Mathematical Reasoning

Logic, Proof, and Set Theory

Table of contents

Introduction

This document builds foundations in logic, proof techniques, and set theory. These topics form the language and reasoning tools for all advanced mathematics.

We start with propositional logic and quantifiers, move through various proof techniques, then develop set theory from basic operations through cardinality and infinite sets. Each concept progresses from intuition through formal definitions to computational methods and examples.

---

1 Logic and Propositions

1.1 Historical Background

In the late 19th century, mathematicians discovered contradictions in seemingly sound reasoning. Russell's paradox (1901) showed that intuitive set theory led to logical impossibilities. This crisis demanded a formal foundation for mathematical logic.

George Boole (1847) first treated logic as algebra. Gottlob Frege (1879) developed predicate logic with quantifiers. By the early 20th century, logic became a rigorous mathematical discipline, establishing clear rules for what constitutes valid reasoning.

1.2 Understanding Propositions

A proposition is a statement that's either true or false—never both, never neither. Think of it as a light switch: on (TRUE) or off (FALSE).

Propositions: - "$2 + 2 = 4$" (TRUE) - "The Earth is flat" (FALSE)
- "P = NP" (unknown, but still a proposition)

Not propositions: - "Close the door" (command) - "Is it raining?" (question) - "$x > 0$" (depends on x—this is a predicate)

Natural language is often ambiguous: "I saw the man with the telescope" could mean two different things. Mathematical language must be precise.

1.3 Formal Definitions

Definition: Proposition

A **proposition** is a declarative statement with exactly one truth value: TRUE (T) or FALSE (F).

1.3.1 Logical Connectives

Negation ($\neg P$):

P	$\neg P$
T	F
F	T

Conjunction ($P \wedge Q$):

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

True only when both are true.

Disjunction ($P \vee Q$):

P	Q	$P \lor Q$
T	T	T
T	F	T
F	T	T
F	F	F

True when at least one is true (inclusive or).

Implication ($P \to Q$):

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

The only false case: P true but Q false.

When P is false, the implication is **vacuously true** regardless of Q. Think of it like a promise: “If you score 100% on the exam, you’ll get an A.” If you score 85%, was the promise broken? No—the condition wasn’t met.

⚠ Warning

A common error: from $P \to Q$ and observing Q is true, concluding P must be true. This is **affirming the consequent** and is invalid.
Example: “If it rains, the ground is wet.” Seeing wet ground doesn’t prove it rained—could be sprinklers.

Biconditional ($P \leftrightarrow Q$):

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

True when P and Q have the same truth value. Equivalent to $(P \to Q) \land (Q \to P)$.

1.3.2 Related Statements

Given $P \to Q$:

Statement	Form	Relationship to Original
Original	$P \to Q$	—
Contrapositive	$\neg Q \to \neg P$	Logically equivalent
Converse	$Q \to P$	NOT equivalent
Inverse	$\neg P \to \neg Q$	NOT equivalent

The contrapositive is equivalent to the original—sometimes proving $\neg Q \to \neg P$ is easier than proving $P \to Q$ directly.

1.3.3 Necessary and Sufficient Conditions

When $P \to Q$ is true: - P is **sufficient** for Q (having P guarantees Q) - Q is **necessary** for P (can't have P without Q)

For a matrix to be invertible, $\det(A) \neq 0$ is both necessary and sufficient. Being square is necessary but not sufficient.

1.4 Key Properties

De Morgan's Laws:

$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$

$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$

Implication equivalences:

$$P \to Q \equiv \neg Q \to \neg P \quad \text{(contrapositive)}$$

$$P \to Q \equiv \neg P \vee Q$$

Negating implication:

$$\neg(P \to Q) \equiv P \wedge \neg Q$$

1.5 Quantifiers

Mathematical statements often involve variables. Quantifiers specify how variables range.

Universal quantifier ($\forall$): "for all"

$$\forall x \in S, P(x)$$

means $P(x)$ is true for every element x in set S.

Examples: - $\forall n \in \mathbb{Z}, (n + 0 = n)$ — TRUE - $\forall n \in \mathbb{Z}, (n^2 > 0)$ — FALSE (fails at $n = 0$)

Existential quantifier ($\exists$): "there exists"

$$\exists x \in S, P(x)$$

means $P(x)$ is true for at least one element x in S.

Examples: - $\exists n \in \mathbb{Z}, (n^2 = 4)$ — TRUE ($n = 2$ or $n = -2$) - $\exists x \in \mathbb{R}, (x^2 = -1)$ — FALSE (no real solution)

1.5.1 Negating Quantifiers

$$\neg(\forall x, P(x)) \equiv \exists x, \neg P(x)$$

"Not all satisfy P" means "some doesn't satisfy P"

$$\neg(\exists x, P(x)) \equiv \forall x, \neg P(x)$$

"There doesn't exist" means "all don't satisfy P"

1.5.2 Order Matters

❗ Important

When quantifiers have different types ($\forall$ vs $\exists$), **order is crucial**.

Statement A: $\forall x \, \exists y \, (x < y)$

"For every x, there exists y bigger than x"

TRUE — given any x, choose $y = x + 1$

Statement B: $\exists y \, \forall x \, (x < y)$

"There exists y bigger than all x"

FALSE — no maximum real number exists

The difference: In A, y depends on x (different y for each x). In B, one fixed y must work for all x simultaneously.

The ε-δ definition of continuity uses this pattern:

$$\forall \varepsilon > 0, \exists \delta > 0, \forall x, (|x - a| < \delta \to |f(x) - f(a)| < \varepsilon)$$

Someone gives you any $\varepsilon > 0$, then you find $\delta > 0$ (depending on that ε), such that the condition holds for all x.

1.5.3 Edge Cases

When working with statements about real numbers or integers, always check: - $x = 0$ (additive identity, no multiplicative inverse) - $x = 1$ (multiplicative identity) - $x = -1$ (sign changer) - Positive and negative cases separately - For squares: negative inputs fail since $x^2 \geq 0$ in $\mathbb{R}$

1.6 Examples

1.6.1 Example 1: Simple Truth Table

Verify $P \to Q \equiv \neg P \vee Q$:

P	Q	$\neg P$	$P \to Q$	$\neg P \vee Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Last two columns match—the statements are equivalent.

1.6.2 Example 2: Quantifier Order

Statement: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, (x + y = 0)$

"Every number has an additive inverse"

TRUE — given any x, choose $y = -x$

Compare: $\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, (x + y = 0)$

"There exists a universal additive inverse"

FALSE — no single y makes $x + y = 0$ for all x

1.6.3 Example 3: Vacuous Truth

Statement: $\forall x \in \emptyset, (x > 100)$

TRUE (vacuously)

The hypothesis "$x \in \emptyset$" is always false (empty set has no elements). By definition of implication, FALSE → Q is TRUE for any Q.

Like saying "all unicorns in this room are purple"—vacuously true.

1.6.4 Example 4: Non-Example

"$x > 0$" is **not a proposition** because truth value depends on x.

To make it a proposition: - Add quantifier: $\forall x \in \mathbb{R}^+, (x > 0)$ — TRUE - Specify value: "$5 > 0$" — TRUE (now it's a proposition)

1.7 Frequent Mistakes

Confusing "or" with "exclusive or":

Mathematical OR is inclusive—$P \vee Q$ is true when both are true. Natural language often implies "one or the other, not both."

Affirming the consequent:

From $P \to Q$ and Q, you cannot conclude P. Ground being wet doesn't prove it rained.

Mishandling vacuous truth:

"If $0 = 1$, then I am Napoleon" is TRUE (vacuously). The hypothesis is false, so the implication holds.

Quantifier scope errors:

"Every student has a favorite professor" is ambiguous. Does each student have their own favorite ($\forall s\, \exists p$), or is there one professor everyone favors ($\exists p\, \forall s$)?

Ignoring edge cases:

Always test $x = 0$, $x = 1$, $x = -1$, and boundary conditions when verifying statements about numbers.

1.8 Prerequisites and Connections

Requires: Basic understanding of true/false, elementary arithmetic

Enables: All of mathematics—proofs, set theory, analysis, probability

Related: Boolean algebra (algebraic structure of logic), circuit design (logic gates), programming (conditionals), database queries (logical operators)

---

2 Proof Techniques

2.1 Historical Background

Before the 19th century, mathematical proofs relied heavily on geometric intuition. But intuition sometimes fails—Zeno's paradoxes seemed to show motion was impossible, and non-Euclidean geometry proved the parallel postulate could be consistently negated.

The solution was rigorous proof from axioms, with no hand-waving. A proof became a finite sequence of statements, each either an axiom, a previously proven theorem, or following from previous statements by logical rules.

2.2 What Is a Proof?

Think of a proof as navigating a maze: you start with hypotheses (what you know) and need to reach the conclusion (what you want to show). The path is a sequence of logical steps.

