Problems on Discrete Mathematics[1]

Chung-Chih Li[2]
Kishan Mehrotra[3]

Syracuse University, New York

LaTeX at January 11, 2007

(Part I)

[2]cli2@ilstu.edu
[3]kishan@ecs.syr.edu

Preface

This is not so much a Preface as it is an explanation of why these notes were prepared in the first place. Year after year, students in CIS275 and CIS375 have commented that the text book was "poor", "useless", or "difficult to read" etc. It is our 'impression' that most of the students were lost in the details and were unable to decide what are the important definitions and results and how to apply these results to solve problems. In these notes we have attempted to summarize the important definitions and results. Neither we have given detailed explanations of the definitions nor we have proved all of the results; students are **strongly** urged to read the recommended text book.

Our main emphasis is to provide the student a large number of problems and their solutions. We expect that the students will attempt to solve the problems on their own and look at a solution only if they are unable to solve a problem.

These problems are collections of home works, quizzes, and exams over the past few years. Most of the problems are from *Discrete Mathematics with applications* by H. F. Mattson, Jr. (Wiley).

We hope that these notes will prepare a student to better understand basic mathematics necessary of computer scientists.

Acknowledgment

Our most sincere thanks to Elaine Weinman for her her help in typing several parts of these notes and, more importantly, for many editorial corrections.

Contents

Part I

Basic Concepts

Chapter 0

Preliminary

Perspicuity is part of proof

– Ludwig Wittgenstein

0.1 Conventions

N : The set of natural numbers, i.e., $\{1, 2, 3, \ldots\}$.

$\mathbf{N}^0$: $\mathbf{N} \cup \{0\}$.

Z : The set of integers.

Q : The set of rational numbers.

R : The set of real numbers.

0.2 Patterns of theorems and proof

1. Implication:

   Let $\mathcal{X}$ and $\mathcal{Y}$ be two mathematical statements.

   $$\text{If } \mathcal{X} \text{ then } \mathcal{Y}. \tag{1}$$

   In logic[1] we denote (1) as $\mathcal{X} \to \mathcal{Y}$. The meaning of (1) is: if the mathematical statement $\mathcal{X}$ is true, or the mathematical condition $\mathcal{X}$ holds, then the mathematical statement $\mathcal{Y}$ is true.

   To prove this kind of theorem, we first assume that the statement $\mathcal{X}$ is true. Then, we have to prove that the statement $\mathcal{Y}$ is a "logical" (informally, we say "reasonable") consequence of $\mathcal{X}$. If we are able to do so, then we can claim that the theorem (statement) (1) is correct.

2. Equivalence:

   Let $\mathcal{X}$ and $\mathcal{Y}$ be two mathematical statements.

   $$\mathcal{X} \text{ if and only if } \mathcal{Y} \tag{2}$$

   The meaning of (2) is:

   $$(\text{if } \mathcal{X} \text{ then } \mathcal{Y}) \text{ and } (\text{if } \mathcal{Y} \text{ then } \mathcal{X}).$$

   In logic we denote (2) as $\mathcal{X} \leftrightarrow \mathcal{Y}$, which is equivalent to

   $$(\mathcal{X} \to \mathcal{Y}) \wedge (\mathcal{Y} \to \mathcal{X}).$$

   To prove that "$\mathcal{X}$ if and only if $\mathcal{Y}$" is true, we have to prove that "if $\mathcal{X}$ then $\mathcal{Y}$" and "if $\mathcal{X}$ then $\mathcal{Y}$" are both true. Many textbooks used " *iff* " or " $\Longleftrightarrow$ " to denote "if and only if".

[1] Refer to the logic chapter.

3. Disproving:

   Given a mathematical theorem as (1), if we can find an example for $\mathcal{X}$ and $\mathcal{Y}$ such that this example makes $\mathcal{X}$ to be true but $\mathcal{Y}$ to be false, then we can claim that the theorem is incorrect. For example,

   $$\text{if } x^2 > 0 \text{ then } x > 0$$

   is incorrect. Because we can find -1 such that $(-1)^2 > 0$ is true but $-1 < 0$. Such examples are called counter examples.

4. Proving by contradiction:

   This is an important technique for proving mathematical results. Suppose a theorem is given as (1). The idea of proving by contradiction is: we first assume that the theorem is wrong, i.e., we can have instances that make $\mathcal{X}$ true and $\mathcal{Y}$ false. Then we argue that, if this is the case, we can lead to a result showing that $\mathcal{X}$ is false. But the result contradicts our assumption that $\mathcal{X}$ is true. Therefore, the assumption will never happen, and hence the theorem is correct.

   For example, consider

   $$\text{if } x + 1 > 2 \text{ then } x > 1.$$

   To prove it by contradiction, we assume that there is an x such that, $x + 1 > 2$ and $x \leq 1$. From the assumption $x \leq 1$, we have

   $$\begin{aligned} x \leq 1 &\Rightarrow x + 1 \leq 1 + 1 \\ &\Rightarrow x + 1 \leq 2. \end{aligned}$$

   The result $x + 1 \leq 2$ contradicts the assumption $x + 1 > 2$. Therefore, the assumption will never happen, and hence the theorem is correct.

5. Proving by cases:

   Suppose we are given a theorem with respect to the domain D. If possible, we exhaust all of the examples in the domain to see if the theorem is correct. But, in general, we are not able to do so because the domain is usually an infinite set, and even worse, the domain can be *uncountable*, e.g., real numbers. To overcome this problem, we divide the domain into several categories and make sure that those categories cover the domain. Then we exam each case to see if the theorem is valid. If the theorem holds in every case, then the theorem is correct in the entire domain. Note that we must use the idea of universal generalization[2] in the proof of each case.

[2] See the logic chapter for more details.

Chapter 1

Sets

One can always make a theory, many theories,
to account known facts,
occasionally to predict new ones.
The test is aesthetic.

– Gorge Thomson

1.1 Definitions and Basic Theorems

Set theory is one of the most rigorous study in mathematics. In fact, the desire to advance the modern set theory had been the desire of mathematicians who wanted to pursue ultimate rigorousness in mathematics. Although the results of securing our mathematical foundations turn out to be rather negative and we are unfortunately in a loosing battle, the concept of sets and the notations used in this battle are proven to be a indispensable tool in the study of mathematics at any level.

Of course, we will not step into the dark side of the road in this book. In stead, we will study some naive concepts of sets; most of them are intuitively understandable from our daily-life experiences. For example, all students of Syracuse University is a set; all students in the United State of America is a *superset* of the set of students at Syracuse University. Since Dennis is a student at Syracuse University, he is a member of the set of the students of Syracuse university. Some students of Syracuse University are also students of Cornell University, but none of them are students of Stanford University...., and so on. Some of the sentences above are a bit awkward, but we live with them without too many complains. However, when mathematicians come along, they have to deal with mathematical objects that very often have to carry some relations that are much more complicate than the descriptions we used in the sentences above. Fortunately, the concepts and some immediate properties in the set theory provide us a simple yet precise notation to simplify our works.

In addition to letting the reader be familiar with the basic terminologies and properties of sets, another purpose of this chapter is to let the reader be used to rigorous mathematical arguments by getting through the proofs step by step.

1.1.1 Definitions

Definition 1.1: A set S is a collection of *distinct* objects without regard to the order of the objects given by any possible method of description. Usually, we use a pair of braces, $\{\}$, to enclose the concerned collection.

Definition 1.2: The empty set is a null collection, denoted as $\emptyset$ or $\{\}$.

Definition 1.3: The *universal* set is the set that contains everything concerned, usually denoted as U. In general, the context of the problem determines U.

Definition 1.4: The objects in a set S are called the *members* of S. Some textbooks use *elements* instead.

Definition 1.5: Suppose a is a member of a set S. We denote this property as $a \in S$. The property is known as the *membership relation*.

Definition 1.6: Let A, B be sets. A is a subset of B if and only if all members of A are members of B. We use $A \subseteq B$ to denote that A is a subset of B. If $A \neq B$, we say that A is a *proper subset* of B, denoted as $A \subset B$.

Definition 1.7: Let A, B be sets. The *intersection* of A and B, denoted as $A \cap B$, is the set C such that every member of C is a member of both A and B. In logic this set is defined as

$$A \cap B = \{x | x \in A \ \& \ x \in B\}.$$

Definition 1.8: Let A, B be sets. If $A \cap B = \emptyset$, we say that A and B are *disjoint*.

Definition 1.9: Let A, B be sets. The *union* of A and B, denoted as $A \cup B$, is the set C such that every member of C is a member of either A or B. In logic this set is defined as

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

Definition 1.10: Let A, B be sets. The set $A - B$ is defined as

$$A - B = \{x | x \in A \ \& \ x \notin B\}.$$

Definition 1.11: Let A, B be sets. The *Cartesian product* of A and B, denoted as $A \times B$, is defined as

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

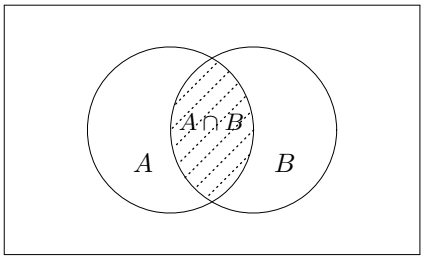
Definition 1.12: Let S be any set, the cardinality of S, denoted as $|S|$, is the number of elements in S[1].

Definition 1.13: Let U be the universal set and A any set in the universe. Define

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

$\overline{A}$ is called the *complement* of A.

Definition 1.14: The Venn diagram consists of figures that show the relations between sets. Example:



Venn Diagram

[1]This naive definition is sufficient for our purpose set up in this book. And, it is intuitively understandable for finite sets. A more serious mathematical setup is needed to understand the cardinality of an infinite set, but that is far beyond the scope of this book.

Definition 1.15: Let A be any set. The *power set* of A, denoted as $\mathbf{Pr}(A)$, is the set of all possible subsets of A. In symbols,

$$\mathbf{Pr}(A) = \{S | S \subseteq A\}.$$

1.1.2 Basic Theorems

The following list contains the most important theorems that are used in many mathematical proofs. We do not prove them here, but ask them as problems in the problem section and prove them in the solution section.

Theorem 1.1: Let A be a set.

$$A \cup \emptyset = A; \quad A \cap \emptyset = \emptyset.$$

Theorem 1.2: Let A be a set.

$$A \cup A = A \cap A = A.$$

Theorem 1.3: Let A, B be sets.

$$A = B \text{ if and only if } (A \subseteq B \ \& \ B \subseteq A).$$

Theorem 1.4: Let A, B, C be sets.

$$\text{If } (A \subseteq B \ \& \ B \subseteq C), \text{ then } A \subseteq C.$$

Theorem 1.5: Let A, B be sets,

$$A \subseteq A \cup B, \quad B \subseteq A \cup B,$$
$$A \cap B \subseteq A, \quad A \cap B \subseteq B.$$

Theorem 1.6: The commutative rules: Let a, b be sets.

$$A \cup B = B \cup A,$$
$$A \cap B = B \cap A.$$

Theorem 1.7: The associative rules: Let A, B, C be sets.

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

Theorem 1.8: The distribution rules: Let A, B, C be sets.

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

Theorem 1.9: De Morgan's laws: Let A, B be sets.

$$\overline{A \cup B} = \overline{A} \cap \overline{B},$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Theorem 1.10: Let A, B be two infinite sets. $|A| = |B|$ if and only if there exists a bijection[2] $f : A \to B$.

[2]For the definition of bijection, please refer to chapter 5.

1.2 Problems

Problem 1: Determine if each of the following objects is a member of $\mathbf{Z}$; $\{5\}$, $\{3,-1\}$, 7.12, $\sqrt{5}$, $a =$ the $2{,}00^{th}$ decimal digit in the base-10 expression for π.

Problem 2: Let A be the set of digits in the base-10 expression of the rational number $\frac{41}{333}$. Let B be the same for $\frac{44}{333}$. Prove that $A = B$.

Problem 3: Prove or disprove: the set C of digits in the base-10 expression of

$$\frac{40363\ 63637}{3\ 33000\ 00000}$$

equals the set A of the previous problem.

Problem 4: Define sets

$$\begin{aligned} A &= \{1, \{4\}, \{2\}, 3, 4, 5\}, \\ B &= \{\{\{1, 4, 5, 3, 1\}\}\}, \\ C &= \{1, \{3\}, 2, 1\}, \\ D &= \{1, 1, 3\}, \\ E &= \{1, 4, \{5\}, \{3\}\}, \\ F &= \{1, 8, \{1, 2, 3, 4\}\}, \end{aligned}$$

and,

$$a_1 = 1, a_2 = \{2\}, a_3 = \{2, 1\}, a_4 = \{2, 1, 3, 4\}, a_5 = \{3, 1, 5\}.$$

For each of $a_1, \ldots, a_5$, determine if it is a member of the sets $A, \ldots, F$ respectively. Present your answer in the following table:

	A	B	C	D	E	F
a_1						
a_2						
a_3						
a_4						
a_5						

Use an "$\in$" to stand for membership and a blank to stand for nonmembership.

Problem 5: Define A, B, C, D, E, and F as in Problem 4. Calculate the following sets.

$A \cap C$ $\quad$ $B \cap F$ $\quad$ $D \cup C$ $\quad$ $C \cap E$ $\quad$ $C \cup (D \cap F)$ $\quad$ $A \cap E$.

Problem 6: Define

$$U = \{3, 1, 3, 2\},$$
$$V = \{1, 3, \{1, 3\}, \{1, 2, 3\}\}.$$

Is $U \in V$? Is $U \subseteq V$?

Problem 7: Let A and B be sets. If $A \subset B$, what does that tell you about $A \cap B$ and $A \cup B$?

Problem 8: Let A, B and S be sets. If $A \subset S$ and $B \subset S$, what can you say about $A \cup B$?

Problem 9: Find the cardinality of the set

$$S = \{p/q \mid p, q \in N^+, p, q, \leq 10\}.$$

Problem 10: List all the subsets of

$$\{1, 2, \{b\}\}.$$

Problem 11: List all the elements of

$$\{b, c, d\} \times \{e, o\}.$$

Problem 12: Describe all sets that have no proper subsets.

Problem 13: Let A, B, C be sets. Suppose that A is a subset of B, and C is a proper subset of B. Is A a proper subset of C?

Problem 14: Let A and B be any sets. From the definition of union it follows that

$$\text{if } x \in A \cup B, \text{ then } x \in A \text{ or } x \in B.$$

Consider now the analogue for inclusion. Can we say that for any set X,

$$\text{if } X \subseteq (A \cup B), \text{ then } X \subseteq A \text{ or } X \subseteq B?$$

Why or why not?

Problem 15: Prove or disprove that

$$\text{if } (A \cup B) \subseteq (A \cap B), \text{ then } A = B.$$

Problem 16: Let A, B, C be sets. Prove the distributive laws:

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
2. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Problem 17: Let A, B be sets. Prove the De Morgan laws:

1. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

2. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Problem 18: Let A, B, C be sets. Prove

$$A - B = A \cap \overline{B}.$$

Problem 19: Let A, B, C be sets. Prove

$$A - (A - B) = A \cap B.$$

Problem 20: Let A, B, C be sets. Prove

$$A \cap B = \emptyset \quad \text{if and only if} \quad A \subseteq \overline{B}.$$

Problem 21: Let $A \cap B = \emptyset$. Show that

$$A \cap \overline{B} = A.$$

Problem 22: Define the symmetric difference of sets A, B as

$$A \triangle B := (A - B) \cup (B - A).$$

Prove that symmetric difference is associative and commutative. Also prove that for all sets A

$$A \triangle A = \emptyset.$$

Problem 23: Let A, B be sets. Use Venn diagrams to show that

$$A \subseteq B \text{ if and only if } A \cap B = A.$$

Problem 24: Let A, B, C be any sets. Use

1. Venn diagrams,
2. set algebra, and
3. epsilon-argument,

respectively, to prove that

$$B - C \subseteq \overline{A} \text{ if and only if } A \cap B \subseteq C.$$

Problem 25: Let $A := \{\alpha, 4\}$ and $B := \{a, 3\}$. List the elements of $A \times B$.

Problem 26: Let A, B, and C be any sets. Show that

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

Problem 27: Let A, B be sets. Prove or disprove that

$$\text{if } (A \times A) = (B \times B), \text{ then } A = B.$$

Problem 28: Let A, B, U, and V be any sets such that $A \subseteq U$ and $B \subseteq V$. Is the following correct? Explain.

$$(A \times B) \subseteq (U \times V).$$

Problem 29: Let A, B, C be sets. Prove

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

Problem 30: Let A, B be sets, and $C := A \cup B$. Use the result in Problem 29 to prove that

$$A \times B \subseteq A \times C \subseteq C \times C.$$

Problem 31: Let A be a set. Define

$$\text{diagonal of } A \times A := \{(a, a) | a \in A\}.$$

Suppose $A \subseteq B$. Prove or disprove the following identities.

1. $(A \times B) \cap (B \times A) = B \times B$.
2. (the diagonal of $A \times A$) $\cap$ $(A \times B)$ = the diagonal of $B \times B$.

Problem 32: Let $X = \{1, 2, 3, a\}$. List the elements of $\mathcal{P}(X)$.

Problem 33: Let X be the set $\{1, 2, 3, 4, 5, 6, \{1\}\}$. Find Y such that

$$Y = X \cup (X \cap \mathcal{P}(X)).$$

Problem 34: List the elements of the following sets.

1. $\mathcal{P}(\emptyset)$
2. $\mathcal{P}(\{\emptyset\})$
3. $\mathcal{P}(\mathcal{P}(\emptyset))$
4. $\{\emptyset\} \times \mathcal{P}(\emptyset)$
5. $\emptyset \times \mathcal{P}(\emptyset)$
6. $\mathcal{P}(\emptyset) \times \mathcal{P}(\emptyset)$

Problem 35: List the elements of $A \times \mathcal{P}(A)$, where $A = \{a, 1\}$.

Problem 36: Let A, B be sets. Prove

$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B).$$

Problem 37: Prove or disprove that

$$\text{if } \ A \in \mathcal{P}(B) \ \& \ B \in \mathcal{P}(A), \ \text{ then } \ A = B.$$

Problem 38: Let A be the set of nonnegative integers and B the set of nonnegative odd integers. Prove that the cardinality of A is equal to the cardinality of B. [See Theorem 1.10 on page 12]

Problem 39: Prove that for any set A, $|A| < |\mathbf{Pr}(A)|$.

1.3 Solutions

Solution 1:

1. $\{5\} \notin \mathbf{Z}$; $\{5\}$ is a set, although the set happens to contain an integer.

2. $\{3, -1\} \notin \mathbf{Z}$; $\{3, -1\}$ is a set not an integer.

3. $7.12 \notin \mathbf{Z}$.

   Note: One should not say that 7.12 is a real number, thus $7.12 \notin \mathbf{Z}$. A number that is real does not mean it cannot be an integer. Don't forget that $\mathbf{Z} \subset \mathbf{R}$. That means all integers are also real numbers.

4. $\sqrt{5} \notin \mathbf{Z}$.

   Note: One should not have a problem in pointing out that $\sqrt{5} \notin \mathbf{Z}$. The reason is that the value of $\sqrt{5}$ is not an integer, and that is. We cannot conclude that the operator $\sqrt{\ }$ will result in a number that is not an integer on any input. For example, $\sqrt{4} \in \mathbf{Z}$. In some computer programming languages, the data type of $\sqrt{4}$ may be real causing the confusion. But in mathematics, $\sqrt{4}$ is an integer; it does not matter how computers treat it.

5. Whatever the number a might be, we are sure that a is an integer, thus $a \in \mathbf{Z}$.

□

Solution 2:

$$\frac{41}{333} = 0.\overline{123}, \text{ and } \frac{44}{333} = 0.\overline{132},$$

where a bar means the integers are repeated in that order forever. Thus,

$$A = \{0, 1, 2, 3\}, \text{ and } B = \{0, 1, 2, 3\}.$$

Therefore, $A = B$. □

Solution 3: We patiently divide to get:

$$\frac{4036363637}{33300000000} = 0.12121212\overline{123}.$$

Thus, $C = \{0, 1, 2, 3\}$. Therefore, $A = C$. □

Solution 4:

	A	B	C	D	E	F
a_1	$\in$		$\in$	$\in$	$\in$	$\in$
a_2	$\in$					
a_3						
a_4						$\in$
a_5						

The set A has six members: 1, $\{4\}$, $\{2\}$, 3, 4, and 5. Only a_1 and a_2 are elements of A.

The set B has only one member, that is $\{\{1, 3, 4, 5\}\}$.

Let's take another example. F contains 3 elements: $1, 8$ and $\{1, 2, 3, 4\}$. Thus, a_1 and a_4 are elements in F. Note that $2 \notin F$ although $2 \in \{1, 2, 3, 4\}$ and $\{1, 2, 3, 4\} \in F$. This example shows that $\in$ is not transitive[3]. □

Solution 5:

1. $A \cap C = \{1\}$.
2. $B \cap F = \emptyset$.
3. $D \cup C = \{1, 2, 3\{3\}\}$.
4. $C \cap E = \{1, \{3\}\}$.
5. $C \cup (D \cap F) = \{1, 2, \{3\}\}$.
6. $A \cap E = \{1, 4\}$.

□

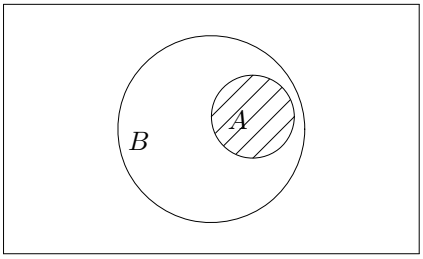
[3]See chapter 4 for the transitivity

Solution 6: Define

$$U = \{3, 1, 3, 2\}$$
$$V = \{1, 3, \{1, 3\}, \{1, 2, 3\}\}.$$

Since we do not consider multiset, thus $U := \{1, 2, 3\}$. Therefore, U is a member of V. However, U is not a subset of V because $2 \in U$, but $2 \notin V$. □

Solution 7: Since $A \subset B$, we obtain the following Venn diagram.



It is clear that $A \cap B = A$ and $A \cup B = B$. □

Solution 8: We can answer this problem by using Venn diagrams, but we have to draw Venn diagrams that cover all possible cases of A and B to make the proof complete.

Let us use another kind of argument for this problem. Two conditions are given, i.e.,

$$A \subset S, \tag{1.1}$$
$$B \subset S. \tag{1.2}$$

Given $x \in A \cup B$. From the definition of union, we have two cases: x is either in A or in B.

Case 1: $x \in A$. Because $A \subset S$, we know $x \in S$.

Case 2: $x \in B$. Because $B \subset S$, we know $x \in S$.

In either case, we conclude that $x \in S$. Therefore, by the definition of $\subseteq$, we have $A \cup B \subseteq S$.

Can we claim that $A \cup B$ is a proper subset of S? The answer is that we cannot. From (1.1) and (1.2), we know only that there is at least one element $x \in S$ such that $x \notin A$, and there is at least one element $y \in S$ such that $y \notin B$, but we don't know if $x = y$. To see this, consider

$$A = \{1\},\ B = \{2\},\ \text{and } S = \{1, 2\}.$$

It is clear that $A \subset S, B \subset S$, and $A \cup B = S$.

In some textbooks the argument used above is called the $\in$-argument, because the above proof procedure is based on the properties of the membership of elements to sets. □

Solution 9: Find the cardinality of the set,

$$S = \{p/q \mid p, q \in N^+, p, q, \leq 10\}.$$

The cardinality of a finite set is simply the number of distinct elements of the set; we do not consider *multisets*. In other words, all identical elements are counted as one. For example, 1/2, 2/4, 3/6, 4/8, and 5/10 are the same element.

In this example, we can list all p/q, remove extra identical elements, and count the remaining. The cardinality of S is 63. □

Solution 10: The subsets of $\{1, 2, \{b\}\}$ are

$$\emptyset, \{1\}, \{2\}, \{\{b\}\}, \{1, 2\}, \{1, \{b\}\}, \{2, \{b\}\}, \{1, 2, \{b\}\}.$$

Remember that the empty set and $\{1, 2, \{b\}\}$ itself are both subsets of the given set. □

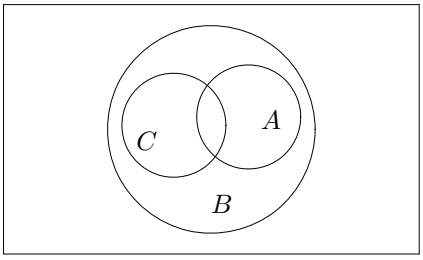
Solution 11:

$$\{b, c, d\} \times \{e, o\} = \{(b, e), (c, e), (d, e), (b, o), (c, o), (d, o)\}.$$

□

Solution 12: The empty set is the only set that has no proper subset. □

Solution 13: The statement is wrong. The following Venn diagram disproves the statement.



$A \subseteq B$

$C \subset B$

$A \not\subset C$

The best way to disprove a theorem is to give a counter example. For example, let

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

It is easy to see that, $A \subseteq B, C \subset B$, but $A \not\subset C$.

The easiest counter example is when $A = C = \emptyset$ and B is any non-empty set. In this case, $A \subseteq B, C \subset B$, but A is not a proper subset of C. □

Solution 14: The following statement is incorrect.

$$\text{If } X \subseteq (A \cup B), \text{ then } X \subseteq A \text{ or } X \subseteq B.$$

We can give a counter example to disprove the statement.

Let $A = \{1\}, B = \{2\}$, and $X = \{1, 2\}$. It is clear that $X \subseteq (A \cup B)$, but neither $X \subseteq A$ nor $X \subseteq B$. □

Solution 15: For any two sets A and B,

$$\text{if } (A \cup B) \subseteq (A \cap B), \text{ then } A = B. \tag{1.3}$$

We assume that

$$(A \cup B) \subseteq (A \cap B). \tag{1.4}$$

Then ask: "Is A equal to B?"

To prove $A = B$, we may prove that $A \subseteq B$ and $B \subseteq A$.

1. To prove $A \subseteq B$, assume $x \in A$.

$$\begin{array}{rcll} x \in A & \Rightarrow & x \in A \cup B & \text{def. of union;} \\ & \Rightarrow & x \in A \cap B & \text{(1.4) and the def. of subset;} \\ & \Rightarrow & x \in B & \text{def. of intersection.} \end{array}$$

   Therefore, $A \subseteq B$.

2. Similarly, to prove $B \subseteq A$, let $x \in B$.

$$\begin{array}{rcll} x \in B & \Rightarrow & x \in A \cup B & \text{def. of union;} \\ & \Rightarrow & x \in A \cap B & \text{(1.4) and the def. of subset;} \\ & \Rightarrow & x \in A & \text{def. of intersection.} \end{array}$$

   Therefore, $B \subseteq A$.

From 1 and 2 above, we conclude that $A = B$. □

Method 2:

We can use another way to prove $A = B$ under the same condition given in (1.4). Let us recall the following basic theorems: For any sets A, B and C,

1. $A \cap B \subseteq A$.
2. $A \subseteq A \cup B$.
3. $A \subseteq B \subseteq C \;\Rightarrow\; A \subseteq C$.

Thus,

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

And, since $(A \cup B) \subseteq (A \cap B)$ is given, we have

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

Therefore, $A \subseteq (A \cup B)$ and $(A \cup B) \subseteq A$, hence $A = A \cup B$. Similarly, $B = A \cup B$. Therefore, $A = B$. □

Method 3:

We can also prove (1.3) by way of contradiction, a very important technique for mathematical reasoning. Mathematicians use this technique very often.

Suppose that

$$(A \cup B) \subseteq (A \cap B), \text{ and } A \neq B.$$

Without loss of generality, we assume that $A \not\subseteq B$[4]. That is, there is an element a in A but not in B. We know that $a \in A \cup B$ and $a \notin A \cap B$. From the definition of subset, we have

$$A \cup B \not\subseteq A \cap B,$$

which contradicts the assumption that $(A \cup B) \subseteq (A \cap B)$. Hence, $A \subseteq B$ must be true. □

Solution 16: Let A, B, C be sets.

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

   (a) To show that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$, suppose $x \in A \cup (B \cap C)$. We have two cases:

   Case 1: $x \in A$. If $x \in A$, then $x \in (A \cup B)$ and $x \in (A \cup C)$. Thus, $x \in (A \cup B) \cap (A \cup C)$.

   Case 2: $x \in (B \cap C)$. If $x \in (B \cap C)$, then $x \in B$ and $x \in C$. Thus, $x \in (A \cup B) \cap (A \cup C)$.

   Therefore, in either case we have $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

   (b) To show that $A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$, suppose $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. We have two cases:

   Case 1: $x \in A$. If $x \in A$, then $x \in A \cup (B \cap C)$.

   Case 2: $x \notin A$. If $x \notin A$, then x must be in B and C, because from the assumption $x \in A \cup B$ and $x \in A \cup C$. Thus, $x \in B \cap C$, and hence $x \in A \cup (B \cap C)$.

   In either case we have $A \cup (B \cap C) \supseteq (A \cup B) \cap (A \cup C)$.

   Therefore,

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

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

[4]The other case is: $A \not\subseteq B$. For this case, the argument is symmetric to the one we give, and there is no need to repeat it again. This is the reason we can say "without loss of generality"

(a) To show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$, suppose $x \in A \cap (B \cup C)$.

$$x \in A \cap (B \cup C) \Rightarrow x \in A \text{ and } x \in (B \cup C).$$

From the definition of union, $x \in (B \cup C)$ gives two cases:

Case 1: $x \in B$. If $x \in B$, then $x \in (A \cap B)$.

Case 2: $x \in C$. If $x \in C$, then $x \in (A \cap C)$.

Thus, $x \in (A \cap B) \cup (A \cap C)$. .

