

THE FOUNDATIONS: LOGIC AND PROOF, SETS, AND FUNCTIONS

1. LOGIC

A **proposition** is a declarative sentence that is either true or false, but not both.

Example 1. *The following declarative sentences are propositions:*

- *Tainan is a city in Taiwan.*
- $1 + 0 = 1$.

The following sentences are not propositions:

- *How many people are enrolled in this class?*
- $x + 1 = y$.

Just like we use letters to denote integer variables, letters are also used to denote propositions. We use p, q, r, s, \dots to denote propositions. For true propositions, their **truth value** is true (denoted by T). On the other hand, the truth value of false proposition is false (denoted by F).

The area of logic that deals with propositions is called the **propositional calculus** or **propositional logic**.

Definition 1. *Let p be a proposition. The statement “It is not the case that p ” is another proposition, called the **negation** of p . The negation of p is denoted by $\neg p$, read “not p .”*

A **truth table** displays the relationships between the truth values of propositions. Figure 1 shows the truth table for the negation of a proposition.

| | |
|-----|----------|
| p | $\neg p$ |
| T | F |
| F | T |

FIGURE 1. Truth Table for Negation of p

The negation of a proposition can also be considered the result of the operation of the **negation operator** on a proposition. There are other logical operators that can be used to form new propositions. These logical operators are called **connectives**.

| p | q | $p \wedge q$ | $p \vee q$ | $p \oplus q$ | $p \rightarrow q$ |
|-----|-----|--------------|------------|--------------|-------------------|
| F | F | F | F | F | T |
| F | T | F | T | T | T |
| T | F | F | T | T | F |
| T | T | T | T | F | T |

FIGURE 2. Truth Table for $p \wedge q$, $p \vee q$, $p \oplus q$ and $p \rightarrow q$

Definition 2. *Let p and q be propositions. The proposition “ p and q ” (write $p \wedge q$) is the proposition that is true only when both p and q are true and false otherwise. The proposition $p \wedge q$ is also called the **conjunction** of p and q .*

Definition 3. *Let p and q be propositions. The proposition “ p or q ” (write $p \vee q$) is the proposition that is false only when both p and q are false and true otherwise. The proposition $p \vee q$ is also called the **disjunction** of p and q .*

Definition 4. *Let p and q be propositions. The **exclusive or** of p and q (write $p \oplus q$) is the proposition that is true only when one of p and q is true and false otherwise.*

Definition 5. *Let p and q be propositions. The **implication** $p \rightarrow q$ is the proposition that is false only when p is true and q is false, and true otherwise.*

| p | q | $p \leftrightarrow q$ |
|-----|-----|-----------------------|
| F | F | T |
| F | T | F |
| T | F | F |
| T | T | T |

FIGURE 3. Truth Table for $p \wedge q$, $p \vee q$, $p \oplus q$ and $p \rightarrow q$

Figure 2 shows the truth table for conjunction, disjunction, exclusive or and implication.

Notice that $p \rightarrow q$ is false when p is true and q is false. For instance,

“If $1 + 1 = 1$, then I am God.”

is true by definition.

Some related implications can be derived from $p \rightarrow q$. The proposition $q \rightarrow p$ is called the **converse** of $p \rightarrow q$. $\neg q \rightarrow \neg p$ is called the **contrapositive** of $p \rightarrow q$. And $\neg p \rightarrow \neg q$ is called the **inverse** of $p \rightarrow q$.

Definition 6. Let p and q be propositions. The **biconditional** $p \leftrightarrow q$ is the proposition that is true when p and q have the same truth values, and false otherwise.

Figure 3 shows the truth table for biconditional $p \leftrightarrow q$.

1.1. **Applications.** We can find propositional calculus in many applications. Here are a few of them.

1.1.1. *System Specifications.*

Example 2. Express the following specification using logical connectives:

- “The diagnostic message is stored in the buffer or it is retransmitted.”
- “The diagnostic message is not stored in the buffer.”
- “If the diagnostic message is stored in the buffer, then it is retransmitted.”

Solution. Let p denote “The diagnostic message is stored in the buffer” and q for “The diagnostic message is retransmitted.” Then the above specification can be formulated as follows.

- $p \vee q$.
- $\neg p$.
- $p \rightarrow q$.