Different proof techniques are different navigation strategies: - **Direct proof:** Walk straight from start to finish - **Contrapositive:** Walk backwards from NOT-finish to NOT-start - **Contradiction:** Assume you're already at finish, derive impossibility - **Cases:** Split maze into sections, solve each separately

2.3 Direct Proof

ℹ Definition: Direct Proof

To prove $P \to Q$:

1. Assume P (hypothesis)
2. Through logical steps, derive Q (conclusion)
3. Each step must be justified

Structure:

```
Proof:
Assume P.
[Statement 1] by [justification]
[Statement 2] follows from statement 1
...
Therefore Q.
```

2.3.1 Example 1: Simple Direct Proof

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

Proof:

Assume n is even.

By definition of even, $n = 2k$ for some integer k.

Therefore:

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

Since $2k^2$ is an integer, n^2 has the form $2m$ where $m = 2k^2$.

By definition, n^2 is even.

2.4 Proof by Contrapositive

> ℹ Definition: Proof by Contrapositive
>
> To prove $P \to Q$, instead prove the equivalent statement $\neg Q \to \neg P$.

Use this when negations are easier to work with than the originals.

2.4.1 Example 2: Contrapositive Proof

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

Direct proof from "n^2 even" isn't obvious. But the contrapositive is straightforward.

Proof:

We prove the contrapositive: If n is odd, then n^2 is odd.

Assume n is odd.

By definition, $n = 2k + 1$ for some integer k.

Therefore:

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

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

By definition, n^2 is odd.

2.5 Proof by Contradiction

ℹ Definition: Proof by Contradiction

To prove statement S:

1. Assume $\neg S$ (opposite of what you want)
2. Derive a logical contradiction $(R \wedge \neg R)$
3. Conclude S must be true

Use this for proving negatives, irrationality, infinitude, or non-existence.

2.5.1 Example 3: Classic Contradiction

Claim: $\sqrt{2}$ is irrational.

Proof:

Assume, for contradiction, that $\sqrt{2}$ is rational.

Then $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b \neq 0$, and $\gcd(a, b) = 1$ (lowest terms).

Squaring both sides:

$$2 = \frac{a^2}{b^2}$$

Multiply by b^2:

$$2b^2 = a^2$$

Therefore a^2 is even.

By our earlier result, if a^2 is even then a is even.

So $a = 2k$ for some integer k.

Substituting:

$$2b^2 = (2k)^2 = 4k^2$$

Divide by 2:

$$b^2 = 2k^2$$

Therefore b^2 is even, which means b is even.

But now both a and b are even, contradicting $\gcd(a, b) = 1$.

This contradiction shows our assumption was false.

Therefore $\sqrt{2}$ is irrational.

2.6 Proof by Cases

ℹ Definition: Proof by Cases

To prove statement S:

1. Partition all possibilities into exhaustive cases
2. Prove S holds in each case separately
3. Conclude S holds universally

Use when a natural partition exists (even/odd, positive/negative/zero).

2.6.1 Example 4: Case Analysis

Claim: For all integers n, $n(n + 1)$ is even.

Proof:

Let $n \in \mathbb{Z}$. Either n is even or n is odd.

Case 1: n is even.

Then $n = 2k$ for some integer k.

So $n(n + 1) = 2k(n + 1) = 2[k(n + 1)]$.

Since $k(n + 1)$ is an integer, $n(n + 1)$ is even.

Case 2: n is odd.

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

So $n + 1 = 2k + 2 = 2(k + 1)$.

Thus $n(n + 1) = (2k + 1) \cdot 2(k + 1) = 2[(2k + 1)(k + 1)]$.

Since $(2k + 1)(k + 1)$ is an integer, $n(n + 1)$ is even.

In both cases, $n(n + 1)$ is even.

2.7 Choosing a Technique

Try this order:

1. **Direct proof** — Can you see a clear path from hypothesis to conclusion?
2. **Contrapositive** — Are the negations simpler to work with?
3. **Contradiction** — Is the statement about non-existence or irrationality?
4. **Cases** — Does the problem naturally split into scenarios?

For proving $P \to Q$:

Contrapositive: Prove $\neg Q \to \neg P$ (still an implication)

Contradiction: Assume $P \land \neg Q$, derive impossibility (different structure)

2.8 Verifying Proofs

A good proof: - States the claim clearly - Defines all variables - Uses precise language - Justifies each step - Handles all cases - Reaches the stated conclusion - Ends with or QED

2.9 What to Watch For

Circular reasoning:

Using the conclusion in the assumption. “Assume $\sqrt{2}$ is irrational. Then it’s irrational. ” This proves nothing.

Proof by example:

“All primes are odd. Proof: 3, 5, 7 are prime and odd. ” Examples don’t prove universal statements. (Also, 2 is prime and even.)

Assuming what you want to prove:

When proving $A = B$, don’t start by assuming $A = B$. Start from definitions or axioms.

Incomplete case analysis:

Proving for positive and negative integers but forgetting zero.

Unjustified steps:

“$x^2 + 5x + 6 = 0$, therefore $x = -2$ or $x = -3$.” Missing steps: factor, apply zero product property.

2.10 Prerequisites and Connections

Requires: Logic (implications, quantifiers), basic algebra

Enables: All of mathematics—every mathematical result needs proof

Related: Axiom systems, formal verification, program correctness

3 Sets and Operations

3.1 Historical Background

Georg Cantor developed set theory in the 1870s-1890s to understand infinity. His work showed that some infinities are “larger” than others—there are more real numbers than natural numbers.

In 1901, Bertrand Russell discovered a paradox: consider “the set of all sets that don’t contain themselves.” Does this set contain itself? Either answer leads to contradiction. This crisis led to axiomatic set theory (Zermelo-Fraenkel with Choice).

3.2 Understanding Sets

A set is a collection of objects. Think of it as a container or bag. The objects inside are called elements or members.

Key properties: - **Unordered:** $\{1, 2, 3\} = \{3, 1, 2\}$ - **Distinct:** $\{1, 1, 2\} = \{1, 2\}$ (duplicates ignored) - **Well-defined:** For any object, we can determine if it’s in the set

Visual: A set is like a basket. An element is like an apple in the basket. The set $\{3\}$ is a basket containing one apple (the number 3). The number 3 itself is just an apple, not a basket.

3.3 Formal Definitions

ℹ Definition: Set

A **set** is an unordered collection of distinct objects called **elements** or **members**.

Notation: - $x \in S$ means “x is an element of S” - $x \notin S$ means “x is not an element of S”

⚠ Warning

Critical distinction: 3 is a number (element). $\{3\}$ is a set containing that number.

- $3 \in \{1, 2, 3\}$ (3 is listed)
- $\{3\} \in \{1, 2, 3\}$ ($\{3\}$ is not listed, only 3 is)
- $\{3\} \subseteq \{1, 2, 3\}$ (subset relationship)

3.3.1 Specifying Sets

Roster notation (list elements):

$$A = \{1, 2, 3, 4, 5\}$$

Set-builder notation:

$$A = \{x \in \mathbb{Z} \mid 1 \leq x \leq 5\}$$

Read as: “x in integers such that $1 \leq x \leq 5$”

General form: {expression | condition}

3.3.2 Special Sets

Empty set: $\emptyset$ or $\{\}$

> ❗ Important
>
> - $|\emptyset| = 0$
> - $\emptyset \subseteq S$ for any set S (vacuously true)
> - $\emptyset \in S$ only if explicitly listed as an element
> - $\emptyset \neq \{\emptyset\}$

Empty box versus box containing an empty box.

Standard number sets:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

$$\mathbb{Q} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$$

$$\mathbb{R} \text{ (real numbers)}$$

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

Hierarchy:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

3.4 Subsets

ℹ Definition: Subset

$A \subseteq B$ means every element of A is also in B.
Formally: $A \subseteq B \Leftrightarrow (\forall x \in A, x \in B)$

Proper subset: $A \subset B$ means $A \subseteq B$ and $A \neq B$

Properties: - **Reflexive:** $A \subseteq A$ - **Transitive:** If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$ - **Antisymmetric:** If $A \subseteq B$ and $B \subseteq A$, then $A = B$

The last property gives us the standard way to prove set equality:

💡 Tip

To prove $A = B$: 1. Show $A \subseteq B$ 2. Show $B \subseteq A$

3.5 Set Operations

3.5.1 Union: $A \cup B$

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

All elements in A or B (or both).

Example: $\{1, 2, 3\} \cup \{3, 4, 5\} = \{1, 2, 3, 4, 5\}$

3.5.2 Intersection: $A \cap B$

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

Elements in both A and B.

Example: $\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$

Disjoint sets: $A \cap B = \emptyset$

3.5.3 Difference: $A \setminus B$

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$$

Elements in A but not in B.

Example: $\{1, 2, 3, 4\} \setminus \{3, 4, 5\} = \{1, 2\}$

Note: $A \setminus B \neq B \setminus A$ in general (not commutative).

3.5.4 Complement: A^c

$$A^c = U \setminus A = \{x \in U \mid x \notin A\}$$

All elements in the universal set U that are not in A. Requires specifying U.

3.5.5 Symmetric Difference: $A \triangle B$

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

Elements in A or B but not both (exclusive or).