(b) To show that $A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$, suppose $x \in (A \cap B) \cup (A \cap C)$. We have two cases.

Case 1: $x \in A \cap B$. If $x \in A \cap B$, then $x \in A$ and $x \in B$. Because $x \in B$, x must be in $B \cup C$. Therefore, $x \in A \cap (B \cup C)$.

Case 2: $x \in A \cap C$. If $x \in A \cap C$, then $x \in A$ and $x \in C$. Because $x \in C$, x must be in $B \cup C$.

In either case, $x \in A \cap (B \cup C)$.

Therefore, by putting (a) and (b) together, we have

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

□

Solution 17: Let A, B be sets. Prove

1. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

   (a) Let $x \in \overline{A \cup B}$.

   $$\begin{aligned} x \in \overline{A \cup B} &\Rightarrow x \notin A \cup B, \\ &\Rightarrow x \notin A \text{ and } x \notin B, \\ &\Rightarrow x \in \overline{A} \text{ and } x \in \overline{B}, \\ &\Rightarrow x \in \overline{A} \cap \overline{B}. \end{aligned}$$

   (b) Let $x \notin \overline{A \cup B}$.

   $$\begin{aligned} x \notin \overline{A \cup B} &\Rightarrow x \in A \cup B, \\ &\Rightarrow x \in A \text{ or } x \in B, \\ &\Rightarrow x \notin \overline{A} \text{ or } x \notin \overline{B}, \\ &\Rightarrow x \notin \overline{A} \cap \overline{B}. \end{aligned}$$

   Therefore, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

2. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

(a) Let $x \in \overline{A \cap B}$.

$$\begin{aligned} x \in \overline{A \cap B} &\Rightarrow x \notin A \cap B, \\ &\Rightarrow x \notin A \text{ or } x \notin B, \\ &\Rightarrow x \in \overline{A} \text{ or } x \in \overline{B}, \\ &\Rightarrow x \in \overline{A} \cup \overline{B}. \end{aligned}$$

(b) Let $x \notin \overline{A \cap B}$.

$$\begin{aligned} x \notin \overline{A \cap B} &\Rightarrow x \in A \cap B, \\ &\Rightarrow x \in A \text{ and } x \in B, \\ &\Rightarrow x \notin \overline{A} \text{ and } x \notin \overline{B}, \\ &\Rightarrow x \notin \overline{A} \cup \overline{B}. \end{aligned}$$

Therefore, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

□

Solution 18: Let A, B, and C be sets. We want to prove

$$A - B = A \cap \overline{B}.$$

From the definition, $A - B$ is the set of all elements in A but not in B. Thus, if $x \in A - B$, then $x \in A$ and $x \notin B$, namely, $x \in A$ and $x \in \overline{B}$. From the definition of intersection, $x \in A \cap \overline{B}$. Therefore,

$$A - B \subseteq A \cap \overline{B}. \tag{1.5}$$

For the other direction, if $x \in A \cap \overline{B}$, then $x \in A$ and $x \in \overline{B}$, namely $x \in A$ and $x \notin B$, thus $x \in A - B$. Therefore,

$$A \cap \overline{B} \subseteq A - B. \tag{1.6}$$

From (1.5) and (1.6), we have

$$A - B = A \cap \overline{B}. \tag{1.7}$$

□

Solution 19: Let A, B, and C be sets. To prove

$$A - (A - B) = A \cap B,$$

we will use the equality (1.7).

Let us start from the left-hand side,

$$\begin{aligned} A-(A-B) &= A-\overline{(A\cap\overline{B})}, && \text{from (1.7)}\\ &= A\cap(A\cap\overline{B}), && \text{from (1.7)}\\ &= A\cap(\overline{A}\cup B), && \text{De Morgan law}\\ &= (A\cap\overline{A})\cup(A\cap B), && \text{distributive law}\\ &= \emptyset\cup(A\cap B),\\ &= A\cap B. \end{aligned}$$

Therefore, the left-hand side is equal to the right-hand side. □

Solution 20: Let A, B, and C be sets. To prove that $A\cap B=\emptyset$ if and only if $A\subseteq\overline{B}$, we split our task into two subtasks.

1. The first subtask is to prove that $A\cap B=\emptyset \;\Rightarrow\; A\subseteq\overline{B}$.

   By way of contradiction, suppose

   $$A\cap B=\emptyset \text{ and } A\not\subseteq\overline{B}.$$

   If $A\not\subseteq\overline{B}$, we can find an x, such that $x\in A$ and $x\notin\overline{B}$. But,

   $$\begin{aligned} x\in A, x\notin\overline{B} &\Rightarrow x\in A \;\&\; x\in B,\\ &\Rightarrow x\in A\cap B,\\ &\Rightarrow A\cap B\neq\emptyset. \end{aligned}$$

   This leads to a contradiction.

2. Our second subtask is to prove that $A\subseteq\overline{B} \;\Rightarrow\; A\cap B=\emptyset$.

   Again, by way of contradiction, suppose

   $$A\subseteq\overline{B} \text{ and } A\cap B\neq\emptyset.$$

   If $A\cap B\neq\emptyset$, there exists an x such that, $x\in A\cap B$. But,

   $$\begin{aligned} x\in A\cap B &\Rightarrow x\in A \;\&\; x\in B,\\ &\Rightarrow x\in A \;\&\; x\notin\overline{B},\\ &\Rightarrow A\not\subseteq\overline{B}. \end{aligned}$$

   This leads to a contradiction.

From 1 and 2, we have proved

$$A\cap B=\emptyset \iff A\subseteq\overline{B}.$$

□

Solution 21: Suppose $A \cap B = \emptyset$. Given any x, we have

$$\begin{array}{rcll} x \in A & \Rightarrow & x \notin B & \text{because } A \cap B = \emptyset \\ & \Rightarrow & x \in \overline{B} & \\ & \Rightarrow & x \in (A \cap \overline{B}) & \\ & \Rightarrow & A \subseteq (A \cap \overline{B}) & \text{def. of subset.} \end{array}$$

From the property of intersection of two sets, we have $(A \cap \overline{B}) \subseteq A$. Thus, $(A \cap \overline{B}) = A$. □

Solution 22: Define

$$A \triangle B := (A - B) \cup (B - A).$$

Because $\cup$ is commutative, thus $(A-B)\cup(B-A) = (B-A)\cup(A-B) = B \triangle A$. Hence $\triangle$ is commutative.

Before proving the associativity of $\triangle$, let us prove an intermediate result:

$$\overline{A \triangle B} = (A \cap B) \cup (\overline{A} \cap \overline{B}). \tag{1.8}$$

Recall equation (1.7), we know that $A - B = A \cap \overline{B}$. Therefore, we can rewrite $A \triangle B$ as

$$A \triangle B = (A \cap \overline{B}) \cup (\overline{A} \cap B). \tag{1.9}$$

$$\begin{array}{rll} \overline{A \triangle B} = \overline{(A \cap \overline{B}) \cup (\overline{A} \cap B)} & & \text{from (1.9),} \\ = \overline{(A \cap \overline{B})} \cap \overline{(\overline{A} \cap B)} & & \text{De Morgan laws,} \\ = (\overline{A} \cup B) \cap (A \cup \overline{B}) & & \text{De Morgan laws,} \\ = [(\overline{A} \cup B) \cap A] \cup [(\overline{A} \cup B) \cap \overline{B}] & & \text{distributive law,} \\ = [(\overline{A} \cap A) \cup (B \cap A)] \cup [(\overline{A} \cap \overline{B}) \cup (B \cap \overline{B})] & & \text{distributive law,} \\ = (A \cap B) \cup (\overline{A} \cap \overline{B}) & & \text{commutative law.} \end{array}$$

Now, we prove the associativity of $\triangle$:

$$(A \triangle B) \triangle C = A \triangle (B \triangle C).$$

$$\begin{array}{ll} (A \triangle B) \triangle C & \\ = [(A \triangle B) \cap \overline{C}] \cup [\overline{(A \triangle B)} \cap C] & (1.9), \\ = [((A \cap \overline{B}) \cup (\overline{A} \cap B)) \cap \overline{C}] \cup [((A \cap B) \cup (\overline{A} \cap \overline{B})) \cap C] & (1.9),(1.8), \\ = [(A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C})] \cup [(A \cap B \cap C) \cup (\overline{A} \cap \overline{B} \cap C)] & \text{distributive,} \\ = (A \cap B \cap C) \cup (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C). & \end{array}$$

Similarly, we can prove that

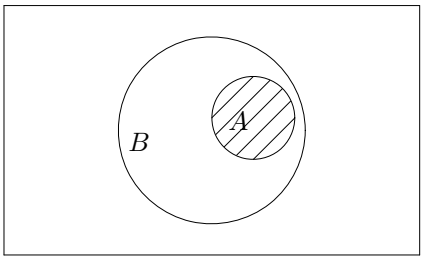
$$A\triangle(B\triangle C) = (A \cap B \cap C) \cup (A \cap \overline{B} \cap \overline{C}) \cup (\overline{A} \cap B \cap \overline{C}) \cup (\overline{A} \cap \overline{B} \cap C).$$

Therefore, $(A\triangle B)\triangle C = A\triangle(B\triangle C)$, i.e., $\triangle$ is associative.

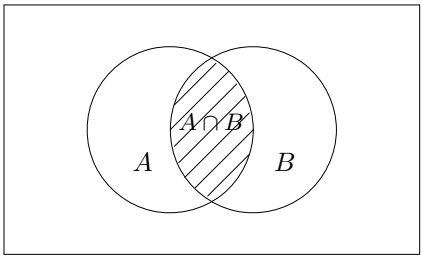
Finally, $A\triangle A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$. □

Solution 23: $A \subseteq B$ if and only if $A \cap B = A$.

(i) A Venn diagram for $A \cap B = A$. Note that $A \subseteq B$.



(ii) A Venn diagram for $A \cap B \neq A$. Note that $A \not\subseteq B$.



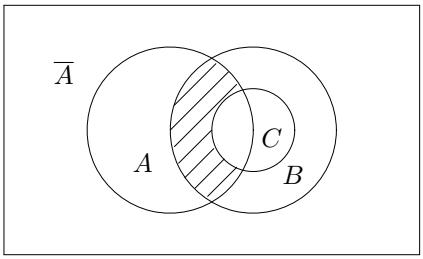
□

Solution 24:

1. Using Venn diagrams:

   (a) $B - C \subseteq \overline{A} \Rightarrow A \cap B \subseteq C$.
   By way of contradiction, suppose $B - C \subseteq \overline{A}$ and $A \cap B \not\subseteq C$. If

$A \cap B \not\subseteq C$, then we can find sets A, B, and C as shown in the following Venn diagram, where the shaded area covers those elements that are in $A \cap B$ but not in C. From the diagram we can see that $B - C \not\subseteq \overline{A}$, because the shaded area is a subset of $B - C$ and is also a subset of A.



(b) $B - C \subseteq \overline{A} \Leftarrow A \cap B \subseteq C$.
Again, by way of contradiction, suppose $A \cap B \subseteq C$ and $B - C \not\subseteq \overline{A}$. We can use the same Venn diagram. If $B - C \not\subseteq \overline{A}$, we can find the shaded area contradicts our assumption that $A \cap B \subseteq C$.

2. Using set algebra;

$$\begin{aligned}
B - C \subseteq \overline{A} &\iff (B - C) - \overline{A} = \emptyset && \text{definition of } -, \\
&\iff (B - C) \cap \overline{\overline{A}} = \emptyset && \text{problem 18}, \\
&\iff (B \cap \overline{C}) \cap A = \emptyset && \text{problem 18}, \\
&\iff A \cap (B \cap \overline{C}) = \emptyset && \text{commutative law}, \\
&\iff (A \cap B) \cap \overline{C} = \emptyset && \text{associative law}, \\
&\iff (A \cap B) - C = \emptyset && \text{problem 18}, \\
&\iff (A \cap B) \subseteq C && \text{definition of } -.
\end{aligned}$$

3. Using epsilon-arguments:

(a) $B - C \subseteq \overline{A} \Rightarrow A \cap B \subseteq C$.
By way of contradiction, suppose $B - C \subseteq \overline{A}$ and $A \cap B \not\subseteq C$. If $A \cap B \not\subseteq C$, then there exists an x such that $x \in A \cap B$ and $x \notin C$. Because $x \in A \cap B$, we know $x \in B$ and $x \notin \overline{A}$. And, because $x \in B$ and $x \notin C$, we know $x \in B - C$. Therefore, $B - C \not\subseteq \overline{A}$.

(b) $B - C \subseteq \overline{A} \Leftarrow A \cap B \subseteq C$.
By way of contradiction, suppose $A \cap B \subseteq C$ and $B - C \not\subseteq \overline{A}$. If $B - C \not\subseteq \overline{A}$, there exists an x such that $x \in B - C$ and $x \notin \overline{A}$. If so, $x \in B$ and $x \notin C$ because $x \in B - C$, and $x \in A$ because $x \notin \overline{A}$. Therefore, $A \cap B \not\subseteq C$ because $x \in A \cap B$ and $x \notin C$.

□

Solution 25:

$$A \times B = \{(\alpha, a), (\alpha, 3), (4, a), (4, 3)\}.$$

□

Solution 26: Let X and Y be two sets. There are two approaches to show that $X = Y$. One approach is to show $X \subseteq Y$ and $X \supseteq Y$, i.e, to show if $a \in X$ then $a \in Y$, and if $a \in Y$ then $a \in X$. The other approach is to show if $a \in X$ then $a \in Y$, and if $a \notin X$ then $a \notin Y$. Let us solve this problem by the second approach.

1. Let $a = (x, y)$, and suppose $a \in A \times (B \cup C)$.

$$\begin{aligned}
&(x, y) \in A \times (B \cup C) \\
&\quad \Rightarrow\ x \in A \text{ and } y \in (B \cup C) \\
&\quad \Rightarrow\ x \in A \text{ and } (y \in B \text{ or } y \in C) \\
&\quad \Rightarrow\ (x \in A \text{ and } y \in B) \text{ or } (x \in A \text{ and } y \in C) \\
&\quad \Rightarrow\ (x, y) \in A \times B \text{ or } (x, y) \in A \times C \\
&\quad \Rightarrow\ (x, y) \in (A \times B) \cup (A \times C).
\end{aligned}$$

   Therefore, $a \in (A \times B) \cup (A \times C)$.

2. Let $a = (x, y)$, and suppose $a \notin A \times (B \cup C)$.

$$\begin{aligned}
&(x, y) \notin A \times (B \cup C) \\
&\quad \Rightarrow\ x \notin A \text{ or } y \notin (B \cup C) \\
&\quad \Rightarrow\ x \notin A \text{ or } (y \notin B \text{ and } y \notin C) \\
&\quad \Rightarrow\ (x \notin A \text{ or } y \notin B) \text{ and } (x \notin A \text{ or } y \notin C) \\
&\quad \Rightarrow\ (x, y) \notin A \times B \text{ and } (x, y) \notin A \times C \\
&\quad \Rightarrow\ (x, y) \notin (A \times B) \cup (A \times C).
\end{aligned}$$

Therefore, $a \notin (A \times B) \cup (A \times C)$.

From (1) and (2), we have proved that

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

□

Solution 27: Suppose that $(A \times A) = (B \times B)$.

1. $x \in A$.

$$\begin{aligned}
x \in A &\Rightarrow (x, x) \in (A \times A) \\
&\Rightarrow (x, x) \in (B \times B) \\
&\Rightarrow x \in B.
\end{aligned}$$

Therefore, $A \subseteq B$.

2. $x \in B$.

$$\begin{aligned} x \in B &\Rightarrow (x, x) \in (B \times B) \\ &\Rightarrow (x, x) \in (A \times A) \\ &\Rightarrow x \in A. \end{aligned}$$

Therefore, $B \subseteq A$.

From the above, $A = B$. □

Solution 28: Let A, B, U, and V be any sets such that $A \subseteq U$ and $B \subseteq V$. Then we have

$$(A \times B) \subseteq (U \times V).$$

To prove this, let $x = (a, b)$ and $x \in A \times B$. Thus, $a \in A$ and $b \in B$. Since $A \subseteq U$ and $B \subseteq V$, we have $a \in U$ and $b \in V$. Therefore, $(a, b) \in U \times V$, i.e., $x \in U \times V$. □

We can prove this result by using the contradiction argument. Suppose the result is incorrect, i.e., we can find sets A, B, U, and V such that

$$A \subseteq U, B \subseteq V \text{ and } A \times B \not\subseteq U \times V.$$

If that is the case, then there exists $(a, b) \in A \times B$ and $(a, b) \notin U \times V$. If $(a, b) \notin U \times V$, then either $a \notin U$ or $b \notin V$. Both cases contradict the assumption: ($A \subseteq U$ and $B \subseteq V$.) □

Solution 29: Let A, B, C be sets.

$$\begin{aligned} (a, b) \in A \times (B \cup C) &\iff a \in A \text{ and } b \in (B \cup C), \\ &\iff a \in A \text{ and } (b \in B \text{ or } b \in \text{ C }), \\ &\iff (a, b) \in (A \times B) \text{ or } (a, b) \in (A \times C), \\ &\iff (a, b) \in (A \times B) \cup (A \times C). \end{aligned}$$

Therefore,

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

Since we can use $\iff$ in every step of the proof above, we don't have to prove the two directions of inclusion explicitly. □

Solution 30: To prove this problem, we will use the result in problem 29, i.e.,

$$X \times (Y \cup Z) = (X \times Y) \cup (X \times Z). \tag{1.10}$$

A similar equality we need is

$$(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z). \tag{1.11}$$

This can be proved in a similar manner discussed in problem 29.

1. To prove $A \times B \subseteq A \times C$,

$$\begin{aligned} A \times C &= A \times (A \cup B) && \text{because } C = (A \cup B), \\ &= (A \times A) \cup (A \times B) && (1.10). \end{aligned}$$

   Because $(A \times B) \subseteq ((A \times A) \cup (A \times B))$, we have $(A \times B) \subseteq (A \times C)$. □

2. To prove $A \times C \subseteq C \times C$,

$$\begin{aligned} C \times C &= (A \cup B) \times C && \text{because } C = (A \cup B), \\ &= (A \times C) \cup (B \times C). && (1.11). \end{aligned}$$

   Because $(A \times C) \subseteq ((A \times C) \cup (B \times C))$, we have $(A \times C) \subseteq (C \times C)$.

□

Solution 31: If $A \subseteq B$, both (1) and (2) are incorrect.

We can give a counter example to disproves (1) and (2) of this problem. Let A be the empty set and B be any non-empty set. Therefore, $A \times B$, $B \times A$, and $A \times A$ are empty sets, while $B \times B$ is not. □

Solution 32: $\mathcal{P}(X) = \Big\{ \emptyset, \{1\}, \{2\}, \{3\}, \{a\}, \{1,2\}, \{1,3\}, \{1,a\}, \{2,3\}, \{2,a\}, \{3,a\}, \{1,2,3\}, \{1,2,a\}, \{1,3,a\}, \{2,3,a\}, \{1,2,3,a\} \Big\}$.

Note: Don't forget to include the empty set and the set X in $\mathcal{P}(X)$. □

Solution 33: We will prove the following equality first, so we do not have to enumerate all elements in $\mathcal{P}(X)$. For any set X,

$$X = [X \cup (X \cap \mathcal{P}(X))].$$

From the definition of union, we know that

$$X \subseteq [X \cup (X \cap \mathcal{P}(X))]. \tag{1.12}$$

From the definition of intersection, we know that

$$(X \cap \mathcal{P}(X)) \subseteq X. \tag{1.13}$$

Union with X on both sides of (1.13), we get

$$[X \cup (X \cap \mathcal{P}(X))] \subseteq (X \cup X).$$

And, since $(X \cup X) = X$,

$$[X \cup (X \cap \mathcal{P}(X))] \subseteq X. \tag{1.14}$$

From (1.12) and (1.14), we get $X \cup (X \cap \mathcal{P}(X)) = X$. For this problem,

$$X \cup (X \cap \mathcal{P}(X)) = X = \{1, 2, 3, 4, 5, 6, \{1\}\}.$$

□

Solution 34:

1. $\mathcal{P}(\emptyset) = \{\emptyset\}$
2. $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
3. $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
4. $\{\emptyset\} \times \mathcal{P}(\emptyset) = \{(\emptyset, \emptyset)\}$
5. $\emptyset \times \mathcal{P}(\emptyset) = \emptyset$
6. $\mathcal{P}(\emptyset) \times \mathcal{P}(\emptyset) = \{(\emptyset, \emptyset)\}$

□

Solution 35:

$$\begin{aligned} A &= \{a, 1\}, \\ \mathcal{P}(A) &= \{\emptyset, \{a\}, \{1\}, \{a, 1\}\}, \\ A \times \mathcal{P}(A) &= \left\{ \begin{array}{l} (a, \emptyset), (a, \{a\}), (a, \{1\}), (a, \{a, 1\}), \\ (1, \emptyset), (1, \{a\}), (1, \{1\}), (1, \{a, 1\}) \end{array} \right\}. \end{aligned}$$

□

Solution 36:

$$\begin{aligned} x \in \mathbf{Pr}(A \cap B) &\Leftrightarrow x \subseteq (A \cap B), \\ &\Leftrightarrow x \subseteq A \text{ and } x \subseteq B, \\ &\Leftrightarrow x \in \mathbf{Pr}(A) \text{ and } x \in \mathbf{Pr}(B), \\ &\Leftrightarrow x \in \mathbf{Pr}(A) \cap \mathbf{Pr}(B). \end{aligned}$$

Therefore, $\mathbf{Pr}(A \cap B) = \mathbf{Pr}(A) \cap \mathbf{Pr}(B)$. □

Solution 37: Suppose that $A \in \mathbf{Pr}(B)$ and $B \in \mathbf{Pr}(A)$. From the definition of power set,

$$\begin{aligned} A \in \mathbf{Pr}(B) &\Rightarrow A \subseteq B, \\ B \in \mathbf{Pr}(A) &\Rightarrow B \subseteq A. \end{aligned}$$

Therefore, $A = B$. □

Solution 38: Let A be the set of natural integers and B the set of odd natural integers. Define function $f : A \longrightarrow B$ as

$$f(n) = 2n - 1.$$

We want to prove that f is a bijective function from A to B.

1. Let $a_1, a_2 \in A$, and $a_1 \neq a_2$. It is clear that $2a_1 - 1 \neq 2a_2 - 1$. Thus, $f(a_1) \neq f(a_2)$, and hence f is injective.

2. Let $b \in B$. Then $\frac{b-1}{2} \in A$, because it is a natural number. Therefore, f is surjective.

From the definition of cardinality, $|A| = |B|$. □

Solution 39: We consider the following axiom:

Let A and B be any sets. $|A| \leq |B|$ if and only if there exists an injection g from A to B.

To prove that $|A| \leq |\mathbf{Pr}(A)|$, we define $g : A \to \mathbf{Pr}(A)$ as

$$g(x) = \{x\}, \text{ for all } x \in A.$$

g is injective because for all $x, y \in A$, if $x \neq y$, then $\{x\} \neq \{y\}$. Thus, by the axiom, $|A| \leq |\mathbf{Pr}(A)|$.

Now, we have to prove that $|A| \neq |\mathbf{Pr}(A)|$. By way of contradiction, suppose $|A| = |\mathbf{Pr}(A)|$. Then there is a bijective function $f : A \to \mathbf{Pr}(A)$. Thus, for any $a \in A$, $f(a)$ is a subset of A. Define the set S as

$$S = \{x | x \notin f(x)\}.$$

It is clear that S is a subset of A. Since f is surjective, there exists $s \in A$ such that $f(s) = S$. We have two cases: $s \in S$ and $s \notin S$.

1. If $s \in S$, that means $s \in f(s)$, then $s \notin S$.
2. If $s \notin S$, that means $s \notin f(s)$, then $s \in S$.

Either case gives a contradiction. Therefore, there is no bijective function from A to $\mathbf{Pr}(A)$, and hence $|A| \neq |\mathbf{Pr}(A)|$.

From $|A| \leq |\mathbf{Pr}(A)|$ and $|A| \neq |\mathbf{Pr}(A)|$, we conclude that $|A| < |\mathbf{Pr}(A)|$. □

Chapter 2

Logic

It presupposes nothing but logic; that is,
logic is the only preceding theory.

– Alfred Tarski

2.1 Definitions

2.1.1 Propositional Logic

Definition 2.1: *Propositions* are mathematical statements such that their truth or falsity can be told without ambiguity. A proposition is also called a primitive statement.

We use letters $p, q, r, \ldots$ to denote propositions. Thus, the values of $p, q, r, \ldots$ are either $True$ or $False$.

Example 2.1

p : $2 + 2 = 5$,
q : $x^2 - 2x + 1$ has two identical roots,
r : $\emptyset \subset \{1, 2, \emptyset\}$,
s : there exists a 100-digit prime number,

are propositions. The value of p is $False$, and the values of q and r are $True$. We will use T to denote $True$ and F to denote $False$ for the rest of this book.

Comment: The statement s in the above example is a proposition, even though we do not know for sure that there exists a 100-digit prime number, but we are sure that s is either T or F. However, not every mathematical statement has a truth value. The following two statements are not propositions.

u : This statement is false.
v : $a \in S$, where S is a set defined as $S = \{x | x \notin S\}$.

Definition 2.2: Suppose $p, q, r, \ldots$ are variables with values either T or F. We call such variables *propositional variables*. We can assign T or F to any propositional variable as we wish. propositional variables are also known as *atoms*.

Definition 2.3: Let p, q be two propositions. We use the symbols:

$$\neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow$$

to construct new propositions such as

$$\neg p,\ p \wedge q,\ p \vee q,\ p \rightarrow q,\ p \leftrightarrow q..$$

These symbols are called *logical connectives*; $\neg$ is read as "not" or "negation", $\wedge$ as "and" or "conjunction", $\vee$ as "or" or "disjunction", $p \rightarrow q$ is read as "if p then q" or "p implies q", and $p \leftrightarrow q$ is read as "p if and only if q".

Recall that all propositions have truth values either T or F. We decide the values of the new propositions constructed above based on the values of p and q and the rules of logical connectives defined below.

Definition 2.4: 1. The negation of p: $\neg p$.

p	$\neg p$
T	F
F	T

2. The conjunction of p and q: $p \wedge q$.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

3. The disjunction of p and q: $p \vee q$.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

4. Implication, if p then q: $p \rightarrow q$.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

5. Equivalence, p if and only if q: $p \leftrightarrow q$.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Definition 2.5: Given $p \rightarrow q$, we call $\neg q \rightarrow \neg p$ the *contrapositive*, call $q \rightarrow p$ the *converse*, and call $\neg p \rightarrow \neg q$ the *inverse* of $p \rightarrow q$.

Definition 2.6: *Propositional formulas* are recursively defined as follows:

1. T and F are propositional formulas.
2. All atoms are propositional formulas.
3. If f_1 and f_2 are propositional formulas, so are

$$\neg f_1,\ f_1 \wedge f_2,\ f_1 \vee f_2,\ f_1 \rightarrow f_2,\ f_1 \leftrightarrow f_2.$$

Only the formulas generated by the rules above are propositional formulas. Propositional formulas are also known as *well-formed-formulas*, or wff's in short.

Example 2.2

$$\begin{array}{lll} pq\wedge, & \neg\vee pq, & \rightarrow(p\wedge q)\vee r \quad \text{are not wff's.} \\ p\wedge q, & \neg p\vee q, & (p\wedge q)\rightarrow r \quad \text{are wff's.} \end{array}$$

We are allowed to use parentheses with their natural purposes.

Definition 2.7: The operational priorities of logical connectives are defined below:

Precedence : $\{\neg\} > \{\wedge,\vee\} > \{\rightarrow,\leftrightarrow\}$.

In other words, "$\neg$" is evaluated before "$\wedge$" and "$\vee$", and "$\wedge$" and "$\vee$" are evaluated before "$\rightarrow$" and "$\leftrightarrow$". For example,

$$a\rightarrow b\wedge\neg c \;\equiv\; a\rightarrow(b\wedge(\neg c)).$$

The equivalence symbol $\equiv$ above means: $a\rightarrow b\wedge\neg c$ is to be interpreted as $a\rightarrow(b\wedge(\neg c))$, and $a\rightarrow(b\wedge(\neg c))$ can be abbreviated as $a\rightarrow b\wedge\neg c$. We can alternatively use one of them without introducing ambiguity.

Associativity : $\wedge$ and $\vee$ are *left associative*; $\rightarrow$ and $\leftrightarrow$ are *right associative*. For example,

$$\begin{aligned} a\wedge b\vee c &\equiv (a\wedge b)\vee c, \\ a\rightarrow b\leftrightarrow c\rightarrow d &\equiv a\rightarrow(b\leftrightarrow(c\rightarrow d)). \end{aligned}$$

Definition 2.8: Let f be a wff in n variables. The *truth table* of f is a table that contains all possible values of the variables in the rows (each row represents one possibility), and the corresponding values of f are in the last column. The tables in definition 2.4 are the truth tables of $\neg p$, $p\wedge q$, $p\vee q$, $p\rightarrow q$, and $p\rightarrow q$, respectively. For complicated formulas, we can add some intermediate columns to help us find the truth values of f.

Example 2.3 Let $f=(p\wedge q)\rightarrow r$. The truth table of f is

p	q	r	$p\wedge q$	$(p\wedge q)\rightarrow r$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	T
T	F	F	F	T
F	T	T	F	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

We have added a column to present the truth values of $p\wedge q$. The 3rd row, for example, indicates that if $p=T, q=F$, and $r=T$, then f is T.

Definition 2.9: Let f be a wff. f is called a *tautology* if and only if f is T everywhere in the last column of its truth table.

Definition 2.10: Let f be a wff. f is called a *contradiction* if and only if f is F everywhere in the last column of its truth table.

