g., zero-knowledge proofs).
  - Computational complexity (e.g., proof that a solution exists without revealing it).
- **Example: Zero-Knowledge Proof:**
  - Prover knows a secret (e.g., a password or solution to a problem).
  - Prover convinces Verifier of the knowledge without revealing the actual secret.

Exercise:

- Research how zero-knowledge proofs are applied in blockchain technology.

Advanced Proof Techniques

- **Invariant Method:**
  - Proves properties that remain unchanged during transformations.
  - Example: In a game where each move swaps two adjacent elements, the parity (odd/even nature) of the number of inversions remains unchanged.
- **Probabilistic Proof:**
  - Uses probability to prove existence.
  - Example: Prove that in a group of n people, two people are likely to share the same birthday (Birthday Paradox).

Exercise:

- Use the invariant method to prove: In a checkerboard, if a square is removed, it cannot be tiled with dominoes.

Proofs in Real-World Contexts

- **Algorithm Correctness:**
  - Example: Proving sorting algorithms (e.g., mergesort) work correctly. Prove Dijkstra's algorithm always finds the shortest path in a weighted graph.
- **Cryptography:**
  - Example: Prove the security of RSA encryption relies on the difficulty of factoring large numbers.
- **Physics and Engineering:**
  - Example: Proving stability or efficiency of systems (e.g., bridges, circuits). Prove the stability of a truss using graph theory principles.

Exercise:

- Write a proof or provide a counterexample: Can a sorting algorithm achieve $O(1)$ runtime for arbitrary input sizes?
- Provide a proof or counterexample: Is it possible to design an unbreakable encryption algorithm?

Introduction to Strong Induction I

- **Definition:** Strong induction is a proof technique where the inductive step assumes the statement is true for all values up to k (not just k itself).
- Useful when the current case depends on multiple previous cases.
- **Steps:**
  1. **Base Case:** Prove the statement for the initial values.
  2. **Inductive Step:** Assume the statement holds for all $n \leq k$ (inductive hypothesis) and prove it for $n = k + 1$.

Introduction to Strong Induction II

- **Example: Prove every integer $n \geq 2$ can be written as a product of prime numbers.**
  - **Base Case:** $n = 2$ is prime. True.
  - **Inductive Hypothesis:** Assume the statement is true for all integers $2, 3, \ldots, k$.
  - **Inductive Step:** For $n = k + 1$, if $k + 1$ is prime, the statement is true. If not, it can be written as $a \cdot b$, where $a, b \leq k$, which are products of primes by the hypothesis.

Exercise:

- Prove the Fibonacci sequence satisfies $F_n = F_{n-1} + F_{n-2}$ using strong induction.

Mathematical Induction (Additional Examples) I

- Recall the steps for induction:
  1. **Base Case:** Prove the statement is true for the first value (e.g., $n = 1$).
  2. **Inductive Step:** Assume the statement is true for $n = k$ (inductive hypothesis), and prove it holds for $n = k + 1$.
- **Example 1: Prove** $1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ **for all** $n \geq 1$**.**
- **Proof:**
  - **Base Case:** For $n = 1$, $1^3 = \left(\frac{1(1+1)}{2}\right)^2 = 1$. True.
  - **Inductive Hypothesis:** Assume $1^3 + 2^3 + \ldots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$.

Mathematical Induction (Additional Examples) II

- **Inductive Step:** Prove for $n = k + 1$:

$$1^3 + 2^3 + \ldots + k^3 + (k+1)^3 = \left(\frac{(k+1)(k+2)}{2}\right)^2.$$

  Expand and simplify using the hypothesis.

- **Example 2:** Prove $2^n > n^2$ for $n \geq 5$.
  - Follow similar steps to show the base case and inductive step.

Exercise:

- Prove $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$ using induction.

Strong Induction (Additional Example)

- **Example: Prove any amount of postage $n \geq 8$ can be obtained using only 3-cent and 5-cent stamps.**
  - **Base Cases:**
    - ★ $n = 8$: Use $3 + 5$.
    - ★ $n = 9$: Use $3 + 3 + 3$.
    - ★ $n = 10$: Use $5 + 5$.
  - **Inductive Hypothesis:** Assume the statement holds for all amounts $n \geq 8$.
  - **Inductive Step:** For $n = k + 1$:
    - ★ $k + 1 - 3 \geq 8$ by assumption.
    - ★ By the hypothesis, $k + 1 - 3$ can be made with 3-cent and 5-cent stamps. Adding a 3-cent stamp proves $k + 1$.

Exercise:

- Prove that any integer $n \geq 12$ can be written as $4a + 5b$, where $a, b \geq 0$.

Induction Proof of Handshaking Theorem I

- **Theorem:** In any undirected graph, the sum of all vertex degrees is equal to twice the number of edges.

$$\sum_{v \in V} \deg(v) = 2|E|$$

- **Proof by Induction:**
  - **Base Case:** For a graph with one edge and two vertices:

$$\deg(v_1) + \deg(v_2) = 1 + 1 = 2 = 2|E|.$$

    True.
  - **Inductive Hypothesis:** Assume the theorem holds for any graph with k edges.

Induction Proof of Handshaking Theorem II

- **Inductive Step:** Consider a graph with $k+1$ edges:
  1. Remove one edge (u, v), reducing the degrees of u and v by 1.
  2. The graph now has k edges, so by the hypothesis:

$$\sum_{v \in V} \deg(v) = 2k.$$

  3. Add the removed edge back, increasing the degree sum by 2:

$$\sum_{v \in V} \deg(v) = 2k + 2 = 2(k+1).$$

- Thus, the theorem holds for all graphs.

Exercise:

- Verify the theorem for a triangle graph (K_3).