□

Specification should not contain conflicting requirements. That is, there should be a way to satisfy all requirements. In this case, the specification is **consistent**. In the above example, we can take p to be false and q to be true. Hence the above specification is consistent.

Example 3. Suppose we add “The diagnostic message is not retransmitted.” Is the specification still consistent?

Solution. No. Since $\neg p$ must be true by second requirement, p must be false. But then q must be true by the first requirement. It is contradictory to $\neg q$, the added requirement. □

1.1.2. *Logic Puzzles.*

Example 4. On an island, there are only two kinds of inhabitants: knights and knaves. Knights always tell the truth, but knaves always lie. You’re visiting the island and encounter two people A and B. A says “B is a knight” and B says “The two of us are of opposite kinds.” Do you know what are A and B?

Solution. Let p denote “A is a knight” and q for “B is a knight.” We would like to find the truth values for p and q . Suppose p is true. Then A tells the truth. So q is true. But then B must also tell the truth. Since p and q are both true, B cannot tell the truth. A contradiction.

On the other hand, Suppose p is false. Then A lies and q is false. Since q is false, B lies. Thus both p and q must have the same truth value. This is exactly the case. We know conclude A and B are knaves. □

1.1.3. Logic and Bit Operations.

Definition 7. A **bit** has two possible values, 0 and 1. A variable is called a **Boolean variable** if its value is either true or false. Hence, a Boolean variable can be represented by a bit.

A **bit string** is a sequence of zero or more bits. The **length** of this string is the number of bits in the string.

Example 5. Let $x = 01\ 1011\ 0110$ and $y = 11\ 0001\ 1101$. Compute their bitwise OR, AND and XOR.

Solution.

| | | | |
|----|------|------|-------------|
| 01 | 1011 | 0110 | |
| 11 | 0001 | 1101 | |
| 11 | 1011 | 1111 | bitwise OR |
| 01 | 0001 | 0100 | bitwise AND |
| 10 | 1010 | 1011 | bitwise XOR |

□

1.2. A Famous Problem in Computer Science. In Example 2, we show how to use propositional logic to write system specifications. Additionally, we mentioned that system specifications should be consistent. That is, we should be able to assign truth values to propositions such that all requirements are satisfied. In Example 2, we are lucky to have simple requirements where there are only 2 propositions p and q . In real world, there may be hundreds, even thousands of propositions in the requirements. How to find proper truth values for them cannot be done by hand. This problem is called **satisfiability** problem.

Since there are so many propositions, one would write a program to find a solution for us. However, if there are 300 propositions in the specification, a brute-force method may try 2^{300} possible combinations. It is worth noting that $2^{300} \approx 10^{90}$ but the number of particles in our universe is roughly 10^{87} . It doesn't sound "efficient". Whether there is an "efficient" way to solve the problem is the famous $P \stackrel{?}{=} NP$ problem.

2. PROPOSITIONAL EQUIVALENCES

Definition 8. A compound proposition that is always true is called a **tautology**. A compound proposition that is always false is called a **contradiction**. A proposition that is neither a tautology nor a contradiction is called a **contingency**.

Example 6. Let p be a proposition. Then $p \vee \neg p$ is a tautology. $p \wedge \neg p$ is a contradiction. p and $\neg p$ are contingencies.

Definition 9. The propositions p and q are called **logically equivalent** if $p \leftrightarrow q$ is a tautology. We write $p \equiv q$ when p and q are logically equivalent.

Remark. The symbol \equiv is *not* a logical connective since $p \equiv q$ is not a compound proposition. We also use \Leftrightarrow for logical equivalence sometimes.

Example 7. Show $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution. We build the following truth table:

| p | q | $p \vee q$ | $\neg(p \vee q)$ | $\neg p \wedge \neg q$ |
|-----|-----|------------|------------------|------------------------|
| F | F | F | T | T |
| F | T | T | F | F |
| T | F | T | F | F |
| T | T | T | F | F |

□

Remark. A truth table of a compound proposition with n different propositions requires 2^n rows in truth table.

Figure 4 shows some important logical equivalences.

Logical equivalences can be used to show two compound propositions are logically equivalent.