Definition 2.11: Let f_1 and f_2 be two wff's. Define

$$f_1 \Rightarrow f_2 \text{ if and only if } f_1 \rightarrow f_2 \text{ is a tautology.}$$

We say f_1 *logically implies* f_2.

Definition 2.12: Let f_1 and f_2 be two wff's. Define

$$f_1 \iff f_2 \text{ if and only if } f_1 \leftrightarrow f_2 \text{ is a tautology.}$$

We say f_1 and f_2 are *logically equivalent.*

Definition 2.13: Let f be a wff. If the logical connectives that f contains are $\wedge$ and $\vee$ only, then the dual of f, denoted as f^d, is a wff obtained from f by the following rules: In f,

1. replace T by F, and F by T,
2. replace $\wedge$ by $\vee$,
3. replace $\vee$ by $\wedge$.

Definition 2.14: Let f be a wff in n variables. The Disjunctive Normal Form, DNF in short, of f is a logical equivalence of f, which is a disjunction of one or more distinct $(x_1 \wedge x_2 \wedge \cdots \wedge x_n)$, where $x_i, 1 \leq i \leq n$, is a propositional variable of f or its negation. Each x_i is known as a literal.

Example 2.4 Let $f = p \rightarrow q$. The DNF of f is

$$(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q). \tag{2.1}$$

Because, (a) both f and the proposition (2.1) have the same truth values for all possible values of p and q, and (b) the proposition (2.1) is a disjunction of distinct formulas using the connective "$\wedge$" between literals.

Definition 2.15: Let f be a wff in n variables. The Conjunctive Normal Form, CNF in short, of f is a logical equivalence of f, which is a conjunction of one or more distinct $(x_1 \vee x_2 \vee \cdots \vee x_n)$, where $x_i, 1 \leq i \leq n$, is a literal.

Example 2.5 Let $f := p \rightarrow q$. The CNF of f is

$$(\neg p \vee q).$$

2.1.2 Predicate Logic

Definition 2.16: A *predicate* $P(x_1, x_2, \cdots, x_n), n \geq 0$ is a mapping from the concerned domains to $\{T, F\}$. In other words, if we replace $x_1, \cdots, x_n$ by instances in their corresponding domains, we will get a proposition.

Example 2.6 The following are all predicates.

$$\begin{array}{lll} P(x,y): & x \geq y^2, & D_x = D_y = \mathbf{N}; \\ Q(x,y): & x \text{ is a } y, & D_x \text{ is the set of names,} \\ & & D_y = \{\text{father, son, cat, dog, table,}\ldots\} \end{array}$$

We use D_x, D_y to denote the domains of x and y, respectively. Note that D_x and D_y do not have to be the same. In the above example, $P(3,2)$ is the proposition $3 \geq 2^2$ with truth value F. Similarly, $Q(\text{Boo}, \text{dog})$ is a proposition with truth value T if there is a dog named Boo.

Note: Any proposition is a predicate in zero variables.

Definition 2.17: Let $P(x_1, x_2, \cdots, x_n), n \geq 0$ be a predicate. The set $D_{x_1} \times D_{x_2} \times \cdots \times D_{x_n}$ is called the *domain of predicate* P.

Definition 2.18: Let $P(x_1, x_2, \cdots, x_n), n \geq 0$ be a predicate. The *truth set* of P, denoted as T_P, is a subset of $D_{x_1} \times D_{x_2} \times \cdots \times D_{x_n}$ such that for all $(a_1, a_2, \ldots, a_n) \in T_P$, $P(a_1, a_2, \ldots, a_n) = T$.

Definition 2.19: Let $P(x_1, x_2, \cdots, x_n), n \geq 0$ be a predicate. The *falsity set* of P, denoted as F_P, is a subset of $D_{x_1} \times D_{x_2} \times \cdots \times D_{x_n}$ such that for all $(a_1, a_2, \ldots, a_n) \in F_P$, $P(a_1, a_2, \ldots, a_n) = F$.

Definition 2.20: Let P, Q be two predicates. We say that P and Q are logically equivalent if and only if $T_p = T_Q$.

Definition 2.21: Let P, Q be two predicates. We say that P logically implies Q if and only if $T_p \subseteq T_Q$.

In addition to the connectives discussed in the previous section, we have two special symbols called quantifiers in predicate logic. The two special symbols are $\forall$ and $\exists$. The quantifiers $\forall$ and $\exists$ are called the *universal quantifier* and the *existential quantifier* and pronounced as "for all" and "there exists" respectively. The meaning of $\forall$ and $\exists$ are defined below.

Definition 2.22: Let $P(x)$ be a predicate in one variable.

1. Universal quantifier: $\forall x \in D_x P(x)$ is a proposition, and its value is T if every instance a in D_x makes $P(a)$ true.
2. Existential quantifier: $\exists x \in D_x P(x)$ is a proposition, and its value is T if there exists some instance a in D_x that makes $P(a)$ true.

If the domain D_x is clear from the context, we usually drop the domain set and rewrite $\forall x \in D_x P(x)$ as $\forall x P(x)$ and $\exists x \in D_x P(x)$ as $\exists x P(x)$. A predicate preceded with one or more quantifiers is called a *quantified predicate*.

Definition 2.23: Let $P(x_1, \ldots, x_i, \ldots, x_n)$ be a predicate in n variables. Then, $\forall x_i P(x_1, \ldots, x_i, \ldots, x_n)$ and $\exists x_i P(x_1, \ldots, x_i, \ldots, x_n)$ are predicates in $n-1$ variables, where x_i is called a *bounded variable* and the rest of the variables are called *unbounded variables* or *free variables*.

Example 2.7 Given the predicate $P(x, y)$ in two variables x and y, $\forall x P(x, y)$ and $\exists x P(x, y)$ are predicates in one variable y. The variable y is a free variable, and x is a bounded variable in $\forall x P(x, y)$ and $\exists x P(x, y)$.

2.1.3 Predicates and Sets

Let $P(x)$ and $Q(x)$ be two predicates in one variable, and let D_x be the universe of x. Then the associated truth and falsity sets satisfy the following properties.

1. $T_P \cup F_P = D_x$.
2. $T_P \cap F_P = \emptyset$.
3. $T_{P \wedge Q} = T_P \cap T_Q$.
4. $T_{P \vee Q} = T_P \cup T_Q$.
5. $\forall x[P(x) \rightarrow Q(x)] \iff T_P \subseteq T_Q$.
6. $\exists x[P(x) \wedge Q(x)] \iff (T_P \cap T_Q) \neq \emptyset$.

2.2 Logical Proof

Logical proof is a formal way of convincing that some statements are correct based on given facts.

Let P and Q be two wff's, predicates, or quantified predicates. Starting from P, if we can find a sequence of applications of laws of logic, rules of inference, or tautologies to arrive at Q, step by step, we say there is a proof for the *theorem*

$$P \Longrightarrow Q.$$

In theorem $P \Rightarrow Q$, P is called the *premise*, and Q is called a *logical conclusion* of P. The sequence of these steps is called a *logical proof* of $P \Rightarrow Q$. A logical proof is usually represented in a table like the following one.

Premises: P
Conclusion: Q

	steps	*reasons*
1.	P	Premises
2.	q_2	$--$
3.	q_3	$--$
$\vdots$	$\vdots$	$\vdots$
$i.$	q_i	$--$
$\vdots$	$\vdots$	$\vdots$
$n.$	Q	$--$

where $--$ are the names of the logical rules.

In short, a logical proof can be written as

$$P \Rightarrow q_2 \Rightarrow q_3 \Rightarrow \cdots \Rightarrow q_i \Rightarrow \ldots \Rightarrow Q.$$

P and Q are not necessarily two single statements; they can be a set of wff's, predicates, and quantified predicates. For example, a theorem may look like

$$\{P_1, P_2, \ldots, P_n\} \Longrightarrow \{Q_1, Q_2, \ldots, Q_m\}. \tag{2.2}$$

On the other hand, a punctuation symbol "," is considered as a "$\wedge$". Therefore, the theorem in (2.2) can be expressed as

$$(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \Longrightarrow (Q_1 \wedge Q_2 \wedge \ldots \wedge Q_m).$$

2.2.1 Laws of Logic

Let $f_1 \leftrightarrow f_2$ be a tautology, i.e., $f_1 \Leftrightarrow f_2$. During the course of deriving the sequence of a logical proof, if one of f_1 and f_2 appears, then we can attach the other one to the sequence of the logical proof.

For example, if we know that $f_1 \Leftrightarrow f_2$ and already have

$$P \Rightarrow q_2 \Rightarrow q_3 \Rightarrow \cdots \Rightarrow f_1,$$

then the proof above can be extended to

$$P \Rightarrow q_2 \Rightarrow q_3 \Rightarrow \cdots \Rightarrow f_1 \Rightarrow f_2.$$

The following is a list of tautologies, where p, q, and r are wff's. One can use the definitions of connectives to prove that they are tautologies. We call them *Laws of Logic*. In a logical proof we are allowed to use the laws of logic directly without further proof.

1. Law of double negation:
$$\neg\neg p \iff p.$$

2. Absorption Laws:
$$p \wedge (p \vee q) \iff p,$$
$$p \vee (p \wedge q) \iff p.$$

3. Idempotent Laws:
$$p \wedge p \iff p,$$
$$p \vee p \iff p.$$

4. Inverse Laws:
$$p \wedge \neg p \iff F,$$
$$p \vee \neg p \iff T.$$

5. Identity Laws:
$$p \wedge T \iff p,$$
$$p \vee F \iff p.$$

6. Domination Laws:
$$p \wedge F \iff F,$$
$$p \vee T \iff T.$$

7. Commutative Laws:
$$(p \wedge q) \iff (q \wedge p),$$
$$(p \vee q) \iff (q \vee p).$$

8. Associative Laws:
$$(p \wedge (q \wedge r)) \iff ((p \wedge q) \wedge r),$$
$$(p \vee (q \vee r)) \iff ((p \vee q) \wedge r).$$

9. Distributive Laws:
$$(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r)),$$
$$(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r)).$$

10. Contrapositive Law:
$$(p \to q) \iff (\neg q \to \neg p)$$

11. De Morgan's Laws:
$$\neg(p \vee q) \iff (\neg p \wedge \neg q),$$
$$\neg(p \wedge q) \iff (\neg p \vee \neg q).$$

12. No specific name is given, but this law is one of the most frequently used laws in logical proof.
$$(p \to q) \iff (\neg p \vee q).$$

2.2.2 Rules of Inference

Let $f_1 \to f_2$ be a tautology, i.e., $f_1 \Rightarrow f_2$. During the course of deriving the sequence of a logical proof, if f_1 appears, then we can attach f_2 to the sequence of the logical proof.

For example, if we know that $f_1 \Rightarrow f_2$, and already have

$$P \Rightarrow q_2 \Rightarrow q_3 \Rightarrow \cdots \Rightarrow f_1,$$

then the proof above can be extended to

$$P \Rightarrow q_2 \Rightarrow q_3 \Rightarrow \cdots \Rightarrow f_1 \Rightarrow f_2.$$

Let p, q, r, and s be wff's. The following tautologies are called *Rules of Inference*.

1. Modus Ponens:
$$(p \wedge (p \to q)) \Longrightarrow q.$$
2. Modus Tollens:
$$(\neg q \wedge (p \to q)) \Longrightarrow \neg p.$$
3. Law of the Syllogism:
$$((p \to q) \wedge (q \to r)) \Longrightarrow (p \to r).$$
4. Rule of Disjunctive Syllogism:
$$((p \vee q) \wedge \neg q) \Longrightarrow p.$$
5. Rule of Contradiction:
$$(\neg p \to F) \Longrightarrow p.$$
6. Rule of Conjunctive Simplification:
$$(p \wedge q) \Longrightarrow p.$$
7. Rule of Disjunctive Amplification:
$$p \Longrightarrow (p \vee q).$$
8. Proof by cases:
$$((p \to r) \wedge (q \to r)) \Rightarrow ((p \vee q) \to r)$$

2.2.3 Inference Rules for Quantified Predicates

Let $P(x)$ and $Q(x, y)$ be two predicates in one and two variables respectively. Following are some basic inference rules for quantified predicates.

1. Negation:
$$\neg\forall xP(x) \Longleftrightarrow \exists x\neg P(x),$$
$$\neg\exists xP(x) \Longleftrightarrow \forall x\neg p(x).$$

2. α-Conversion (changing the name of the bounded variable):
$$\forall xP(x) \Longleftrightarrow \forall yP(y),$$
$$\exists xP(x) \Longleftrightarrow \exists yP(y).$$

3. Reordering quantifiers of the same kind:
$$\forall x\forall yQ(x, y) \Longleftrightarrow \forall y\forall xQ(x, y),$$
$$\exists x\exists yQ(x, y) \Longleftrightarrow \exists y\exists xQ(x, y).$$

4. Universal Specification:
$$\forall xP(x) \Longrightarrow P(a), \text{ any } a \in D_x.$$

5. Existential Specification:
$$\exists xP(x) \Longrightarrow P(a), \text{ some } a \in D_x.$$

6. Universal Generalization:
$$(\text{any } a \in D_x, P(a) = T) \Longrightarrow \forall xP(x).$$

7. Existential Generalization:
$$(\text{some } a \in D_x, P(a) = T) \Longrightarrow \exists xP(x).$$

Comment: We do not have a standard notation to distinguish a between "any a" in 6 and "some a" in 7. One should find a way to make them clear in the proof without confusion. See problem 50 of this chapter.

2.3 DNF and CNF

In this section we introduce a systematic way to find the DNF and CNF of any given wff. The DNF and CNF are perhaps not mathematically dignified for presenting any wff, but they are essentially the underlying presentation inside

modern digital computers. The DNF and CNF provide a convenient apparatus in applications of Artificial Intelligence, Logical Programming, and many other areas of research. Therefore, it behooves us to pay more attention to the DNF and CNF.

We will pedagogically discuss wff's in three variables. One can easily extend the method to a more general case.

Definition 2.24: Let f be a wff in variables x_1, x_2 and x_3, and let $i \in \{1, 2, 3\}$.

1. Each term x_i or its complement $\neg x_i$ is called a *literal.*
2. A term of the form $y_1 \wedge y_2 \wedge y_3$, where $y_i = x_i$ or $y_i = \neg x_i$ is called a *fundamental conjunction.*
3. A term of the form $y_1 \vee y_2 \vee y_3$, where $y_i = x_i$ or $y_i = \neg x_i$ is called a *fundamental disjunction.*
4. A representation of f in a disjunction of fundamental conjunctions is called a *disjunctive normal form* (DNF) or *sum-of-product* from.
5. A representation of f in a conjunction of fundamental disjunctions is called a *conjunctive normal form* (CNF) or *product-of-sum* from.

2.3.1 The DNF of a given wff

$$\text{DNF:} \quad D_1 \vee D_2 \vee \cdots \vee D_n. \tag{2.3}$$

Let f be a wff in three variables a, b, and c. There are eight possible fundamental conjunctions for a D in (2.3). These fundamental conjunctions are also known as the building blocks for f in DNF. Let d_i be the i^{th} building block defined in the follows.

$$\left.\begin{array}{ll} d_1: & a \wedge b \wedge c \\ d_2: & a \wedge b \wedge \overline{c} \\ d_3: & a \wedge \overline{b} \wedge c \\ d_4: & a \wedge \overline{b} \wedge \overline{c} \\ d_5: & \overline{a} \wedge b \wedge c \\ d_6: & \overline{a} \wedge b \wedge \overline{c} \\ d_7: & \overline{a} \wedge \overline{b} \wedge c \\ d_8: & \overline{a} \wedge \overline{b} \wedge \overline{c} \end{array}\right\} \text{Building Blocks for DNF in three variables.}$$

We use $\overline{x}$ to denote $\neg x$ due to space consideration.

Step 1: Evaluate the truth value of each building block. It is convenient to use a truth table as shown below, where the truth value associated with each building block is evaluated and followed by the truth value of f.

a	b	c	$a \wedge b \wedge c$	$a \wedge b \wedge \overline{c}$	$a \wedge \overline{b} \wedge c$	$\cdots$	$\cdots$	$f(a,b,c)$	
T	T	T	T ✓	F	F	$\cdots$	$\cdots$	T	✓
T	T	F	F	T	F	$\cdots$	$\cdots$	F	
T	F	T	F	F	T ✓	$\cdots$	$\cdots$	T	✓
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$		$\vdots$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\ddots$	$\vdots$	

Step 2: We check the last column and mark the rows in which f's value is T. For each marked row, we find and mark the building block with value T in the row. Note that for each row, there is exactly one building block with value T, and for each column of a building block, there is exactly one row with value T.

Step 3: Finally, the DNF is the disjunction of the building blocks marked in step 2. In the above partial example, a part of the DNF is

$$f(a,b,c) = (a \wedge b \wedge c) \vee (a \wedge \overline{b} \wedge c) \vee \cdots$$

□

Example 2.8 Find the DNF of $(a \longrightarrow b) \vee c$.

Let $f(a,b,c) = (a \longrightarrow b) \vee c$, and $d_1, d_2, \ldots, d_8$ be the building blocks we just defined. Follow the rules we just described step by step, we have the following table.

a	b	c	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	f	
T	T	T	T ✓	F	F	F	F	F	F	F	T	✓
T	T	F	F	T ✓	F	F	F	F	F	F	T	✓
T	F	T	F	F	T ✓	F	F	F	F	F	T	✓
T	F	F	F	F	F	T	F	F	F	F	F	
F	T	T	F	F	F	F	T ✓	F	F	F	T	✓
F	T	F	F	F	F	F	F	T ✓	F	F	T	✓
F	F	T	F	F	F	F	F	F	T ✓	F	T	✓
F	F	F	F	F	F	F	F	F	F	T ✓	T	✓

According to the rule in step 3, the DNF of f is

$$d_1 \vee d_2 \vee d_3 \vee d_5 \vee d_6 \vee d_7 \vee d_8.$$

I.e.,

$$\begin{aligned}(a \rightarrow b) \vee c \quad = \quad & (a \wedge b \wedge c) \vee (a \wedge b \wedge \overline{c}) \vee (a \wedge \overline{b} \wedge c) \vee (\overline{a} \wedge b \wedge c) \vee \\ & (\overline{a} \wedge b \wedge \overline{c}) \vee (\overline{a} \wedge \overline{b} \wedge c) \vee (\overline{a} \wedge \overline{b} \wedge \overline{c}).\end{aligned}$$

□

2.3.2 The CNF of a given wff

$$\text{CNF:} \quad C_1 \wedge C_2 \wedge \cdots \wedge C_n.$$

Let f be a wff in 3 variables a, b, and c. There are 8 building blocks for f in CNF. Let c_i be the i^{th} building block defined in the follows.

$$\left.\begin{array}{ll} c_1: & a \vee b \vee c \\ c_2: & a \vee b \vee \overline{c} \\ c_3: & a \vee \overline{b} \vee c \\ c_4: & a \vee \overline{b} \vee \overline{c} \\ c_5: & \overline{a} \vee b \vee c \\ c_6: & \overline{a} \vee b \vee \overline{c} \\ c_7: & \overline{a} \vee \overline{b} \vee c \\ c_8: & \overline{a} \vee \overline{b} \vee \overline{c} \end{array}\right\} \text{ Building Blocks for CNF in 3 variables.}$$

Step 1: We construct the following truth table. As we did for finding DNF, each building block must occupy one column, and the last column contains the truth values of f.

a	b	c	$a \vee b \vee c$	$a \vee b \vee \overline{c}$	$\cdots\ \cdots$	$\overline{a} \vee \overline{b} \vee c$	$\cdots$	$f(a,b,c)$	
T	T	T	T	T	$\cdots\ \cdots$	T	$\cdots$	T	
T	T	F	T	T	$\cdots\ \cdots$	F ✓	$\cdots$	F	✓
T	F	T	T	T	$\cdots\ \cdots$	T	$\cdots$	T	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	
F	F	F	F ✓	T	$\cdots\ \cdots$	T	$\cdots$	F	✓

Step 2: Check the last column and mark the rows in which f's value is F. For each marked row, we find and mark the building block with value F in the row. Note that for each row, there is exactly one building block with value F, and there is exactly one row with value F in each building block's column.

Step 3: Finally, the CNF is the conjunction of the building blocks marked in step 2. In the above partial example, a part of the CNF is

$$f(a,b,c) = (a \vee b \vee c) \ \wedge\ (\overline{a} \vee \overline{b} \vee c) \ \wedge\ \cdots$$

□

Example 2.9 Find the CNF of $(a \longrightarrow b) \vee c$.

Let, $f(a,b,c) = (a \longrightarrow b) \vee c$, and $c_1, c_2, \ldots, c_8$ be the building blocks we just defined.

a	b	c	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	f	
T	T	T	T	T	T	T	T	T	T	F	T	
T	T	F	T	T	T	T	T	T	F	T	T	
T	F	T	T	T	T	T	T	F	T	T	T	
T	F	F	T	T	T	T	F ✓	T	T	T	F	✓
F	T	T	T	T	T	F	T	T	T	T	T	
F	T	F	T	T	F	T	T	T	T	T	T	
F	F	T	T	F	T	T	T	T	T	T	T	
F	F	F	F	T	T	T	T	T	T	T	T	

Therefore,

$$(a \longrightarrow b) \vee c = (\overline{a} \vee b \vee c).$$

□

Example 2.10 Find the DNF and CNF of $a \wedge (b \longleftrightarrow c)$.

Let $f = a \wedge (b \longleftrightarrow c)$, and $d_1, d_2, \ldots, d_8$ be the building blocks for DNF and $c_1, c_2, \ldots, c_8$ the building blocks for CNF as defined.

For DNF:

a	b	c	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	f	
T	T	T	T ✓	F	F	F	F	F	F	F	T	✓
T	T	F	F	T	F	F	F	F	F	F	F	
T	F	T	F	F	T	F	F	F	F	F	F	
T	F	F	F	F	F	T ✓	F	F	F	F	T	✓
F	T	T	F	F	F	F	T	F	F	F	F	
F	T	F	F	F	F	F	F	T	F	F	F	
F	F	T	F	F	F	F	F	F	T	F	F	
F	F	F	F	F	F	F	F	F	F	T	F	

Therefore, the DNF of f is $d_1 \wedge d_4$, i.e.,

$$(a \wedge b \wedge c) \vee (a \wedge \overline{b} \wedge \overline{c}).$$

For CNF:

a	b	c	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	f	
T	T	T	T	T	T	T	T	T	T	F	T	
T	T	F	T	T	T	T	T	T	F ✓	T	F	✓
T	F	T	T	T	T	T	T	F ✓	T	T	F	✓
T	F	F	T	T	T	T	F	T	T	T	T	
F	T	T	T	T	T	F ✓	T	T	T	T	F	✓
F	T	F	T	T	F ✓	T	T	T	T	T	F	✓
F	F	T	T	F ✓	T	T	T	T	T	T	F	✓
F	F	F	F ✓	T	T	T	T	T	T	T	F	✓

Therefore, the CNF of f is $c_1 \wedge c_2 \wedge c_3 \wedge c_4 \wedge c_6 \wedge c_7$, i.e.,

$$(a \vee b \vee c) \wedge (a \vee b \vee \overline{c}) \wedge (a \vee \overline{b} \vee c) \wedge (a \vee \overline{b} \vee \overline{c}) \wedge (\overline{a} \vee b \vee \overline{c}) \wedge (\overline{a} \vee \overline{b} \vee c).$$

□

2.3.3 A shortcut to find the DNF and CNF

Given any wff f, we can find the DNF and CNF directly from its truth set and falsity set. Let us assume that f has three variables a, b, and c, and let the format of the truth set T_f and the falsity set F_f be $D_a \times D_b \times D_c$.

Step 1: Find out the truth set T_f and the falsity set F_f of f.

Step 2: For DNF, we will use the truth set T_f. The building blocks that should appear in the DNF of f are those having truth value T if we apply some elements in T_f to them. In other words, for each $(t_a, t_b, t_c) \in T_f$, we choose $(x_a \wedge x_b \wedge x_c)$ according to the following rules.

1. $x_a = a$ if $t_a = T$.
2. $x_a = \neg a$ if $t_a = F$.
3. x_b and x_c are decided by the same principle above.

For CNF, we will use the falsity set F_f. The building blocks that should appear in the CNF of f are those having truth value F if we apply some elements in F_f to them. In other words, for each $(t_a, t_b, t_c) \in F_f$, we choose $(x_a \wedge x_b \wedge x_c)$ according to the following rules.

1. $x_a = \neg a$ if $t_a = T$.
2. $x_a = a$ if $t_a = F$.
3. x_b and x_c are decided by the same principle above.

Basically, the shortcut method and the truth table addressed with building blocks are essentially the same. Let's consider the following example.

Example 2.11 Find the DNF and CNF of $(a \leftrightarrow b) \leftrightarrow c$ from its truth set and falsity set directly.

Let $f = (a \leftrightarrow b) \leftrightarrow c$. We first find T_f and F_f by using the following truth table.

a	b	c	$a \leftrightarrow b$	$(a \leftrightarrow b) \leftrightarrow c$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	F
T	F	F	F	T
F	T	T	F	F
F	T	F	F	T
F	F	T	T	T
F	F	F	T	F

We have

$$\begin{aligned} T_f &= \{(T,T,T),(T,F,F),(F,T,F),(F,F,T)\}, \\ F_f &= \{(T,T,F),(T,F,T),(F,T,T),(F,F,F)\}. \end{aligned}$$

For DNF of f, consider T_f. We apply the rule described on all four elements of T_f to get the associated blocks.

$$\begin{aligned} (T,T,T) &\implies (a \wedge b \wedge c), \\ (T,F,F) &\implies (a \wedge \overline{b} \wedge \overline{c}), \\ (F,T,F) &\implies (\overline{a} \wedge b \wedge \overline{c}), \\ (F,F,T) &\implies (\overline{a} \wedge \overline{b} \wedge c). \end{aligned}$$

Thus, the DNF of f is

$$(a \wedge b \wedge c) \vee (a \wedge \overline{b} \wedge \overline{c}) \vee (\overline{a} \wedge b \wedge \overline{c}) \vee (\overline{a} \wedge \overline{b} \wedge c).$$

In a similar manner, we use F_f of f to find CNF.

$$\begin{aligned} (T,T,F) &\implies (\overline{a} \vee \overline{b} \vee c), \\ (T,F,T) &\implies (\overline{a} \vee b \vee \overline{c}), \\ (F,T,T) &\implies (a \vee \overline{b} \vee \overline{c}), \\ (F,F,F) &\implies (a \vee b \vee c). \end{aligned}$$

Thus, the CNF of f is

$$(\overline{a} \vee \overline{b} \vee c) \wedge (\overline{a} \vee b \vee \overline{c}) \wedge (a \vee \overline{b} \vee \overline{c}) \wedge (a \vee b \vee c).$$

□

2.4 Problem

Problem 1: Define sets

$$A = \{1, \ldots, 10\}, B = \{3, 7, 11, 12\}, C = \{0, 1, \ldots, 20\}.$$

Which of the following are propositions?

(1) $1 + 1 = 3$
(2) $(A \cup B) \subseteq C$
(3) $A \cap B$
(4) $(8 + 22)^3/10^2$
(5) $7 \in A$
(6) $(B \cap C) \in 9$
(7) C is an infinite set

Problem 2: Find the possible wff's f and g in the following truth table.

a	b	f	g
T	T	F	T
T	F	T	T
F	T	T	F
F	F	T	T

Problem 3: If $p \to q$ is false, what is the truth value of

$$((\neg p) \wedge q) \longleftrightarrow (p \vee q)?$$

Problem 4: Construct the truth tables for the following:

1. $(a \longrightarrow T) \wedge (F \longrightarrow b)$
2. $(F \vee a) \longrightarrow (b \wedge F)$
3. $(a \vee b) \wedge (a \vee \neg b)$

Problem 5: Which of the following is a tautology?

1. $(a \longleftrightarrow b) \to (a \wedge b)$,
2. $(a \longleftrightarrow b) \longleftrightarrow (a \wedge b) \vee (\neg a \wedge \neg b)$

Problem 6: Show that

$$(a \vee b \longrightarrow c) \Longrightarrow (a \wedge b \longrightarrow c),$$

but the converse (i.e., $(a \wedge b \to c) \Rightarrow (a \vee b \to c)$) is not true.

Problem 7: Let p, q, r denote the following statements about a triangle ABC.

p : Triangle ABC is isosceles;
q : Triangle ABC is equilateral;
r : Triangle ABC is equiangular.

Translate each of the following into an English sentence.

1. $q \longrightarrow p$
2. $\neg p \longrightarrow \neg q$
3. $q \longleftrightarrow r$
4. $p \wedge \neg q$
5. $r \longrightarrow p$

Problem 8: Let p, q, r denote primitive statements. Use truth tables to prove the following logical equivalences.

1. $p \to (q \wedge r) \iff (p \to q) \wedge (p \to r)$
2. $[(p \vee q) \to r] \iff [(p \to r) \wedge (q \to r)]$

Problem 9: Let p, q, r denote primitive statements. Use the laws of logic to show that

$$[p \longrightarrow (q \vee r)] \iff [(p \wedge \neg q) \longrightarrow r].$$

Problem 10: Let p, q, and r be primitive statements. Write the dual for the following statements.

1. $q \longrightarrow p$
2. $p \longrightarrow (q \wedge r)$
3. $p \longleftrightarrow q$

Problem 11: Show that

$$((a \wedge b) \longrightarrow c) \Longleftrightarrow ((a \longrightarrow c) \vee (b \longrightarrow c)).$$

Problem 12: Work out the truth tables for *modus ponens* to show that it is a logical implication but not an equivalence.

Problem 13: Consider

Premises: If there was a ball game, then traveling was difficult. If they arrived on time, then traveling was not difficult. They arrived on time.

Conclusion: There was no ball game.