Induction Proof of Euler's Formula I

- **Theorem:** For any connected planar graph:

$$V - E + F = 2,$$

  where V is the number of vertices, E the number of edges, and F the number of faces.
- **Proof by Induction:**
  - **Base Case:** A single edge connecting two vertices ($V = 2$, $E = 1$, $F = 1$):

$$V - E + F = 2 - 1 + 1 = 2.$$

    True.
  - **Inductive Hypothesis:** Assume the formula holds for any planar graph with k edges.

Induction Proof of Euler's Formula II

- **Inductive Step:** Consider a graph with $k+1$ edges:
  1. Removing an edge reduces both E and F by 1:
  $$V - (E-1) + (F-1) = 2.$$
  2. Adding the edge back restores the original values:
  $$V - E + F = 2.$$

- Thus, the formula holds for all connected planar graphs.

Exercise:

- Verify Euler's formula for a square with a diagonal.

Outline

Outline

Commonly Used Mathematical Symbols

Groups, Rings, and Fields Notations:

- G, H, K — Groups or subgroups
- R, S, T — Rings
- F, K, L — Fields
- e — Identity element
- a^{-1} — Inverse of an element
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ — Integer, Rational, Real, and Complex numbers

Operations:

- $+, -, \cdot$ — Addition, Subtraction, Multiplication
- $a \cdot b$ or ab — Multiplication in a ring or field
- a^n — Repeated multiplication
- $|G|$ — Order of a group

Definition of a Group

Definition: A set G with a binary operation $\cdot : G \times G \to G$ is called a **group** if it satisfies:

- **Closure:** $a \cdot b \in G \ \forall a, b \in G$
- **Associativity:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **Identity:** There exists an element $e \in G$ such that $a \cdot e = a = e \cdot a$
- **Inverses:** For every $a \in G$, there exists an $a^{-1} \in G$ such that $a \cdot a^{-1} = e$

Example:

- $(\mathbb{Z}, +)$ is a group with addition.
- $(\mathbb{R}^*, \cdot)$ is a group under multiplication.

Cayley Table for Group

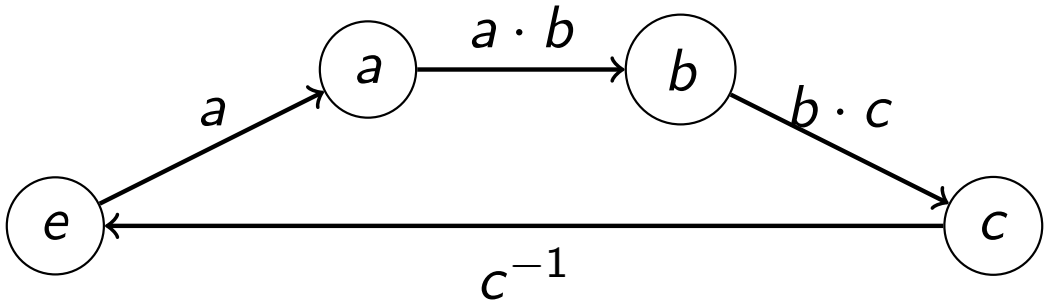
Example: Consider the group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under addition modulo 4.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Properties Checked:

- Closure
- Associativity
- Identity: 0
- Inverse: $a + (-a) = 0$

Visualizing Group Properties



Explanation: This represents a cyclic group of order 4. Each arrow shows the multiplication of elements.

Types of Groups

Based on Structure:

- **Abelian Group:** Every pair of elements commutes: $a \cdot b = b \cdot a$
- **Cyclic Group:** Generated by a single element: $G = \langle a \rangle$
- **Finite Group:** Group with a finite number of elements.
- **Infinite Group:** Group with infinitely many elements.
- **Symmetry Group:** Group of transformations preserving a structure.

Based on Properties:

- **Simple Group:** Non-trivial group with no normal subgroups other than the trivial group.
- **Dihedral Group:** Symmetry group of a regular polygon.
- **Matrix Group:** Group of matrices under multiplication (e.g., $GL_n(\mathbb{R})$).

Key Theorems in Group Theory

1. Lagrange's Theorem: Let G be a finite group and H a subgroup of G. Then:

$$|G| = |H| \cdot [G : H]$$

where $[G : H]$ is the index of H in G.

2. Cauchy's Theorem: If G is a finite group and p is a prime divisor of $|G|$, then G has an element of order p.

3. Fundamental Theorem of Finite Abelian Groups: Every finite abelian group can be expressed as a direct product of cyclic groups of prime-power order.

Definition of a Ring

Definition: A set R with two operations $+$ and $\cdot$ is called a **ring** if:

- $(R, +)$ forms an abelian group.
- $(R, \cdot)$ is associative.
- $\cdot$ distributes over $+$ (Distributivity):

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Examples:

- $(\mathbb{Z}, +, \cdot)$
- $(\mathbb{M}_n(\mathbb{R}), +, \cdot)$ — Matrices under addition and multiplication

Types of Rings

Based on Properties:

- **Commutative Ring:** Multiplication is commutative: $a \cdot b = b \cdot a$
- **Ring with Unity:** Has a multiplicative identity: $1 \neq 0$
- **Integral Domain:** No zero divisors: $ab = 0 \implies a = 0$ or $b = 0$
- **Division Ring:** Every non-zero element has a multiplicative inverse.

Special Types of Rings:

- **Polynomial Rings:** $R[x]$ where R is a commutative ring.
- **Matrix Rings:** $M_n(R)$ — Ring of all $n \times n$ matrices over a ring R.
- **Quotient Rings:** R/I where I is an ideal of R.

Key Theorems in Ring Theory

1. Ring Homomorphism Theorem: If $\phi : R \to S$ is a ring homomorphism, then:

$$\ker(\phi) \text{ is an ideal of } R \text{ and } \operatorname{im}(\phi) \text{ is a subring of } S.$$

2. Properties of Integral Domains: In an integral domain:

$$ab = ac \text{ and } a \neq 0 \implies b = c$$

This is called the **Cancellation Law**.