Example 8. Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent.

| Equivalence | Name |
|--|---------------------|
| $p \wedge T \equiv p$ $p \vee F \equiv p$ | Identity laws |
| $p \vee T \equiv T$ $p \wedge F \equiv F$ | Domination laws |
| $p \vee p \equiv p$ $p \wedge p \equiv p$ | Idempotent laws |
| $\neg(\neg p) \equiv p$ | Double negation law |
| $p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$ | commutative laws |
| $(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ | Associative laws |
| $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ | Distributive laws |
| $\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$ | De Morgan's laws |
| $p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$ | Absorption laws |
| $p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$ | Negation laws |
| $p \rightarrow q \equiv \neg p \vee q$ $p \rightarrow q \equiv \neg q \rightarrow \neg p$ $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$ $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$ $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$ $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$ | |
| $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$ | |

FIGURE 4. Logical Equivalences

Proof.

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) \\
&\equiv \neg p \wedge (p \vee \neg q) \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) \\
&\equiv \neg p \wedge \neg q
\end{aligned}$$

□

3. PREDICATES AND QUANTIFIERS

Let $P(x)$ be a proposition with x as its parameter. Then P is called a **predicate** or **propositional function**.

Example 9. Let $P(x)$ denote “ $x > 3$.” What are the truth values for $P(3)$ and $P(4)$?

Solution. $P(3)$ stands for “ $3 > 3$,” which is false. Therefore $P(3)$ is false. $P(4)$ stands for “ $4 > 3$.” Hence $P(4)$ is true. □

We can generalize to multiple parameters. A statement of the form $P(x_1, x_2, \dots, x_n)$ is the value of the **propositional function** P at the n -tuple (x_1, x_2, \dots, x_n) . P is also called a **predicate**.

In addition to assign values to parameters, we can also make predicates become propositions by **quantification**. The area of logic that deals with predicates and quantifiers is called the **predicate calculus**.

Definition 10. The **universal quantification** of $P(x)$ is the proposition “ $P(x)$ is true for all values of x in the universe of discourse.” We write $\forall x P(x)$ for the universal quantification of $P(x)$.

Example 10. What is the truth value of $\forall x (x^2 \geq x)$ when x ranges over integers and real numbers respectively?

Solution. If x ranges over integers, $x^2 \geq x$. Hence $\forall x(x^2 \geq x)$ is true. On the other hand, $x^2 \leq x$ when $|x| \leq 1$. Therefore $\forall x(x^2 \geq x)$ is false when x ranges over real numbers. \square

Definition 11. The *existential quantification* of $P(x)$ is the proposition “There exists an element x in the universe of discourse such that $P(x)$ is true.”

Example 11. Let $Q(x)$ be “ $x \neq x$.” What is the truth value of $\exists xQ(x)$?

Solution. False, apparently. \square

When a quantifier is used on the variable x or when we assign a value of it, we say that this occurrence of x is **bound**. An occurrence of a variable that is not bound is said to be **free**. The part of a logical expression where a quantifier is applied is called the **scope** of the quantifier.

Consider $\neg\forall xP(x)$. Since $\forall xP(x)$ means “for all values of x , $P(x)$ is true,” its negation should be “it is not the case that for all values of x , $P(x)$ is true.” In other words, there is a value for x such that $P(x)$ is false. Hence $\exists x\neg P(x)$. In fact, we have the following logical equivalences:

$$\begin{aligned}\neg\forall xP(x) &\equiv \exists x\neg P(x) \\ \neg\exists xP(x) &\equiv \forall x\neg P(x)\end{aligned}$$

Example 12. What are the negations of $\forall x(x^2 > x)$ and $\exists x(x^2 = 2)$?

Solution. $\neg\forall x(x^2 > x) \equiv \exists x\neg(x^2 > x) \equiv \exists x(x^2 \not> x) \equiv \exists x(x^2 \leq x)$. Similarly, $\neg\exists x(x^2 = 2) \equiv \forall x\neg(x^2 = 2) \equiv \forall x(x^2 \neq 2)$. \square

Example 13. Consider the following two statements:

- “All lions are fierce.”
- “Some lions do not drink coffee.”

Can you deduce “Some fierce creatures do no drink coffee?”