Determine whether the conclusion follows logically from the premises. Explain by representing the statements symbolically and using rules of inference.

Problem 14: Consider

Premises: If Claghorn has wide support, then he'll be asked to run for the senate. If Claghorn yells "Eureka" in Iowa, he will not be asked to run for the senate. Claghorn yells "Eureka" in Iowa.

Conclusion: Claghorn does not have wide support.

Determine whether the conclusion follows logically from the premises. Explain by representing the statements symbolically and using rules of inference.

Problem 15: Write the converse, inverse, contrapositive, and negation of the following statement.

"If Sandra finishes her work, she will go to the basketball game."

Problem 16: Simplify

$$(p \wedge (\neg r \vee q \vee \neg q)) \vee ((r \vee t \vee \neg r) \wedge \neg q).$$

Problem 17: Simplify

$$(p \vee (p \wedge q) \vee (p \wedge q \wedge \neg r)) \wedge ((p \wedge r \wedge t) \vee t).$$

Problem 18: The following is a logical proof for

$$(p \wedge (p \to q) \wedge (s \vee r) \wedge (r \to \neg q)) \to (s \vee t).$$

Refer to the laws of logic and inference rule, and give reasons to justify each step of the proof.

steps		reasons
1.	p	
2.	$p \to q$	
3.	q	
4.	$r \to \neg q$	
5.	$q \to \neg r$	
6.	$\neg r$	
7.	$s \vee r$	
8.	s	
9.	$s \vee t$	

Problem 19: The following is a logical proof for the inference:

Premises :	$(\neg p \vee q) \to r$
	$r \to (s \vee t)$
	$\neg s \wedge \neg u$
	$\neg u \to \neg t$
Conclusion :	p

Give a reason to justify each step of the proof.

	steps	reasons
1.	$\neg s \wedge \neg u$	
2.	$\neg u$	
3.	$\neg u \rightarrow \neg t$	
4.	$\neg t$	
5.	$\neg s$	
6.	$\neg s \wedge \neg t$	
7.	$r \rightarrow (s \vee t)$	
8.	$\neg(s \vee t) \rightarrow \neg r$	
9.	$(\neg s \wedge \neg t) \rightarrow \neg r$	
10.	$\neg t$	
11.	$(\neg p \vee q) \rightarrow r$	
12.	$\neg r \rightarrow \neg(\neg p \vee q)$	
13.	$\neg r \rightarrow (p \vee \neg q)$	
14.	$p \wedge \neg q$	
15.	p	

Problem 20: The following is a logical proof for

$$((p \rightarrow q) \wedge (\neg r \vee s) \wedge (p \vee r)) \rightarrow (\neg q \rightarrow s).$$

	steps	reasons
1.	$\neg(\neg q \rightarrow s)$	
2.	$\neg q \wedge \neg s$	
3.	$\neg s$	
4.	$\neg r \vee s$	
5.	$\neg r$	
6.	$p \rightarrow q$	
7.	$\neg q$	
8.	$\neg p$	
9.	$p \vee r$	
10.	r	
11.	$\neg r \wedge r$	
12.	$\neg q \rightarrow s$	

1. Give a reason to justify each step of the proof. (Note: This is a proof by contradiction.)
2. Give a direct proof.

Problem 21: Prove that the following inference is valid.

Premises :	$\neg p \leftrightarrow q$
	$q \rightarrow r$
	$\neg r$
Conclusion :	p

Problem 22: Show that the following premises are inconsistent.

1. If Jack misses many classes through illness, then he fails high school.
2. If Jack fails high school, then he is uneducated.
3. If Jack reads a lot of books, then he is not uneducated.
4. Jack misses many classes through illness and reads a lot of books.

Problem 23: Let $D_x := \mathbf{R}$. Which of the following are predicates?

(1) $x^2 + 1 < 0$
(2) x is odd
(3) $(x^2 - 1)/(x + 1)$
(4) $1 + 2 = 3$
(5) $x \in \mathbf{N}$
(6) $\sin^2 x + \cos^2 x$

Problem 24: Define

$$\begin{aligned} A &= \{x | x \in \mathbf{N},\ x \leq 10\}; \\ B &= \{y;\ y \in \mathbf{N},\ y \leq 15,\ y \text{ is even}\}. \end{aligned}$$

Write two predicates, of which $A - B$ and $B - A$ are the truth sets respectively.

Problem 25: Let P and Q be two predicates, and let their truth sets be denoted as T_P, T_Q, and falsity sets be denoted as F_P, F_Q. Prove the following identities.

1. $T_P \cap T_Q = T_{P \wedge Q}$
2. $T_P \cup T_Q = T_{P \vee Q}$
3. $F_P \cap F_Q = F_{P \vee Q}$
4. $F_P \cup F_Q = F_{P \wedge Q}$

Problem 26: What are the most general conditions on the truth sets T_P and T_Q making

1. $(P(x) \longrightarrow Q(x)) \Longrightarrow P(x)$ true
2. $(P(x) \longrightarrow Q(x)) \Longrightarrow Q(x)$ true

Problem 27: Suppose the domain D for predicates P, Q, and S is $\{a, b, c\}$. Express the following propositions without using quantifiers.

1. $\forall x\ P(x)$
2. $(\forall x\ R(x)) \wedge (\exists x\ S(x))$

Problem 28: Let $D_x = D_y = \{1, 2, 3, 4, 5\}$. Define the predicate $P(x, y)$ as

$$P(x, y) \ := \ (y \geq x) \text{ or } (x + y > 6).$$

Find the truth sets of the following predicates:

1. $P(x, y)$.
2. $\exists x P(x, y)$
3. $\exists y P(x, y)$
4. $\forall x P(x, y)$
5. $\forall y P(x, y)$

Problem 29: Let V be the truth set of $P(x, y)$. Thus, $V \subseteq D_x \times D_y$.

1. Prove that the truth set of $\exists x \in D_x P(x, y)$ is the set of all second coordinates of ordered pairs in V.
2. Prove that the truth set of $\forall x \in D_x P(x, y)$ is

$$\{b;\ b \in D_y,\ \ D_x \times \{b\} \subseteq V\}.$$

Problem 30: Let sets

$$\begin{aligned} D_x &= \{t;\ t \in \mathbf{R},\ -1 \leq t \leq 1\} \ \text{ and} \\ D_y &= \{r;\ r \in \mathbf{R},\ 0 \leq r \leq 1\} \end{aligned}$$

be the universes of x and y, respectively. Define

$$\begin{aligned} P(x, y) &= (x + y \leq 1) \wedge (y - x \leq 1); \\ Q(x, y) &= x^2 + y^2 \leq 1. \end{aligned}$$

Prove that $T_P \subseteq T_Q$, where T_P is the truth set of P and T_Q is the truth set of Q.

Problem 31: Let A, B and S be sets. The following is a wrong proof to claim that

$$S \subseteq (A \cup B) \Rightarrow (S \subseteq A \text{ or } S \subseteq B).$$

Wrong proof: If $S \subseteq (A \cup B)$, then

$$\begin{aligned} &x \in S \Rightarrow x \in (A \cup B), && (1) \\ &x \in S \Rightarrow (x \in A \text{ or } x \in B), && (2) \\ &(x \in S \Rightarrow x \in A) \text{ or } (x \in S \Rightarrow x \in B), && (3) \\ &S \subseteq A \text{ or } S \subseteq B. && (4) \end{aligned}$$

Point out which step is problematic and explain why.

[Hint: consider the definition of subset in term of quantified predicates.]

Problem 32: Let $P(x, y)$ be a predicate defined as

$$P(x, y) : (x \vee y) \rightarrow z.$$

Express the negation of $\forall x \exists y\ P(x, y)$ without "$\neg$" in front of any quantifier.

Problem 33: Find the negations of the following two quantified predicates without "$\neg$" in front of any quantifier.

1. $\forall x\ \forall y\ [(x > y) \rightarrow (x - y > 0)]$.
2. $\forall x\ \forall y\ [(x < y) \rightarrow \exists z(x < z < y)]$.

Problem 34: Take $P1$ through $P7$ as premises. See what conclusion you can logically derive. Explain.

$P1$: All the policemen on this beat eat with our cook.

$P2$: No man with long hair can fail to be a poet.

$P3$: Amos Judd has never been in prison.

$P4$: Our cook's cousins all love cold mutton.

$P5$: None but policemen on this beat are poets.

$P6$: None but her cousins ever eat with the cook.

$P7$: Men with short hair have all been to prison.

Problem 35: Consider "No pigs have wings". Write this proposition as a quantified predicate.

Problem 36: Consider

Premises:
All soldiers can march.
Some babies are not soldiers.

Conclusion:
Some babies cannot march.

Determine whether the conclusion follows logically from the premises. Explain.

Problem 37: Let $D_x = \mathbf{N}$ and $D_y = \mathbf{N}^0$. Define $P(x, y)$ as "x divides y". Find the truth values of the following quantified predicates.

1. $\forall y P(1, y)$
2. $\forall x P(x, 0)$
3. $\forall x P(x, x)$
4. $\forall y \exists x P(x, y)$
5. $\exists y \forall x P(x, y)$

6. $\forall x \forall y[(P(x,y) \wedge P(y,x)) \rightarrow (x = y)]$
7. $\forall x \forall y \forall x[(P(x,y) \wedge P(y,x)) \rightarrow P(x,z)]$

Problem 38: Let D_x and D_y denote the domains of x and y, respectively. Consider the following quantified statement

$$\forall x \; \exists y \; [x + y = 17].$$

Determine the truth value of the quantified predicate in different domains.

1. $D_x = D_y =$ the set of integers.
2. $D_x = D_y =$ the set of positive integers.
3. $D_x =$ the set of integers and $D_y =$ the set of positive integers.
4. $D_x =$ the set of positive integers and $D_y =$ the set of integers.

Problem 39: What is the DNF of

$$(a \longrightarrow b) \wedge (\neg a \longrightarrow \neg b)?$$

Problem 40: What is the DNF of

$$(a \longrightarrow b) \wedge (a \longrightarrow \neg b)?$$

Problem 41: Find the CNF's of

1. $a \longrightarrow \neg b$.
2. $(a \wedge b) \vee c$.

Problem 42: Let the wff f be $a \wedge (b \longleftrightarrow c)$.

1. Use the shortcut method (use the falsity set) to find the CNF of f.
2. Use the propositional calculus to find the DNF of f.

Problem 43: Consider the following mathematical statement in number theory:

"For every integer n bigger than 1, there is a prime strictly between n and $2n$."

1. Express the statement in terms of quantifiers, variable(s), predicates, and the inequality symbols $<$ or $>$.
2. Express the negation of the predicate found in 1 without using $\neg$.

[Be careful to define the domain(s) of your variable(s)]

Problem 44: Let x and y range over all integers. Prove that for all x, y, if xy is even, then at least one of x and y is even.

Problem 45: Are the following arguments logically correct?

Premises:
All who are anxious to learn work hard.
Some of these boys work hard.

Conclusion:
Therefore some of these boys are anxious to learn.

Problem 46: Are the following arguments logically correct?

Premises:
There are men who are soldiers.
All soldiers are strong.
All soldiers are brave.

Conclusion:
Therefore some strong men are brave.

Problem 47: Let the universe be a social club, and let x and y range over the members of the club. Define the predicate $P(x, y)$ as

$$P(x, y) := x \text{ loves } y.$$

Translate the following quantified predicates into English sentences

1. $\forall x \forall y\ P(x, y)$
2. $\exists x \exists y\ P(x, y)$
3. $\forall x \exists y\ P(x, y)$
4. $\exists x \forall y\ P(x, y)$

Problem 48: Let the domain range over all real numbers. Find a possible conclusion from the given premises.

Premises:
All integers are rational numbers.
The real number π is not a rational number.

Problem 49: Let the domain range over all people in the USA. Find a possible premise for the following inference.

Premises:
All librarians know the Library of Congress Classification System.
(unknown premise)

Conclusion:
Margaret knows the Library of Congress Classification System.

Problem 50: Let P and Q be two predicates. Prove that

$$\exists x[P(x) \vee Q(x)] \iff \exists x P(x) \vee \exists x Q(x).$$

Problem 51: Let P and Q be two predicates. Prove that

$$\forall x[P(x) \wedge Q(x)] \iff \forall x P(x) \wedge \forall x Q(x).$$

Problem 52: Let P and Q be two predicates. Prove that

$$\forall x P(x) \vee \forall x Q(x) \quad \Rightarrow \quad \forall x[P(x) \vee Q(x)].$$

Problem 53: Let P and Q be two predicates. Disprove that

$$\forall x[P(x) \vee Q(x)] \quad \Rightarrow \quad \forall x P(x) \vee \forall x Q(x).$$

Problem 54: Prove or disprove the following statement.

There exist a and b, where a and b are irrational and a^b is rational.

[Hint: Use the fact that $\sqrt{2}$ is irrational; a and b don't have to be distinct.]

2.5 Solutions

Solution 1: (1), (2), (5), and (7) are propositions.

(3), (4) and (6) are not propositions.

Note: (6) $(B \cap C) \in 9$ is not a proposition. It is meaningless, but that does not mean its truth value is F.

□

Solution 2: There are infinitely many wff's that satisfy the given truth table. The simplest two we can think of are

$$f = \neg(a \wedge b), \text{ and } \quad g = b \longrightarrow a.$$

□

Solution 3: Let $p \to q$ be false. The only case in which $p \to q$ is false is when $p = T$ and $q = F$. We can replace the occurrences of p and q by their values and find the result step by step as the following:

$$\begin{array}{rl} & ((\neg p) \wedge q) \leftrightarrow (p \vee q) \\ = & ((\neg T) \wedge F) \leftrightarrow (T \vee F) \\ = & (F \wedge F) \leftrightarrow T \\ = & F \leftrightarrow T \\ = & F \end{array}$$

Refer to the laws of logic to justify each step above. □

Solution 4:

1. Let $f(a,b) = (a \to T) \wedge (F \to b)$

a	b	T	F	$a \to T$	$F \to b$	$f(a,b)$
T	T	T	F	T	T	T
T	F	T	F	T	T	T
F	T	T	F	T	T	T
F	F	T	F	T	T	T

2. Let $f(a,b) = (F \vee a) \to (b \wedge F)$

a	b	T	F	$F \vee a$	$b \wedge F$	$f(a,b)$
T	T	T	F	T	F	F
T	F	T	F	T	F	F
F	T	T	F	F	F	T
F	F	T	F	F	F	T

3. Let $f(a,b) = (a \vee b) \wedge (a \vee \neg b)$.

a	b	$\neg b$	$a \vee b$	$a \vee \neg b$	$f(a,b)$
T	T	F	T	T	T
T	F	T	T	T	T
F	T	F	T	F	F
F	F	T	F	T	F

□

Solution 5: We will check the truth tables to tell whether the statements are tautologies or not.

1. Let $f = (a \leftrightarrow b) \to (a \wedge b)$.

a	b	$a \leftrightarrow b$	$a \wedge b$	f
T	T	T	T	T
T	F	F	F	T
F	T	F	F	T
F	F	T	F	F

   The last column of the truth table contains an F in the last row. Thus, f is not a tautology.

2. Let $g = (a \leftrightarrow b) \leftrightarrow (a \wedge b) \vee (\neg a \wedge \neg b)$.

   Note: g should be read as $(a \leftrightarrow b) \leftrightarrow ((a \wedge b) \vee (\neg a \wedge \neg b))$, but not as $((a \leftrightarrow b) \leftrightarrow (a \wedge b)) \vee (\neg a \wedge \neg b)$, because the precedence priority of $\vee$ is higher than the precedence priority of $\leftrightarrow$.

$$s = (a \wedge b) \vee (\neg a \wedge \neg b).$$

a	b	$a \leftrightarrow b$	$a \wedge b$	$\neg a \wedge \neg b$	s	g
T	T	T	T	F	T	T
T	F	F	F	F	F	T
F	T	F	F	F	F	T
F	F	T	F	T	T	T

Therefore, g is a tautology because every truth value in the last column of its truth table is true.

□

Solution 6: Let

$$\begin{aligned} p &= a \vee b \longrightarrow c \\ q &= a \wedge b \longrightarrow c \\ r &= (a \vee b \longrightarrow c) \longrightarrow (a \wedge b \longrightarrow c) \\ s &= (a \vee b \longrightarrow c) \longleftarrow (a \wedge b \longrightarrow c) \end{aligned}$$

a	b	c	$a \wedge b$	$a \vee b$	p	q	r	s
T	T	T	T	T	T	T	T	T
T	T	F	T	T	F	F	T	T
T	F	T	F	T	T	T	T	T
T	F	F	F	T	F	T	T	F
F	T	T	F	T	T	T	T	T
F	T	F	F	T	F	T	T	F
F	F	T	F	F	T	T	T	T
F	F	F	F	F	T	T	T	T

From the truth table above, r is a tautology and s is not. Therefore,

$$(a \vee b \longrightarrow c) \Longrightarrow (a \wedge b \longrightarrow c),$$

but its converse is not true. □

Solution 7: Let p: Triangle ABC is isosceles;
q: Triangle ABC is equilateral;
r: Triangle ABC is equiangular.

1. $q \longrightarrow p$: If triangle ABC is equilateral, then it is isosceles.
2. $\neg p \longrightarrow \neg q$: If triangle ABC is not isosceles, then it is not equilateral.
3. $q \longleftrightarrow r$: Triangle ABC is equilateral if and only if it is equiangular.
4. $p \wedge \neg q$: Triangle ABC is isosceles, but not equilateral.
5. $r \longrightarrow p$: If triangle ABC is equiangular, then it is isosceles.

□

Solution 8:

1. To prove that $p \rightarrow (q \wedge r) \iff (p \rightarrow q) \wedge (p \rightarrow r)$, let

$$\begin{aligned} s &= p \rightarrow (q \wedge r), \\ t &= (p \rightarrow q) \wedge (p \rightarrow r), \\ u &= (p \rightarrow (q \wedge r)) \leftrightarrow ((p \rightarrow q) \wedge (p \rightarrow r)). \end{aligned}$$

p	q	r	$q \wedge r$	$p \rightarrow q$	$p \rightarrow r$	s	t	u
T	T	T	T	T	T	T	T	T
T	T	F	F	T	F	F	F	T
T	F	T	F	F	T	F	F	T
T	F	F	F	F	F	F	F	T
F	T	T	T	T	T	T	T	T
F	T	F	F	T	T	T	T	T
F	F	T	F	T	T	T	T	T
F	F	F	F	T	T	T	T	T

Since the last column contains truth value T for all possible values of $p.q$, and r, therefore, $p \rightarrow (q \wedge r)$ and $(p \rightarrow q) \wedge (p \rightarrow r)$ are logically equivalent.
□

2. To prove that $((p \vee q) \rightarrow r) \iff ((p \rightarrow r) \wedge (q \rightarrow r))$, let

$$\begin{aligned} s &= (p \vee q) \rightarrow r, \\ t &= (p \rightarrow r) \wedge (q \rightarrow r), \\ u &= ((p \vee q) \rightarrow r) \leftrightarrow ((p \rightarrow r) \wedge (q \rightarrow r)), \end{aligned}$$

and construct the truth table:

p	q	r	$p \vee q$	$p \to r$	$q \to r$	s	t	u
T	T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	F	T	T	T	T	T	T	T
T	F	F	T	F	T	F	F	T
F	T	T	T	T	T	T	T	T
F	T	F	T	T	F	F	F	T
F	F	T	F	T	T	T	T	T
F	F	F	F	T	T	T	T	T

Clearly, $(p \vee q) \to r$ and $(p \to r) \wedge (q \to r)$ are logically equivalent.

□

Solution 9: Using the laws of logic we obtain:

$$
\begin{array}{ll}
p \to (q \vee r) & \\
\iff \neg p \vee (q \vee r) & \text{Logical equivalence} \\
\iff (\neg p \vee q) \vee r & \text{Associative law} \\
\iff \neg\neg(\neg p \vee q) \vee r & \text{Double negation law} \\
\iff \neg(\neg\neg p \wedge \neg q) \vee r & \text{De Morgan's law} \\
\iff \neg(p \wedge \neg q) \vee r & \text{Double negation law} \\
\iff (p \wedge \neg q) \to r & \text{Logical equivalence}
\end{array}
$$

Therefore, $[p \longrightarrow (q \vee r)] \iff [(p \wedge \neg q) \longrightarrow r]$. □

Solution 10: From the definition of duality it is not possible to give the dual of a logical statement that contains "$\to$" or "$\leftrightarrow$". We have to find its logical equivalent statements that contain no logical connectives other than "$\wedge$" and "$\vee$".

1. Since $q \to p \equiv \neg q \vee p$, hence the dual of $q \to p$ is $\neg q \wedge p$.

2. Since $p \to (q \wedge r) \equiv \neg p \vee (q \wedge r)$ its dual is $\neg p \wedge (q \vee r)$.

3. Reduction of $p \leftrightarrow q$ to a formula that contains connectives only $\wedge, \vee$, and

$\neg$ is given below.

$$\begin{aligned} p \leftrightarrow q &\equiv (p \rightarrow q) \wedge (q \rightarrow p) \\ &\equiv (\neg p \vee q) \wedge (\neg q \vee p) \\ &\equiv [(\neg p \vee q) \wedge \neg q] \vee [(\neg p \vee q) \wedge p] \\ &\equiv (\neg p \wedge \neg q) \vee (q \wedge \neg q) \vee (\neg p \wedge p) \vee (q \wedge p) \\ &\equiv (\neg p \wedge \neg q) \vee F \vee F \vee (q \wedge p) \\ &\equiv (\neg p \wedge \neg q) \vee (q \wedge p). \end{aligned}$$

Thus, the dual of $p \leftrightarrow q$ is $(\neg p \vee \neg q) \wedge (q \vee p)$.

□

Solution 11: Our goal is to show that the values in the last column of the truth table are all true. Let,

$$\begin{aligned} &s = (a \wedge b) \rightarrow c, \\ &t = (a \rightarrow c) \vee (b \rightarrow c), \\ &u = ((a \wedge b) \rightarrow c) \leftrightarrow ((a \rightarrow c) \vee (b \rightarrow c)). \end{aligned}$$

a	b	c	$a \wedge b$	$a \rightarrow c$	$b \rightarrow c$	s	t	u
T	T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	F	T	F	T	T	T	T	T
T	F	F	F	F	T	T	T	T
F	T	T	F	T	T	T	T	T
F	T	F	F	T	F	T	T	T
F	F	T	F	T	T	T	T	T
F	F	F	F	T	T	T	T	T

Therefore, u is a tautology. □

Solution 12: Recall that the Modus Ponens rule is: $(a \wedge (a \rightarrow b)) \Rightarrow b$. Let,

$$\begin{aligned} &s = (a \wedge (a \rightarrow b)) \rightarrow b, \\ &t = (a \wedge (a \rightarrow b)) \leftrightarrow b. \end{aligned}$$

a	b	$a \rightarrow b$	$a \wedge (a \rightarrow b)$	s	t
T	T	T	T	T	T
T	F	F	F	T	T
F	T	T	F	T	F
F	F	T	F	T	T

From the truth table above, we know that s is a tautology. Therefore,

$$(a \wedge (a \to b)) \Rightarrow b.$$

But t is not a tautology, and hence the Modus Ponens is not a logical equivalence. □

Solution 13: Let BG: there was a ball game,
TD: traveling was difficult,
AO: they arrived on time.

Premises: $BG \longrightarrow TD$, $AO \longrightarrow \neg TD$, AO.

Conclusion: $\neg BG$.

	steps	*reasons*
1.	$BG \to TD$	Premises
2.	$AO \to \neg TD$	Premises
3.	AO	Premises
4.	$\neg TD$	2,3, Modus Ponens
5.	$\neg TD \to \neg BG$	1, Contrapositive
6.	$\neg BG$	4,5, Modus Ponens

Therefore, the conclusion that there was no ball game is logically correct based on the given premises. □

Solution 14: Let CS: Claghorn has wide support,
RS: Claghorn is asked to run for the senate,
CY: Claghorn yells "Eureka"

Premises: $CS \longrightarrow RS$, $CY \longrightarrow \neg RS$, CY.

Conclusion: $\neg CS$.

	steps	*reasons*
1.	$CS \to RS$	Premises
2.	$CY \to \neg RS$	Premises
3.	CY	premises
4.	$CY \wedge (CY \to \neg RS)$	$2 \wedge 3$
5.	$\neg RS$	4, Modus Ponens
6.	$\neg RS \to \neg CS$	1, Contrapositive
7.	$\neg RS \wedge (\neg RS \to \neg CS)$	$5 \wedge 6$
8.	$\neg CS$	7, Modus Ponens

Therefore, "Claghorn doesn't have wide support" is logically correct from the given premises. □

Solution 15: Let p : Sandra finishes her work.
q : Sandra goes to the basketball game.

Implication: $(p \rightarrow q)$
If Sandra finishes her work, she will go to the basketball game.

Converse: $(q \rightarrow p)$
If Sandra goes to the basketball game, she will finish her work.

Inverse: $(\neg p \rightarrow \neg q)$
If Sandra does not finish her work, she will not go to the basketball game.

Contrapositive: $(\neg q \rightarrow \neg p)$
If Sandra does not go to the basketball game, she does not finish her work.

Negation: $(p \ \wedge \neg q)$
Sandra finishes her work, and she does not go to the basketball game.

□

Solution 16:

$$\begin{aligned}
&(p \wedge (\neg r \vee q \vee \neg q)) \vee ((r \vee t \vee \neg r) \wedge \neg q) \\
&\quad \Leftrightarrow \quad (p \wedge (\neg r \vee T)) \vee ((t \vee T) \wedge \neg q) \\
&\quad \Leftrightarrow \quad (p \wedge T) \vee (T \wedge \neg q) \\
&\quad \Leftrightarrow \quad p \vee \neg q.
\end{aligned}$$

□

Solution 17:

$$(p \vee (p \wedge q) \vee (p \wedge q \wedge \neg r)) \wedge ((p \wedge r \wedge t) \vee t)$$

$$\begin{aligned}
&\Leftrightarrow (p \vee (p \wedge q \wedge T) \vee (p \wedge q \wedge \neg r)) \wedge ((p \wedge r \wedge t) \vee (T \wedge t) && (1)\\
&\Leftrightarrow (p \vee (((p \wedge q) \wedge T) \vee ((p \wedge q) \wedge \neg r))) \wedge (((p \wedge r) \wedge t) \vee (T \wedge t) && (2)\\
&\Leftrightarrow (p \vee ((p \wedge q) \wedge (T \vee \neg r)) \wedge (((p \wedge r) \vee T) \wedge t) && (3)\\
&\Leftrightarrow (p \vee ((p \wedge q) \wedge T) \wedge (T \wedge t) && (4)\\
&\Leftrightarrow (p \vee (p \wedge q)) \wedge t) && (5)\\
&\Leftrightarrow ((p \wedge T) \vee (p \wedge q)) \wedge t && (6)\\
&\Leftrightarrow (p \wedge (T \vee q)) \wedge t && (7)\\
&\Leftrightarrow (p \wedge T) \wedge t && (8)\\
&\Leftrightarrow p \wedge t && (9)
\end{aligned}$$

Explanation: In (1) identity law is used to have $(p \wedge q) \Leftrightarrow (p \wedge q \wedge T)$ and $t \Leftrightarrow (T \wedge t)$. Associative law is use is (2). Distributive law is used in (3). Domination law is used is (4). Identity law is used in (5) and (6) to drop two T's and add one T, respectively. Distributive law is used in (7). Domination law is used is (8). Finally, we use identity law in the last step. □

Solution 18: To prove $(p \wedge (p \rightarrow q) \wedge (s \vee r) \wedge (r \rightarrow \neg q)) \rightarrow (s \vee t)$, we will take p, $p \rightarrow q$, $s \vee r$, and $r \rightarrow \neg q$ as the given assumptions.

steps		*reasons*
1.	p	Assumption
2.	$p \rightarrow q$	Assumption
3.	q	1,2, Modus Ponens
4.	$r \rightarrow \neg q$	Assumption
5.	$q \rightarrow \neg r$	4, Contrapositive
6.	$\neg r$	3,5, Modus Ponens
7.	$s \vee r$	Assumption
8.	s	6,7, Disjunctive Syllogism
9.	$s \vee t$	8, Disjunctive Amplification

□

Solution 19:

Premises :	$(\neg p \vee q) \rightarrow r,\ r \rightarrow (s \vee t),\ \neg s \wedge \neg u,\ \neg u \rightarrow \neg t$
Conclusion :	p

	steps	*reasons*
1.	$\neg s \wedge \neg u$	Premises
2.	$\neg u$	1, Conjunctive Simplification
3.	$\neg u \rightarrow \neg t$	Premises
4.	$\neg t$	2,3, Modus Ponens
5.	$\neg s$	1, Conjunctive Simplification
6.	$\neg s \wedge \neg t$	4,5, Conjunction
7.	$r \rightarrow (s \vee t)$	Premises
8.	$\neg(s \vee t) \rightarrow \neg r$	7, Contrapositive
9.	$(\neg s \wedge \neg t) \rightarrow \neg r$	8, De Morgan's law
10.	$\neg r$	6,9, Modus Ponens
11.	$(\neg p \vee q) \rightarrow r$	Premises
12.	$\neg r \rightarrow \neg(\neg p \vee q)$	11, Contrapositive
13.	$\neg r \rightarrow (p \vee \neg q)$	12, De Morgan's law
14.	$p \wedge \neg q$	10,13, Modus Ponens
15.	p	14, Conjunctive Simplification

□

Solution 20:

$$((p \rightarrow q) \wedge (\neg r \vee s) \wedge (p \vee r)) \rightarrow (\neg q \rightarrow s) \tag{2.4}$$

1. The following proof for (2.4) is a contradiction argument. By contradiction, we assume that the premises and the negation of the consequence are both true, i.e., we have

   Assumptions: $p \rightarrow q,\ \neg r \vee s,\ p \vee r,\ \neg(\neg q \rightarrow s)$.

	steps	*reasons*
1.	$\neg(\neg q \rightarrow s)$	Assumption, by Contradiction)
2.	$\neg q \wedge \neg s$	Negation of implication
3.	$\neg s$	2, Conjunctive Simplification
4.	$\neg r \vee s$	Assumption
5.	$\neg r$	3,4, Disjunctive syllogism
6.	$p \rightarrow q$	Assumption
7.	$\neg q$	2, Conjunctive Simplification
8.	$\neg p$	6,7, Modus Tollens
9.	$p \vee r$	Assumption
10.	r	8,9, Disjunctive syllogism
11.	$\neg r \wedge r$	5,10, Conjunction
12.	$\neg q \rightarrow s$	Since 11 is a contradiction, 1 can't be true

   □

2. A direct proof for (2.4).

   Assumptions: $p \rightarrow q,\ \neg r \vee s,\ p \vee r$.

steps		reasons
1.	$p \to q$	Assumption
2.	$\neg q \to \neg p$	Equivalence of 1
3.	$p \vee r$	Assumption
4.	$\neg p \to r$	Equivalence of 3
5.	$\neg q \to r$	2,4, Syllogism
6.	$\neg r \vee s$	Assumption
7.	$r \to s$	Equivalence of 6
8.	$\neg q \to s$	5,7, Syllogism

□

Solution 21:

Premises :	$\neg p \leftrightarrow q,\ q \to r,\ \neg r$
Conclusion :	p

steps		*reasons*
1.	$\neg p \leftrightarrow q$	Premises
2.	$\neg p \to q$	From 1
3.	$q \to \neg p$	From 1
4.	$q \to r$	Premises
5.	$\neg r \to \neg q$	4, Contrapositive
6.	$\neg r$	Premises
7.	$\neg q$	5,6 Modus Ponens
8.	$\neg q \to p$	2 Contrapositive
9.	p	7,8 Modus Ponens

□

Solution 22: We say a system (a set of premises) is inconsistent if and only if we can obtain some results from the system that contradict each other.