3. Polynomial Rings: If F is a field, then the ring of polynomials $F[x]$ is a Euclidean domain.

Definition of a Field

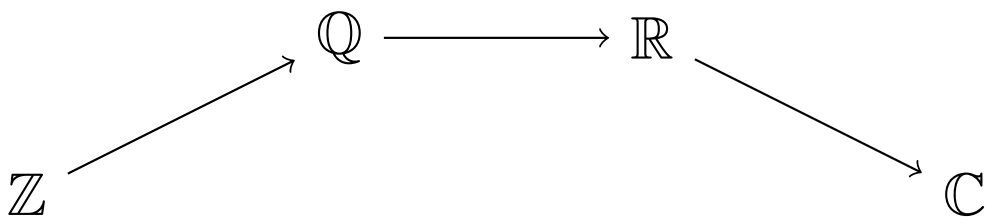
Definition: A field is a set F with two operations, $+$ and $\cdot$, such that:

- $(F, +)$ is an abelian group.
- $(F \setminus \{0\}, \cdot)$ is an abelian group.
- $\cdot$ distributes over $+$.

Examples:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- Finite Field $\mathbb{F}_p$ where p is prime

Field Visualization



Explanation:

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
- Fields extend the concept of numbers with more operations and properties.

Types of Fields

Finite Fields:

- $\mathbb{F}_p$ — Field with p elements, where p is prime.
- $\mathbb{F}_{p^n}$ — Field with p^n elements.

Familiar Fields:

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ — Rational, Real, and Complex numbers.
- $\mathbb{Z}/p\mathbb{Z}$ — Field of integers modulo a prime.

Extension Fields:

- $\mathbb{Q}(\sqrt{2})$ — Field formed by adjoining $\sqrt{2}$ to $\mathbb{Q}$.
- Galois Fields and Algebraic Closures.

Key Theorems in Field Theory

1. Fundamental Theorem of Algebra: Every non-constant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$.

2. Field Extension Theorem: If $F \subseteq K$ is a field extension, then:

$$[K : F] = \text{degree of the extension}$$

3. Finite Field Existence Theorem: For any prime power p^n, there exists a finite field with p^n elements.

Exercise Problems

Group Theory:

- Prove that the group of integers under addition is cyclic.
- Find the inverse of 7 modulo 13.

Ring Theory:

- Prove that $\mathbb{Z}[x]$ is not a field.
- Show that $\mathbb{Z}_6$ is not an integral domain.

Field Theory:

- Determine the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
- Construct a finite field with 4 elements.

Other Algebraic Structures

Monoids and Semigroups:

- **Monoid:** A set with an associative binary operation and identity.
- **Semigroup:** A set with an associative binary operation, but not necessarily an identity.

Modules and Vector Spaces:

- **Module:** Generalization of vector spaces where scalars are elements of a ring.
- **Vector Space:** Set of vectors with operations of addition and scalar multiplication over a field.

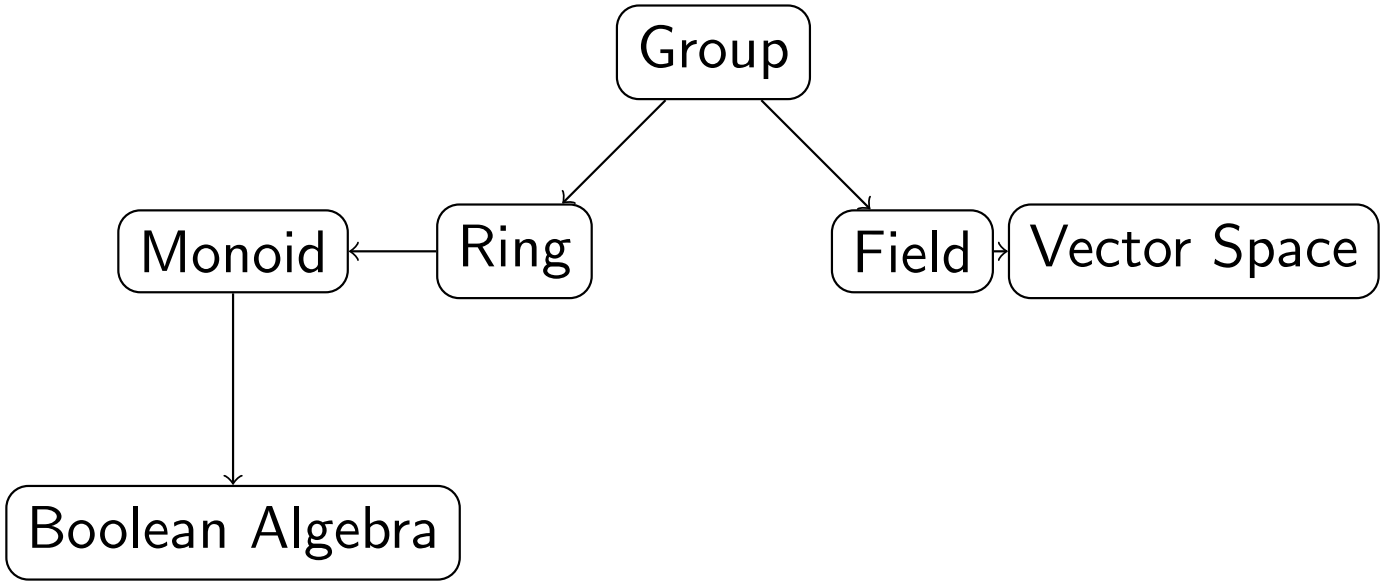
Lattices and Boolean Algebras:

- **Lattice:** Partially ordered set where any two elements have a least upper bound and greatest lower bound.
- **Boolean Algebra:** Algebraic structure used in logic and set theory.

Quasigroups and Loops:

- **Quasigroup:** A set with a binary operation where division is always possible.
- **Loop:** A quasigroup with an identity element.