Solution. Let $P(x)$, $Q(x)$ and $R(x)$ be the statement “ x is a lion,” “ x is fierce” and “ x drinks coffee” respectively. Then we have $\forall x(P(x) \rightarrow Q(x))$ and $\exists x(P(x) \wedge \neg R(x))$. We prove $\exists x(Q(x) \wedge \neg R(x))$ as follows. By $\exists x(P(x) \wedge \neg R(x))$, we have an x_0 such that $P(x_0) \wedge \neg R(x_0)$. Since $\forall x(P(x) \rightarrow Q(x))$, $P(x_0) \rightarrow Q(x_0)$ in particular. Therefore $Q(x_0) \wedge \neg R(x_0)$. By taking x to x_0 , we have $\exists x(Q(x) \wedge \neg R(x))$. \square

4. NESTED QUANTIFIERS

We can have nested quantification. In fact, you have seen it in calculus!

Example 14. The definition of limit uses nested quantifiers. Recall the definition of

$$\begin{aligned}\lim_{x \rightarrow a} f(x) = b : \\ \forall \epsilon \exists \delta (|x - a| < \delta \rightarrow |f(x) - b| < \epsilon).\end{aligned}$$

The order of nested quantification is important.

Example 15. Consider $\forall x \exists y(x = y)$ and $\exists y \forall x(x = y)$. What are their truth values? What about $\forall x \exists y(y \leq |x|)$ and $\exists y \forall x(y \leq |x|)$?

Solution. $\forall x \exists y(x = y)$ is true, simply take y to be x . But $\exists y \forall x(x = y)$ is false. Since no matter what y is, $y + 1 \neq y$.

Both $\forall x \exists y(y \leq |x|)$ and $\exists y \forall x(y \leq |x|)$ are true, simply take y to be 0. \square

In fact, we have $\exists y \forall x P(x, y) \rightarrow \forall x \exists y P(x, y)$. Can you prove it?

5. METHODS OF PROOF

Please read Section §1.5 of your textbook. It takes effort to know how to write correct proofs. When you read the text, please try to understand *how* the statements are proved, instead of *what* the statements are proving.

Figure 5 shows some rules of inferences which are useful when you write proofs.

Here we demonstrate the proof methods by two simple theorems in elementary number theory. Dr. Hardy (a renowned mathematician) thinks both theorems are of the highest class (in *A Mathematician’s Apology*). They are actually proved by the Greek two thousands years ago!

| Rule of Inference | Name |
|--|----------------------------|
| $\therefore \frac{p}{p \vee q}$ | Addition |
| $\therefore \frac{p \wedge q}{p}$ | Simplification |
| $\therefore \frac{p \quad q}{p \wedge q}$ | Conjunction |
| $\therefore \frac{p \quad p \rightarrow q}{q}$ | Modus ponens |
| $\therefore \frac{\neg q \quad p \rightarrow q}{\neg p}$ | Modus tollens |
| $\therefore \frac{p \rightarrow q \quad q \rightarrow r}{p \rightarrow r}$ | Hypothetical syllogism |
| $\therefore \frac{p \vee q \quad \neg p}{q}$ | Disjunctive syllogism |
| $\therefore \frac{p \vee q \quad \neg p \vee r}{q \vee r}$ | Resolution |
| $\therefore \frac{\forall x P(x)}{P(c)}$ | Universal instantiation |
| $\therefore \frac{P(c) \text{ for an arbitrary } c}{\forall x P(x)}$ | Universal generalization |
| $\therefore \frac{\exists x P(x)}{P(c) \text{ for some element } c}$ | Existential instantiation |
| $\therefore \frac{P(c) \text{ for some element } c}{\exists x P(x)}$ | Existential generalization |

FIGURE 5. Rules of Inferences

Theorem 1. (Euclid) *There are infinitely many primes.*

Proof. Suppose there are finitely many primes. And $2, 3, 5, \dots, p$ is the list of all primes. Consider $q = (2 \times 3 \times 5 \times \dots \times p) + 1$. Clearly, q is not divisible by any of the primes $2, 3, 5, \dots, p$. A contradiction. \square

Theorem 2. (Pythagoras) $\sqrt{2}$ is not rational.