Example: $\{1, 2, 3\} \triangle \{2, 3, 4\} = \{1, 4\}$

3.6 Properties of Set Operations

De Morgan's Laws:

$$(A \cup B)^c = A^c \cap B^c$$

$$(A \cap B)^c = A^c \cup B^c$$

Commutative:

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

Associative:

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

Distributive:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

3.7 Cartesian Products

ℹ Definition: Cartesian Product

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

The set of all **ordered pairs** with first element from A, second from B.

Important: $(a, b) \neq (b, a)$ unless $a = b$ (order matters)

Cardinality: $|A \times B| = |A| \cdot |B|$

Example:

$$\{1, 2\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b)\}$$

Higher dimensions:

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

The plane. Similarly $\mathbb{R}^3$ is 3D space, $\mathbb{R}^n$ is n-dimensional space.

3.8 Power Sets

ℹ Definition: Power Set

$$\mathcal{P}(A) = \{S \mid S \subseteq A\}$$

The set of **all subsets** of A.

Elements of $\mathcal{P}(A)$ are sets themselves.

❗ Important

If $|A| = n$, then $|\mathcal{P}(A)| = 2^n$

Why 2^n? For each element: include it in the subset or don't (2 choices). With n elements: $2 \times 2 \times \cdots \times 2 = 2^n$ total subsets.

3.8.1 Example 1: $A = \{1, 2\}$

$$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

4 subsets total ($2^2 = 4$).

3.8.2 Example 2: $A = \{a, b, c\}$

$$\mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$

8 subsets total ($2^3 = 8$).

3.8.3 Example 3: $A = \emptyset$

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

Not empty! Contains one element (the empty set itself). $|\mathcal{P}(\emptyset)| = 2^0 = 1$.

Power set growth:

$\|A\|$	$\|\mathcal{P}(A)\|$
0	1
1	2
2	4
3	8
10	1,024
20	1,048,576

Exponential explosion makes searching all subsets intractable for large sets.

3.9 Examples

3.9.1 Example 1: Element vs. Subset

Given $S = \{1, 2, \{3\}, \emptyset\}$ (4 elements: numbers 1, 2, the set $\{3\}$, and empty set):

- $1 \in S$
- $\{1\} \in S$ (only 1 is listed, not $\{1\}$)
- $\{1\} \subseteq S$ (element 1 is in S)
- $3 \in S$ (3 is not listed, only $\{3\}$ is)
- $\{3\} \in S$ (explicitly listed)
- $\emptyset \in S$ (explicitly listed as element)
- $\emptyset \subseteq S$ (vacuously true for any set)

3.9.2 Example 2: Set Operations

Let $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$

- $A \cup B = \{1, 2, 3, 4, 5, 6\}$
- $A \cap B = \{3, 4\}$
- $A \setminus B = \{1, 2\}$
- $B \setminus A = \{5, 6\}$
- $A \triangle B = \{1, 2, 5, 6\}$

3.9.3 Example 3: Proving Set Equality

Claim: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof:

($\subseteq$) Let $x \in A \cap (B \cup C)$.

Then $x \in A$ and $x \in (B \cup C)$.

So $x \in A$ and ($x \in B$ or $x \in C$).

Case 1: $x \in B$. Then $x \in A$ and $x \in B$, so $x \in A \cap B$, thus $x \in (A \cap B) \cup (A \cap C)$.

Case 2: $x \in C$. Then $x \in A$ and $x \in C$, so $x \in A \cap C$, thus $x \in (A \cap B) \cup (A \cap C)$.

Therefore $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

($\supseteq$) Let $x \in (A \cap B) \cup (A \cap C)$.

Then $x \in A \cap B$ or $x \in A \cap C$.

Case 1: $x \in A \cap B$. Then $x \in A$ and $x \in B$, so $x \in B \cup C$, thus $x \in A \cap (B \cup C)$.

Case 2: $x \in A \cap C$. Then $x \in A$ and $x \in C$, so $x \in B \cup C$, thus $x \in A \cap (B \cup C)$.

Therefore $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Since both inclusions hold, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

3.9.4 Example 4: Non-Example

"The set of all sets" is **not a valid set** in standard set theory. It leads to Russell's paradox.

Let $R = \{S \mid S \notin S\}$ (set of all sets not containing themselves).

Is $R \in R$?

- If $R \in R$, then by definition $R \notin R$ (contradiction)
- If $R \notin R$, then by definition $R \in R$ (contradiction)

Resolution: can't form "set of all sets" (requires proper classes).

3.10 Typical Errors

Confusing element and set:

Wrong: $3 \subseteq \{1, 2, 3\}$

3 is a number, not a set. Can't use $\subseteq$ with elements.

Right: $3 \in \{1, 2, 3\}$ or $\{3\} \subseteq \{1, 2, 3\}$

Empty set confusion:

$\emptyset \neq \{\emptyset\}$

- $|\emptyset| = 0$ (no elements)
- $|\{\emptyset\}| = 1$ (one element: the empty set)

Set operation results:

Wrong: $\{1, 2\} \cap \{2, 3\} = 2$

Results of set operations are always sets.

Right: $\{1, 2\} \cap \{2, 3\} = \{2\}$

Forgetting empty set in power set:

$\mathcal{P}(\{a, b\})$ includes both $\emptyset$ and $\{a, b\}$ itself.

3.11 Building Blocks

Requires: Logic (quantifiers for defining operations), basic notation

Enables: Relations, functions, vector spaces, topology, measure theory, probability

Related: Category theory, type theory, logic

---

4 Relations and Functions

4.1 Relations

ℹ Definition: Relation

A **relation** R from A to B is a subset of $A \times B$.

$$R \subseteq A \times B$$

If $(a, b) \in R$, we write $a\,R\,b$. Meaning that the element a is related to the element b by the relation R.

Example: Less-than on integers

$$A = B = \{1, 2, 3, 4\}$$

$$R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$$

This represents: $1 < 2$, $1 < 3$, $1 < 4$, $2 < 3$, $2 < 4$, $3 < 4$

4.1.1 Properties of Binary Relations

For a relation $R \subseteq A \times A$:

Reflexive: $\forall a \in A, (a, a) \in R$

Every element related to itself.

Symmetric: $\forall a, b \in A$, if $(a, b) \in R$ then $(b, a) \in R$

If a relates to b, then b relates to a. In other words, if a is related to b, then b is related to a. Bidirectional relationship should exist in a symmetric relation.

Transitive: $\forall a, b, c \in A$, if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$

Chaining works.

Antisymmetric: $\forall a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$

In antisymmetrical relation sets, bidirection only exists when the elements are equal. In other words, if a is related to b, then b is not related to a unless $a = b$.

4.1.2 Equivalence Relations

ℹ Definition: Equivalence Relation

A relation is an **equivalence relation** if it is: 1. Reflexive 2. Symmetric 3. Transitive

Examples: - Equality $(=)$ - Congruence mod n: $a \equiv b \pmod{n}$ if n divides $(a - b)$ - Similarity of matrices

4.2 Functions

ℹ Definition: Function

A **function** $f : A \to B$ assigns to each element of A exactly one element of B. **Components:** - **Domain:** A - **Codomain:** B - **Range:** $\{f(a) \mid a \in A\} \subseteq B$

Each input maps to **exactly one** output.

4.2.1 Types of Functions

Injective (one-to-one):

Different inputs produce different outputs.

$$\forall x_1, x_2 \in A, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2$$

Equivalently (contrapositive): If $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$

Surjective (onto):

Every element of codomain is hit.

$$\forall b \in B, \exists a \in A \text{ such that } f(a) = b$$

Equivalently: Range = Codomain

Bijective:

Both injective and surjective. Perfect one-to-one pairing.

> **!** Important
>
> Only bijective functions have inverses.

4.3 Examples

4.3.1 Example 1: Injective Function

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = 2x + 3$$

Injective? YES

If $f(x_1) = f(x_2)$, then $2x_1 + 3 = 2x_2 + 3$, so $2x_1 = 2x_2$, thus $x_1 = x_2$.

4.3.2 Example 2: Not Injective

$$g : \mathbb{R} \to \mathbb{R}, \quad g(x) = x^2$$

Injective? NO

$g(2) = 4 = g(-2)$, but $2 \neq -2$.

4.3.3 Example 3: Surjective Function

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^3$$

Surjective? YES

For any $y \in \mathbb{R}$, choose $x = \sqrt[3]{y}$, then $f(x) = y$.

4.3.4 Example 4: Not Surjective

$$g : \mathbb{R} \to \mathbb{R}, \quad g(x) = x^2$$

Surjective? NO

Range is $[0, \infty)$, which doesn't equal codomain $\mathbb{R}$. For $y = -1$, no real x satisfies $x^2 = -1$.

4.3.5 Example 5: Bijective Function

$$h : [0, \infty) \to [0, \infty), \quad h(x) = x^2$$

Injective? YES (for $x_1, x_2 \geq 0$, if $x_1^2 = x_2^2$ then $x_1 = x_2$)

Surjective? YES (for any $y \geq 0$, choose $x = \sqrt{y}$)

Therefore bijective. Inverse: $h^{-1}(y) = \sqrt{y}$

4.3.6 Example 6: Surjectivity Depends on Codomain

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2$$

NOT surjective (as shown above).

$$h : \mathbb{R} \to [0, \infty), \quad h(x) = x^2$$

IS surjective (changed codomain to match range).