Visual Representation of Structures



Explanation: - This diagram visualizes the relationship between different algebraic structures. - Rings generalize groups, while fields are special types of rings. - Boolean algebra arises from monoids.

Outline

Introduction to Mathematical Series

Definition: A series is the sum of the terms of a sequence. It can be expressed as:

$$S_n = a_1 + a_2 + a_3 + \cdots + a_n = \sum_{k=1}^{n} a_k$$

Applications of Series:

- Approximations and numerical computations
- Mathematical modeling
- Solving differential and integral equations
- Physics, engineering, and computer science

Geometric Series

Formula:

$$S_n = \sum_{k=0}^{n-1} ar^k = a\frac{1-r^n}{1-r} \text{ if } r \neq 1$$

Applications:

- Computing interest rates in finance
- Digital signal processing
- Physics for analyzing wave propagation

Arithmetic Series

Formula:

$$S_n = \frac{n}{2}(a + l) \text{ where } l \text{ is the last term}$$

Or equivalently,

$$S_n = \frac{n}{2}(2a + (n-1)d) \text{ where } d \text{ is the common difference}$$

Applications:

- Data analysis
- Construction problems
- Distribution modeling

Harmonic Series

Formula:

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

Applications:

- Number theory and prime number analysis
- Analysis of algorithms (e.g., complexity analysis)
- Physics and fluid dynamics

Binomial Series

Expansion Formula:

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

Applications:

- Probability theory
- Statistical modeling
- Algebra and combinatorics

Taylor Series

Expansion Formula:

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots$$

Applications:

- Approximating complex functions
- Physics and engineering
- Numerical analysis

Maclaurin Series (Special Case of Taylor Series)

Expansion Formula:

$$f(x) = f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \cdots$$

Applications:

- Calculating trigonometric and exponential functions
- Estimating irrational numbers
- Error analysis

Exponential Series

Formula:

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

Applications:

- Population modeling
- Physics (radioactive decay, Newton's law of cooling)
- Financial mathematics (compound interest)

Fourier Series

Expansion Formula:

$$f(x) \sim \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos(nx) + b_n \sin(nx))$$

Applications:

- Signal and image processing
- Sound wave analysis
- Solving partial differential equations

Power Series

General Form:

$$\sum_{n=0}^{\infty} a_n(x-c)^n$$

Applications:

- Approximating functions
- Solving differential equations
- Complex analysis

Riemann Zeta Series

Definition: The Riemann Zeta function is defined as:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \text{ where } s > 1$$

Applications:

- Number theory and prime number distribution
- Analytical continuation and complex analysis
- Quantum physics and statistical mechanics

Catalan Series

Definition: The Catalan numbers are given by the series:

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

Applications:

- Combinatorics and lattice path problems
- Binary tree counting
- Geometric triangulations

Alternating Series

Definition: A series whose terms alternate in sign is called an alternating series.

$$S_n = a_1 - a_2 + a_3 - a_4 + \cdots$$

Applications:

- Numerical analysis and error estimation
- Calculating logarithmic and trigonometric values
- Physical oscillations and wave theory

Fibonacci Series

Definition: The Fibonacci sequence is defined as:

$$F_n = F_{n-1} + F_{n-2}, \text{ with } F_0 = 0, F_1 = 1$$

Applications:

- Population growth modeling
- Computer algorithms (e.g., Fibonacci search)
- Nature (spiral patterns in shells, flowers)

Dirichlet Series

Definition: A Dirichlet series takes the form:

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Applications:

- Number theory (L-functions and prime analysis)
- Analytic continuation
- Solving functional equations

Lambert Series

Definition: The Lambert series is represented as:

$$S(x) = \sum_{n=1}^{\infty} \frac{a_n x^n}{1 - x^n}$$

Applications:

- Number theory and partition problems
- Cryptography and combinatorics
- Analysis of recurrence relations

Hypergeometric Series

Definition: The general form of a hypergeometric series is:

$$ {}_2F_1(a, b; c; z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!} $$

Applications:

- Quantum mechanics
- Calculus and mathematical physics
- Complex function analysis

Outline

Proof Challenges

1. **Complete the Proof:** Prove that the sum of two odd numbers is even. Start with:

$$\text{Let } a = 2k + 1 \text{ and } b = 2m + 1 \ldots.$$

2. **Find the Error:**

"All numbers are equal because $a = b \implies a^2 = ab$*."*

Identify and explain the logical error.

3. **Group Discussions:** Prove that among any 101 numbers one can find two numbers whose difference is divisible by 100.

4. **Correct the following:** (Proof done using incorrect reasoning)

$$1 = 1 \implies \sqrt{1} = \sqrt{1} \implies -1 = 1.$$

5. **Prove or disprove:** For all integers n, $n^3 - n$ is divisible by 6.

More Proof Challenges I

- **Challenge 1: Complete the Proof**
  - **Problem:** Prove that the sum of the first n odd numbers is n^2.
  - **Partially Given Proof:**
    - ⋆ Base Case: For $n = 1$, $1 = 1^2$. True.
    - ⋆ Inductive Hypothesis: Assume the sum of the first k odd numbers is k^2.
    - ⋆ Inductive Step: Show the statement holds for $n = k + 1$.
    - ⋆ To Do: Complete the proof and simplify expressions.
- **Challenge 2: Find the Error**
  - **Problem:** "Prove: All integers are equal."
  - **Flawed Proof:**

    Let $a = b$. Then $a^2 = ab$. Subtract b^2: $a^2 - b^2 = ab - b^2$. Factori
    $(a-b)(a+b) = b(a-b)$. Cancel $a-b$ to get $a+b = b$. Thus, $a =$
  - **Task:** Identify and explain the logical error in the proof.