Let MC: Jack misses many classes.
FS: Jack fails school.
UE: Jack is uneducated.
RB: Jack reads a lot of books.

Premises : $MC \to FS,\ FS \to UE,\ RB \to \neg EU,\ MC \wedge RB.$

	steps	*reasons*
1.	$MC \wedge RB$	Premises
2.	MC	1, Conjunctive Simplification
3.	$MC \longrightarrow FS$	Premises
4.	FS	2,3, Modus Ponens
5.	$FS \longrightarrow UE$	Premises
6.	UE	4,5, Modus Ponens
7.	$RB \longrightarrow \neg UE$	Premises
8.	RB	1, Conjunctive Simplification
9.	$\neg UE$	7,8, Modus Ponens
10.	$UE \wedge \neg UE$	6,9, Conjunction

We have both UE and $\neg UE$, and hence the premises are inconsistent. □

Solution 23: Recall the definition of predicates: A statement is a predicate if we can replace every variable in the statement by any instance in its domain to form a proposition.

(1), (2), (4) and (5) are predicates. (3) and (6) are not predicates.

Note: A predicate may not have any variable. Therefore, all propositions are also predicates, and hence (4) is a predicate.

□

Solution 24: Let $D_x = \mathbf{N}$ be the universe of x. We find $A - B$ and $B - A$ as

$$A - B = \{1, 3, 5, 7, 9\} \text{ and } B - A = \{12, 14\}.$$

Define predicates $P(x)$ and $Q(x)$ as

$$P(x) = (x \in A) \wedge (x \notin B) \text{ and } Q(x) = (x \notin A) \wedge (x \in B).$$

Thus, $T_P = A - B$ and $T_Q = B - A$.

Note: One does not give, for example, $\{x : x \in \mathbf{N}, 10 < x \leq 15, x \text{ is even } \}$ as the answer because it is the true-set of Q, but not a predicate with the truth set $B - A$.

□

Solution 25:

1. $T_P \cap T_Q = T_{P \wedge Q}$

$$\begin{aligned} x \in T_P \cap T_Q &\Leftrightarrow x \in T_P \text{ and } x \in T_Q \\ &\Leftrightarrow P(x) = T \text{ and } Q(x) = T \\ &\Leftrightarrow (P \wedge Q)(x) = T \\ &\Leftrightarrow x \in T_{P \wedge Q}. \end{aligned}$$

2. $T_P \cup T_Q = T_{P \vee Q}$

$$\begin{aligned} x \in T_P \cup T_Q &\Leftrightarrow x \in T_P \text{ or } x \in T_Q \\ &\Leftrightarrow P(x) = T \text{ or } Q(x) = T \\ &\Leftrightarrow (P \vee Q)(x) = T \\ &\Leftrightarrow x \in T_{P \vee Q}. \end{aligned}$$

3. $F(P) \cap F(Q) = F_{P \vee Q}$

$$\begin{aligned} x \in F(P) \cap F(Q) &\Leftrightarrow x \in F(P) \text{ and } x \in F(Q) \\ &\Leftrightarrow P(x) = F \text{ and } Q(x) = F \\ &\Leftrightarrow (P \vee Q)(x) = F \qquad \text{(why?)} \\ &\Leftrightarrow x \in F_{P \vee Q}. \end{aligned}$$

4. $F(P) \cup F(Q) = F_{P \wedge Q}$

$$\begin{aligned} x \in F(P) \cup F(Q) &\Leftrightarrow x \in F(P) \text{ or } x \in F(Q) \\ &\Leftrightarrow P(x) = F \text{ or } Q(x) = F \\ &\Leftrightarrow (P \wedge Q)(x) = F \qquad \text{(why?)} \\ &\Leftrightarrow x \in F_{P \wedge Q}. \end{aligned}$$

□

Solution 26: Let $T_{P \to Q}$ denote the truth set of $P(x) \to Q(x)$.

1. $(P(x) \to Q(x)) \Rightarrow P(x)$.

$$\begin{aligned} [(P(x) \to Q(x)) \Rightarrow P(x)] &\Leftrightarrow T_{P \to Q} \subseteq T_P \\ &\Leftrightarrow (F_P \cup T_Q) \subseteq T_P \\ &\Leftrightarrow (\overline{T_P} \cup T_Q) \subseteq T_P \\ &\Leftrightarrow \overline{T_P} \subseteq T_P \text{ and } T_Q \subseteq T_P. \end{aligned}$$

The only possibility to make $\overline{T_P} \subseteq T_P$ is when $\overline{T_P} = \emptyset$, namely, $T_P = U$. If $T_P = U$, then $T_Q \subseteq T_P$ is satisfied for any T_Q. Therefore, $T_P = U$ is the most general condition for $(P(x) \to Q(x)) \Rightarrow P(x)$ to be true.

2. $(P(x) \to Q(x)) \Rightarrow Q(x)$.

$$\begin{aligned}[(P(x) \to Q(x)) \Rightarrow Q(x)] &\Leftrightarrow T_{P\to Q} \subseteq T_Q \\ &\Leftrightarrow (F_P \cup T_Q) \subseteq T_Q \\ &\Leftrightarrow F_P \subseteq T_Q \text{ and } T_Q \subseteq T_Q \\ &\Leftrightarrow F_P \subseteq T_Q.\end{aligned}$$

Therefore, $F_P \subseteq T_Q$ is the most general condition for $(P(x) \to Q(x)) \Rightarrow Q(x)$ to be true.

Note: The most general condition means the least restricted or the weakest condition. For example, consider $1 < a < 10$ and $1 < a$. $1 < a$ is weaker than $1 < a < 10$, hence $1 < a$ is more general than $1 < a < 10$. □

Solution 27: Let $D_x = \{a, b, c\}$.

1. $\forall x P(x) \;=\; P(a) \wedge P(b) \wedge P(c)$.
2. $(\forall x R(x)) \wedge (\exists x S(x)) \;=\; (R(a) \wedge R(b) \wedge R(c)) \wedge (S(a) \vee S(b) \vee S(c))$.

□

Solution 28: Let $D_x = D_y = \{1, 2, 3, 4, 5\}$, and $P(x, y) := (y \geq x) \vee (x + y > 6)$. Thus, the truth set of $P(x, y)$ is a subset of $D_x \times D_y$.

1. $T_{P(x,y)} = T_{y\geq x} \cup T_{x+y>6}$.

$$T_{y\geq x} = \left\{ \begin{array}{l} (1,1), \\ (1,2),(2,2), \\ (1,3),(2,3),(3,3), \\ (1,4),(2,4),(3,4),(4,4), \\ (1,5),(2,5),(3,5),(4,5),(5,5) \end{array} \right\},$$

$$T_{x+y>6} = \left\{ \begin{array}{r} (5,2), \\ (4,3),(5,3), \\ (3,4),(4,4),(5,4), \\ (2,5),(3,5),(4,5),(5,5) \end{array} \right\}.$$

$$T_{y\geq x} \cup T_{x+y>6} = \left\{ \begin{array}{l} (1,1), \\ (1,2),(2,2), \qquad\qquad (5,2), \\ (1,3),(2,3),(3,3),(4,3),(5,3), \\ (1,4),(2,4),(3,4),(4,4),(5,4), \\ (1,5),(2,5),(3,5),(4,5),(5,5) \end{array} \right\}.$$

2. $T_{\exists x P(x,y)} = T_{P(1,y)} \cup T_{P(2,y)} \cup T_{P(3,y)} \cup T_{P(4,y)} \cup T_{P(5,y)}$.

$$\begin{aligned} T_{P(1,y)} &= \{y : (y \geq 1) \vee (y > 5)\} = \{1,2,3,4,5\}, \\ T_{P(2,y)} &= \{y : (y \geq 2) \vee (y > 4)\} = \{2,3,4,5\}, \\ T_{P(3,y)} &= \{y : (y \geq 3) \vee (y > 3)\} = \{3,4,5\}, \\ T_{P(4,y)} &= \{y : (y \geq 4) \vee (y > 2)\} = \{3,4,5\}, \\ T_{P(5,y)} &= \{y : (y \geq 5) \vee (y > 1)\} = \{2,3,4,5\}. \end{aligned}$$

   Therefore, $T_{\exists x P(x,y)} = \{1,2,3,4,5\}$.

3. $T_{\exists y P(x,y)} = T_{P(x,1)} \cup T_{P(x,2)} \cup T_{P(x,3)} \cup T_{P(x,4)} \cup T_{P(x,5)}$.

$$\begin{aligned} T_{P(x,1)} &= \{x : (1 \geq x) \vee (x > 5)\} = \{1\}, \\ T_{P(x,2)} &= \{x : (2 \geq x) \vee (x > 4)\} = \{1,2,5\}, \\ T_{P(x,3)} &= \{x : (3 \geq x) \vee (x > 3)\} = \{1,2,3,4,5\}, \\ T_{P(x,4)} &= \{x : (4 \geq x) \vee (x > 2)\} = \{1,2,3,4,5\}, \\ T_{P(x,5)} &= \{x : (5 \geq x) \vee (x > 1)\} = \{2,3,4,5\}. \end{aligned}$$

   Therefore, $T_{\exists y P(x,y)} = \{1,2,3,4,5\}$.

4. $T_{\forall x P(x,y)} = T_{P(1,y)} \cap T_{P(2,y)} \cap T_{P(3,y)} \cap T_{P(4,y)} \cap T_{P(5,y)} = \{3,4,5\}$.

5. $T_{\forall y P(x,y)} = T_{P(x,1)} \cap T_{P(x,2)} \cap T_{P(x,3)} \cap T_{P(x,4)} \cap T_{P(x,5)} = \{1\}$.

□

Solution 29: Let $V = T_{P(x,y)}$.

1. The set of all second coordinates of ordered pairs in V can be expressed as $S = \{y : \exists x, (x,y) \in V\}$. Given any b,

$$\begin{aligned} b \in T_{\exists x P(x,y)} &\Leftrightarrow \exists x P(x,b) \\ &\Leftrightarrow \exists x, (x,b) \in V \\ &\Leftrightarrow b \in S. \end{aligned}$$

   Therefore, $T_{\exists x P(x,y)} = S$.

2. Given any k,

$$\begin{aligned} k \in T_{\forall x P(x,y)} &\Leftrightarrow \forall x P(x,k) \\ &\Leftrightarrow \forall x \in D_x, (x,k) \in T_{P(x,y)} \\ &\Leftrightarrow \forall x \in D_x, (x,k) \in V \\ &\Leftrightarrow D_x \times \{k\} \subseteq V \\ &\Leftrightarrow k \in \{b : b \in D_y, D_x \times \{b\} \subseteq V\}. \end{aligned}$$

Therefore, $T_{\forall x \in D_x P(x,y)} = \{b : b \in D_y, D_x \times \{b\} \subseteq V\}$.

□

Solution 30: Recall that $T_P \subseteq T_Q$ is equivalent to $P \Rightarrow Q$. Suppose $x \in D_x$, $y \in D_y$, and $(x + y \leq 1) \wedge (y - x \leq 1)$. We prove $P \Rightarrow Q$ in the following.

1. From $x + y \leq 1$:

	steps	*reasons*
(1)	$x + y \leq 1$	given
(2)	$-1 \leq x$	$x \in D_x$
(3)	$0 \leq y$	$y \in D_y$
(4)	$-1 \leq x + y$	(2) + (3)
(5)	$-1 \leq x + y \leq 1$	(1) + (4)
(6)	$(x + y)^2 \leq 1$	math (5)
(7)	$x^2 + 2xy + y^2 \leq 1$	math (6)

2. $y - x \leq 1$

	steps	*reasons*
(1)	$y - x \leq 1$	given
(2)	$0 \leq y$	$y \in D_y$
(3)	$1 \geq x$	$x \in D_x$
(4)	$-1 \leq -x$	(3) $\times -1$
(5)	$-1 \leq y - x \leq 1$	(2) + (4)
(6)	$(y - x)^2 \leq 1$	math (5)
(7)	$x^2 - 2xy + y^2 \leq 1$	math (6)

From $x + y \leq 1$ and $y - x \leq 1$ we have derived

$$x^2 + 2xy + y^2 \leq 1, \tag{2.5}$$

$$x^2 - 2xy + y^2 \leq 1. \tag{2.6}$$

Take (2.5) + (2.6), we have

$$2x^2 + 2y^2 \leq 2 \quad \Longrightarrow \quad x^2 + y^2 \leq 1.$$

Therefore, we conclude that $x^2 + y^2 \leq 1$, i.e.

$$((x + y \leq 1) \wedge (y - x \leq 1)) \Rightarrow (x^2 + y^2 \leq 1).$$

□

Solution 31: Recall the definition of subset. We say that S is a subset of X if and only if for all x, if x is in S, then x is in X. We may rewrite the definition as

$$S \subseteq X \quad \text{iff} \quad (x \in S) \Rightarrow (x \in X).$$

Please note that we are using "⇒" in the above definition instead of "→", i.e., S is a subset of X if and only if $(x \in S \rightarrow\ x \in X)$ is a tautology. Therefore, it is legitimate not to express "for all" explicitly in the second definition.[1]

In order to easily find the error in this problem, let us rewrite the definition of subset without omitting the universal quantifier.

$$S \subseteq X \quad \text{iff} \quad \forall x(x \in S \rightarrow x \in X).$$

Therefore, $S \subseteq (A \cup B)$ iff

$$\begin{array}{lll} \forall x(x \in S \rightarrow x \in (A \cup B)) & & (1) \\ \Rightarrow \quad \forall x(x \in S \rightarrow (x \in A \text{ or } x \in B)) & & (2) \\ \Rightarrow \quad \forall x[(x \in S \rightarrow x \in A) \text{ or } (x \in S \rightarrow x \in B)] & & \\ \not\Rightarrow \quad \forall x(x \in S \rightarrow x \in A) \text{ or } \forall x(x \in S \rightarrow x \in B) & & (3) \\ \Rightarrow \quad (S \subseteq A \text{ or } S \subseteq B). & & (4) \end{array}$$

Step (3) in the original proof is incorrect.

We may consider an easy example to see why (2) $\not\Rightarrow$ (3). Let S, A, and B be sets defined as the following.

[1] Please bear in mind that, in mathematics, if the universe is clear or of no importance in the discourse, it is not uncommon to discard the universal quantifier *if it is the outermost quantifier* in a predicate.

$$S = \text{all children},\ A = \text{all boys},\ B = \text{all girls}.$$

It is clear that (2) is true, which means "for all x, if x is a child, then x is either a boy or a girl." However, (3) is not true, which means "either all children are boys, or all children are girls." □

Solution 32:

$$\begin{aligned} \neg\forall x\exists y[(x \vee y) \to z] &\Leftrightarrow \exists x\neg\exists y[(x \vee y) \to z] \\ &\Leftrightarrow \exists x\forall y\neg[(x \vee y) \to z] \\ &\Leftrightarrow \exists x\forall y[(x \vee y) \wedge \neg z]. \end{aligned}$$

□

Solution 33: To find the negations of the given formulas, we use the basic rules and De Morgan's laws. Recall that $\neg\exists x p(x) \equiv \forall x\neg p(x)$ and $\neg\forall x p(x) \equiv \exists x\neg p(x)$ for any predicate $p(x)$. Thus,

1. $\neg\forall x\ \forall y\ [(x > y) \to (x - y > 0)]$

$$\begin{aligned} &\Leftrightarrow \exists x\ \neg\forall y\ [(x > y) \to ((x - y) > 0)] \\ &\Leftrightarrow \exists x\ \exists y\ \neg[(x > y) \to ((x - y) > 0)] \\ &\Leftrightarrow \exists x\ \exists y\ [(x > y) \wedge \neg((x - y) > 0)] \\ &\Leftrightarrow \exists x\ \exists y\ [(x > y) \wedge ((x - y) \leq 0)] \\ &\Leftrightarrow \exists x\ \exists y\ [(x > y) \wedge (x \leq y)]. \end{aligned}$$

2. $\neg\forall x\ \forall y\ [(x < y) \to \exists z(x < z < y)]$

$$\begin{aligned} &\Leftrightarrow \exists x\ \neg\forall y\ [(x < y) \to \exists z\ (x < z < y)] \\ &\Leftrightarrow \exists x\ \exists y\ \neg[(x < y) \to \exists z\ (x < z < y)] \\ &\Leftrightarrow \exists x\ \exists y\ [(x < y) \wedge \neg\exists z\ (x < z < y)] \\ &\Leftrightarrow \exists x\ \exists y\ [(x < y) \wedge \forall z\ \neg(x < z < y)] \\ &\Leftrightarrow \exists x\ \exists y\ [(x < y) \wedge \forall z\ ((z \leq x) \vee (y \leq z))] \\ &\Leftrightarrow \exists x\ \exists y\ \forall z\ [(x < y) \wedge ((z \leq x) \vee (y \leq z))] \\ &\Leftrightarrow \exists x\ \exists y\ \forall z\ [((x < y) \wedge (z \leq x)) \vee ((x < y) \wedge (y \leq z))] \\ &\Leftrightarrow \exists x\ \exists y\ \forall z\ [(z \leq x < y) \vee (x < y \leq z)]. \end{aligned}$$

□

Solution 34: Let the domain D_x be the set of all people. Define the following predicates.

$PB(x)$: x is a policeman in this beat.
$SC(x)$: x eats with our cook.
$ML(x)$: x is a man with long hair.
$PE(x)$: x is a poet.
$PR(x)$: x has been in prison.
$CC(x)$: x is our cook's cousin.
$HC(x)$: x is her cousin.
$LC(x)$: x loves cold mutton.
a : Amos Judd, who is a man.

Note: a is a constant in D. We don't think it is necessary to define another predicate to test if x is a man. Thus, we simply assume Amos Judd is a man.

Now, we can rewrite the premises in term of the predicates above.

$$\begin{aligned}
p1: &\ \forall x[PB(x) \rightarrow SC(x)].\\
p2: &\ \neg\exists x[ML(x) \wedge \neg PE(x)]\\
p3: &\ \neg PR(a).\\
p4: &\ \forall x[CC(x) \rightarrow LC(x)].\\
p5: &\ \forall x[PE(x) \rightarrow PB(x)].\\
p6: &\ \forall x[SC(x) \rightarrow HC(x)].\\
p7: &\ \forall x[\neg ML(x) \rightarrow PR(x)].
\end{aligned}$$

And, we know that $p2$ is equivalent to the follows.

$$\begin{aligned}
\neg\exists x[ML(x) \wedge \neg PE(x)] &\equiv \forall x\neg[ML(x) \wedge \neg PE(x)]\\
&\equiv \forall x[\neg ML(x) \vee PE(x)]\\
&\equiv \forall x[ML(x) \rightarrow PE(x)].
\end{aligned}$$

Since $a \in D$ and all predicates above except $P3$ are quantified with universal quantifiers, we can apply the universal specification rule and replace the variable x by a to obtain propositions with truth values T as follows.

$$\begin{aligned}
p_1: &\ PB(a) \rightarrow SC(a).\\
p_2: &\ ML(a) \rightarrow PE(a).\\
p_3: &\ \neg PR(a).\\
p_4: &\ CC(a) \rightarrow LC(a).\\
p_5: &\ PE(a) \rightarrow PB(a).\\
p_6: &\ SC(a) \rightarrow HC(a).\\
p_7: &\ \neg ML(a) \rightarrow PR(a).
\end{aligned}$$

We have

steps		*reasons*
1	$\neg PR(a) \rightarrow ML(a)$	p_7, Contrapositive
2	$ML(a)$	$1, p_3$, Modus Ponens
3	$PE(a)$	$2, p_2$, Modus Ponens
4	$PB(a)$	$3, p_5$, Modus Ponens
5	$SC(a)$	$4, p_1$, Modus Ponens
6	$HC(a)$	$5, p_6$, Modus Ponens

Now, we can transfer the propositions back to English, which will tell us some facts about Amos Judd.

$ML(a)$: Amos Judd is a man with long hair.
$PE(a)$: Amos Judd is a poet.
$PB(a)$: Amos Judd is a policeman on this beat.
$SC(a)$: Amos Judd eats with our cook.
$HC(a)$: Amos Judd is her cousin.

We do not know if Amos Judd is our cook's cousin, and we do not know if Amos Judd loves cold mutton. □

Solution 35: Let D_x be the set of all living things.

Define $P(x)$: x is a pig.
$W(x)$: x has wings.

The following predicates are equivalent.

$$\begin{aligned} & \neg\exists x[P(x) \wedge W(x)] \\ \Longleftrightarrow \quad & \forall x \neg[P(x) \wedge W(x)] \\ \Longleftrightarrow \quad & \forall x[\neg P(x) \vee \neg W(x)] \\ \Longleftrightarrow \quad & \forall x[P(x) \rightarrow \neg W(x)]. \end{aligned}$$

We can choose any one of them as the answer. □

Solution 36: The following conclusion is logically incorrect.

Premises:	All soldiers can march.
	Some babies are not soldiers.
Conclusion:	Some babies cannot march.

To see this, let us define the following predicates,

$S(x)$: x is a soldier.
$B(x)$: x is a baby.
$M(x)$: x can march.

We can restate our question as: Is the following inference valid?

$$\frac{\begin{array}{l}\forall x(S(x) \to M(x)) \\ \exists x(B(x) \wedge \neg S(x))\end{array}}{\exists x(B(x) \wedge \neg M(x))}$$

From the first premise and by the rule of universal specification we have, for any a,

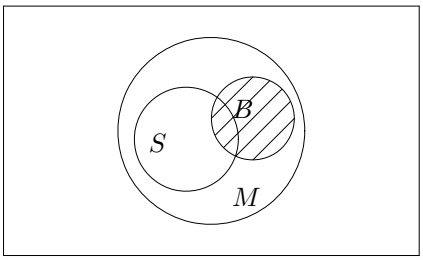
$$S(a) \to M(a),$$

but we cannot say

$$\neg S(a) \to \neg M(a)$$

because, unlike the contrapositive, the inverse is not an equivalence. Therefore, although from the premises we know that there are some babies who are not soldiers, we cannot use Modus Ponens to conclude that those babies cannot march. In other words, if one is not a soldier, that doesn't mean one cannot march. It is possible that all babies can march, while some of them are not soldiers.

To see this more clearly, consider the following Venn diagram.



Where M is the set of all creatures that can march, B is the set of babies, and S is the set of all soldiers. We interpret $x \in S$ as $S(x)$ is true, likewise for $x \in M$.

Recall $S \subseteq M \iff \forall x(x \in S \to x \in M)$. In the Venn diagram $S \subseteq M$, which gives the first premise: $\forall x(S(x) \to M(x))$.

The diagram shows $S - B \neq \emptyset$. Therefore, there are some elements that are in B but not in S, which is the second premise: $\exists x(B(x) \wedge \neg S(x))$.

However, the Venn diagram also shows that the conclusion is incorrect, because B is a subset of M, i.e., there is no baby that can't march. □

Solution 37: Let $D_x = \mathbf{N}$ and $D_y = \mathbf{N}^0$, and define two variable predicate P as

$$P(x, y) = x \text{ divides } y.$$

1. $\forall y P(1, y) = T$.
2. $\forall x P(x, 0) = T$.
3. $\forall x P(x, x) = T$.
4. $\forall y \exists x P(x, y) = T$.
   Given any number y, there exists x, say $x = 1$, such that x divides y.
5. $\exists y \forall x P(x, y) = T$. Such a y is 0.
6. $\forall x \forall y[(P(x, y) \wedge P(y, x)) \to (x = y)] = T$.
   Given any x and y, suppose that $(P(x, y) \wedge P(y, x))$ is true.
   $$P(x, y) \Rightarrow y = ax, a \in \mathbf{N}^0;$$
   $$P(y, x) \Rightarrow x = by, b \in \mathbf{N}.$$
   Thus, $x = by = b(ax) = abx$, and hence $ab = 1$. Because both a and b are nonnegative integers, we know that $a = b = 1$. Therefore, $x = y$.
7. $\forall x \forall y \forall z[(P(x, y) \wedge P(y, z)) \to P(x, z)] = T$.
   Given any x, y, and z, suppose that $(P(x, y) \wedge P(y, z))$ is true.
   $$P(x, y) \Rightarrow y = ax, a \in \mathbf{N}^0;$$
   $$P(y, z) \Rightarrow z = by, b \in \mathbf{N}^0.$$
   Thus, $z = by = b(ax) = abx$. Since $ab \in \mathbf{N}^0$, therefore, $P(x, z)$ is true.

□

Solution 38: Consider the quantified statement, $\forall x \ \exists y \ [x + y = 17]$. Let D_x and D_y denote the universes of x and y, respectively.

1. $D_x = D_y =$ the set of integers.

$$\forall x \; \exists y \; [x + y = 17] \; = \; True.$$

In this case, given any integer x, we always can find one integer $y = 17 - x$, such that $x + y = 17$. □

2. $D_x = D_y =$ the set of positive integers.

$$\forall x \; \exists y \; [x + y = 17] \; = \; False.$$

In this case, given any integer $x > 17$, we are not able to find another positive integer y, such that $x + y = 17$. □

3. $D_x =$ the set of integers and $D_y =$ the set of positive integers.

$$\forall x \; \exists y \; [x + y = 17] \; = \; False.$$

In this case, given any integer $x > 17$, we are not able to find another positive integer y, such that $x + y = 17$. □

4. $D_x =$ the set of positive integers and $D_y =$ the set of integers.

$$\forall x \; \exists y \; [x + y = 17] \; = \; True.$$

In this case, given any integer x, we always can find $y = 17 - x$, such that $x + y = 17$.

□

Solution 39: Let $f(a, b) = (a \rightarrow b) \wedge (\neg a \rightarrow \neg b)$. Let's find the truth table of f first.

a	b	$a \rightarrow b$	$\neg a \rightarrow \neg b$	$f(a, b)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

The building blocks for the DNF of a propositional formula with two variables are $(a \wedge b)$, $(a \wedge \neg b)$, $(\neg a \wedge b)$, and $(\neg a \wedge \neg b)$.

a	b	$a \wedge b$	$a \wedge \overline{b}$	$\overline{a} \wedge b$	$\overline{a} \wedge \overline{b}$	$f(a, b)$	
T	T	T ✓	F	F	F	T	✓
T	F	F	T	F	F	F	
F	T	F	F	T	F	F	
F	F	F	F	F	T ✓	T	✓

Therefore, $f(a,b) = (a \wedge b) \vee (\neg a \ \wedge \neg b)$. □

Solution 40: Let $f(a,b) = (a \rightarrow b) \wedge (a \rightarrow \ \neg b)$. The truth table of f:

a	b	$a \rightarrow b$	$a \rightarrow \ \neg b$	$f(a,b)$
T	T	T	F	F
T	F	F	T	F
F	T	T	T	T
F	F	T	T	T

The associated truth table for the building blocks is:

a	b	$a \wedge b$	$a \wedge \overline{b}$	$\overline{a} \wedge b$	$\overline{a} \wedge \overline{b}$	$f(a,b)$	
T	T	T	F	F	F	F	
T	F	F	T	F	F	F	
F	T	F	F	T ✓	F	T	✓
F	F	F	F	F	T ✓	T	✓

Therefore, $f(a,b) = (\neg a \wedge b) \vee (\neg a \ \wedge \neg b)$. □

Solution 41: Remark: Since using building blocks and the truth tables to find the DNF or CNF is pretty mechanical, it should not be difficult to find the DNF and CNF in this way. Let us solve this problem by using propositional calculus. Sometimes the propositional calculus method is easier than the truth table approach, sometimes it isn't.