4.4 Function Composition

$$(g \circ f)(x) = g(f(x))$$

Apply f first, then g.

Example:

$$f(x) = x + 1, \quad g(x) = x^2$$

$$(g \circ f)(x) = g(x + 1) = (x + 1)^2$$

$$(f \circ g)(x) = f(x^2) = x^2 + 1$$

Different functions! Composition is not commutative: $g \circ f \neq f \circ g$ in general.

Composition preserves properties: - f, g injective $\Rightarrow$ $g \circ f$ injective - f, g surjective $\Rightarrow$ $g \circ f$ surjective - f, g bijective $\Rightarrow$ $g \circ f$ bijective

4.5 Common Errors

Thinking relation = function:

Relations can have one input mapping to multiple outputs. Functions must have exactly one output per input.

Claiming function not surjective without specifying codomain:

Always state the codomain explicitly. $f(x) = x^2$ is surjective onto $[0, \infty)$ but not onto $\mathbb{R}$.

Confusing injective with surjective:

Injective: different inputs → different outputs

Surjective: all outputs are hit

Different concepts!

---

5 Cardinality

5.1 Understanding Infinity

Before Cantor, infinity was treated as a single concept. Cantor asked: can we compare sizes of infinite sets? Are there more real numbers than natural numbers?

His shocking answer: yes, some infinities are strictly larger than others.

5.2 Comparing Set Sizes

For finite sets, size means counting. For infinite sets, we can't "count to infinity," but we can establish pairings.

ℹ Definition: Same Cardinality

Sets A and B have the **same cardinality** (written $|A| = |B|$) if there exists a bijection $f : A \to B$.

Think of it as a perfect pairing—each element of A pairs with exactly one element of B, and vice versa.

5.3 Countably Infinite Sets

ℹ Definition: Countably Infinite

A set is **countably infinite** if $|A| = |\mathbb{N}|$.
Equivalently: elements can be listed as $a_0, a_1, a_2, a_3, \ldots$

5.3.1 Example 1: Even Natural Numbers

Claim: $|\{0, 2, 4, 6, \ldots\}| = |\mathbb{N}|$

Define $f : \mathbb{N} \to \{\text{evens}\}$ by $f(n) = 2n$:

$$f(0) = 0 \tag{1}$$
$$f(1) = 2 \tag{2}$$
$$f(2) = 4 \tag{3}$$
$$f(3) = 6 \tag{4}$$

Injective: If $2n_1 = 2n_2$, then $n_1 = n_2$

Surjective: For any even $2k$, choose $n = k$, then $f(n) = 2k$

Therefore bijection exists. Even though evens are a proper subset of naturals, they have the same cardinality!

5.3.2 Example 2: Integers

Claim: $|\mathbb{Z}| = |\mathbb{N}|$

List integers by alternating positive and negative:

$$0, 1, -1, 2, -2, 3, -3, 4, -4, ...$$

Define:

$$f(n) = \begin{cases} 0 & n = 0 \\ n/2 & n \text{ even and } n > 0 \\ -(n-1)/2 & n \text{ odd} \end{cases}$$

Each integer appears exactly once—bijection exists.

5.3.3 Example 3: Rational Numbers

Claim: $|\mathbb{Q}| = |\mathbb{N}|$

Arrange positive rationals in a grid:

```
1/1  1/2  1/3  1/4  1/5  ...
2/1  2/2  2/3  2/4  2/5  ...
3/1  3/2  3/3  3/4  3/5  ...
4/1  4/2  4/3  4/4  4/5  ...
```

"Snake" through diagonally, skipping duplicates (like $2/2 = 1/1$):

$$1/1 \to 1/2 \to 2/1 \to 3/1 \to 2/2(\text{skip}) \to 1/3 \to 1/4 \to 2/3 \to ...$$

This gives a listing of all positive rationals. Include negative rationals and zero (like we did for integers), get $|\mathbb{Q}| = |\mathbb{N}|$.

Rationals are countable despite being "everywhere" (dense in the reals).

5.4 Uncountably Infinite Sets

Definition: Uncountable

A set is **uncountable** if it is infinite but NOT countably infinite.
Cannot be put in bijection with $\mathbb{N}$.

5.4.1 Cantor's Diagonal Argument

Theorem: $\mathbb{R}$ is uncountable ($|\mathbb{R}| > |\mathbb{N}|$)

Proof:

Assume $\mathbb{R}$ is countable. Then we can list all reals in $[0, 1)$:

$$r_1 = 0.d_{11}d_{12}d_{13}d_{14} \ldots \quad (5)$$
$$r_2 = 0.d_{21}d_{22}d_{23}d_{24} \ldots \quad (6)$$
$$r_3 = 0.d_{31}d_{32}d_{33}d_{34} \ldots \quad (7)$$
$$r_4 = 0.d_{41}d_{42}d_{43}d_{44} \ldots \quad (8)$$

Construct new number $x = 0.x_1x_2x_3x_4 \ldots$ where $x_n \neq d_{nn}$ and $x_n \neq 0, 9$.

Example:

$$r_1 = 0.\mathbf{5}123456 \ldots \quad (9)$$
$$r_2 = 0.3\mathbf{9}87654 \ldots \quad (10)$$
$$r_3 = 0.14\mathbf{1}5926 \ldots \quad (11)$$
$$r_4 = 0.271\mathbf{8}281 \ldots \quad (12)$$

Diagonal: 5, 9, 1, 8, …

Choose: $x = 0.6129 \ldots$ (each digit different from diagonal)

Then: - $x \neq r_1$ (differ in position 1: 6 vs 5) - $x \neq r_2$ (differ in position 2: 1 vs 9) - $x \neq r_3$ (differ in position 3: 2 vs 1) - $x \neq r_4$ (differ in position 4: 9 vs 8)

So $x \in [0, 1)$ but x is not in our "complete" list! Contradiction.

Therefore $\mathbb{R}$ cannot be listed—it's uncountable.

Why avoid 0 and 9? To prevent issues like $0.999 \ldots = 1.000 \ldots$

5.5 Hierarchy of Infinities

Cantor's Theorem: For any set A, $|A| < |\mathcal{P}(A)|$

Power set is always strictly larger.

Consequence:

$$|\mathbb{N}| = \aleph_0 < |\mathbb{R}| = 2^{\aleph_0} = c < |\mathcal{P}(\mathbb{R})| = 2^c < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| = 2^{2^c} < \cdots$$

Infinite hierarchy of infinities—no "largest" infinity.

5.5.1 Summary Table

Set	Cardinality	Type
$\emptyset$	0	Finite
$\{1, 2, 3\}$	3	Finite
$\mathbb{N}$	$\aleph_0$	Countably infinite
$\mathbb{Z}$	$\aleph_0$	Countably infinite
$\mathbb{Q}$	$\aleph_0$	Countably infinite
$\mathbb{R}$	$c = 2^{\aleph_0}$	Uncountably infinite
$[0, 1]$	c	Uncountably infinite
$\mathcal{P}(\mathbb{N})$	c	Uncountably infinite
$\mathcal{P}(\mathbb{R})$	2^c	Larger infinity

5.6 Examples

5.6.1 Example 1: Interval [0,1]

Claim: $|[0, 1]| = |\mathbb{R}|$

Seems impossible—finite interval same size as entire real line?

Define $f : (0, 1) \to \mathbb{R}$ by:

$$f(x) = \tan\left(\pi\left(x - \frac{1}{2}\right)\right)$$

This is a bijection mapping the open interval onto all reals. Similar construction works for $[0, 1]$.

5.6.2 Example 2: Power Set of Naturals

Claim: $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$

Each subset of $\mathbb{N}$ corresponds to an infinite binary sequence. These can be mapped to real numbers in $[0, 1]$ via binary representation. With care about duplicates, this gives a bijection.

5.6.3 Example 3: Non-Example

Can't use diagonal argument on integers because integers aren't in decimal expansion form. The argument specifically applies to reals.

5.7 What to Watch For

Thinking "larger" means what it does for finite sets:

Rationals are denser than integers (between any two rationals, there's another), yet $|\mathbb{Q}| = |\mathbb{Z}|$.

Assuming proper subset must be smaller:

Evens are half the naturals in finite sense, but $|\{\text{evens}\}| = |\mathbb{N}|$ (for infinite sets).

Misapplying diagonal argument:

Only works for objects with infinite expansions (like reals in decimal form). Can't use it on integers.

Thinking all infinities are equal:

$|\mathbb{N}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < \cdots$

Multiple distinct infinite cardinalities exist.

Confusing countable with finite:

"Countable" means finite OR countably infinite. Both $\{1, 2, 3\}$ and $\mathbb{N}$ are countable.

5.8 Prerequisites and Connections

Requires: Set theory (bijections), logic (proof by contradiction)

Enables: Measure theory, topology, analysis, learning theory

Related: Cardinal arithmetic, ordinal numbers, continuum hypothesis

---

6 Mathematical Induction

6.1 Historical Background

The principle of mathematical induction has roots in ancient mathematics, but its modern formalization emerged in the 16th-17th centuries. Blaise Pascal (1653) used a form of induction in his work on binomial coefficients. Francesco Maurolico (1575) proved results about sums using inductive reasoning.