More Proof Challenges II

- **Challenge 3: Prove or Disprove**
  - Statement: "For all integers $n \geq 2$, $n! > 2^n$."
  - **Task:**
    - ★ Verify for small values of n.
    - ★ Provide a rigorous proof or a counterexample.
- **Challenge 4: Group Discussion**
  - **Problem:** Use the Pigeonhole Principle to prove:
    Among every 1000 people there are two which selebrate their birthd
    on the same day. Can one find a day when 3 people selebrate th
    birthdays? How about 4 people?
  - **Task:** Discuss and collaboratively explain the reasoning.

Bonus Challenge:

- Prove that in any connected graph, there is always a path that visits every edge exactly once if and only if all vertices have even degrees (Eulerian Path Theorem).

Even More Proof Challenges I

- **Challenge 5: Fill in the Gaps**
  - **Problem:** Prove that for any positive integer n, $n^3 - n$ is divisible by 6.
  - **Partially Given Proof:**
    - ★ Rewrite: $n^3 - n = n(n-1)(n+1)$.
    - ★ Note: $n(n-1)(n+1)$ represents the product of three consecutive integers.
    - ★ To Do: Explain why one of these is divisible by 2 and another by 3, ensuring divisibility by 6.
- **Challenge 6: Prove a Generalization**
  - **Problem:** Prove that any tree with n vertices has exactly $n-1$ edges.
  - **Hint:**
    - ★ Use induction on n, the number of vertices.
    - ★ Base Case: A single vertex tree ($n = 1$) has no edges ($n - 1 = 0$).
    - ★ Inductive Step: Show that adding a vertex and an edge preserves the property.

Even More Proof Challenges II

- **Challenge 7: Construct and Verify**
  - **Problem:** Construct a graph with the degree sequence $(3, 3, 3, 3, 2, 2)$ and verify its properties.
  - **Task:**
    - ⋆ Draw the graph.
    - ⋆ Verify the sum of degrees equals $2|E|$.
    - ⋆ Check if the graph is connected.
- **Challenge 8: Apply Strong Induction**
  - **Problem:** Prove that any amount of postage $n \geq 12$ can be obtained using only 4-cent and 5-cent stamps.
  - **Hint:**
    - ⋆ Base Cases: Verify for $n = 12, 13, 14$.
    - ⋆ Inductive Step: Assume the statement holds for all values up to k, and prove it for $k + 1$ by adding a 4-cent or 5-cent stamp.

Even More Proof Challenges III

- **Challenge 9: Explore Counterexamples**
  - **Problem:** Disprove the statement: "All connected graphs are Eulerian."
  - **Task:**
    - ⋆ Provide a connected graph with a vertex of odd degree and explain why it fails to be Eulerian.

Bonus Challenge:

- Prove or disprove: The sum of degrees of all vertices in a graph is always even.
- There are 1091 small bugs on a table of size 2 ft by 3 ft. Prove that at any time you can catch at least 6 of them by covering them with a cylindrical drinking glass of diameter 3 in.

Advanced Proof Challenges I

- **Challenge 10: Advanced Induction**
  - **Problem:** Prove that the Fibonacci sequence satisfies:

$$F_1 + F_2 + \ldots + F_n = F_{n+2} - 1$$

    for all $n \geq 1$.
  - **Hint:**
    - ⋆ Base Case: Verify for $n = 1$.
    - ⋆ Inductive Hypothesis: Assume the statement holds for $n = k$.
    - ⋆ Inductive Step: Show it holds for $n = k + 1$ using the Fibonacci recurrence relation.
- **Challenge 11: Graph Decomposition**
  - **Problem:** Prove that any tree with n vertices can be decomposed into $n - 1$ paths of length 1.
  - **Hint:**
    - ⋆ Use induction on the number of vertices in the tree.
    - ⋆ Base Case: For $n = 2$, a single edge is a path of length 1.
    - ⋆ Inductive Step: Remove a leaf and decompose the remaining tree.

Advanced Proof Challenges II

- **Challenge 12: Prove a General Property**
  - **Problem:** Prove that in any bipartite graph, the sum of degrees of vertices in one part is equal to the sum of degrees in the other part.
  - **Hint:**
    - ⋆ Use the definition of bipartite graphs and the concept of edge incidence.
    - ⋆ Relate the degrees to the total number of edges.
- **Challenge 13: Constructive Proof**
  - **Problem:** Prove that there exists a connected graph with 5 vertices and exactly 6 edges.
  - **Task:**
    - ⋆ Construct such a graph and verify its connectivity and edge count.

Advanced Proof Challenges III

- **Challenge 14: Logical Deduction**
  - **Problem:** Prove or disprove: If all vertices in a connected graph have even degrees, the graph is Eulerian.
  - **Hint:**
    - ★ Analyze the definition of Eulerian graphs.
    - ★ Consider the role of connected components and vertex degrees.

Bonus Challenge:

- Use the Pigeonhole Principle to prove that in any set of n integers, there exists a subset whose sum is divisible by n.
- There are 6 people at a party. Use the Pigeonhole Principle to prove that either 3 of them knew each other before the party or 3 of them were complete strangers before the party.
- A student solves math problems every day. It is known that he never solves more than 12 problems per week. Prove that there are several consecutive days in one year when he solved exactly 20 problems.

Outline

Comprehensive Summary of Proof Techniques I

- **Purpose of Proofs:**
  - Establish the truth or falsity of mathematical statements rigorously.
  - Build on axioms, definitions, and previously proven results.
- **Proof Techniques Covered:**
  1. **Direct Proof:** Deduce the conclusion logically from the premises.
  2. **Proof by Contradiction:** Assume the negation of the statement and derive a contradiction.
  3. **Proof by Contrapositive:** Prove $\neg Q \implies \neg P$ for a statement $P \implies Q$.
  4. **Mathematical Induction:** Prove statements for natural numbers using:
     - ⋆ Base Case
     - ⋆ Inductive Step
     - ⋆ Strong Induction: Assume the statement for all smaller cases to prove the next.