1. $a \longrightarrow \ \neg b \ = \ \neg a \vee \neg b \ = \ (\neg a \vee \neg b)$.
2. For $(a \wedge b) \vee c$:

$$\begin{aligned}(a \wedge b) \vee c &= (a \vee c) \wedge (b \vee c) \\ &= ((a \vee c) \vee F) \wedge (F \vee (b \vee c)) \\ &= ((a \vee c) \vee (b \wedge \neg b)) \wedge ((a \wedge \neg a) \vee (b \vee c)) \\ &= ((a \vee c \vee b) \wedge (a \vee c \vee \neg b)) \wedge ((a \vee b \vee c) \wedge (\neg a \vee b \vee c)) \\ &= (a \vee b \vee c) \wedge (a \vee \neg b \vee c) \wedge (\neg a \vee b \vee c).\end{aligned}$$

Note: Why can we insert F without changing the value of the formula of the problem? How about the " $\wedge$ " case? □

Solution 42: Let $f = a \wedge (b \leftrightarrow c)$. We will use the shortcut method to find the CNF of f and propositional calculus to find the DNF.

1. Shortcut Method: First, we find the truth table for f.

a	b	c	$b \leftrightarrow c$	$a \wedge (b \leftrightarrow c)$
T	T	T	T	T
T	T	F	F	F ✓
T	F	T	F	F ✓
T	F	F	T	T
F	T	T	T	F ✓
F	T	F	F	F ✓
F	F	T	F	F ✓
F	F	F	T	F ✓

Consequently, the falsity set of f is:

$$F_f = \{(T,T,F),(T,F,T),(F,T,T),(F,T,F),(F,F,T),(F,F,F)\}.$$

Thus, the CNF of f is

$$(\overline{a},\overline{b},c) \wedge (\overline{a},b,\overline{c}) \wedge (a,\overline{b},\overline{c}) \wedge (a,\overline{b},c) \wedge (a,b,\overline{c}) \wedge (a,b,c).$$

2. Propositional Calculus:

$$\begin{aligned} a \wedge (b \leftrightarrow c) &= a \wedge ((b \wedge c) \vee (\neg b \wedge \neg c)) \\ &= (a \wedge (b \wedge c)) \vee (a \wedge (\neg b \wedge \neg c)) \\ &= (a \wedge b \wedge c) \vee (a \wedge \neg b \wedge \neg c). \end{aligned}$$

The last formula above is the DNF of f.

□

Solution 43: In general, "if ... then ..." can be translated into a logical implication ($\rightarrow$), and "there is" or "there are" should use an existential quantifier ($\exists$). We need a predicate for a property described. "And," "or," and "all" used in English sentences are equal to $\wedge, \vee$, and $\forall$, respectively, in the corresponding mathematical expressions. With this in mind, let's examine the statement from the number theory:

> "*For every integer n bigger than 1, there is a prime strictly between n and $2n$.*"

Let's move one step forward:

> "*For all integers, if the integer n is bigger than 1, then there is a number which is a prime and strictly between n and $2n$.*"

Let D_x be the set of all integers, and define predicate $P(x)$ as

$$P(x) : x \text{ is prime.}$$

1. We can obtain a logical sentence from the statement above:

$$\forall n[(n > 1) \rightarrow \exists x(P(x) \wedge (n < x < 2n))]. \tag{2.7}$$

2. The negation of (2.7) is:

$$\begin{aligned}
&\neg\forall n((n > 1) \rightarrow \exists x(P(x) \wedge (n < x < 2n))) \\
&\quad \Leftrightarrow \quad \exists n\neg((n > 1) \rightarrow \exists x(P(x) \wedge (n < x < 2n))) \\
&\quad \Leftrightarrow \quad \exists n\neg(\neg(n > 1) \vee \exists x(P(x) \wedge (n < x < 2n))) \\
&\quad \Leftrightarrow \quad \exists n((n > 1) \wedge \neg\exists x(P(x) \wedge (n < x < 2n))) \\
&\quad \Leftrightarrow \quad \exists n((n > 1) \wedge \forall x\neg(P(x) \wedge (n < x < 2n))) \\
&\quad \Leftrightarrow \quad \exists n((n > 1) \wedge \forall x(\neg P(x) \vee \neg(n < x < 2n))) \\
&\quad \Leftrightarrow \quad \exists n((n > 1) \wedge \forall x(P(x) \rightarrow \neg(n < x < 2n))) \\
&\quad \Leftrightarrow \quad \exists n((n > 1) \wedge \forall x(P(x) \rightarrow \neg((n < x) \wedge (x < 2n)))) \\
&\quad \Leftrightarrow \quad \exists n((n > 1) \wedge \forall x(P(x) \rightarrow (\neg(n < x) \vee \neg(x < 2n)))) \\
&\quad \Leftrightarrow \quad \exists n((n > 1) \wedge \forall x(P(x) \rightarrow ((x \leq n) \vee (x \geq 2n))))
\end{aligned}$$

□

Solution 44: We will use two different methods to prove this result. The

first method uses the contradiction argument, and the second one will check *all* the possible cases to show that the result is valid for all of them.

Let D_x be the set of integers. Define

$$P(x) : x \text{ is even.}$$

We can restate the given result as the predicate,

$$P(xy) \longrightarrow (P(x) \vee P(y)). \tag{2.8}$$

Method 1: By way of contradiction, assume that

$$P(xy) \wedge \neg(P(x) \vee P(y)). \tag{2.9}$$

By De Morgan's law, (2.9) is equivalent to

$$P(xy) \wedge \neg P(x) \wedge \neg P(y). \tag{2.10}$$

If x and y are not even, then they are odd and can be expressed as

$$x = 2k + 1, y = 2q + 1$$

for some integers k and q. Thus,

$$\begin{aligned} xy &= (2k+1)(2q+1) \\ &= 4kq + 2k + 2q + 1 \\ &= 2(2kq + k + q) + 1 \end{aligned}$$

Because k and q are both integers, we know that $2kq + k + q$ is an integer too. Thus, xy is not even, i.e., $P(xy)$ is false. This contradicts our assumption that $P(xy)$ is true. Therefore, (2.8) is correct. □

Method 2: Given any two integers, we have three cases: 1. both are even, 2. both are odd, 3. one is odd and the other one is even. We want to show that, in each case, (2.8) is correct.

1. Both are even: Let $x = 2k, y = 2q$ for some integers k and q.

$$\begin{aligned} P(xy) &\rightarrow (P(x) \vee P(y)) \\ &\equiv P(4kq) \rightarrow (P(2k) \vee P(2q)) \\ &\equiv T \rightarrow (T \vee T) \\ &\equiv T \rightarrow T \\ &\equiv T \end{aligned}$$

2. Both are odd: Let $x = 2k + 1, y = 2q + 1$ for some integers k and q.

$$\begin{aligned} P(xy) &\rightarrow (P(x) \vee P(y)) \\ &\equiv P(4kq + 2k + 2q + 1) \rightarrow (P(2k+1) \vee P(2q+1)) \\ &\equiv F \rightarrow (F \vee F) \\ &\equiv F \rightarrow F \\ &\equiv T \end{aligned}$$

3. One odd and one even: Let $x = 2k+1, y = 2q$ for some integers k and q.

$$\begin{aligned} P(xy) &\rightarrow (P(x) \vee P(y)) \\ &\equiv P(4kq+2q) \rightarrow (P(2k+1) \vee P(2q)) \\ &\equiv T \rightarrow (F \vee T) \\ &\equiv T \rightarrow T \\ &\equiv T \end{aligned}$$

We have seen that, in all cases, (2.8) is true. Therefore, it is a correct statement for all integers.

□

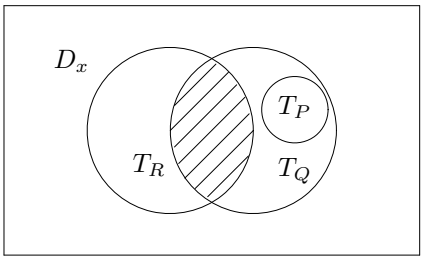
Solution 45: Let the domain D_x be the set of all people. Define the following predicates with variables over D_x.

$P(x)$: x is anxious to learn.
$Q(x)$: x works hard.
$R(x)$: x is one of those boys.

Now we can rewrite the premises and the conclusion in terms of the predicates defined above.

$$\begin{aligned} P1: &\quad \forall x[P(x) \rightarrow Q(x)] \\ P2: &\quad \exists x[R(x) \wedge Q(x)] \\ \hline C: &\quad \exists x[R(x) \wedge P(x)] \end{aligned}$$

The conclusion C is not logically correct from the premises. Consider the following Venn diagram for the truth sets of predicates P, Q, and R.



$T_P \subset T_Q$ that satisfies $P1$. The shaded area, $T_R \cap T_Q$, that is not empty satisfies $P2$. $T_R \cap T_P = \emptyset$ indicates that there is no instance in the universe D_x such that both $R(x)$ and $P(x)$ are true. Therefore, the conclusion C does not follow from the premises. □

Solution 46: Let the domain D_x be the set of all people. Define the following predicates with variables over D_x.

$P(x)$: x is a man.
$Q(x)$: x is a soldier.
$R(x)$: x is strong.
$S(x)$: x is brave.

The premises and the conclusion in terms of the predicates defined above are:

$$\begin{array}{rl} P1: & \exists x[P(x) \wedge Q(x)] \\ P2: & \forall x[Q(x) \rightarrow R(x)] \\ P3: & \forall x[Q(x) \rightarrow S(x)] \\ \hline C: & \exists x[P(x) \wedge R(x) \wedge S(x)] \end{array}$$

We use two different approaches to solve this problem.

Method 1: Let T_P, T_Q, T_R, and T_S be the truth sets of the predicates defined above. From the premises we can have the following facts:

$$\begin{array}{lcl} P1 & \Longleftrightarrow & T_P \cap T_Q \neq \emptyset \\ P2 & \Longleftrightarrow & T_Q \subseteq T_R \\ P3 & \Longleftrightarrow & T_Q \subseteq T_S \end{array}$$

Based on the facts above, we want to prove the conclusion that is equivalent to

$$(T_P \cap T_R \cap T_S) \neq \emptyset.$$

From $P1$, we know there is a nonempty set α such that $T_P \cap T_Q = \alpha$.

steps		*reasons*
1.	$\alpha \subseteq T_Q$	Definition of $\cap$
2.	$T_Q \subseteq T_R$	$P2$
3.	$\alpha \subseteq T_R$	$1, 2,$ Definition of $\subseteq$
4.	$T_Q \subseteq T_S$	$P3$
5.	$\alpha \subseteq T_S$	$1, 4,$ Definition of $\subseteq$
6.	$\alpha \subseteq T_P$	Definition of $\cap$
7.	$\alpha \subseteq (T_P \cap T_R \cap T_S)$	$3, 5, 6,$ Definition of $\cap$
8.	$\alpha \neq \emptyset$	$P1$
9.	$(T_P \cap T_R \cap T_S) \neq \emptyset$	steps $7, 8$

Since $(T_P \cap T_R \cap T_S) \neq \emptyset$, there must be at least one element a in the universe (domain D_x) such that $(P(a) \wedge R(a) \wedge S(a))$ is true. Thus, we can conclude that

$$\exists x(P(x) \wedge R(x) \wedge S(x)) = T,$$

i.e., conclusion C is correct. □

Method 2: Proof by using the laws of logic and inference rules for quantified predicate calculus.

	steps	*reasons*
1.	$\exists x[P(x) \wedge Q(x)]$	$P1$
2.	$P(a) \wedge Q(a)$	1, Existential Specification
3.	$\forall x[Q(x) \rightarrow R(x)]$	$P2$
4.	$Q(a) \rightarrow R(a)$	3, Universal Specification
5.	$Q(a)$	2, Conjunctive Simplification
6.	$R(a)$	4, 5, Modus Ponens
7.	$\forall x[Q(x) \rightarrow S(x)]$	$P3$
8.	$Q(a) \rightarrow S(a)$	7, Universal Specification
9.	$S(a)$	5, 8Modus Ponens
10.	$P(a)$	2, Conjunctive Simplification
11.	$P(a) \wedge R(a) \wedge S(a)$	6, 9, 10, conjunction
12.	$\exists x(P(x) \wedge R(x) \wedge S(x))$	11, Existential Generalization

□

Solution 47:

1. All members love each other.
2. There are some members who love some of the other members.
3. All members love some members.
4. There are some members who love all of the other members.

□

Solution 48: There are many alternatives for the conclusion that can be derived from the given premises. Let us just write down three of the most obvious, but not trivial, conclusions and see how to derive them logically from the premises.

We first define some needed predicates and translate the English sentences into logical formulas:

$$\begin{array}{ll} P(x): & x \text{ is an integer.} \\ Q(x): & x \text{ is a rational number.} \\ R(x): & x \text{ is a real number.} \end{array}$$

Premises:

$$\begin{array}{ll} P1: & \forall x[P(x) \rightarrow Q(x)] \\ P2: & R(\pi) \wedge \neg Q(\pi) \end{array}$$

	steps	*reasons*
1.	$\forall x(P(x) \rightarrow Q(x))$	$P1$
2.	$R(\pi) \wedge \neg Q(\pi)$	$P2$
3.	$P(\pi) \rightarrow Q(\pi)$	1, Universal Specification
4.	$\neg Q(\pi) \rightarrow \neg P(\pi)$	3, Contrapositive
5.	$\neg Q(\pi)$	2, Conjunctive Simplification
• 6.	$\neg P(\pi)$	4, 5, Modus Ponens
7.	$R(\pi)$	2, Conjunctive Simplification
8.	$R(\pi) \wedge \neg P(\pi)$	6, 7, Conjunction
• 9.	$\exists x(R(x) \wedge \neg P(x))$	8, Existential Generalization
10.	$\neg P(\pi) \vee \neg R(\pi)$	6, Disjunctive Amplification
11.	$\neg[P(\pi) \wedge R(\pi)]$	10, De Morgan's Law
12.	$\exists x \neg(P(x) \wedge R(x))$	11, Existential Generalization
• 13.	$\neg\forall x(P(x) \wedge R(x))$	12, Logical Equivalence

- In step 6, π *is not an integer.*

- In step 9, *there is a real but not rational number.*

- In step 13, *not all numbers are both integer and real.*

□

Solution 49: Let m denote Margaret. Define

$$\begin{aligned} P(x): &\quad x \text{ is a librarian.} \\ Q(x): &\quad x \text{ knows the system.} \end{aligned}$$

We want to use the rule of universal specification and Modus Ponens. If the unknown premise is "Margaret is a librarian," then we can have the following inference.

$$\begin{array}{rl} P1: & \forall x[P(x) \to Q(x)] \\ P2: & P(m) \\ \hline C: & Q(m) \end{array}$$

steps		*reasons*
1.	$\forall x(P(x) \to Q(x))$	$P1$
2.	$P(m)$	$P2$
3.	$P(m) \to Q(m)$	1, Universal Specification
4.	$Q(m)$	$2, 3$, Modus Ponens

Where $P(m)$ means: *Margaret is a librarian.* □

Solution 50: Prove $\exists x[P(x) \vee Q(x)] \iff \exists x P(x) \vee \exists x Q(x)$.

For $\Rightarrow$ direction, assume $\exists x[P(x) \vee Q(x)]$.

steps		reasons
1.	$\exists x[P(x) \vee Q(x)]$	Assumption
2.	$P(a) \vee Q(a)$	Existential Specification, 1
3.	$\exists x P(x) \vee Q(a)$	Existential Generalization, 2
4.	$\exists x P(x) \vee \exists x Q(x)$	Existential Generalization, 3

For $\Leftarrow$ direction, assume $\exists x P(x) \vee \exists x Q(x)$,

steps		*reasons*
1.	$\exists x P(x) \vee \exists x Q(x)$	Assumption
2.	$P(a) \vee \exists x Q(x)$	1, Existential Specification
3.	$P(a) \vee Q(b)$	2, Existential Specification
4.	$[P(a) \vee Q(b)] \vee [P(b) \vee Q(a)]$	3, Disjunctive Amplification
5.	$[P(a) \vee Q(a)] \vee [P(b) \vee Q(b)]$	4, Associative, Commutative
6.	$\exists x[P(x) \vee Q(x)] \vee \exists x[P(x) \vee Q(x)]$	5, Existential Generalization
7.	$\exists x[P(x) \vee Q(x)]$	$A \vee A \equiv A$

This completes the proof.

Note: Be very careful in step 3 of the proof of $\Leftarrow$ direction. We have to use two different symbols, a and b, because they are specified from two different existential quantifiers, and they may or may not be equal.

□

Solution 51: Prove $\forall x[P(x) \wedge Q(x)] \iff \forall x P(x) \wedge \forall x Q(x)$.

For $\Rightarrow$ direction, by way of contradiction, assume

$$\forall x[P(x) \wedge Q(x)] \quad \wedge \quad \neg[\forall x P(x) \wedge \forall x Q(x)].$$

steps		*reasons*
1.	$\neg[\forall x P(x) \wedge \forall x Q(x)]$	Assumption
2.	$\neg[P(a) \wedge \forall x Q(x)]$	1, Universal Specification
3.	$\neg[P(a) \wedge Q(a)]$	2, Universal Specification
4.	$\exists x \neg[P(x) \wedge Q(x)]$	3, Existential Specification
5.	$\neg\forall x[P(x) \wedge Q(x)]$	4, Logical Equivalence

The conclusion in step 5 contradicts our assumption.

Note: We choose the same a in steps 2 and 3.

For $\Leftarrow$ direction, by way of contradiction, assume

$$[\forall x P(x) \wedge \forall x Q(x)] \wedge \neg\forall x[P(x) \wedge Q(x)]$$

steps		*reasons*
1.	$\neg\forall x[P(x) \wedge Q(x)]$	Assumption
2.	$\exists x \neg[P(x) \wedge Q(x)]$	1, Logical Equivalence
3.	$\neg[P(a) \wedge Q(a)]$	2, Existential Specification
4.	$\neg P(a) \vee \neg Q(a)$	3, De Morgan's law
5.	$\exists x \neg P(x) \vee \exists x \neg Q(x)$	4, Existential Generalization
6.	$\neg\forall x P(x) \vee \neg\forall x Q(x)$	5, Logical Equivalence
7.	$\neg[\forall x P(x) \wedge \forall x Q(x)]$	6, De Morgan's law

Step 7 gives a conclusion that contradicts our assumption:

$$\forall x P(x) \wedge \forall x Q(x).$$

Therefore, both directions hold. This completes the proof. □

Solution 52: To prove $\forall x P(x) \vee \forall x Q(x) \Rightarrow \forall x[P(x) \vee Q(x)]$, by contradiction, assume that

$$[\forall x P(x) \vee \forall x Q(x)] \wedge \neg\forall x[P(x) \vee Q(x)].$$

steps		reasons
1.	$\neg\forall x[P(x) \vee Q(x)]$	Assumption
2.	$\exists x\neg[P(x) \vee Q(x)]$	1, Logical Equivalence
3.	$\neg[P(a) \vee Q(a)]$	2, Existential Specification
4.	$\neg P(a) \wedge \neg Q(a)$	3, De Morgan's law
5.	$\neg P(a)$	4, Conjunctive Simplification
6.	$\exists x\neg P(x)$	5, Existential Generalization
7.	$\neg\forall x P(x)$	6, Logical Equivalence
8.	$\neg Q(a)$	4, Conjunctive Simplification
9.	$\exists x\neg Q(x)$	8, Existential Generalization
10.	$\neg\forall x Q(x)$	9, Logical Equivalence
11.	$\neg\forall x P(x) \wedge \neg\forall x Q(x)$	7, 10, Conjunction
12.	$\neg[\forall x P(x) \vee \forall x Q(x)]$	11, De Morgan's law

Step 12 gives a conclusion that contradicts our assumption:

$$\forall x P(x) \vee \forall x Q(x).$$

This proves the theorem. □

Solution 53: To disprove $\forall x[P(x) \vee Q(x)] \Rightarrow \forall xP(x) \vee \forall xQ(x)$, we will construct a counter example.

Let the universe be $\{a, b\}$, and let p, q be two predicates with the truth values defined in the following table.

	a	b
$P(x)$	T	F
$Q(x)$	F	T

$$\begin{aligned}\forall x[P(x) \vee Q(x)] &= [P(a) \vee Q(a)] \wedge [P(b) \vee Q(b) \\ &= [T \vee F] \wedge [F \vee T] \\ &= T \wedge T \\ &= T\end{aligned}$$

$$\begin{aligned}\forall xP(x) \vee \forall xQ(x) &= [P(a) \wedge P(b)] \vee [Q(a) \wedge Q(b)] \\ &= F \vee F \\ &= F\end{aligned}$$

Therefore, $\forall x[P(x) \vee Q(x)] \not\Rightarrow \forall xP(x) \vee \forall xQ(x)$. □

Solution 54: We already know that $\sqrt{2}$ is irrational. Now, consider the number $\sqrt{2}^{\sqrt{2}}$. We don't know whether $\sqrt{2}^{\sqrt{2}}$ is irrational or not. But it is certain that there are only two cases.

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Let $a = \sqrt{2}$ and $b = \sqrt{2}$. Then both a and b are irrational and a^b is rational.

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.

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

Therefore, both a and b are irrational and a^b is rational.

In both cases we can claim that there are a and b, where a and b are irrational and a^b is rational. □

Chapter 3

Mathematical Induction

To develop the skill of correct thinking is in the first place
to learn what you have to disregard.
In order to go on, you have to leave out;
this is the essence of effective thinking.

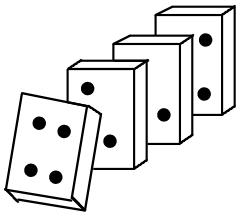
– Kurt Gödel

3.1 Concepts

Mathematical induction is one of the most important and powerful techniques for verifying mathematical statements. Many complicated mathematical theorems about integers can be proved easily by mathematical induction. It is easy because the frame of the proof is unique and the underlying idea of mathematical induction is intuitively understandable.

Think of infinitely many dominoes lined up. The proof by mathematical induction is like the domino effect illustrated in the following figure:

If the first domino falls, and for any n if the fall of the n^{th} domino would result in the knockdown of the $(n+1)^{st}$ domino, then any domino in the line will fall.



3.1.1 Necessary Conditions of Using Mathematical Induction

In the domino analogue above, to be able to (1) line up the dominoes, and (2) identify the first domino in the line are two necessary conditions for knocking down all of the dominoes. The two conditions are exactly the same necessary conditions for being able to make use of mathematical induction.

Suppose a given mathematical statement is about a property over the domain S. If all elements in S can be *well ordered*, i.e., (1) we can enumerate all elements in S one by one, and (2) we can identify the first element in the enumeration, then mathematical induction is very likely to be the approach for verifying the statement.

In particular, any well-ordered set S can be represented as

$$S = \{s_0, s_1, s_2, \ldots\}.$$

In this representation, (1) for any element a in S, there is $n \in \mathbf{N}$ such that $a = s_n$ (all dominoes have been lined up properly), and (2) s_0 is identified, which is called the *least element* (s_0 serves as the first domino in the line to fall.)

Example 3.1 Sets such as natural numbers, integers, even numbers, odd

numbers, multiples of 5, etc., are typical well-ordered sets that are often encountered in mathematics. They can be represented as:

$$\begin{aligned} \text{Natural numbers} &: \{1, 2, 3, 4, \ldots\}; \\ \text{Integers} &: \{0, 1, -1, 2, -2, 3, -3, \ldots\}; \\ \text{Even numbers} &: \{0, 2, -2, 4, -4, \ldots\}; \\ \text{Odd numbers} &: \{1, -1, 3, -3, 5, -5, \ldots\}; \\ \text{Multiples of 5} &: \{0, 5, -5, 10, -10, \ldots\}. \end{aligned}$$

For more advanced mathematical inductive proof, the domain set may be rational numbers, prime numbers, or any other well-ordered sets.

3.1.2 The Underlying Theory of Mathematical Induction

The underlying theory of mathematical induction is very simple. It is nothing but repeated application of the logical rule, Modus Ponens. Suppose

$$S = \{s_0, s_1, s_2, \ldots\},$$

and we have proved that

$$[P(s_0) = T] \text{ and } [\forall n \in \mathbf{N} P(s_n) \rightarrow P(s_{n+1})].$$

Given any $i \in \mathbf{N}$, we can claim that $P(s_i) = T$ by the following inferences.

steps		*reasons*
1.	$P(s_0)$	proved
2.	$P(s_0) \rightarrow P(s_1)$	proved
3.	$P(s_1)$	1,2, Modus Ponens
4.	$P(s_1) \rightarrow P(s_2)$	proved
5.	$P(s_2)$	3,4, Modus Ponens
6.	$P(s_2) \rightarrow P(s_3)$	proved
7.	$P(s_3)$	5,6, Modus Ponens
	$\vdots$	$\vdots$
	$P(s_{i-1})$	Modus Ponens
	$P(s_{i-1}) \rightarrow P(s_i)$	proved
	$P(s_i)$	Modus Ponens

Therefore, we can claim that for all a in S, $P(a)$ is a true statement.

Comment: In most problems, to prove $P(s_0) = T$ is trivial. The main task is to prove that $P(s_n) \rightarrow P(s_{n+1})$ for any n.

3.1.3 Mathematical Induction of the First Form (Weak Induction)

Suppose that the universal set (domain) is the set of non-negative integers, and $P(n)$ is any property of non-negative integers. We wish to prove that $P(n)$ is true for all $n = 0, 1, 2, \ldots$; i.e., $\forall n P(n)$. Then the following procedure can be applied.

Step 1: Prove that $P(0)$ is true. This step is known as the *basis step*, and the proved result, $P(0) = T$, is called the *basis of induction.*

Step 2: Let n be an arbitrary fixed integer, and assume that $P(n)$ is true. This assumption is called the *weak inductive hypothesis.*

Step 3: Use the assumption in step 2 to prove that $P(n+1)$ is true. This step is known as the *inductive step.*

If we can prove the basis in step 1 and the implication in step 3, then we can claim that $P(n)$ is true for all $n = 0, 1, 2, \ldots$. This method of proof is known as the *mathematical induction of the first form* or the *weak induction.*

Comment: The above proof procedure is an application of the following rule of inference,

$$\begin{array}{ll} 1. & P(0) \\ 2. & \forall n[P(n) \longrightarrow P(n+1)] \\ \hline 3. & \forall n P(n), \end{array}$$

where the first assertion, $P(0)$, is proved in step 1, and the second assertion, $\forall n[P(n) \longrightarrow P(n+1)]$, is shown by picking an arbitrary value of n for $P(n)$ in step 2 and by the implication proved in step 3.

Comment: One should not be confused by the statement in step 2 "let n be an arbitrary fixed integer, and assume that $P(n) = T$" and the goal "for all n $P(n) = T$" that we want to prove. The letter n in step 2 denotes an instance in the domain, and the letter n in the statement $\forall n P(n)$ is a variable that ranges over the domain. After step 2, the instance n is fixed. The following modification makes the difference explicit, but it also makes the proof awkward, and hence, for simplicity, most textbooks do not use it.

Step 2: For the inductive hypothesis, we assume that

$$P(n) = T \text{ when } n = i \text{ for some } i \text{ in the domain.}$$

Step 3: In the inductive step, we prove that

$$P(i) \longrightarrow P(i+1).$$

Then we conclude that for all n in the domain, $P(n) = T$.

Comment: In some instances, a weak inductive hypothesis cannot provide sufficient ground to prove that $P(n+1)$ is true in step 3. We need a stronger inductive hypothesis that is introduced in the next subsection.

3.1.4 Mathematical Induction of the Second Form (Strong Induction)

Suppose that the universal set (domain) is the set of non-negative integers, and $P(n)$ is any property of non-negative integers. We wish to prove that $P(n)$ is true for all $n = 0, 1, 2, \ldots$; i.e., $\forall n P(n)$. The following procedure can be applied.

Step 1: Prove that $P(0)$ is true. This step is known as the *basis step*, and the proved result $P(0) = T$ is called the *basis of induction.*

Step 2: Let n be an arbitrary fixed integer in the domain, and assume that $P(0), P(1), \ldots,$ and $P(n)$ are true. This assumption is called the *strong inductive hypothesis.*

Step 3: Use the assumption to prove that $P(n+1)$ is true. This step is known as the *inductive step.*

If we can prove the basis in step 1 and the implication in step 3, then we can claim that that $P(n)$ is true for all $n = 0, 1, 2, \ldots$. This method of proof is known as the *mathematical induction of the second form,* or the *strong induction.*

Comment: The above proof procedure is an application of the following rule of inference,

$$\begin{array}{ll} 1. & P(0) \\ 2. & \forall n[(P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \longrightarrow P(n+1)] \\ \hline 3. & \forall n P(n) \end{array}$$

Comment: Sometimes we prove that $P(n)$ is true for $n \in S$, where $S = \{s_0, s_1, s_2, \ldots\}$, and s_0 may not be equal to 0, or in some cases S may not be a set of numbers at all. If that is the case, the basis step changes to:

Step 1: Show that $P(s_0)$ is true.

Comment: In some problems, one may claim that $P(n)$ is true for all $n \in \{0, 1, 2, \ldots\}$, but the basis is not $P(0)$, but $P(1)$ or $P(2)$. It is important to recognize this property; otherwise, incorrect proofs are obtained. See problem 17 in the problem section of this chapter and its note on page 133.

3.2 Mathematical Induction and Recursive Definition

Mathematical induction and recursive definitions are intimately related. They should be viewed as two sides of the same coin. Recursion is a very useful apparatus for defining sets, functions,[1] and the programming syntax.[2]

3.2.1 Recursive Definitions for Functions

Theoretically, any *computable* function can be defined recursively. In the following we take the point of view that the argument of the function f takes values in the set of non-negative integers. In general, recursively defined functions have an infinitely large domain set.

A function f can be recursively defined as follows:

1: Define the value of the function at a few points. For example, $f(0), f(1)$ are specified. Such values are called the *initial values*.