The term "mathematical induction" was coined by Augustus De Morgan in the 1830s. Giuseppe Peano (1889) incorporated induction as an axiom in his axiomatization of natural numbers—the fifth Peano axiom explicitly states the principle of mathematical induction.

Why was formalization necessary? Early mathematicians observed patterns (like $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$) and verified them for many cases. But mathematical truth requires proof for ALL cases, infinitely many of them. Induction provides a rigorous method to prove statements about all natural numbers without checking each one individually.

This wasn't about applications—it was about establishing a logically sound foundation for reasoning about infinite sequences of statements.

6.2 Understanding Mathematical Induction

Imagine an infinite line of dominoes. You want to prove they all fall down. How?

Two steps: 1. **Knock down the first domino** (base case) 2. **Ensure each domino knocks down the next** (inductive step)

If both conditions hold, all dominoes must fall.

Mathematical induction works the same way for statements about natural numbers: - Prove the statement for $n = 1$ (base case) - Prove: "if true for $n = k$, then true for $n = k + 1$" (inductive step)

Together, these guarantee the statement holds for all $n \geq 1$.

Physical analogy: Think of climbing an infinite ladder. You can reach any rung if: 1. You can reach the first rung (base case) 2. From any rung you can reach, you can reach the next one (inductive step)

Why it works: Suppose the statement fails for some number. Let m be the smallest number where it fails. But we proved it for $n = 1$, so $m > 1$. Since m is smallest, it works for $m - 1$. But the inductive step says if it works for $m - 1$, it works for m. Contradiction! Therefore, no such m exists.

6.3 Formal Definition

ℹ Principle of Mathematical Induction

Let $P(n)$ be a statement about natural number n. If:

1. **Base case:** $P(1)$ is true
2. **Inductive step:** For all $k \geq 1$, if $P(k)$ is true, then $P(k + 1)$ is true

Then $P(n)$ is true for all natural numbers $n \geq 1$.

Components unpacked:

- $P(n)$: A predicate (statement depending on n)
- **Base case**: Verify $P(1)$ directly
- **Inductive hypothesis**: Assume $P(k)$ is true for arbitrary k
- **Inductive step**: Using the hypothesis, prove $P(k + 1)$
- **Conclusion**: By induction, $P(n)$ holds for all $n \geq 1$

Variants: - Can start at any n_0 (not just 1): prove $P(n_0)$ and $P(k) \Rightarrow P(k+1)$ - **Strong induction**: Assume $P(1), P(2), \ldots, P(k)$ all true, prove $P(k + 1)$ - **Backward induction**: Sometimes prove $P(k + 1) \Rightarrow P(k)$ with a different base

6.4 Why This Definition

Why two separate steps?

The base case alone isn't enough—verifying $P(1), P(2), P(3), ...$ for finitely many values proves nothing about ALL values.

The inductive step alone isn't enough either. Consider the statement $P(n)$: "$n = n + 1$". The inductive step is vacuously true (if $k = k + 1$, then $k + 1 = k + 2$), but the statement is false for all n.

Why assume what we're trying to prove?

This confuses many students. We're NOT proving $P(k)$—we're proving the implication: $P(k) \Rightarrow P(k + 1)$.

Think of it as proving: "IF the statement works for some number, THEN it works for the next number." We're allowed to assume the hypothesis of an implication to prove the conclusion.

Why start at 1 (or any specific base)?

Because the chain must start somewhere. The inductive step links k to $k + 1$, but without an anchor (base case), we can't conclude anything. It's like having dominoes arranged but never knocking the first one over.

What makes this different from assuming what we want to prove?

We prove: 1. $P(1)$ (established independently) 2. $P(1) \Rightarrow P(2)$ (from inductive step with $k = 1$) 3. Therefore $P(2)$ (modus ponens) 4. $P(2) \Rightarrow P(3)$ (from inductive step with $k = 2$) 5. Therefore $P(3)$ (modus ponens) 6. …continues infinitely

Each specific case is proven, though we can't write them all. The induction principle formalizes this infinite process.

6.5 Key Properties

6.5.1 Property 1: Well-Ordering Principle (Equivalent)

Mathematical induction is equivalent to the well-ordering principle: every nonempty subset of natural numbers has a smallest element.

Why equivalent?

Induction ⇒ Well-ordering: Suppose $S \subseteq \mathbb{N}$ is nonempty with no minimum. Let $P(n) =$ "$n \notin S$". Then $P(1)$ holds (otherwise 1 would be minimum). If $P(k)$ holds, then $P(k+1)$ must hold (otherwise $k + 1$ would be minimum). By induction, $P(n)$ holds for all n, so S is empty. Contradiction.

Well-ordering ⇒ Induction: Suppose $P(1)$ and $P(k) \Rightarrow P(k + 1)$, but $P(n)$ fails for some n. Let S $= \{n : P(n) \text{ is false}\}$. By well-ordering, S has minimum element m. We know $m \neq 1$ (base case). So $m > 1$ and $m - 1 \notin S$, meaning $P(m - 1)$ is true. By inductive step, $P(m)$ is true, contradicting $m \in S$.

This equivalence means you can use either principle depending on which is more convenient for a given problem.

6.5.2 Property 2: Strong Induction

ℹ Strong Induction Principle

If: 1. $P(1)$ is true (base case) 2. For all $k \geq 1$: if $P(1), P(2), \ldots, P(k)$ are all true, then $P(k+1)$ is true
Then $P(n)$ is true for all $n \geq 1$.

Why is this equivalent to regular induction?

Strong induction appears stronger (assume more), but they're equivalent in power.

Proof of equivalence: Let $Q(n) =$ "$P(1) \wedge P(2) \wedge \cdots \wedge P(n)$". Then strong induction on P is equivalent to regular induction on Q.

When to use strong induction:

When proving $P(k+1)$ requires knowing P holds for multiple previous values, not just $P(k)$. Example: Fibonacci recurrence, fundamental theorem of arithmetic.

6.5.3 Property 3: Structural Induction

Beyond numbers, induction applies to any well-founded structure: - Trees (induction on tree depth or node count) - Strings (induction on length) - Formulas (induction on complexity) - Recursively defined objects

The principle: prove for base structures, then prove the property is preserved under construction operations.

6.6 Main Theorems

! Theorem: Equivalence of Induction and Well-Ordering

The following are equivalent over the natural numbers: 1. Principle of Mathematical Induction 2. Well-Ordering Principle 3. Strong Induction Principle

Proof sketch: Already shown in Key Properties above. The key insight is that all three capture the fundamental structure of $\mathbb{N}$ as built from 1 by repeatedly adding 1.

! Theorem: Induction as Proof Technique

For any predicate $P(n)$ on natural numbers, if the base case and inductive step are proven, then $\forall n \geq n_0, P(n)$ is established with certainty.

This formalizes that induction is a valid proof method, not just heuristic reasoning.

6.7 Computational Methods

6.7.1 Algorithm: Writing an Induction Proof

Template:

```
Theorem: [State what you're proving: P(n) for all n   n ]

Proof by induction:

Base case (n = n ):
  [Verify P(n ) directly by computation/argument]
  [Show result: "Therefore P(n ) holds."]

Inductive step:
  Inductive hypothesis: Assume P(k) is true for arbitrary k   n .
  [State explicitly what P(k) says with k substituted]

  Goal: Prove P(k+1)
  [State explicitly what P(k+1) says]

  [Proof of P(k+1) using P(k)]
  [Chain of implications/equalities]
  [Point out where you used inductive hypothesis]

  Therefore P(k+1) holds.

Conclusion:
  By the principle of mathematical induction, P(n) holds for all n   n .
```

6.7.2 Example: Sum Formula

Prove: For all $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Proof:

Base case ($n = 1$):

$$\sum_{i=1}^{1} i = 1 \quad \text{and} \quad \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Therefore $P(1)$ holds.

Inductive step:

Inductive hypothesis: Assume for some $k \geq 1$:

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

Goal: Prove:

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

Proof:

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k+1) \tag{13}$$

$$= \frac{k(k+1)}{2} + (k+1) \quad \text{[by inductive hypothesis]} \tag{14}$$

$$= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \tag{15}$$

$$= \frac{k(k+1) + 2(k+1)}{2} \tag{16}$$

$$= \frac{(k+1)(k+2)}{2} \tag{17}$$

Therefore $P(k+1)$ holds.

Conclusion: By mathematical induction, the formula holds for all $n \geq 1$.

6.8 Examples and Worked Problems

6.8.1 Worked Example 1: Proving a Summation Formula

[Heavily Scaffolded]

Problem: Prove that for all $n \geq 1$: $\sum_{i=1}^{n}(2i-1) = n^2$

Complete Solution:

This is the sum of the first n odd numbers. We'll prove it equals n^2.

Proof by induction:

Base case ($n = 1$):

Left side: $\sum_{i=1}^{1}(2i-1) = 2(1) - 1 = 1$

Right side: $1^2 = 1$

Since $1 = 1$, the base case holds.