Comprehensive Summary of Proof Techniques II

5. **Proof by Exhaustion:** Verify all possible cases explicitly.
6. **Proof by Counterexample:** Disprove a universal statement with a single counterexample.
7. **Graphical Proofs:** Use diagrams (e.g., Venn diagrams, graphs) to visualize and verify statements.

- **Common Challenges and Logical Fallacies:**
  - Circular reasoning assumes the conclusion within the proof, while hasty generalization draws conclusions from insufficient evidence.
  - Overgeneralization extends conclusions beyond their valid scope, and false analogy compares unrelated scenarios.
  - Ambiguous definitions use vague terms, and ignoring contradictions means proceeding despite evident inconsistencies.
  - Proof by intimidation relies on asserting correctness without solid reasoning, and misleading visualizations involve inaccurate diagrams or graphs.
  - Lastly, not checking all previous cases in an inductive proof can lead to errors.

Comprehensive Summary of Proof Techniques III

- **Applications in Graph Theory and Beyond:**
  - Handshaking Theorem and Euler's Formula (proved via induction).
  - Use of proofs in real-world contexts such as algorithm correctness and cryptography.
  - Inductive reasoning for graph properties (e.g., planar graphs, connected graphs).
- **Interactive Learning:**
  - Solve incomplete proofs and find errors in flawed reasoning.
  - Engage in group activities to tackle challenging problems.

Key Takeaway:

- Proofs form the backbone of mathematical reasoning and problem-solving.
- Common logical fallacies can undermine proofs.
- Mastery requires a deep understanding of techniques, practice, and attention to logical precision.

Outline

Extensive Examples: Maximal/Minimum vs. Maximum/Minimum I

Example 1: Divisibility Poset

Consider the set $S = \{1, 2, 3, 4, 6, 12\}$ ordered by divisibility $(a \mid b)$.

- **Minimum:** 1 is the minimum element because $1 \mid x$ for all $x \in S$.
- **Maximum:** 12 is the maximum element because every $x \in S$ divides 12.
- **Maximal Elements:** In this poset, the maximum is unique so the only maximal element is 12.
- **Minimal Elements:** The minimum is unique (1) in this complete divisibility poset.

Extensive Examples: Maximal/Minimum vs. Maximum/Minimum II

Example 2: Poset of Subsets

Consider the power set $\mathcal{P}(\{a, b, c\})$ ordered by set inclusion $\subseteq$.

- The **maximum** element is $\{a, b, c\}$, and the **minimum** is $\emptyset$.
- If we restrict to the collection $\mathcal{F} = \{\{a\}, \{b\}, \{a, b\}\}$:
  - The only **maximum** element is $\{a, b\}$.
  - The sets $\{a\}$ and $\{b\}$ are both **minimal** (no other set in $\mathcal{F}$ is a proper subset of them).
  - Both $\{a\}$ and $\{b\}$ are also **maximal** in $\mathcal{F}$ if no other set contains them except $\{a, b\}$, but since $\{a, b\}$ is present, they are not maximal in the entire $\mathcal{F}$—this demonstrates that in a partially ordered set, maximal elements may not be unique or globally optimal.

Extensive Examples: Maximal/Minimum vs. Maximum/Minimum III

Example 3: Poset with Incomparable Elements

Consider a set $P = \{x, y, z\}$ with the partial order defined by:

$$x \preceq y, \quad x \preceq z,$$

but y and z are incomparable.

- There is no unique maximum; both y and z are **maximal** since neither is less than the other.
- If no element is comparable to both y and z, then the poset does not have a maximum.
- The **minimum** is x, as it is less than both y and z, and is unique.

Extensive Examples: Maximal/Minimum vs. Maximum/Minimum IV

Key Observations:

- Every **maximum** (or minimum) is also **maximal** (or minimal), but not every **maximal** (or minimal) element is the absolute maximum (or minimum) in the set.
- In total orders (like the natural numbers with $\leq$), maximal equals maximum; in partial orders, there may be multiple maximal elements with no single maximum.

Exercise:

- In the poset $(\mathcal{P}(\{1, 2, 3, 4\}), \subseteq)$, identify all maximal and minimal elements.
- Given the set $S = \{2, 3, 5, 6, 10, 15, 30\}$ with the divisibility relation, determine the minimal, maximal, minimum, and maximum elements.

Examples of Proof Using WLOG I

AM-GM Inequality Proof

Problem: Prove that for any two positive real numbers a and b, we have

$$\frac{a+b}{2} \geq \sqrt{ab}$$

Proof using WLOG:

- **WLOG, assume** $a \leq b$.
- Consider the difference:

$$\frac{a+b}{2} - \sqrt{ab} = \frac{(a-b)^2}{2(\sqrt{a}+\sqrt{b})} \geq 0.$$

- Since the assumption $a \leq b$ does not change the validity of the proof, the result holds for all $a, b > 0$.

Examples of Proof Using WLOG II

Triangle Inequality
Problem: Prove that in any triangle with sides a, b, c, the triangle inequality holds:

$$a + b > c, \quad b + c > a, \quad a + c > b.$$

Proof using WLOG:

- **WLOG, assume** $a \leq b \leq c$.
- The inequality to prove reduces to showing $a + b > c$.
- Since the sides are positive and form a triangle, the sum of any two sides must be greater than the third.
- The assumptions do not change the problem's generality.

Examples of Proof Using WLOG III

Example 3: Vertex Degrees in a Graph

Problem: Prove that in any simple graph with at least two vertices, there exist two vertices with the same degree.

Proof using WLOG:

- A simple graph with n vertices has vertex degrees in $\{0, 1, \ldots, n-1\}$.
- If no two vertices have the same degree, one vertex must have degree $n-1$ (connected to all other $n-1$ vertices).
- However, no vertex can have degree 0 in this case.
- **WLOG, assume a vertex has degree $n-1$ and show a contradiction.**

Conclusion: By the Pigeonhole Principle, two vertices must share a degree.