Proof. Suppose $\sqrt{2} = \frac{a}{b}$ where $\gcd(a, b) = 1$. Then $2 = (\frac{a}{b})^2$. $a^2 = 2b^2$. Since a^2 is even, a must be even. Let $a = 2k$. Then $a^2 = (2k)^2 = 4k^2 = 2b^2$. $2k^2 = b^2$. And b must be even. This is a contradiction since $\gcd(a, b) = 1$. \square

As another example, let us examine a fallacious argument. We need the following definition:

Definition 12. A binary relation \sim is called an **equivalence relation** if

- (Reflexivity) $\forall x \ x \sim x$.
- (Symmetry) $\forall x \forall y \ (x \sim y \rightarrow y \sim x)$.
- (Transitivity) $\forall x \forall y \forall z \ ((x \sim y \wedge y \sim z) \rightarrow x \sim z)$.

The following example is borrowed from *Topology: A First Course* by James R. Munkre.

Example 16. The following argument “proves” that symmetry and transitivity entails reflexivity. Can you identify the flaw?

By symmetry, we have $x \sim y$ and thus $y \sim x$. By transitivity, $x \sim y$ and $y \sim x$ implies $x \sim x$. Therefore reflexivity $x \sim x$ is derived from symmetry and transitivity.

6. SETS

Definition 13. A **set** is an unordered collection of objects. The objects in a set are also called **elements** or **members** of the set. They are **contained** in the set.

Example 17. We’ll use the following symbols to represent their respective sets:

- $\mathbb{N} = \{0, 1, 2, \dots\}$, *natural numbers*
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, *integers*
- $\mathbb{Z}^+ = \{1, 2, \dots\}$, *positive integers*
- $\mathbb{Q} = \{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$, *rational numbers*
- \mathbb{R} , *real numbers*

Definition 14. Two sets are *equal* if and only if they have the same elements.

Definition 15. The set A is a *subset* of set B , write $A \subseteq B$, if and only if every element of A is also an element of B .

Theorem 3. For any set S .

- $\emptyset \subseteq S$; and
- $S \subseteq S$.

Note that when $A = B$, $A \subseteq B$ as well. Sometimes we'd like to exclude this case. We write $A \subset B$ ("A is a **proper subset** of B") for $A \subseteq B$ and $A \neq B$.

Definition 16. Let S be a set. If there are n distinct elements in S ($0 \leq n < \infty$), we say S is a **finite set** and n is the **cardinality** of S . Write $|S| = n$.

Definition 17. A set is **infinite** if it is not finite.

Remark. We'll talk about the cardinality of infinite sets in Section §9.2.

Definition 18. Given a set S , the **power set** $\wp(S)$ of S is the set of all subsets of S . In other words, $\wp(S) = \{x : x \subseteq S\}$.

Example 18. Compute $\wp(\emptyset)$ and $\wp(\{\emptyset\})$.

Solution. $\wp(\emptyset) = \{x : x \subseteq \emptyset\} = \{\emptyset\}$. $\wp(\{\emptyset\}) = \{x : x \subseteq \{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$. □

Definition 19. Let A and B be sets. The **Cartesian product** of A and B , $A \times B$, is defined by

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

Cartesian products can be generalized to more than two sets.

Definition 20. The **Cartesian product** of the sets A_0, A_1, \dots, A_n , $A_0 \times A_1 \times \dots \times A_n$, is defined by

$$A_0 \times A_1 \times \dots \times A_n = \{(a_0, a_1, \dots, a_n) : a_i \in A_i \text{ for } i = 0, 1, \dots, n\}$$

7. SET OPERATIONS

Definition 21. Let A and B be sets. The **union** of A and B , $A \cup B$, is the set containing elements from A or B .

$$A \cup B = \{x : x \in A \vee x \in B\}$$

Definition 22. Let A and B be sets. The **intersection** of A and B , $A \cap B$, is the set contains elements in both A and B .

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

As usual, we can generalize union and intersection as follows.