Inductive step:

Inductive hypothesis: Assume that for some $k \geq 1$:

$$\sum_{i=1}^{k}(2i-1) = k^2$$

This is our assumption—we're assuming the formula works for $n = k$.

Goal: We need to prove it works for $n = k + 1$:

$$\sum_{i=1}^{k+1}(2i-1) = (k+1)^2$$

Proof: Starting with the left side of what we want to prove:

$$\sum_{i=1}^{k+1}(2i-1) = \left[\sum_{i=1}^{k}(2i-1)\right] + (2(k+1)-1) \tag{18}$$

$$\tag{19}$$

We separated out the last term ($i = k+1$) from the sum. Now we can apply our inductive hypothesis to the first part:

$$= k^2 + (2k + 2 - 1) \quad \text{[using inductive hypothesis]} \tag{20}$$

$$= k^2 + 2k + 1 \tag{21}$$

$$= (k+1)^2 \quad \text{[factor as perfect square]} \tag{22}$$

This is exactly what we needed to prove! Therefore $P(k + 1)$ holds.

Conclusion: By the principle of mathematical induction, the formula $\sum_{i=1}^{n}(2i - 1) = n^2$ holds for all natural numbers $n \geq 1$.

Key insight: The sum of the first n odd numbers is always a perfect square. This is a beautiful geometric fact—you can visualize this as an $n \times n$ square built from L-shaped odd numbers.

6.8.2 Worked Example 2: Divisibility

[Heavily Scaffolded]

Problem: Prove that for all $n \geq 1$, $7^n - 1$ is divisible by 6.

Complete Solution:

Let $P(n)$ be the statement: "$7^n - 1$ is divisible by 6", or equivalently, "$6|(7^n - 1)$".

Base case ($n = 1$):

$$7^1 - 1 = 7 - 1 = 6 = 6 \cdot 1$$

Since 6 divides 6, the base case holds.

Inductive step:

Inductive hypothesis: Assume for some $k \geq 1$ that $6|(7^k - 1)$.

This means: $7^k - 1 = 6m$ for some integer m, or equivalently, $7^k = 6m + 1$.

Goal: Prove $6|(7^{k+1} - 1)$.

Proof: We need to show $7^{k+1} - 1$ is divisible by 6.

$$
\begin{aligned}
7^{k+1} - 1 &= 7 \cdot 7^k - 1 && (23)\\
&= 7(6m + 1) - 1 \quad \text{[substitute from inductive hypothesis]} && (24)\\
&= 42m + 7 - 1 && (25)\\
&= 42m + 6 && (26)\\
&= 6(7m + 1) && (27)
\end{aligned}
$$

Since $7m + 1$ is an integer, we've expressed $7^{k+1} - 1$ as 6 times an integer. Therefore $6|(7^{k+1} - 1)$.

Conclusion: By mathematical induction, $7^n - 1$ is divisible by 6 for all $n \geq 1$.

Why this works: Each power of 7 exceeds the previous by a factor of 7. Since $7 \equiv 1 \pmod 6$, we have $7^n \equiv 1^n \equiv 1 \pmod 6$, so $7^n - 1 \equiv 0 \pmod 6$.

6.8.3 Guided Problem 3: Inequality

[Moderately Scaffolded]

Problem: Prove that for all $n \geq 5$, $2^n > n^2$.

Setup Provided:

This is a common inequality. Notice it's false for $n = 1, 2, 3, 4$ (check: $2^4 = 16 \not> 16$), so our base case must start at $n = 5$.

Base case ($n = 5$):

$$2^5 = 32 \quad \text{and} \quad 5^2 = 25$$

Since $32 > 25$, the base case holds for $n = 5$.

Your Task:

Complete the inductive step. Assume $2^k > k^2$ for some $k \geq 5$. Prove $2^{k+1} > (k + 1)^2$.

Hint: Start with $2^{k+1} = 2 \cdot 2^k$ and use the inductive hypothesis. You'll need to show that $2k^2 > (k + 1)^2$ for $k \geq 5$.

Guidance for the algebraic step:

Expand $(k+1)^2 = k^2 + 2k + 1$. You want to show $2k^2 > k^2 + 2k + 1$, which simplifies to $k^2 > 2k + 1$, or $k^2 - 2k - 1 > 0$. For $k \geq 5$, verify this is true.

[Try completing this yourself before checking the solution in the Solutions section]

6.8.4 Practice Problem 4: Geometric Sum

[Lightly Scaffolded]

Problem: Prove that for all $n \geq 0$ and $r \neq 1$:

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

[This is a standard formula you should prove from scratch using induction. Remember to handle the base case, state your inductive hypothesis clearly, and manipulate the algebra carefully.]

6.8.5 Challenge Problem 5: Fibonacci Inequality

[Independent]

Problem: Let F_n be the n-th Fibonacci number defined by: - $F_1 = 1, F_2 = 1$ - $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$

Prove that for all $n \geq 1$:

$$F_n < 2^n$$

Hint: This will require strong induction since the Fibonacci recurrence depends on two previous terms.

[This is a novel application requiring you to choose the right induction variant and handle the recursive definition carefully.]

6.9 Frequent Mistakes and Debugging

6.9.1 Error Pattern 1: Not Stating the Inductive Hypothesis

What goes wrong: Students jump into the inductive step without explicitly writing what they're assuming.

Why it happens: Rushing through the proof structure, not understanding that the assumption is the key tool.

How to catch it: Before proving $P(k+1)$, ask yourself: "What exactly am I allowed to assume?"

How to fix it: Always write: "Inductive hypothesis: Assume $P(k)$ is true, i.e., [write out $P(k)$ with k substituted]."

Example:

Wrong:

```
Inductive step: We need to prove the formula for n = k+1.
[proceeds to manipulate]
```

Correct:

```
Inductive step:
Inductive hypothesis: Assume Σ   i = k(k+1)/2

Goal: Prove Σ   ¹ i = (k+1)(k+2)/2
```

6.9.2 Error Pattern 2: Proving the Base Case for n = 0 When Statement is n   1

What goes wrong: Verifying $P(0)$ when the theorem statement says "for all $n \geq 1$".

Why it happens: Confusion about where to start; 0 feels like the "first" natural number.

How to catch it: Read the problem statement carefully. What is the domain of n?

How to fix it: Match your base case to the problem's starting value. If it says $n \geq 1$, verify $P(1)$. If $n \geq 5$, verify $P(5)$.

Example:

Problem: "For all $n \geq 1$, prove $n! \geq 2^{n-1}$"

Wrong: Base case $n = 0$: $0! = 1$ and $2^{-1} = 0.5$...

Correct: Base case $n = 1$: $1! = 1$ and $2^0 = 1$, so $1 \geq 1$.

6.9.3 Error Pattern 3: Circular Reasoning (Using P(k+1) to Prove P(k+1))

What goes wrong: In the inductive step, accidentally assuming what you're trying to prove.

Why it happens: Losing track of what's assumed vs. what's to be proven.

How to catch it: After completing the proof, check: did I use the statement $P(k+1)$ anywhere? If yes, it's circular.

How to fix it: Clearly separate: - What you HAVE: $P(k)$ (inductive hypothesis) - What you WANT: $P(k+1)$ (goal)

Only use $P(k)$ in your proof.

Example:

Wrong:

```
Want to prove: Σ   ¹ i = (k+1)(k+2)/2

Since this is true [assuming it], we have proven it.
```

Correct:

```
Σ   ¹ i = [Σ   i] + (k+1)
         = k(k+1)/2 + (k+1)  [using P(k)]
         = (k+1)(k+2)/2
```

6.9.4 Error Pattern 4: Incomplete Base Case (Multiple Base Cases Needed)

What goes wrong: For strong induction or two-term recurrences, verifying only one base case when two are needed.

Why it happens: Not recognizing that strong induction may require multiple starting values.

How to catch it: If your recurrence is $P(k+1)$ depends on both $P(k)$ and $P(k-1)$, you need base cases for two consecutive values.

How to fix it: Verify all necessary base cases. For Fibonacci-style recurrences, verify $n = 1$ and $n = 2$.

Example (Fibonacci):

Wrong:

```
Base case (n = 1): F  = 1 < 2¹ = 2
Inductive step: Assume F  < 2 ...
```

Correct:

```
Base case (n = 1): F  = 1 < 2¹ = 2
Base case (n = 2): F  = 1 < 2² = 4
Inductive step: Assume F   < 2 ¹ and F  < 2  for k   2...
```

6.9.5 Error Pattern 5: Algebra Errors in Inductive Step

What goes wrong: Correct proof structure but computational mistakes in manipulating expressions.

Why it happens: Working too quickly, not checking intermediate steps.

How to catch it: Verify each algebraic manipulation. Substitute specific values (like $k = 5$) to check.