2: Define the value of the function at $n+1$ in terms of $f(0)$, $f(1)$, $\ldots$, $f(n)$, and n itself.

3: Write a closing statement that in most cases reads "Steps 1 and 2 are the only two steps that define the function f."

Comment: The essence of recursive definition is its simplicity that helps us to understand the function being defined, but not its efficiency when we are asked to actually find the value of the function. We prefer to compute a function by using its *closed-form* formula instead of by using its recursive definition directly. Mathematical induction has nothing to do with finding a closed-form formula for a given function,[3] but it is a powerful technique for verifying that a given closed-form formula is a correct one for the recursively defined function.

Example 3.2 Let f be a function taking a non-negative integer as its argument, and be recursively defined as follows.

1: $f(0) = 0$.

[1] Basic concepts associated with functions are considered in Chapter 5.

[2] The definition 2.6 in Chapter 2 is an example of recursive definitions for the syntax of well-formed formulas.

[3] Chapter 8 will discuss details about solving recurrence relations.

2: For all $n \geq 0$, $f(n+1) = f(n) + (n+1)$.

We note that

$$\begin{aligned} &f(0) = 0, \\ &f(1) = f(0) + 1 = 0 + 1 = 1, \\ &f(2) = f(1) + 2 = 0 + 1 + 2 = 3, \\ &f(3) = f(2) + 3 = 0 + 1 + 2 + 3 = 6, \\ &\vdots \end{aligned}$$

and conjecture that $f(n)$ is the summation of the first n natural numbers, i.e., the closed-form of f is given as

$$f(n) = \frac{n(n+1)}{2}, \quad \text{for all } n \geq 0. \tag{3.1}$$

We can use mathematical induction to prove that equality (3.1) is correct.[4]

Inductive Basis: The initial value of f serves as the basis of the induction. In particular, we prove that $f(0) = \frac{0\times(0+1)}{2}$. It's clear that the equality (3.1) holds when $n = 0$, and hence the basis holds.

Note: $f(0) = 0$ is given as a part of the definition of f, and we have verified it by using formula (3.1).

Inductive Hypothesis: Assume that given any fixed $n \geq 0$, the equality (3.1) holds, i.e.,

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

Note: We removed the universal quantifier in the equality (3.1), because n is fixed after this step.

Inductive Step: In this step, we need to prove that

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

We first use the recursive definition of f to have

$$f(n+1) = f(n) + (n+1). \tag{3.2}$$

[4] We do not explicitly define a predicate to be proved true in its domain for this example. Implicitly, the predicate is:

$$P(n) \ : \ f(n) = \frac{n(n+1)}{2},$$

and $D_n = \mathbf{N}^0$. In general, if the predicate is clear from the problem context, we can omit it to improve the compactness of the proof. Please compare the solutions to Problems 6 and 7. On the other hand, if the subject is not clear, a well-stated predicate and its domain can help us to move the first step (see Problem 32.) We will explicitly define a predicate in most solutions in Section 3.5.

Then, we use the hypothesis to replace $f(n)$ in (3.2) by $\frac{n(n+1)}{2}$. We have

$$\begin{aligned} f(n+1) &= f(n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Therefore, we can claim that for all $\forall n \geq 0, f(n) = \frac{n(n+1)}{2}$, and hence the given closed-form for f is correct. □

3.2.2 Recursive Definitions for Sets and Structural Induction

We will introduce an important variant of mathematical induction called *structural induction* in this subsection. Let us first study how to define a set by using recursive definitions. The idea is: (1) give a few initial elements for the set, and (2) specify a few rules to construct new elements by using old elements that are already in the set.

A set S can be recursively defined as follows:

1: Identify a few elements of the set S.

2: Explain how to obtain new elements of the set S from the old elements of the set.

3: Write a closing statement that in most cases reads "(1) and (2) are the only two ways to generate elements of the desired set S."

Example 3.3 Let set S be a set of strings of 1's and 0's and be recursively defined as follows:

1: $1 \in S$, $100 \in S$.

2: If $s \in S$, then $11s \in S$.

3: If $s \in S$, then $00s \in S$.

4: Nothing but strings generated according to rules 1, 2, and 3 are elements in S.

The following table shows some elements in the set and the rules used to

generate each element in the table, respectively.

	elements	rules used
s_0	1	1
s_1	001	1, 3
s_2	1100111	1, 2, 3, 2
s_3	001100001	1, 3, 3, 2, 3
s_4	11001100001	1, 3, 3, 2, 3, 2
s_5	00001100001	1, 3, 3, 2, 3, 3

In the example above, given any element $s \in S$, according to the rules we can construct two new elements from s, i.e., $11s$ (using rule 2) and $00s$ (using rule 3). For example, if we know that $s_3 \in S$, then we can apply rules 2 and 3 to s_3 to obtain $11s_3$ and $00s_3$ which are s_4 and s_5, respectively, and they are also to be included in S. On the other hand, 1111, for example, is not a member of S because we cannot have 1111 by using the given rules.

Now, the question is, what is the relation between a recursively defined set and mathematical induction? To answer this question, let's observe the elements $s_0, \ldots, s_5$ of the set S obtained above. We find that every element has an even number of $0's$ and an odd number of $1's$. Is this observation correct in general. How can we prove it? The best technique for proving this kind of problem is mathematical induction. In general, if a set is recursively defined and we observe that the recursive definition gives a common property shared by all elements in the set, then we can use mathematical induction to prove the observation.

The difficulty is that the order of elements in the set S is no longer obvious (although S is still a well-ordered set). To overcome this problem, we introduce a variant of mathematical induction called *structural induction*. We do not visually line up the elements in the set. Instead, we imagine that the elements in the set are lined up according to the numbers of times the rules used to generate them. For example, if s is somewhere in the line, then the next elements are $00s$ and $11s$, because $00s$ and $11s$ are obtained from s by applying one of the given rules one more time.

Therefore, if a given property P is claimed to be universal in the set S, then we should be able to prove the implication:

$$\forall s \in S\ [P(s) \rightarrow P(00s) \wedge P(11s)].$$

The steps of proof by structural induction are stated below. In general, let set S be recursively defined as follows:

1. $s_0, s_1, \ldots, s_k \in S$.

2. If $s \in S$, then $r_0(s), r_1(s), \ldots, r_l(2) \in S$.

3. Only elements specified in **1** or generated by rules in **2** are elements in S.

We wish to prove that all elements in S have the property P, i.e.,

$$\forall s \in S\ [P(s) = T].$$

Then the following procedure can be applied.

Step 1: Prove that $P(s_0), P(s_1), \ldots, P(s_k)$ are all true. This step is the *basis step* of structure induction.

Step 2: Let s be any arbitrary fixed element in the set S, and assume that $P(s)$ is true. This is the *inductive hypothesis.*

Step 3: Use the assumption to prove that $P(r_0(s))$, $P(r_1(s))$, $\ldots$, $P(r_l(s))$ are all true. This step is the *inductive step.*

If we can prove the basis in step 1 and the implication in step 3, then we can claim that that $P(s)$ is true for all $s \in S$.

This method is called *structural induction*, because we are examining the structure of the elements in the set, where the structure is given by the rules. Any non-initial element can be decomposed into a few small fragments, and its property is the result of its fragments' properties.

Example 3.4 Consider the set S defined in the example on page 109. Prove by structural induction that every element in S has an even number of $0's$ and an odd number of $1's$.

Inductive Basis: It is clear that both strings "1" and "100" have an even number of $0's$ and an odd number of $1's$. Thus the inductive basis holds.

Inductive Hypothesis: Assume $s \in S$ and s has an even number of $0's$ and an odd number of $1's$.

Inductive Step: It is clear that, if the assumption is true, then both $00s$ and $11s$ have an even number of $0's$ and an odd number of $1's$.

Therefore, the observation is correct. □

3.3 Nested Induction

Nested induction is a special form of mathematical induction, by which we can prove a mathematical statement that has more than one variables involved. Nested induction is also known as *double induction* in case that the subject mathematical statement has two variables. Consider the Ackerman function

$A : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ defined as follows. For every $m, n \in \mathbf{N}$,

$$\begin{array}{rl} (i) & A(0,m) = m+1; \\ (ii) & A(n+1,0) = A(n,1); \\ (iii) & A(n+1,m+1) = A(n,A(n+1,m)). \end{array}$$

Theorem: For all $m, n \in \mathbf{N}$, $A(n,m) > m$.

We will prove the theorem by nested induction directly before we give its underlying theory to justify our steps. Let m and n range over $\mathbf{N}$.

Basis: $\forall m A(0,m) > m$. It plainly appears from definition (i).

Inductive Hypothesis: Fix $n \in \mathbf{N}$, assume that

$$\forall m[A(n,m) > m].$$

Inductive Steps: We want to prove that $\forall m[A(n+1,m) > m]$.

For $m = 0$, we have $A(n+1,0) = A(n,1)$ by definition (ii), and by the hypothesis, $A(n,1) > 1$, Thus, $A(n+1,0) > 1 > 0$.

For $m > 0$, we have

$$\begin{array}{lcll} A(n+1,m) & = & A(n,A(n+1,m-1)) & \text{by def } (iii) \\ & > & A(n+1,m-1) & \text{by the hypothesis} \\ A(n+1,m) & \geq & A(n+1,m-1)+1 & \\ & = & A(n,A(n+1,m-2))+1 & \text{by def } (iii) \\ & > & A(n+1,m-2)+1 & \text{by the hypothesis} \\ A(n+1,m) & \geq & A(n+1,m-2)+2 & \\ & \vdots & & \\ A(n+1,m) & \geq & A(n+1,m-m)+m & \\ & = & A(n+1,0)+m & \\ & = & A(n,1)+m & \\ & > & 1+m & \text{by the hypothesis} \end{array}$$

Therefore, $\forall m[A(n+1,m) > m]$. □

3.3.1 The underlying logic of nested induction

We use the previous example, and define two-place and one-place predicates Q and P, respectively, over natural numbers as follows.

$$\begin{array}{rcl} Q(n,m) & \triangleq & A(n,m) > m; \\ P(n) & \triangleq & \forall m Q(n,m). \end{array}$$

Thus, we can rewrite the theorem according the following logic equivalences.

$$\forall n \forall m[A(n,m) > m] \iff \forall n \forall m Q(n,m) \iff \forall n P(n).$$

To prove $\forall n P(n)$ by mathematical induction, we apply the inference rule we have been familiar with:

$$\frac{\begin{array}{l} P(0) \\ \forall n[P(n) \Rightarrow P(n+1)] \end{array}}{\forall n P(n).}$$

Use the definition of P, the inference above can be rewritten as:

$$\frac{\begin{array}{l} \forall m Q(0,m) \\ \forall n[\forall m Q(n,m) \Rightarrow \forall m Q(n+1,m)] \end{array}}{\forall n \forall m Q(n,m).}$$

Therefore, in the inductive proof we just shown, the inductive basis is $\forall m Q(0,m)$ and the inductive hypothesis is $\forall m Q(n,m)$.

3.4 Problems

Conventions for the rest of this chapter:

- Unless we state otherwise, n ranges over $\mathbf{N}^0$, i.e., $n \in \{0, 1, 2, 3, \ldots\}$.
- All indexing variables in $\sum$ notation are integers.
- **TH** stands for inductive hypothesis.

Problem 1: The assertion

$$\sum_{1 \le k \le n} 2^k = 2^{n+1}, \quad \forall n \ge 1$$

is incorrect. Find the mistake of the invalid proof in the following:

1. Assume that for a fixed n

$$\sum_{1 \le k \le n} 2^k = 2^{n+1}.$$

2. Add 2^{n+1} to both sides of the above equality. We have

$$\begin{aligned} \sum_{1 \le k \le n} 2^k + 2^{n+1} &= 2^{n+1} + 2^{n+1} \\ \sum_{1 \le k \le n+1} 2^k &= 2 \times 2^{n+1} \\ \sum_{1 \le k \le n+1} 2^k &= 2^{n+1+1}. \end{aligned}$$

This proves the result.

Problem 2: Consider the sequence $a_0, a_1, a_2, \ldots$, defined as:

1: $a_0 = 2$, and $a_1 = 3$.

2: For $n \ge 2$, define $a_n = 2a_{n-1} - a_{n-2}$.

We are given the following assertion:

"There is no element in the sequence equal to 1".

We present the following proof. What is wrong with the proof?

If we can prove that $a_0 \ne 1$ and the sequence is increasing, i.e., for all n, $a_{n+1} > a_n$, then we can claim that no element in the sequence can be equal to 1.

Inductive Basis: It's clear that $a_0 \neq 1$. **[The Basis Holds.]**

Inductive Hypothesis: Assume $a_{n+1} > a_n$.

Inductive Step: From the definition of the sequence and the hypothesis, we have

$$\begin{aligned} a_{n+2} &= 2a_{n+1} - a_n \\ &> 2a_{n+1} - a_{n+1} = a_{n+1}. \end{aligned}$$

Thus, $a_{n+2} > a_{n+1}$. **[The Inductive Step Holds.]**

Problem 3: Let $n \in \mathbf{N}$, and consider

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n!. \tag{3.3}$$

1. Use the $\sum$ notation to express the above expression.
2. Find the formula for it.

Problem 4: Prove the formula obtained for (3.3) by mathematical induction.

Problem 5: Let $n \in \mathbf{N}$, and consider

$$\frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \frac{1}{7 \cdot 10} + \cdots + \frac{1}{(3n-2) \cdot (3n+1)}. \tag{3.4}$$

1. Use the $\sum$ notation to express the expression above.
2. Find the formula for it.

Problem 6: Prove the formula obtained for (3.4) by mathematical induction.

Problem 7: Prove that

$$\sum_{1 \leq k \leq n} k(k+1) = n(n+1)(n+2)/3.$$

Problem 8: Prove by mathematical induction that

$$\sum_{0 \leq k \leq n} 3^k = \frac{(3^{n+1} - 1)}{2}.$$

Problem 9: Prove by mathematical induction that

$$\sum_{1 \leq k \leq n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{3.5}$$

Problem 10: Prove by mathematical induction that

$$\sum_{1\le k\le n} k(k-1) = \frac{1}{3}(n+1)n(n-1). \tag{3.6}$$

Problem 11: Prove by mathematical induction that

$$\sum_{1\le k\le n} k(k-1)(k-2) = \frac{1}{4}(n+1)n(n-1)(n-2). \tag{3.7}$$

Problem 12: Use the equalities (3.5), (3.6), and (3.7) to derive a formula for

$$\sum_{1\le k\le n} k^3. \tag{3.8}$$

Problem 13: Prove the closed form obtained for (3.8) by mathematical induction .

Problem 14: Prove by mathematical induction that for all positive odd n,

$$\sum_{0\le k\le n} (-2)^k = \frac{1}{3}(1-2^{n+1}).$$

Problem 15: Prove by mathematical induction that for all $n \ge 1$,

$$\sum_{1\le k\le n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}.$$

Problem 16: Prove by mathematical induction that for all $n \ge 1$,

$$\sum_{1\le k\le n} \frac{2k+1}{k^2(k+1)^2} = 1 - \frac{1}{(n+1)^2}.$$

Problem 17: Prove the following by mathematical induction :

$$\overline{\bigcup_{1\le i\le n} A_i} = \bigcap_{1\le i\le n} \overline{A_i},$$

where n is any integer and $n \ge 2$, and $A_1, \ldots, A_n$ are any sets. This is a generalized De Morgan's law.

Problem 18: Let a and b be two integers. Prove by mathematical induction that for all integers $n \ge 1$, $a^n - b^n$ is a multiple of $a - b$.

Note that you are asked to prove this by mathematical induction, so you cannot simply use the following fact:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}).$$

Problem 19: Let x be any real number and $x > 1$. Prove that for all $n > 1$

$$(1+x)^n > 1 + nx.$$

Problem 20: Let x be any real number such that $x > 0$ and $x \neq 1$. Prove that

$$x, x^x, x^{(x^x)}, x^{(x^{(x^x)})}, \ldots$$

is an increasing sequence.

Problem 21: Prove by mathematical induction that if n is any positive odd integer, then $1 + 3^n$ is divisible by 4.

Problem 22: Prove that the sum of the cubes of any three consecutive integers is divisible by 9.

Problem 23: Prove by mathematical induction that for all $n \in \mathbf{Z}$

$$(-1)^n = \begin{cases} 1 & \text{if } n \text{ is even,} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

$\mathbf{Z}$ is the set of all integers.

Problem 24: Let $c(n)$ be a sequence of integers such that

$$c(0) = 1, c(1) = 1, c(2) = 3,$$

and for all $n \geq 1$,

$$c(n+2) = 3c(n+1) - 3c(n) + c(n-1).$$

Prove that for all $n \geq 0$,

$$c(n) = n^2 - n + 1.$$

Problem 25: Define $b(n)$ as follows:

$$b(n+2) + 2b(n+1) + b(n) = 0, n \geq 0,$$

and $b(0) = 1$ and $b(1) = 1$. Prove that

$$b(n) = (1-2n)(-1)^n, n \geq 0.$$

Problem 26: Using the same definition of $b(n)$ given in problem 25, prove that if $b(0) = 1$ and $b(1) = -3$, then

$$b(n) = (1+2n)(-1)^n, n \geq 0.$$

Problem 27: Let us consider a famous sequence called Fibonacci numbers:

$$\begin{aligned} &f_0 = 0, \\ &f_1 = 1, \\ &f_n = f_{n-1} + f_{n-2}, \text{ for } n \geq 2. \end{aligned}$$

Prove by mathematical induction that, for all $n \geq 0$,

$$f_n = \frac{1}{\sqrt{5}} \times \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Problem 28: Let S be a set with n elements. Prove by mathematical induction that the total number of subsets of S having exactly two elements is $n(n-1)/2$.

Problem 29: Let $p(n)$ be the maximum number of intersection points of n distinct lines in the plane. Prove by mathematical induction that for all integers $n \geq 2$, $p(n) = n(n-1)/2$.

Problem 30: Let $x_1 = 1$ and $x_{n+1} = \sqrt{x_n^2 + \frac{1}{x_n^2}}$. Prove by mathematical induction that for all $n \geq 1$,

$$1 \leq x_n \leq \sqrt{n}.$$

Problem 31: Define the harmonic numbers as

$$H_n = \sum_{1 \leq i \leq n} \frac{1}{i}, \quad n \geq 1.$$

Prove by mathematical induction that

$$H_{2^n} \geq \left(1 + \frac{n}{2}\right), \quad n \geq 0.$$

Problem 32: Let λ denote the empty string. Let A be any finite nonempty set. A *palindrome* over A can be defined as a string that reads the same forward as backward. For example, "mom" and "dad" are palindromes over the set of English alphabets.

We define a set S as follows:

1. $\lambda \in S$
2. $\forall a \in A,\ a \in S$
3. $\forall a \in A\ \forall x \in S,\ axa \in S$
4. All the elements in S must be generated by the rules above.

Prove by structural induction that S equals the set of all palindromes over A.

Problem 33: Let set S be a set of strings of a's and b's recursively defined as follows:

1. $a \in S$, $b \in S$.

2. If $\mu \in S$ and $\nu \in S$, then $\mu\nu \in S$.

3. Nothing but strings generated according to rules 1 and 2 are elements in S.

We also recursively define the reverse operation R on S as:

1. $R(a) = a$, and $R(b) = b$.

2. If $\mu \in S$, then $R(a\mu) = R(\mu)a$, and $R(b\mu) = R(\mu)b$.

Prove by structural induction that for all $\mu, \nu \in S$,

$$R(\mu\nu) = R(\nu)R(\mu).$$

Problem 34: Let S and R be as defined in the previous problem. Prove that, for all $\mu \in S$,

$$R(R(\mu)) = \mu.$$

Problem 35: Let $\Sigma = \{a, b\}$ and Λ be the null string. Define $A \subseteq \Sigma^*$ by the following rules.

1. $\Lambda \in A$.
2. If $\omega \in A$, then $a\omega b \in A$.
3. If $\mu, \nu \in A$, then $\mu\nu \in A$.
4. Every $\omega \in A$ must come from a finite number of applications of rules 1, 2, or 3.

Prove by mathematical induction that, for every $\omega \in A$, ω has equally many a's and b's.

Problem 36: Let A be defined as the previous problem. Prove by mathematical induction that, if $\omega \in A$, then the number of a's is equal to or greater than the number of b's in every prefix of ω.

Note: A prefix of ω is Λ or any initial segment of ω. For example, if $\omega = aabbad$, then Λ, a, aa, aab, $aabb$, $aabba$, and $aabbab$ are all possible prefixes of ω.

3.5 Solutions

Solution 1: The basis of the induction is not proved. It is incorrect, because for $n = 1$,

$$\sum_{1 \le k \le 1} 2^k = 2^1 = 2,$$

which is not equal to $2^{1+1} = 4$. □

Solution 2: The proof is incorrect. The proof shows that $a_0 \neq 1$ and claims that it is the basis of the induction. According to the hypothesis given in the proof, the correct basis is $a_0 \neq 1$ and $a_1 > a_0$.

To see the mistake more clearly, let's change the initial values of the sequence to $a_0 = 3$, and $a_1 = 2$. We thus have $a_2 = 1$. The inductive basis only proves that $a_0 \neq 1$, but does not mention the problem that $a_0 > a_1$. □

Solution 3:

1. $$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! \; = \; \sum_{1 \le k \le n} k \cdot k!.$$

2. In order to obtain a closed form for the sum above, we note that $k = (k+1) - 1$ for any k. Thus,

   $$\begin{aligned} &1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! \\ &\quad = (2 \cdot 1! - 1!) + (3 \cdot 2! - 2!) + (4 \cdot 3! - 3!) + \cdots + ((n+1) \cdot n! - n!) \\ &\quad = (2! - 1!) + (3! - 2!) + (4! - 3!) + \cdots + ((n+1)! - n!) \\ &\quad = (n+1)! - 1. \end{aligned}$$

   Therefore,

   $$\sum_{1 \le k \le n} k \cdot k! = (n+1)! - 1. \tag{3.9}$$

□

Solution 4: Recall that our goal is to prove that equation (3.9) holds for all values of $n \geq 1$.

by mathematical induction:

- **Inductive Basis:** $n = 1$.

$$\sum_{1 \leq k \leq 1} k \cdot k! = 1 \cdot 1! = 1,$$
$$(1+1)! - 1 = 1.$$

That means both sides of (3.9) are equal to 1. **[The Basis Holds.]**

- **Inductive Hypothesis:** Suppose

$$\sum_{1 \leq k \leq n} k \cdot k! = (n+1)! - 1.$$

Inductive Step:

$$\begin{aligned}\sum_{1 \leq k \leq n+1} k \cdot k! &= \sum_{1 \leq k \leq n} k \cdot k! + (n+1) \cdot (n+1)! \\ &= (n+1)! - 1 + (n+1) \cdot (n+1)! \qquad [\textbf{by IH}] \\ &= (n+2) \cdot (n+1)! - 1 \\ &= (n+2)! - 1.\end{aligned}$$

[The Inductive Step Holds.]

Therefore, for all $n \in \mathbf{N}$, (3.9) is correct. □

Solution 5:

1.

$$\frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \frac{1}{7 \cdot 10} + \cdots + \frac{1}{(3n-2) \cdot (3n+1)} = \sum_{1 \leq k \leq n} \frac{1}{(3k-2) \cdot (3k+1)}.$$

2. In this problem we make use of the equality, for any k, $1 \leq k \leq n$,

$$\begin{aligned}\frac{1}{3}\left(\frac{1}{3k-2} - \frac{1}{3k+1}\right) &= \frac{1}{3}\frac{3k+1-3k+2}{(3k-2)(3k+1)} \\ &= \frac{1}{(3k-2)(3k+1)}.\end{aligned}$$

$$\begin{aligned}
&\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\frac{1}{7\cdot 10}+\cdots+\frac{1}{(3n-2)\cdot(3n+1)}\\
&=\frac{1}{3}(\frac{1}{1}-\frac{1}{4})+\frac{1}{3}(\frac{1}{4}-\frac{1}{7})+\frac{1}{3}(\frac{1}{7}-\frac{1}{10})+\cdots+\frac{1}{3}(\frac{1}{3n-2}-\frac{1}{3n+1})\\
&=\frac{1}{3}\left(\frac{1}{1}-\frac{1}{4}+\frac{1}{4}-\frac{1}{7}+\frac{1}{7}-\frac{1}{10}+\cdots+\frac{1}{3n-2}-\frac{1}{3n+1}\right)\\
&=\frac{1}{3}\left(1-\frac{1}{3n+1}\right).
\end{aligned}$$

Therefore, the closed form expression of the sum is

$$\sum_{1\le k\le n}\frac{1}{(3k-2)\cdot(3k+1)} \;=\; \frac{1}{3}\left(1-\frac{1}{3n+1}\right). \tag{3.10}$$

□

Solution 6: Our goal is to prove (3.10) by mathematical induction.

- **Inductive Basis:** $n=1$.

$$\begin{aligned}
\text{LHS} &= \frac{1}{3\cdot 1-2}\times\frac{1}{3\cdot 1+1} \;=\; \frac{1}{4},\\
\text{RHS} &= \frac{1}{3}\left(1-\frac{1}{3\cdot 1+1}\right) \;=\; \frac{1}{4}.
\end{aligned}$$

[The Basis Holds.]

- **Inductive Hypothesis:** Suppose

$$\sum_{1\le k\le n}\frac{1}{(3k-2)\cdot(3k+1)}=\frac{1}{3}\left(1-\frac{1}{3n+1}\right).$$

Inductive Step:

$$\begin{aligned}
&\sum_{1\le k\le n+1} \frac{1}{(3k-2)\cdot(3k+1)} \\
=&\left(\sum_{1\le k\le n} \frac{1}{(3k-2)\cdot(3k+1)}\right) + \frac{1}{(3n+1)\cdot(3n+4)} \\
=&\frac{1}{3}\left(1-\frac{1}{3n+1}\right) + \frac{1}{(3n+1)\cdot(3n+4)} \qquad \textbf{[by IH]} \\
=&\frac{1}{3}\left(1-\frac{1}{3n+1}+\frac{3}{(3n+1)\cdot(3n+4)}\right) \\
=&\frac{1}{3}\left(1-\frac{3n+4-3}{(3n+1)\cdot(3n+4)}\right) \\
=&\frac{1}{3}\left(1-\frac{3n+1}{(3n+1)\cdot(3n+4)}\right) \\
=&\frac{1}{3}\left(1-\frac{1}{3n+4}\right)
\end{aligned}$$

[The Inductive Step Holds.]

Therefore, for all $n \in \mathbf{N}$, (3.10) is correct. □

Solution 7: Let $D_n = \mathbf{N}$, and [5]

$$P(n)^{[6]} : \sum_{1\le k\le n} k(k+1) = \frac{1}{3}n(n+1)(n+2).$$

- **Inductive Basis:** $n = 1$.

  $$1\times 2 = \frac{1}{3}(1\times 2\times 3).$$

  Therefore, $P(1) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume $P(n) = T$, i.e.

  $$\sum_{1\le k\le n} k(k+1) = \frac{1}{3}n(n+1)(n+2).$$

[5] Beginning from this problem and onwards, we will explicitly define the predicate and its domain.