Definition 23. Let A_0, A_1, \dots, A_n be sets. Define

$$\bigcup_{i=0}^n A_i = A_0 \cup A_1 \cup \dots \cup A_n$$

and

$$\bigcap_{i=0}^n A_i = A_0 \cap A_1 \cap \dots \cap A_n.$$

| Identity | Name |
|--|---------------------|
| $A \cup \emptyset = A$ $A \cap U = A$ | Identity laws |
| $A \cup U = U$ $A \cap \emptyset = \emptyset$ | Domination laws |
| $A \cup A = A$ $A \cap A = A$ | Idempotent laws |
| $\overline{\overline{A}} = A$ | Complementation law |
| $A \cup B = B \cup A$ $A \cap B = B \cap A$ | Commutative laws |
| $A \cup (B \cap C) = (A \cup B) \cap C$ $A \cap (B \cup C) = (A \cap B) \cup C$ | Associative laws |
| $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ | Distributive laws |
| $\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$ | De Morgan's laws |
| $A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$ | Absorption laws |
| $A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$ | Complement laws |

FIGURE 6. Set Identities

Remark. In fact, we can do a little better. Let I be a set (not necessarily finite). Suppose we have a set A_i for each $i \in I$. Then

$$\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ for some } i \in I\}$$

and

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for all } i \in I\}.$$

Definition 24. Two sets are **disjoint** if their intersection is the empty set.

Definition 25. Let A and B be sets. The **difference** of A and B , $A - B$, is the set contains elements in A but not in B .

$$A - B = \{x : x \in A \wedge x \notin B\}$$

Definition 26. Let U be the universal set. The **complement** of the set A , \overline{A} or A^c , is the complement of A with respect to U .

$$\overline{A} = U - A$$

Figure 6 shows some useful set identities.

Example 19. Let A , B and C be sets. Show $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$.

Solution. $\overline{A \cup (B \cap C)} = \overline{A} \cap \overline{(B \cap C)} = \overline{A} \cap (\overline{B} \cup \overline{C}) = (\overline{B} \cup \overline{C}) \cap \overline{A} = (\overline{C} \cup \overline{B}) \cap \overline{A}$. \square

8. FUNCTIONS

Definition 27. Let A and B be sets. A **function** f from A to B , $f : A \rightarrow B$, is an assignment of exactly one element of B to each element of A . Sometimes, we say f **maps** A to B as well.

Definition 28. Let A and B be sets and $f : A \rightarrow B$. We say A is the **domain** of f and B is the **codomain** of f . If $f(a) = b$, we say b is the **image** of a and a is a **preimage** of b . The **range** of f is the set of all images of elements of A .

$$\begin{array}{l}
(1a) \quad \lfloor x \rfloor = n \text{ if and only if } n \leq x < n + 1 \\
(1b) \quad \lceil x \rceil = n \text{ if and only if } n - 1 < x \leq n \\
(1c) \quad \lfloor x \rfloor = n \text{ if and only if } x - 1 < n \leq x \\
(1d) \quad \lceil x \rceil = n \text{ if and only if } x \leq n < x + 1 \\
\hline
(2) \quad x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1 \\
\hline
(3a) \quad \lfloor -x \rfloor = -\lceil x \rceil \\
(3b) \quad \lceil -x \rceil = -\lfloor x \rfloor \\
\hline
(4a) \quad \lfloor x + n \rfloor = \lfloor x \rfloor + n \\
(4b) \quad \lceil x + n \rceil = \lceil x \rceil + n
\end{array}$$

where $x \in \mathbb{R}$ and $n \in \mathbb{Z}$

FIGURE 7. Properties of Floor and Ceiling Functions

Definition 29. Let f and g be functions from A to \mathbb{R} . Then

$$\begin{aligned}
(f + g)(x) &= f(x) + g(x) \\
(fg)(x) &= f(x)g(x) \\
(f \circ g)(x) &= f(g(x))
\end{aligned}$$

Definition 30. Let f be a function from A to B and $S \subseteq A$. The **image** of S , $f(S)$, is defined by

$$f(S) = \{f(s) : s \in S\}.$$

Definition 31. A function $f : A \rightarrow B$ is said to be **one-to-one**, or **injective**, if and only if $f(x) = f(y)$ implies $x = y$.

A function $f : A \rightarrow B$ is said to be **onto**, or **surjective**, if and only if for any $b \in B$ there is an $a \in A$ such that $f(a) = b$.

A function f is a **one-to-one correspondence**, or a **bijection**, if it is both injective and surjective.

Definition 32. A function f whose domain and codomain are subsets of \mathbb{R} is called **strictly increasing** if $f(x) < f(y)$ whenever $x < y$. f is called **strictly decreasing** if $f(x) > f(y)$ whenever $x < y$.