Direct Proof - Example

- **Statement:** The sum of two even integers is even.
- **Proof:**
  - Let a and b be two even integers. By definition of even, $a = 2k$ and $b = 2m$, where k and m are integers.
  - Their sum is:
$$a + b = 2k + 2m = 2(k + m).$$
  - Since $k + m$ is an integer, $a + b$ is divisible by 2, and therefore even.
- **Conclusion:** The sum of two even integers is even.

Exercise:

- Prove: The sum of two odd integers is even.

Direct Proof - Example

- **Statement:** The square of an odd integer is odd.
- **Proof:**
  - Let n be an odd integer. By definition, $n = 2k + 1$ for some integer k.
  - The square of n is:

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

  - The result is of the form $2m + 1$, where $m = 2k^2 + 2k$, which is an integer.
  - Thus, n^2 is odd.
- **Conclusion:** The square of an odd integer is odd.

Exercise:

- Prove: The square of an even integer is even.

Direct Proof - Advanced Example

- **Statement:** The product of two rational numbers is rational.
- **Proof:**
  - Let $a = \frac{p}{q}$ and $b = \frac{r}{s}$ be two rational numbers, where p, q, r, s are integers and $q, s \neq 0$.
  - The product of a and b is:

$$a \cdot b = \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}.$$

  - Since pr and qs are integers and $qs \neq 0$, $\frac{pr}{qs}$ is rational.
- **Conclusion:** The product of two rational numbers is rational.

Exercise:

- Prove: The sum of two rational numbers is rational.

Direct Proof - Advanced Example

- **Statement:** For any integers a and b, if a and b are divisible by d, then $a + b$ is divisible by d.
- **Proof:**
  - Assume a and b are divisible by d. Then, $a = dk$ and $b = dm$ for some integers k and m.
  - Their sum is:
$$a + b = dk + dm = d(k + m).$$
  - Since $k + m$ is an integer, $a + b$ is divisible by d.
- **Conclusion:** $a + b$ is divisible by d.

Exercise:

- Prove: If a and b are divisible by d, then $a - b$ is divisible by d.

Direct Proof - Advanced Example

- **Statement:** For any integer n, if n is divisible by 4, then n^2 is divisible by 16.
- **Proof:**
  - Assume n is divisible by 4. Then, $n = 4k$ for some integer k.
  - The square of n is:
$$n^2 = (4k)^2 = 16k^2.$$
  - Since $16k^2$ is divisible by 16, n^2 is divisible by 16.
- **Conclusion:** If n is divisible by 4, then n^2 is divisible by 16.

Exercise:

- Prove: For any integer n, if n is divisible by 3, then n^2 is divisible by 9.

Direct Proof - Advanced Example

- **Statement:** The sum of the degrees of all vertices in any graph is equal to twice the number of edges, i.e., $\sum_{v \in V} \deg(v) = 2|E|$
- **Proof:**
  - Let $G = (V, E)$ be a graph, where V is the set of vertices and E is the set of edges.
  - Each edge $e \in E$ connects two vertices, contributing exactly 1 to the degree of each vertex it connects.
  - Thus, each edge contributes exactly 2 to the total sum of the degrees of the vertices.
  - Therefore, summing over all edges: $\sum_{v \in V} \deg(v) = 2 \cdot |E|$.
- **Conclusion:** The sum of the degrees of all vertices is twice the number of edges, which holds for all graphs.

Exercise:

- Verify this theorem for:
  1. A triangle graph (K_3).
  2. A path graph with 4 vertices (P_4).

Proof by Contradiction - Advanced Example

- **Statement:** There is no largest prime number.
- **Proof:**
  - Assume the contrary: There exists a largest prime number, say p.
  - Consider the number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$, where $p_1, p_2, \ldots, p_k$ are all the prime numbers up to p.
  - N is greater than p and not divisible by any of $p_1, p_2, \ldots, p_k$ (remainder is 1 for all divisions).
  - Therefore, N is either prime or divisible by a prime greater than p, contradicting the assumption.
- **Conclusion:** There is no largest prime number.

Exercise:

- Use a similar argument to prove: There are infinitely many composite numbers.

Proof by Contrapositive - Advanced Example

- **Statement:** If $x^2 \leq y^2$, then $|x| \leq |y|$.
- **Proof by Contrapositive:**
  - Contrapositive: If $|x| > |y|$, then $x^2 > y^2$.
  - Assume $|x| > |y|$. By definition of absolute value:

$$|x| > |y| \implies x^2 = (|x|)^2 > (|y|)^2 = y^2.$$

  - Therefore, $x^2 > y^2$, which completes the proof of the contrapositive.
- **Conclusion:** If $x^2 \leq y^2$, then $|x| \leq |y|$.

Exercise:

- Prove: If $a \cdot b$ is negative, then a and b have opposite signs, using contrapositive reasoning.

Mathematical Induction - Advanced Example

- **Statement:** Prove that $n! > 2^n$ for all $n \geq 4$.
- **Proof:**
  - **Base Case:** For $n = 4$:
    $4! = 24 \quad \text{and} \quad 2^4 = 16 \quad \Longrightarrow \quad 24 > 16.$ True.
  - **Inductive Hypothesis:** Assume the statement holds for $n = k$:

$$k! > 2^k.$$

  - **Inductive Step:** Prove for $n = k + 1$:

$$(k+1)! = (k+1) \cdot k! > (k+1) \cdot 2^k.$$

    Since $k + 1 \geq 5$ for $k \geq 4$, and $2^k \geq 2$, we have:

$$(k+1) \cdot 2^k > 2^{k+1}.$$

    Thus, $(k+1)! > 2^{k+1}$.
- **Conclusion:** $n! > 2^n$ for all $n \geq 4$.