How to fix it: - Show all intermediate steps - Factor carefully - Check: does LHS = RHS after substitution? - For inequalities, preserve inequality direction

6.9.6 Debugging Checklist for Induction Proofs

Before finalizing:

- ☐ Base case verified for correct starting value (n_0 from problem statement)
- ☐ Inductive hypothesis explicitly stated with k substituted into $P(n)$
- ☐ Goal ($P(k+1)$) clearly stated before proving it
- ☐ Inductive hypothesis actually USED in the proof (point out where)
- ☐ No circular reasoning (didn't assume $P(k+1)$ to prove $P(k+1)$)
- ☐ All algebra steps are correct (verified by checking)
- ☐ Conclusion statement: "By mathematical induction, $P(n)$ holds for all $n \geq n_0$"

□ For strong induction: all necessary base cases verified
□ For inequalities: inequality directions preserved throughout

6.10 Mathematical Connections

6.10.1 Prerequisites

To understand mathematical induction, you need:

Essential: - **Natural numbers** (concept of $\mathbb{N} = \{1, 2, 3, ...\}$) - Why: Induction works over $\mathbb{N}$ - Specific use: Understanding successor function ($n \to n + 1$)

- **Logical implications** ($P \Rightarrow Q$)
  - Why: Inductive step is proving an implication
  - Specific use: Understanding "if $P(k)$ then $P(k + 1)$"
- **Predicates and quantifiers**
  - Why: $P(n)$ is a predicate, we prove $\forall n, P(n)$
  - Specific use: Substituting values into P

Helpful: - Basic algebra (for manipulating expressions in proofs) - Summation notation ($\sum$) - Understanding of what constitutes a proof

6.10.2 What This Enables

Mathematical induction unlocks:

Immediate consequences: - Proving formulas for sums: $\sum_{i=1}^{n} f(i)$ - Proving divisibility results for all n - Proving inequalities for all n (e.g., $2^n > n^2$ for $n \geq 5$)

Subsequent topics: - **Recursive algorithms**: Proving correctness (algorithm works for input size n) - **Recurrence relations**: Solving and proving solutions (Fibonacci, divide-and-conquer) - **Graph theory**: Proving properties about trees (nodes $n \Rightarrow$ edges $n - 1$) - **Combinatorics**: Proving identities (binomial theorem, Pascal's triangle) - **Number theory**: Proving divisibility and congruence results - **Analysis**: Proving convergence of sequences defined recursively

Mathematical structures enabled: - Well-founded recursion and induction on arbitrary well-founded sets - Structural induction (trees, formulas, programs) - Transfinite induction (ordinals beyond $\mathbb{N}$)

6.10.3 Related Concepts

Well-Ordering Principle: - Relationship: Equivalent to mathematical induction over $\mathbb{N}$ - Difference: WOP says every nonempty subset has a minimum; induction is proof technique - When to use which: WOP useful for proof by contradiction; induction for direct proofs

Strong Induction: - Relationship: Equivalent in power to regular induction - Difference: Can assume $P(1), \dots, P(k)$ all true instead of just $P(k)$ - When to use: When $P(k+1)$ depends on multiple previous cases

Complete Induction: - Another name for strong induction

Structural Induction: - Generalization: Induction on recursively defined structures (not just numbers) - Examples: Trees, lists, formulas, programs - Same principle: prove base cases, prove inductive step preserves property

Recursion: - Connection: Induction proves properties of recursive definitions - Recursion defines objects; induction proves things about them - Example: Fibonacci sequence (recursive def) + induction (proves properties)

6.10.4 Synthesis: The Bigger Mathematical Picture

Induction's foundational role:

Mathematical induction is the bridge between finite and infinite. It allows us to make statements about infinitely many objects (all natural numbers) using finite reasoning (base case + one implication).

Across mathematical domains:

Discrete mathematics: - Proves combinatorial identities - Central to algorithm analysis - Foundation for discrete structures

Analysis: - Sequence convergence proofs - Series convergence (ratio test involves inductive reasoning) - Defining real numbers from rationals

Algebra: - Proving properties of algebraic structures - Polynomial division algorithm - Fundamental theorem of arithmetic (uses strong induction)

Computer Science: - Loop invariants (induction on iteration count) - Proving program correctness - Complexity analysis (Master theorem, recurrences)

Generalization hierarchy:

1. $\mathbb{N}$: Mathematical induction (finite ordinals)
2. Structural induction: Recursively defined objects
3. Well-founded induction: Any well-founded partial order
4. Transfinite induction: Infinite ordinals $\omega, \omega + 1, \dots$

Unifying principle:

"Building from base cases through construction rules"

In numbers: Start with 1, build using +1 In logic: Start with axioms, build using inference rules In sets: Start with $\emptyset$, build using operations In programs: Start with base cases, build using recursive calls

The pattern repeats throughout mathematics: define a minimal base, define construction operations, prove properties by induction on the construction.

Why induction is indispensable:

Without induction, we cannot rigorously prove statements about all natural numbers. We'd be limited to checking finitely many cases, leaving infinitely many unverified. Induction completes the logical foundation for reasoning about discrete infinite objects.

6.11 Exploring Further

6.11.1 Generate Your Own Examples

1. Create induction proofs for new summation formulas:

Try proving: - $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ - $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$ - $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$

Verification: After creating your proof, check that the base case and algebra are correct by substituting $n = 1, 2, 3$ into both sides.

2. Design divisibility problems:

Create statements like: - For all $n \geq 1$, $5^n - 1$ is divisible by ***? (find what works) - For all*** $n \geq 1$***,*** $n^3 - n$ ***is divisible by*** ?

Guidance: Pick a base (like a^n) and compute $a^1 - 1, a^2 - 1, a^3 - 1$. Find the GCD—that's what divides $a^n - 1$ for all n.

3. Construct inequality chains:

Create problems like: - Find the smallest n_0 such that $n! > 3^n$ for all $n \geq n_0$ - Prove $n^2 < 2^n$ for $n \geq 5$ (test variations)

6.11.2 Create Your Own Problems

Problem creation framework:

Modify existing: - Original: Prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ - Your variation: Change to $\sum_{i=1}^{n}(3i-2) = \frac{n(3n-1)}{2}$ [verify first!]

Combine concepts: - Induction + modular arithmetic: Prove $7^n \equiv 1 \pmod{6}$ for all $n \geq 1$ - Induction + inequalities: Prove $\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{2n+1}}$

Reverse engineer: - Pick a formula you know is true (from textbook, etc.) - Write a clean induction proof - Now modify one part and see what needs to change

6.11.3 Extend the Concept

1. Relax to backward induction:

Instead of $P(k) \Rightarrow P(k+1)$, what if we prove $P(k+1) \Rightarrow P(k)$ with a different starting point?

- When does this work?
- What's a problem suited to backward induction?
- Try: Prove $n! > 2^n$ for $n \geq 4$ by showing $P(k+1) \Rightarrow P(k)$ and verifying a large base case.

2. Generalize to two-dimensional induction:

Prove statements about pairs (m, n) by induction on $m+n$ or by nested induction.

Example: Prove $\binom{m+n}{m} = \binom{m+n}{n}$ by induction on $m+n$.

3. Apply to non-numeric structures:

- **Trees:** Prove that a binary tree with n nodes has $n+1$ null pointers (use structural induction on tree height)
- **Strings:** Prove properties about strings of length n
- **Graphs:** Prove a graph with n vertices and $n-1$ edges that is connected must be a tree

4. Strong induction variants:

Define: **Complete induction** assumes $P(1), P(2), \ldots, P(k)$ (all previous) to prove $P(k+1)$.

When is this necessary vs. regular induction?

Create problems that require complete induction (like Fundamental Theorem of Arithmetic).

6.11.4 Prove Related Results

1. Prove variations:

We proved: For all $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Your challenges: - Prove: $\sum_{i=1}^{n}(2i-1) = n^2$ [sum of odd numbers] - Prove: $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$ - Generalize: Can you find a pattern for $\sum_{i=1}^{n} i^k$?

2. Prove consequences:

Using mathematical induction, prove:

- **Bernoulli's Inequality:** For $x \geq -1$ and $n \geq 1$: $(1+x)^n \geq 1 + nx$
- **AM-GM for 2^n terms:** $\frac{a_1+\cdots+a_{2^n}}{2^n} \geq \sqrt[2^n]{a_1 \cdots a_{2^n}}$ (use induction on n)
- **Binomial Theorem:** $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

3. Prove the equivalences:

Show rigorously: - Induction $\Leftrightarrow$ Well-Ordering Principle - Regular Induction $\Leftrightarrow$ Strong Induction

(Detailed proof of both directions)

6.11.5 Hints and Ideas for Exploration

For further investigation:

1. Double induction:

Read: How to prove statements about two variables using nested induction

Try: Prove the general binomial theorem: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ using induction on n

Extend: Prove Pascal's identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ by double induction

2. Combinatorial proofs vs. induction:

Explore: The formula $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ has a beautiful visual proof (arranging dots in triangular array). Can you find combinatorial proofs for other induction results?

Question: When is induction necessary vs. when can you give a direct combinatorial argument?

3. Limits of induction:

Investigate: Can you prove $\sum_{i=1}^{\infty} i = \frac{\infty(\infty+1)}{2}$? Why not?

Question: What properties of $\mathbb{N}$ make induction work that fail for infinite sums?

4. Strengthening the inductive hypothesis:

Sometimes to prove $P(n)$, you must prove a stronger $Q(n)$ by induction because $Q(k) \Rightarrow Q(k+1)$ works but $P(k) \Rightarrow P(k+1)$ doesn't.