Definition 33. Let $f : A \rightarrow B$ be a bijection. The **inverse function** of f , f^{-1} , is a function from B to A such that $f^{-1}(b) = a$ when $f(a) = b$.

Remark. Is f^{-1} well-defined? That is, is it a function?

Definition 34. The **floor function** $\lfloor x \rfloor$ assigns the largest integer that is less than or equal to x . The **ceiling function** $\lceil x \rceil$ assigns the smallest integer that is greater than or equal to x .

Figure 7 shows some properties of floor and ceiling functions.

Example 20. Let $x \in \mathbb{R}$. Show $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Solution. Let $x = n + \epsilon$ where $n \in \mathbb{Z}$ and $0 \leq \epsilon < 1$. Then $n = \lfloor x \rfloor$. Consider the following two cases:

- $0 \leq \epsilon < \frac{1}{2}$. $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor$. Hence $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = 2n$. On the other hand, $\lfloor 2x \rfloor = \lfloor 2n + 2\epsilon \rfloor = 2n$ for $\epsilon < \frac{1}{2}$.
- $\frac{1}{2} \leq \epsilon < 1$. $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor + 1$. Hence $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = 2n + 1$. On the other hand, $\lfloor 2x \rfloor = \lfloor 2n + 2\epsilon \rfloor = 2n + 1$ for $\epsilon \geq \frac{1}{2}$.

□

Definition 35. The **factorial function** $n!$ is defined by

$$n! = 1 \cdot 2 \cdot \dots \cdot (n - 1) \cdot n.$$

9. SUPPLEMENTS

9.1. Russell's paradox. Consider the following statement: "The Serbian barber only shaves those who do not shave themselves." Now ask yourself: does the barber shave himself or not? There are only two cases: either he shaves himself, or he doesn't. Suppose he shaves himself. We are told that he does not shave those who shave themselves. Hence he does not shave himself. Now suppose he does not shave himself. We are told that he shaves

those who do not shave themselves. Hence he does shave himself. Both cases lead to contradiction. What's going on here?

The barber paradox is an intriguing question raised by philosophers. It seems like a tricky game of words. And nobody expects it would have anything to do with mathematics. However, Russell is able to exploit the idea and create a similar paradox in mathematics in 1903.

Consider the set

$$A = \{x : x \notin x\}.$$

Since $\emptyset \notin \emptyset$, we have $\emptyset \in A$. A does seem to make sense. Now, can you tell me whether $A \in A$?

Again, there are only two possibilities: either $A \in A$ or $A \notin A$. Suppose $A \in A$. Since any element x of A has the property that $x \notin x$, in particular $A \notin A$. A contradiction. On the other hand, suppose $A \notin A$. Then by the definition of A , $A \in A$. Another contradiction.

We can see the arguments of Russell's paradox are similar to those in barber's paradox. In both cases, we cannot tell the truth value of a proposition. In philosophy, it may be a game of language. But it is a serious matter in the foundation of mathematics.

Mathematicians now distinguish *small* from *large* sets. Mathematics is still good if we pay close attention to the collection of all sets (thus the name *large set*). In fact, Russell's paradox can be avoided if we do not allow the collection of all sets as the universe.

In computer science, you can also find similar argument. It is often used in proving negative results. Consider the question: what can't computers do? Of course, we know they can't do poetry, write novels, nor compose a sheet of music. What about a mathematical function? Is it always possible to write programs for arbitrary mathematical functions? The following example shows a mathematical problem (called the **halting problem**) which cannot be solved by computers.

Example 21. Write a program $T(P)$ which accepts program text P as input and returns 1 if P will terminate, 0 if not.

Solution. Suppose there is such a program T . Let us consider the following program M :

- (1) **program** M
- (2) **if** $T(M) = 1$ **then**
- (3) **while true do od**
- (4) **else** $\{T(M) = 0\}$
- (5) **exit**

What is $T(M)$? Suppose $T(M) = 1$, M terminates. Therefore $T(M) = 0$, or it would end in an infinite loop. On the other hand, suppose $T(M) = 0$, M does not terminate. Hence $T(M) = 1$ because this is the only case where M does not terminate. Both cases are contradiction. We conclude our assumption is incorrect. Hence T does not exist. \square

9.2. Cardinality of Infinite Sets. In Section §6, we define the cardinality of a finite set A to be the number of its distinct members. In this section, we'll briefly discuss the cardinalities of infinite sets.