Proof by Exhaustion - Advanced Example

- **Statement:** Prove that a triangle with integer side lengths and a perimeter of 12 must have sides $(3, 4, 5)$.
- **Proof:**
  - Let the side lengths be a, b, c with $a + b + c = 12$ and $a \leq b \leq c$.
  - Exhaust all possibilities for a:
    - ★ If $a = 3$, then $b + c = 9$: Possible values: $(3, 4, 5)$ (valid as it satisfies the triangle inequality).
    - ★ If $a = 4$, then $b + c = 8$: No valid combinations satisfy the triangle inequality.
    - ★ If $a \geq 5$, no valid combinations exist.
- **Conclusion:** The only valid triangle is $(3, 4, 5)$.

Exercise:

- Prove by exhaustion: The only Pythagorean triple with a perimeter of 30 is $(5, 12, 13)$.

Proof by Exhaustion - Advanced Example

- **Statement:** Prove that a quadratic equation $ax^2 + bx + c = 0$ has real roots if $b^2 - 4ac \geq 0$.
- **Proof by Exhaustion:**
  - Consider all cases for $b^2 - 4ac$:
    1. **Case 1:** $b^2 - 4ac = 0$.

       $$x = \frac{-b}{2a}.$$

       This root is real.
    2. **Case 2:** $b^2 - 4ac > 0$.

       $$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

       The roots involve a real square root, so both roots are real.
  - In both cases, the roots are real when $b^2 - 4ac \geq 0$.
- **Conclusion:** A quadratic equation has real roots if $b^2 - 4ac \geq 0$.

Exercise:

- Prove: A quadratic equation has complex roots if $b^2 - 4ac < 0$.

Proof by Contradiction - Bipartite Graphs

- **Statement:** A graph is bipartite if and only if it contains no odd-length cycles.
- **Proof:**
  - **Direction 1:** Assume the graph is bipartite. Then every cycle in the graph alternates between two sets of vertices, making the cycle length even. True by construction.
  - **Direction 2:** Prove by contradiction: Assume the graph contains an odd-length cycle and is still bipartite.
  - Let the cycle be $C = (v_1, v_2, \ldots, v_k)$, where k is odd.
  - In a bipartite graph, vertices in the same set cannot be adjacent.
  - To traverse C, vertices would alternate between the two sets. After k steps (odd), v_1 and v_k would end in the same set.
  - This contradicts the definition of a bipartite graph.
- **Conclusion:** A graph is bipartite if and only if it contains no odd-length cycles.

Exercise:

- Prove: A tree is bipartite.

Direct Proof - Degree of Trees

- **Statement:** A tree with n vertices has exactly $n - 1$ edges.
- **Proof:**
  - A tree is a connected, acyclic graph.
  - Start with a single vertex ($n = 1$). No edges are needed ($n - 1 = 0$).
  - Adding a new vertex to the tree requires exactly one edge to maintain connectivity and avoid cycles.
  - Repeat this process for n vertices:

$$\text{Edges required} = n - 1.$$

  - Since any tree is built this way, it must have $n - 1$ edges.
- **Conclusion:** A tree with n vertices always has $n - 1$ edges.

Exercise:

- Prove: A tree has at least two vertices with degree 1.

Proof by Exhaustion - Planar Graphs

- **Statement:** Prove that K_5 (complete graph on 5 vertices) is not planar.
- **Proof:**
  - By Euler's formula for planar graphs: $V - E + F = 2$.
  - For K_5, $V = 5$ and $E = 10$.
  - Substitute into Euler's formula: $5 - 10 + F = 2 \implies F = 7$.
  - In a planar graph, each face must be bounded by at least 3 edges: $3F \leq 2E$.
  - Substitute $F = 7$ and $E = 10$: $3(7) \leq 2(10) \implies 21 \leq 20$.
  - This is a contradiction, so K_5 is not planar.
- **Conclusion:** K_5 is not planar.

Exercise:

- Prove that $K_{3,3}$ (complete bipartite graph) is not planar.

Direct Proof - Handshaking Lemma

- **Statement:** For any integers a and b, if a is odd and b is odd, then $a \cdot b$ is odd.
- **Proof:**
  - By definition of odd integers, $a = 2k + 1$ and $b = 2m + 1$ for some integers k and m.
  - The product $a \cdot b$ is: $a \cdot b = (2k + 1)(2m + 1)$.
  - Expanding the terms: $a \cdot b = 4km + 2k + 2m + 1$.
  - Factoring out 2: $a \cdot b = 2(2km + k + m) + 1$.
  - Since $2km + k + m$ is an integer, $a \cdot b$ is of the form $2n + 1$, where $n = 2km + k + m$.
  - By definition, $a \cdot b$ is odd.
- **Conclusion:** The product of two odd integers is odd.

Exercise:

- Prove: The product of an even integer and an odd integer is even.

Proof by Induction - Handshaking Lemma

- **Statement:** In any undirected graph, the sum of the degrees of all vertices is twice the number of edges: $\sum_{v \in V} \deg(v) = 2|E|$.
- **Proof by Induction:**
  - **Base Case:** For a graph with one edge connecting two vertices: $\deg(v_1) + \deg(v_2) = 1 + 1 = 2 = 2 \cdot 1$. True.
  - **Inductive Hypothesis:** Assume the lemma holds for any graph with k edges: $\sum_{v \in V} \deg(v) = 2k$.
  - **Inductive Step:** Consider a graph with $k + 1$ edges. Add an edge (u, v) to the graph:
    - ⋆ The degrees of u and v each increase by 1.
    - ⋆ The new sum of degrees is: $2k + 2 = 2(k + 1)$.
- **Conclusion:** The lemma holds for all graphs.

Exercise:

- Verify the lemma for a triangle graph (K_3).