Example: Try proving $F_n < 2^n$ directly vs. proving $F_n \leq 2^{n-1}$ (the latter works better with strong induction).

7 Applications to Machine Learning

Now that we have foundations in logic, proof, and set theory, we can see how these concepts underpin machine learning.

7.1 Training and Test Sets

Data is a set of input-output pairs:

$$D = \{(x_i, y_i)\}_{i=1}^{n} \subset X \times Y$$

where X is the input space and Y is the output space.

Training set: $D_{\text{train}} \subset X \times Y$

Test set: $D_{\text{test}} \subset X \times Y$

Requirement: $D_{\text{train}} \cap D_{\text{test}} = \emptyset$ (disjoint)

Without disjoint sets, we'd test on data we trained on—overly optimistic performance estimates.

7.2 Hypothesis Classes

A learning algorithm searches over a **hypothesis class**:

$$\mathcal{H} = \{h : X \to Y \mid h \text{ satisfies constraints}\}$$

Cardinality affects learnability:

Finite hypothesis class:

$$\mathcal{H} = \{h_1, h_2, \dots, h_n\}$$

Can exhaustively search. Always PAC-learnable with enough samples.

Countably infinite:

$$\mathcal{H} = \text{all polynomials with rational coefficients}$$

$|\mathcal{H}| = \aleph_0$. PAC-learnable if VC dimension is finite.

Uncountably infinite:

$$\mathcal{H} = \text{all continuous functions } \mathbb{R}^d \to \mathbb{R}$$

$|\mathcal{H}| = 2^c$ (very large). Requires regularization or other constraints for practical learning.

7.3 Feature Spaces

Discrete (finite):

$$X = \{0, 1\}^n$$

Binary features. $|X| = 2^n$ (exponentially large but finite).

Continuous (uncountable):

$$X = \mathbb{R}^n$$

$|X| = c$ (continuum). Requires measure-theoretic probability—we can't assign probability to every individual point.

7.4 PAC Learning and Quantifiers

Probably Approximately Correct (PAC) learning definition:

“For all $\varepsilon > 0$ and $\delta > 0$, there exists m such that for all distributions and target functions, with probability at least $1 - \delta$ over samples of size m, the learned hypothesis has error at most ε”

$$\forall \varepsilon, \delta > 0, \exists m, \forall D, f, P_{|S|=m}[\text{error}(h) \leq \varepsilon] \geq 1 - \delta$$

This is a complex nested quantifier statement—understanding quantifier order is essential.

7.5 Function Spaces

Neural networks approximate functions in continuous function spaces:

$$C([0,1]^d) = \{\text{continuous functions } [0,1]^d \to \mathbb{R}\}$$

This space has cardinality $|C([0,1]^d)| = 2^c$ (uncountably infinite).

Universal approximation theorems show neural networks can approximate any function in $C([0,1]^d)$ arbitrarily well (with enough neurons). But we can never achieve actual surjectivity—the set of representable functions is a dense subset, not the whole space.

---

8 Practice Problems

8.1 Problem Set 1: Logic

Problem 1: Construct truth table for $(P \to Q) \land (Q \to R)$.

Problem 2: Negate the following statement: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, (x + y > 0)$

Problem 3: Determine if the following are logically equivalent: - $P \to (Q \lor R)$ - $(P \to Q) \lor (P \to R)$

Problem 4: State the contrapositive, converse, and inverse of: “If n is divisible by 4, then n is even.”

8.2 Problem Set 2: Proofs

Problem 5: Prove: For all integers n, if n^3 is even then n is even.

Problem 6: Prove: $\sqrt{3}$ is irrational.

Problem 7: Prove: For all integers n, $n^2 - n$ is even.

Problem 8: Prove or disprove: For all real numbers x and y, if $xy = 0$ then $x = 0$ or $y = 0$.

8.3 Problem Set 3: Sets

Problem 9: Let $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$. Compute: - $A \triangle B$ - $\mathcal{P}(A \cap B)$

Problem 10: Prove: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Problem 11: List all elements of $\mathcal{P}(\{a, b, c\})$.

Problem 12: Given $S = \{1, 2, \{3\}, \emptyset\}$, determine true or false: - $2 \in S$ - $\{2\} \in S$ - $\{2\} \subseteq S$ - $\emptyset \in S$ - $\emptyset \subseteq S$

8.4 Problem Set 4: Functions

Problem 13: For $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3 - x$, determine: - Is f injective? - Is f surjective? - What domain/codomain restrictions make f bijective?

Problem 14: Prove: The composition of two injective functions is injective.

Problem 15: Find a bijection between $(0, 1)$ and $(0, \infty)$.

Problem 16: Give an example of functions f, g where $g \circ f$ is injective but g is not injective.

8.5 Problem Set 5: Cardinality

Problem 17: Prove: $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

(Hint: Use the pairing function or diagonal argument for listing)

Problem 18: Prove: $|[0, 1]| = |(0, 1)|$

(Open vs closed interval)

Problem 19: Explain why $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$

Problem 20: Which is larger: $|\mathbb{Q} \times \mathbb{Q}|$ or $|\mathbb{Q}|$? Justify.

8.6 Problem Set 6: Mathematical Induction

8.6.1 Solution to Guided Problem 3

Problem: Prove that for all $n \geq 5$, $2^n > n^2$.

Complete Solution:

Base case ($n = 5$):

$$2^5 = 32 \quad \text{and} \quad 5^2 = 25$$

Since $32 > 25$, the base case holds.

Inductive step:

Inductive hypothesis: Assume for some $k \geq 5$ that $2^k > k^2$.

Goal: Prove $2^{k+1} > (k+1)^2$.

Proof:

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k && (28) \\ &> 2k^2 \quad \text{[by inductive hypothesis]} && (29) \end{aligned}$$

Now we need to show $2k^2 > (k+1)^2$ for $k \geq 5$.

Expanding:

$$(k+1)^2 = k^2 + 2k + 1 \tag{30}$$

We want to show:

$$2k^2 > k^2 + 2k + 1$$

Simplifying:

$$k^2 > 2k + 1$$

$$k^2 - 2k - 1 > 0$$

For $k = 5$: $25 - 10 - 1 = 14 > 0$

For $k > 5$, since k^2 grows much faster than $2k$, the inequality continues to hold.

More rigorously: For $k \geq 5$, we have $k^2 - 2k - 1 = k(k-2) - 1 \geq 5(3) - 1 = 14 > 0$.

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

Conclusion: By mathematical induction, $2^n > n^2$ for all $n \geq 5$.

8.6.2 Solution to Practice Problem 4

Problem: Prove that for all $n \geq 0$ and $r \neq 1$:

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Solution:

Base case ($n = 0$):

Left side: $\sum_{i=0}^{0} r^i = r^0 = 1$

Right side: $\frac{r^1 - 1}{r-1} = \frac{r-1}{r-1} = 1$

Since $1 = 1$, the base case holds.

Inductive step:

Inductive hypothesis: Assume for some $k \geq 0$:

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}$$

Goal: Prove:

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}$$

Proof:

$$\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \left(\sum_{i=0}^{k} r^i\right) + r^{k+1} && (31)\\
&= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} \quad \text{[inductive hypothesis]} && (32)\\
&= \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r-1)}{r - 1} && (33)\\
&= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r - 1} && (34)\\
&= \frac{r^{k+2} - 1}{r - 1} && (35)
\end{aligned}$$

This is exactly what we needed to prove.

Conclusion: By mathematical induction, the geometric sum formula holds for all $n \geq 0$ when $r \neq 1$.

8.6.3 Solution to Challenge Problem 5

Problem: Prove that for all $n \geq 1$, $F_n < 2^n$.

Solution using Strong Induction:

Base cases: - $n = 1$: $F_1 = 1 < 2^1 = 2$ - $n = 2$: $F_2 = 1 < 2^2 = 4$

Inductive step:

Inductive hypothesis: Assume for all $1 \leq j \leq k$ (where $k \geq 2$) that $F_j < 2^j$.

In particular, we have $F_{k-1} < 2^{k-1}$ and $F_k < 2^k$.

Goal: Prove $F_{k+1} < 2^{k+1}$.

Proof:

$$
\begin{align}
F_{k+1} &= F_k + F_{k-1} \quad \text{[Fibonacci recurrence]} \tag{36}\\
&< 2^k + 2^{k-1} \quad \text{[by inductive hypothesis]} \tag{37}\\
&= 2^{k-1}(2+1) \tag{38}\\
&= 3 \cdot 2^{k-1} \tag{39}\\
&< 4 \cdot 2^{k-1} \quad \text{[since } 3 < 4\text{]} \tag{40}\\
&= 2^2 \cdot 2^{k-1} \tag{41}\\
&= 2^{k+1} \tag{42}
\end{align}
$$

Therefore $F_{k+1} < 2^{k+1}$.

Conclusion: By strong induction, $F_n < 2^n$ for all $n \geq 1$.

Note: We needed strong induction because the Fibonacci recurrence requires knowledge of both F_k and F_{k-1}, not just the immediately preceding term.