For finite sets, we see that cardinality intuitively corresponds to the size of sets. If A and B are of the same size, we have $|A| = |B|$. For infinite sets, if there is a way to compare their sizes, we may define their cardinalities accordingly. The following definition provides a hint for comparing two infinite sets:

Definition 36. A set A is **countably infinite** if there is a bijection $f : \mathbb{N} \rightarrow A$. In this case, define the cardinality of A , $|A|$, to be \aleph_0 . A set A is **countable** if it is finite or countably infinite.

In other words, if there is a bijection from \mathbb{N} to A , we think \mathbb{N} and A are of the same size. For finite sets A and B , if there is a bijection from A to B , $|A| = |B|$. This corresponds to our intuition of cardinality for finite sets as well.

Example 22. Show the following sets are countably infinite: $\mathbb{N}, \mathbb{Z}^+, \mathbb{Z}, \mathbb{N} \times \mathbb{N}$.

Solution.

$f(n) = n$ is a bijection from \mathbb{N} to \mathbb{N} . Thus \mathbb{N} is countable. Similarly, $g(n) = n + 1$ is a bijection from \mathbb{N} to \mathbb{Z}^+ . $|\mathbb{Z}^+| = \aleph_0$.

Now consider the infinite sequence $0, 1, -1, 2, -2, 3, -3, \dots$. It is easy to see all integers appear in the sequence exactly once. One can define a bijection accordingly.

Similarly, consider the infinite sequence

$$(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), (3, 0), (2, 1), (1, 2), (0, 3), \dots$$

Each element of $\mathbb{N} \times \mathbb{N}$ appears in the sequence exactly once. The desired bijection can be constructed as well. \square

Surprisingly, $|\mathbb{N}| = |\mathbb{Z}| = \aleph_0$, although it looks like \mathbb{Z} has twice as many elements in \mathbb{N} . Here is an even more surprising theorem:

Theorem 4. \mathbb{Q} is countable.

In fact, we can construct a countable set out of several countable sets.

Theorem 5. A finite product of countable sets is countable.

Proof. (sketch) Let A_0, A_1, \dots, A_n be countable sets and $A = A_0 \times A_1 \times \dots \times A_n$. Then $A = (\dots((A_0 \times A_1) \times A_2) \times \dots \times A_n)$. \square

Theorem 6. A countable union of countable sets is countable.

Example 23. The following sets are countable:

- $\overbrace{\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}}^i$ for any finite $i > 0$;
- $\cup_{i=1}^n \overbrace{\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}}^i$ for any finite $n > 0$;
- $\cup_{i=1}^{\infty} \overbrace{\mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}}^i$;
- The set of all C programs.

We have seen many infinite sets so far. And they are all of the same cardinality of \mathbb{N} . Is there any set “larger” than \mathbb{N} ? Let us first define the following term:

Definition 37. A set which is not countable is said to be **uncountable**.

Theorem 7. Let \mathbb{B} be $\{F, T\}$. Then $A = \mathbb{B} \times \mathbb{B} \times \dots \times \mathbb{B} \times \dots$ is uncountable.

Proof. Suppose there is a bijection $f : \mathbb{N} \rightarrow A$. Let

$$f(i) = b_{i0}b_{i1} \dots b_{ij} \dots$$

Define

$$c_i = \begin{cases} F & \text{if } b_{ii} = T \\ T & \text{if } b_{ii} = F \end{cases}$$

Then $c \neq f(i)$ for all i . But $c \in A$, a contradiction. \square

This technique is first used by Cantor to prove that \mathbb{R} is uncountable. It is called *diagonalization*.

Theorem 8. \mathbb{R} is uncountable.

Surprisingly, we can construct not only infinite sets “larger” than \mathbb{N} , but also much more “larger” sets.

Theorem 9. Let A be a set. $|\wp(A)| > |A|$.

Therefore, $|\wp(\mathbb{R})| > |\mathbb{R}|$, $|\wp(\wp(\mathbb{R}))| > |\wp(\mathbb{R})|$, etc.