[6] **Note:** $P(n)$ is a predicate; for any fixed value of n, its value is either $True$ or $False$. It does not represent the sum or its value on the other side of the equality, i.e.,

$$P(n) \neq \sum_{1\le k\le n} k(k+1) \text{ and } P(n) \neq \frac{1}{3}n(n+1)(n+2).$$

- **Inductive Step:** We want to prove that $P(n+1) = True$. In other words, we want to prove that the following equality is correct:

$$\sum_{1\le k\le n+1} k(k+1) = \frac{1}{3}(n+1)(n+2)(n+3).$$

$$\begin{aligned}
\sum_{1\le k\le n+1} k(k+1) &= \left(\sum_{1\le k\le n} k(k+1)\right) + (n+1)((n+1)+1) \\
&= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \qquad \textbf{[by IH]} \\
&= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \\
&= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3} \\
&= \frac{(n+1)(n+2)(n+3)}{3} \\
&= \frac{(n+1)((n+1)+1)((n+1)+2)}{3} \\
&= \frac{1}{3}(n+1)(n+2)(n+3).
\end{aligned}$$

$P(n+1) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \in D_n, P(n)$ is true. □

Solution 8: Let $D_n = \mathbf{N}$, and

$$P(n) : \sum_{0\le k\le n} 3^k = \frac{(3^{n+1}-1)}{2}.$$

- **Inductive Basis:** $n = 1$.

$$\begin{aligned}
\sum_{0\le k\le 1} 3^k &= 3^0 + 3^1 = 4, \\
\frac{(3^{1+1}-1)}{2} &= \frac{9-1}{2} = 4.
\end{aligned}$$

Therefore, $P(1) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume $P(n) = T$, i.e.,

$$\sum_{0\le k\le n} 3^k = \frac{(3^{n+1}-1)}{2}.$$

- **Inductive Step:** We want to prove that $P(n+1)$ is true, i.e., we want to prove that

$$\sum_{0\le k\le n+1} 3^k = \frac{(3^{n+2}-1)}{2}.$$

$$\begin{aligned}
\sum_{0\le k\le n+1} 3^k &= \left(\sum_{0\le k\le n} 3^k\right) + 3^{n+1} \\
&= \frac{3^{n+1}-1}{2} + 3^{n+1} \qquad [\textbf{by IH}] \\
&= \frac{3^{n+1}-1+2\cdot 3^{n+1}}{2} \\
&= \frac{3\cdot 3^{n+1}-1}{2} \\
&= \frac{3^{n+1+1}-1}{2} \\
&= \frac{3^{n+2}-1}{2}.
\end{aligned}$$

$P(n+1) = T$. **[The Inductive Step Holds.]**

Therefore, $P(n)$ is true for all n in D_n. □

Solution 9: Let $D_n = \mathbf{N}$, and

$$P(n): \sum_{1\le k\le n} k^2 = \frac{1}{6}n(n+1)(2n+1).$$

- **Inductive Basis:** $n = 1$.

$$1^2 = \frac{1}{6}\times 1\times 2\times 3$$

Therefore, $P(1)$ is true. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n$, and assume $P(i) = T$, i.e.,

$$\sum_{1\le k\le i} k^2 = \frac{1}{6}i(i+1)(2i+1).$$

- **Inductive Step:** Consider $P(i+1)$,

$$\begin{aligned}\sum_{1\le k\le i+1} k^2 &= \left(1^2+2^2+\cdots+i^2\right)+(i+1)^2\\ &= \left(\sum_{1\le k\le i} k^2\right)+(i+1)^2\\ &= \frac{1}{6}i(i+1)(2i+1)+(i+1)^2 \qquad [\textbf{by IH}]\\ &= \frac{1}{6}(i+1)(i(2i+1)+6(i+1))\\ &= \frac{1}{6}(i+1)(2i^2+7i+6)\\ &= \frac{1}{6}(i+1)(i+2)(2i+3))\\ &= \frac{1}{6}(i+1)((i+1)+1)(2(i+1)+1)).\end{aligned}$$

$P(i+1)=T$. **[The Inductive Step Holds.]**

Therefore, $\forall n\in D_n, P(n)$ is $True$. □

Solution 10: Let $D_n=\mathbf{N}$, and

$$P(n): \sum_{1\le k\le n} k(k-1)=\frac{1}{3}(n+1)n(n-1).$$

- **Inductive Basis:** $n=1$.

$$1\times(1-1)=\frac{1}{3}\times(1+1)\times 1\times(1-1).$$

Therefore, $P(1)=True$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i\in D_n$, and assume $P(i)=T$, i.e.,

$$\sum_{1\le k\le i} k(k-1)=\frac{1}{3}(i+1)i(i-1).$$

- **Inductive Step:** Consider $P(i+1)$,

$$\begin{aligned}\sum_{1\le k\le i+1} k(k-1) &= \left(\sum_{1\le k\le i} k(k-1)\right) + (i+1)((i+1)-1)\\ &= \frac{1}{3}(i+1)i(i-1) + i(i+1) \qquad \textbf{[by IH]}\\ &= \frac{1}{3}(i+1)i(i-1+3)\\ &= \frac{1}{3}(i+1)i(i+2).\end{aligned}$$

$P(i+1) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \in D_n, P(n)$ is $True$. □

Solution 11: Let $D_n = \mathbf{N}$, and

$$P(n) \ : \ \sum_{1\le k\le n} k(k-1)(k-2) = \frac{1}{4}(n+1)n(n-1)(n-2).$$

- **Inductive Basis:** For $n = 1$, the LHS of $P(n)$ is $1(1-1)(1-2) = 0$, and the RHS is $\frac{1}{4}(1+1)1(1-1)(1-2) = 0$. Since both sides are equal, $P(1) = (0 = 0) = T$. **[The Basis Holds.]**
- **Inductive Hypothesis:** Let $i \in D_n$, and assume $P(i) = T$, i.e.,

$$\sum_{1\le k\le i} k(k-1)(k-2) = \frac{1}{4}(i+1)i(i-1)(i-2).$$

- **Inductive Step:** To prove that $P(i+1)$ is true, we need to show that

$$\sum_{1\le k\le i+1} k(k-1)(k-2) = \frac{1}{4}(i+2)(i+1)i(i-1).$$

$$\begin{aligned}\sum_{1\le k\le i+1} & k(k-1)(k-2)\\ &= \sum_{1\le k\le i} k(k-1)(k-2) + (i+1)i(i-1)\\ &= \frac{1}{4}(i+1)i(i-1)(i-2) + (i+1)i(i-1) \qquad \textbf{[by IH]}\\ &= \frac{1}{4}(i+1)i(i-1)\left((i-2)+4\right)\\ &= \frac{1}{4}(i+1)i(i-1)(i+2).\end{aligned}$$

$P(i+1) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \in D_n, P(n)$ is $True$. □

Solution 12: Let's observe the following properties first. Let $f(k)$ and $g(k)$ be two functions of k, and a be any constant. We have the following equalities.

$$\sum_{1\le k\le n}(f(k)+g(k)) = \sum_{1\le k\le n} f(k) + \sum_{1\le k\le n} g(k).$$

$$\sum_{1\le k\le n} af(k) = a\left(\sum_{1\le k\le n} f(k)\right).$$

One can verify that,

$$\begin{aligned} k^3 &= k(k-1)(k-2) + 3k^2 - 2k. \\ &= k(k-1)(k-2) + 2k(k-1) + k^2. \end{aligned}$$

Therefore,

$$\sum_{1\le k\le n} k^3 = \left(\sum_{1\le k\le n} k(k-1)(k-2)\right) + 2\left(\sum_{1\le k\le n} k(k-1)\right) + \sum_{1\le k\le n} k^2.$$

Then, we use the results from the previous problems to get,

$$\begin{aligned} \sum_{1\le k\le n} k^3 &= \frac{1}{4}(n+1)n(n-1)(n-2) + \frac{2}{3}(n+1)n(n-1) + \frac{1}{6}n(n+1)(2n+1) \\ &= \frac{1}{12}n(n+1)[3(n-1)(n-2) + 8(n-1) + 2(2n+1)] \\ &= \frac{1}{12}n(n+1)(3n^2 - 9n + 6 + 8n - 8 + 4n + 2) \\ &= \frac{1}{12}n(n+1)(3n + 3n^2) \\ &= \frac{1}{4}n^2(n+1)^2. \end{aligned}$$

□

Solution 13: Let $D_n = \mathbf{N}$, and

$$P(n): \quad \sum_{1\le k\le n} k^3 = \frac{1}{4}n^2(n+1)^2.$$

- **Inductive Basis:** $n = 1$. It is easy to verify that, for $n = 1$, both sides of the equality are 1i, i.e.,

$$1^3 = \frac{1}{4}1^2(1+1)^2.$$

Therefore, $P(1) = True$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n$, and assume $P(i) = T$, i.e.,

$$\sum_{1 \le k \le i} k^3 = \frac{1}{4}i^2(i+1)^2.$$

- **Inductive Step:** Consider $P(i+1)$,

$$\begin{aligned}
\sum_{1 \le k \le i+1} k^3 &= \sum_{1 \le k \le i} k^3 + (i+1)^3 \\
&= \frac{1}{4}i^2(i+1)^2 + (i+1)^3 \qquad \textbf{[by IH]} \\
&= \frac{1}{4}(i+1)^2(i^2 + 4(i+1)) \\
&= \frac{1}{4}(i+1)^2(i^2 + 4i + 4) \\
&= \frac{1}{4}(i+1)^2(i+2)^2.
\end{aligned}$$

Thus, $P(i+1) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \in D_n, P(n) = T$. □

Solution 14: Let $D_n = \{1, 3, 5, 7, 9, \ldots\}$, and define,

$$P(n) : \sum_{0 \le k \le n} (-2)^k = \frac{1}{3}(1 - 2^{n+1}).$$

- **Inductive Basis:** $n = 1$. We choose 1 as the basis because 1 is the first element of D_n in our enumeration, and note that the LHS of the equality is

$$\sum_{0 \le k \le 1} (-2)^k = (-2)^0 + (-2)^1 = -1,$$

and the RHS of the equality is

$$\frac{1}{3}(1 - 2^2) = -1.$$

Therefore, $P(1) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n$, and assume $P(i) = T$, i.e.,

$$\sum_{0 \le k \le i} (-2)^k = \frac{1}{3}(1 - 2^{i+1}).$$

- **Inductive Step:** Let $n = i + 2$. We choose $i + 2$ because $i + 2$ is the positive odd integer next to i.

$$\begin{aligned}
\sum_{0 \le k \le i+2} (-2)^k &= \sum_{0 \le k \le i} (-2)^k + \sum_{i+1 \le k \le i+2} (-2)^k \\
&= \frac{1}{3}(1 - 2^{i+1}) + (-2)^{i+1} + (-2)^{i+2} \qquad [\textbf{by IH}] \\
&= \frac{1}{3}[1 - 2^{i+1} + 3(-2)^{i+1} + 3(-2)^{i+2}] \\
&= \frac{1}{3}[1 - 2^{i+1} + 3(-2)^{i+1} + 3(-2)(-2)^{i+1}] \\
&= \frac{1}{3}[1 - 2^{i+1} + 3(-2)^{i+1} - 6(-2)^{i+1}] \\
&= \frac{1}{3}[1 - (1 - 3 + 6) \times 2^{i+1}] \\
&= \frac{1}{3}(1 - (-2)^2(-2)^{i+1}) \quad \text{since } i+1 \text{ is even} \\
&= \frac{1}{3}(1 - (-2)^{i+3}) \\
&= \frac{1}{3}(1 - 2^{i+3}) \quad \text{since } i+3 \text{ is even.}
\end{aligned}$$

$P(i + 2) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \in D_n, P(n)$ is true. □

Solution 15: Define $P(n)$ for all $n \ge 1$ as,

$$P(n) : \sum_{1 \le k \le n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}.$$

- **Inductive Basis:** For $n = 1$, it is easy to verify that both sides of the equality are equal to $\frac{1}{2}$.

$$\text{LHS} = \sum_{1 \le k \le 1} \frac{1}{k(k+1)} = \frac{1}{1 \cdot 2} = 1/2.$$

$$\text{RHS} = 1 - \frac{1}{1+1} = 1/2.$$

Therefore, $P(1)$ is true. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume $P(n)$ is true, i.e.,

$$\sum_{1\le k\le n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}.$$

- **Inductive Step:** To prove $P(n+1)$ is true.

$$\begin{aligned}
\sum_{1\le k\le n+1} \frac{1}{k(k+1)} &= \sum_{1\le k\le n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \\
&= 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} \qquad \textbf{[by IH]} \\
&= 1 - \frac{(n+2)-1}{(n+1)(n+2)} \\
&= 1 - \frac{n+1}{(n+1)(n+2)} \\
&= 1 - \frac{1}{n+2}
\end{aligned}$$

Therefore, $P(n+1)$ is true. **[The Inductive Step Holds.]**

□

Solution 16: Define $P(n)$ for all $n \ge 1$ as,

$$P(n) : \sum_{1\le k\le n} \frac{2k+1}{k^2(k+1)^2} = 1 - \frac{1}{(n+1)^2}.$$

- **Inductive Basis:** $n = 1$.

$$\sum_{1\le k\le 1} \frac{2k+1}{k^2(k+1)^2} = \frac{2+1}{1^2\cdot 2^2} = 3/4.$$
$$1 - \frac{1}{(1+1)^2} = 3/4.$$

Therefore, $P(1)$ is true. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume $P(n)$ is true, i.e.

$$\sum_{1\le k\le n} \frac{2k+1}{k^2(k+1)^2} = 1 - \frac{1}{(n+1)^2}.$$

- **Inductive Step:** To prove $P(n+1)$ is true.

$$\begin{aligned}
\sum_{1\le k\le n+1} \frac{2k+1}{k^2(k+1)^2} &= \sum_{1\le k\le n} \frac{2k+1}{k^2(k+1)^2} + \frac{2(n+1)+1}{(n+1)^2(n+2)^2} \\
&= 1 - \frac{1}{(n+1)^2} + \frac{2(n+1)+1}{(n+1)^2(n+2)^2} \qquad [\textbf{by IH}] \\
&= 1 - \frac{(n+2)^2 - 2(n+1) - 1}{(n+1)^2(n+2)^2} \\
&= 1 - \frac{n^2+4n+4-2n-2-1}{(n+1)^2(n+2)^2} \\
&= 1 - \frac{n^2+2n+1}{(n+1)^2(n+2)^2} \\
&= 1 - \frac{(n+1)^2}{(n+1)^2(n+2)^2} \\
&= 1 - \frac{1}{(n+2)^2}
\end{aligned}$$

  Therefore, $P(n+1)$ is true. **[The Inductive Step Holds.]**

□

Solution 17: Let A_i denote a set for any $i \in \mathbf{N}$, and $P(n)$ be the predicate, for $n \in \{2, 3, 4, \ldots\}$,

$$P(n) : \overline{\bigcup_{1\le i\le n} A_i} = \bigcap_{1\le i\le n} \overline{A_i}.$$

- **Inductive Basis:** For $n = 2$, we need to prove that

$$\overline{A_1 \cup A_2} = \overline{A_1} \cap \overline{A_2}.$$

  It is the classical De Morgan's law in logic, and is known to be true. Hence, the basis follows.

- **Inductive Hypothesis:** Assume $n = k$ and $P(k) = T$, i.e.,

$$\overline{\bigcup_{1\le i\le k} A_i} = \bigcap_{1\le i\le k} \overline{A_i}.$$

- **Inductive Step:** Let $n = k + 1$.

$$\overline{\bigcup_{1\le i\le k+1} A_i} = \overline{(\bigcup_{1\le i\le k} A_i) \cup A_{k+1}}.$$

If we take $(\bigcup_{1\le i\le k} A_i)$ as A, and A_{k+1} as B, we have

$$\overline{(\bigcup_{1\le i\le k} A_i) \cup A_{k+1}} = (\overline{\bigcup_{1\le i\le k} A_i}) \cap \overline{A_{k+1}}.$$

Using the inductive hypothesis, we have

$$\begin{aligned}(\overline{\bigcup_{1\le i\le k} A_i}) \cap \overline{A_{k+1}} &= (\bigcap_{1\le i\le k} \overline{A_i}) \cap \overline{A_{k+1}} \\ &= \bigcap_{1\le i\le k+1} \overline{A_i}.\end{aligned}$$

That proves $P(k+1) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \ge 2, P(n)$ is T.

Note: If we want to claim that $[\forall n \ge 1, P(n)]$ is also true, we have to prove the special case, $n = 1$, and the inductive basis, $n = 2$, separately. It is trivial to prove $P(1)$ is true, but $P(1) = T$ is not the basis of the induction. We have to prove $P(2) = T$ as the inductive basis, because $P(1)$ does not imply $P(2)$.

□

Solution 18: Let $D_n = \mathbf{N}$, and

$$P(n) : (a-b)|(a^n - b^n),$$

where $(a-b)|(a^n-b^n)$ means a^n-b^n is divisible by $a-b$. In other words, we have to prove that for any fixed n, there exists an integer k such that $a^n-b^n = a(a-b)$. Note that k may be a function of a, b, and n.

- **Inductive Basis:** For $n = 1$, $a^n - b^n = a - b$ and it is obvious that $(a-b)$ divides $(a-b)$, i.e.,

  $$(a-b)|(a^1 - b^1) \text{ is true.}$$

  Therefore, $P(1) = True$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n, i > 1$, and assume $P(i) = T$, i.e.,

  $$(a-b)|(a^i - b^i),$$

- **Inductive Step:** We want to know if $a^{i+i} - b^{i+1}$ is divisible by $a - b$.

$$a^{i+1} - b^{i+1} = aa^i - ba^i + ba^i - bb^i = a^i(a-b) + b(a^i - b^i).$$

From the inductive hypothesis, we know that there exists an integer k such that,

$$(a^i - b^i) = k(a-b).$$

Therefore,

$$\begin{aligned} a^{i+1} - b^{i+1} &= a^i(a-b) + bk(a-b) \\ &= (a-b)(a^i + bk). \end{aligned}$$

It is clear that $a^i + bk$ is an integer because a, b, i, and k are all integers. Thus,

$$(a-b)|(a^{i+1} - b^{i+1}).$$

$P(i+1)$ is true. **[The Inductive Step Holds.]**

Therefore, for all $n \geq 1$, $a^n - b^n$ is divisible by $a - b$. □

Solution 19: Suppose $x > 0, D_n = \{2, 3, 4, \ldots\}$, and

$$P(n) : (1+x)^n > 1 + nx.$$

- **Inductive Basis:** $n = 2$.

$$(1+x)^2 = 1 + 2x + x^2 > 1 + 2x, \quad \text{because } n^2 > 0.$$

[The Basis Holds.]

- **Inductive Hypothesis:** Let $i \in D_n$, and assume $P(i) = T$, i.e.,

$$(1+x)^i > 1 + ix.$$

- **Inductive Step:** We want to prove that $P(i+1)$ is true.

$$\begin{aligned} (1+x)^{i+1} &= (1+x)^i(1+x) \\ &> (1+ix)(1+x) \qquad [\textbf{by IH}] \text{ and } x > 0 \\ &= 1 + (i+1)x + ix^2 \\ &> 1 + (i+1)x \text{ by } n^2 > 0, i > 0. \end{aligned}$$

[The Inductive Step Holds.]

Note: The given condition $x > 0$ and the inductive hypothesis are both needed to claim that

$$(1+x)^i(1+x) > (1+ix)(1+x).$$

One can easily find a counter example if $x < 0$.

□

Solution 20: We express the sequence

$$x, x^x, x^{(x^x)}, x^{(x^{(x^x)})}, \ldots$$

as

$$a_1, a_2, a_3, \ldots, \ldots$$

. Thus,

$$\begin{aligned} a_1 &= x, \\ a_2 &= x^x = x^{a_1}, \\ a_3 &= x^{(x^x)} = x^{a_2}, \\ &\cdots \ \cdots \end{aligned}$$

In general, $a_n = x^{a_{n-1}}$ for $n \geq 2$. Let $D_n = \mathbf{N}$, and

$$P(n) : a_n < a_{n+1}.$$

We want to prove that, if $x > 1$, then for all n, $P(n)$ is true.

- **Inductive Basis:** $n = 1$. We discuss the two cases: $x > 1$ and $0 < x < 1$.

  1. Suppose that $0 < x < 1$. In this case, we know that $\log x < 0$. Since $0 < x < 1$, we have $\log x < x \cdot \log x$. It follows that $x < x^x$.
  2. If $x > 1$, then it is clear that $x < x^x$ if $x > 1$.

  Thus, in both cases, we have

  $$a_1 < a_2, \quad P(1) = True.$$

  [The Basis Holds.]

- **Inductive Hypothesis:** Assume $P(i)$ is true for some i in D_n, i.e.

  $$a_i < a_{i+1}.$$

- **Inductive Step:** We want to prove $P(i+1)$ is also true. Using the hypothesis, we have

$$\begin{aligned} a_i < a_{i+1} &\Rightarrow x^{a_i} < x^{a_{i+1}} \qquad \text{because } x > 1 \\ &\Rightarrow P(i+1) = T. \end{aligned}$$

[The Inductive Step Holds.]

Therefore, it is an increasing sequence. □

Solution 21: Let D_n be the set of all positive odd integers, i.e, $D_n = \{1, 3, 5 \ldots\}$, and define

$$P(n) : 1 + 3^n \text{ is divisible by 4.}$$

- **Inductive Basis:** $n = 1$. We choose 1 as the base because 1 is the first element in D_n. Apparently, $1 + 3^1 = 4$, which is divisible by 4. Therefore, $P(1) = T$. **[The Basis Holds.]**
- **Inductive Hypothesis:** Assume $P(n) = T$, i.e., $1 + 3^n$ is divisible by 4. Note: n is a positive odd integer.
- **Inductive Step:** We want to prove $P(n+2) = T$, i.e., we want to prove that $1 + 3^{n+2}$ is divisible by 4.

  Note: We choose $n + 2$ instead of $n + 1$ because $n + 2$ is the odd number next to n fixed in the inductive hypothesis, whereas $n + 1$ is not an element in D_n.

  From the inductive hypothesis, we can assume that $1 + 3^n = 4k$, where k is an integer. We have

$$\begin{aligned} 1 + 3^{n+2} &= 1 + 9 \cdot 3^n \\ &= (1 + 3^n) + 8 \cdot 3^n \\ &= 4k + 8 \cdot 3^n \\ &= 4(k + 2 \cdot 3^n). \end{aligned}$$

  Because k and n are integers, $k + 2 \cdot 3^n$ must be an integer. Therefore, $1 + 3^{n+2}$ is divisible by 4, and hence $P(n + 2) = T$.

  [The Inductive Step Holds.]

Therefore, $P(n)$ is true for all n in D_n. □

Solution 22: The domain of this problem includes both positive and negative integers. The easiest way is to split the domain into two parts: positive integers and negative integers. Then, we prove the statement by mathematical induction in the two sub-domain separately.

(1) Let $D_n = \{0, 1, 2, 3, \ldots\}$ Define:

$$P(n) : 9 \,\big|\, \left(n^3 + (n+1)^3 + (n+2)^3\right) .$$

- **Inductive Basis:** $n = 0$.

  $$0^3 + 1^3 + 2^3 = 9.$$

  $P(0)$ is true. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume $i \in D_n$, and $P(i)$ is true, i.e.,

  $$i^3 + (i+1)^3 + (i+2)^3 = 9k,$$

  for some integer k.

- **Inductive Step:** Prove $P(i+1)$ is true.

  $$\begin{aligned}
  &(i+1)^3 + (i+2)^3 + (i+3)^3 \\
  &\quad = (i+1)^3 + (i+2)^3 + i^3 + 9i^2 + 27i + 27 \\
  &\quad = (i^3 + (i+1)^3 + (i+2)^3) + 9i^2 + 27i + 27 \\
  &\quad = 9k + 9(i^2 + 3i + 3) \qquad [\textbf{by IH}] \\
  &\quad = 9(k + i^2 + 3i + 3)
  \end{aligned}$$

  Because $k + i^2 + 3i + 3$ is an integer, therefore

  $$9 \,\big|\, \left((i+1)^3 + (i+2)^3 + (i+3)^3\right) ,$$

  $P(i+1)$ is true. **[The Inductive Step Holds.]**

(2) Let $D_n = \{0, -1, -2, -3, \ldots\}$ Define:

$$P(n) : 9 \,\big|\, \left(n^3 + (n-1)^3 + (n-2)^3\right)$$

- **Inductive Basis:** $n = 0$.

  $$0^3 + 1^3 + 2^3 = 9.$$

  $P(0)$ is true. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume $i \in D_n$, and $P(i)$ is true, i.e.,

$$i^3 + (i-1)^3 + (i-2)^3 = 9k,$$

for some integer k.

- **Inductive Step:** Prove $P(i-1)$ is true.

$$\begin{aligned}
&(i-1)^3 + (i-2)^3 + (i-3)^3 \\
&\quad = (i-1)^3 + (i-2)^3 + i^3 - 9i^2 + 27i - 27 \\
&\quad = (i^3 + (i-1)^3 + (i-2)^3) - 9i^2 + 27i - 27 \\
&\quad = 9k + 9(-i^2 + 3i - 3) \qquad [\textbf{by IH}] \\
&\quad = 9(k - i^2 + 3i - 3)
\end{aligned}$$

Because $k - i^2 + 3i - 3$ is an integer, therefore

$$9 \,\big|\, \left((i-1)^3 + (i-2)^3 + (i-3)^3\right),$$

$P(i-1)$ is true. **[The Inductive Step Holds.]**

Putting the two domains together, we have that the sum of the cubes of any three consecutive integers is divisible by 9. □

Solution 23: We first prove that the statement is correct in the non-negative part of the domain. Let $D_n = \{0\} \cup \mathbf{N}$, and define

$$P(n): \ (-1)^n = \begin{cases} 1 & \text{if } n \text{ is even,} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

We will prove that $P(n) = T$ for all $n \in D_n$.

- **Inductive Basis:** $n = 0$.

  0 is even and $(-1)^0 = 1$. Thus $P(0) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** $n = i$.

  Suppose $P(i) = T$, i.e.,

$$(-1)^i = \begin{cases} 1 & \text{if } i \text{ is even,} \\ -1 & \text{if } i \text{ is odd.} \end{cases}$$

- **Inductive Step:** $n = i + 1$.

$$\begin{aligned}(-1)^{i+1} &= -1 \cdot (-1)^i \\ &= \begin{cases} -1 \cdot 1 & \text{if } i \text{ is even,} \\ -1 \cdot -1 & \text{if } i \text{ is odd.} \end{cases} \\ &= \begin{cases} -1 & \text{if } i \text{ is even,} \\ 1 & \text{if } i \text{ is odd.} \end{cases} \\ &= \begin{cases} -1 & \text{if } i+1 \text{ is odd,} \\ 1 & \text{if } i+1 \text{ is even.} \end{cases}\end{aligned}$$

Therefore, $P(i+1)$ is true. **[The Inductive Step Holds.]**

We have proved that the predicate is true for all non-negative integers. We can use the same technique shown in the previous problem, i.e., we can further prove that the statement is correct for the other part of the domain (negative integers). Or, we can use the result we just got and the following arguments.

From the proved result above, if n is a non-negative integer, we know that $2n$ is even and $(-1)^{2n} = 1$. Observe the following fact: if $n \in \mathbf{N}$, then

$$(-1)^{-n} = \frac{1}{(-1)^n} = \frac{(-1)^{2n}}{(-1)^n} = (-1)^n.$$

Therefore, we can claim that for all $i \in \mathbf{Z}$, the predicate $P(i)$ is always true. That proves the theorem. □

The following is another proof for the above problem. It is a bit awkward, but it shows how to reorder the domain so we can examine the entire domain without missing any element of it. Let's consider the following ordered sequence,

$$\mathcal{Z} \ : \ 0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$$

It is clear that any number in $\mathbf{Z}$ must be in the sequence $\mathcal{Z}$ somewhere. Let z_i denote the i^{th} number in $\mathcal{Z}$, where $i \geq 1$. Let $D_n = \mathbf{N}$. Define

$$P(n) : \ (-1)^{z_n} = \begin{cases} 1 & \text{if } z_n \text{ is even,} \\ -1 & \text{if } z_n \text{ is odd.} \end{cases}$$

Thus, our original problem can be viewed as:

Prove that for all $n \in D_n$, $P(n)$ is true.

- **Inductive Basis:** $n = 1$.

  $z_1 = 0$, therefore z_1 is even and $(-1)^0 = 1$. Thus $P(1) = T$.

  [The Basis Holds.]

- **Inductive Hypothesis:** $n = i$.

  Suppose $P(i) = T$, i.e.

$$(-1)^{z_i} = \begin{cases} 1 & \text{if } z_i \text{ is even,} \\ -1 & \text{if } z_i \text{ is odd.} \end{cases}$$

- **Inductive Step:** $n = i + 1$.

  There are only two possible values for z_{i+1} in terms of z_i, i.e., $.z_{i+1} = -z_i$ if z_i is positive or $z_{i+1} = -z_i + 1$ if z_i is negative. We will discuss this by cases.

  case 1: $z_{i+1} = -z_i$.

$$(-1)^{z_{i+1}} = (-1)^{-z_i} = \frac{1}{(-1)^{z_i}} = \begin{cases} 1/1 & = 1 & \text{if } z_i \text{ is even,} \\ 1/-1 & = -1 & \text{if } z_i \text{ is odd.} \end{cases}$$

  From $\mathcal{Z}$ we know that in this case if z_i is even, then z_{i+1} is even, and if z_i is odd, then z_{i+1} is odd. Therefore,

$$(-1)^{z_{i+1}} = \begin{cases} 1 & \text{if } z_{i+1} \text{ is even,} \\ -1 & \text{if } z_{i+1} \text{ is odd.} \end{cases}$$

  case 2: $z_{i+1} = -z_i + 1$.

$$(-1)^{z_{i+1}} = (-1)^{-z_i+1} = \frac{-1}{(-1)^{z_i}} = \begin{cases} -1/1 = -1 & \text{if } z_i \text{ is even,} \\ -1/-1 = 1 & \text{if } z_i \text{ is odd.} \end{cases}$$

  From $\mathcal{Z}$ we know that in this case if z_i is even, then z_{i+1} is odd, and if z_i is odd, then z_{i+1} is even. Therefore,

$$(-1)^{z_{i+1}} = \begin{cases} 1 & \text{if } z_{i+1} \text{ is even,} \\ -1 & \text{if } z_{i+1} \text{ is odd.} \end{cases}$$

  In both cases, $P(i+1)$ is true. **[The Inductive Step Holds.]**

This proves the problem. □

Solution 24: Let us rewrite the recurrent relation first:

$$\begin{aligned} \forall n \geq 1,\ c(n+2) &= 3c(n+1) - 3c(n) + c(n-1) \\ \Rightarrow \forall n \geq 3,\ c(n) &= 3c(n-1) - 3c(n-2) + c(n-3). \end{aligned}$$

Given $c(0) = c(1) = 1$, and $c(2) = 3$.

To prove that for all $n \geq 0$, $c(n) = n^2 - n + 1$, let $D_n = \mathbf{N}^0$, and define

$$P(n) \ :\ c(n) = n^2 - n + 1.$$

- **Inductive Basis:** $n = 0, 1, 2$.

$$\begin{aligned} c(0) &= 0 - 0 + 1 = 1. \\ c(1) &= 1 - 1 + 1 = 1. \\ c(2) &= 4 - 2 + 1 = 3. \end{aligned}$$

  Therefore, $P(0) = P(1) = P(2) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume that, for a fixed $n \in D_n$, if $0 \leq i \leq n$, then $P(i) = T$, i.e.,

$$c(i) = i^2 - i + 1.$$

  This is a strong hypothesis.

- **Inductive Step:** To prove that $P(n + 1) = T$.

  To calculate the value of $c(n+1)$, we can use the values of $c(n), c(n-1)$, and $c(n-2)$ given in the strong inductive hypothesis, because the arguments, n, $n-1$, and $n-2$, are in the domain of the inductive hypothesis. We have:

$$\begin{aligned} c(n) &= n^2 - n + 1, \\ c(n-1) &= (n-1)^2 - (n-1) + 1, \\ c(n-2) &= (n-2)^2 - (n-2) + 1. \end{aligned}$$

  Therefore,

$$\begin{aligned} & c(n+1) \\ &= 3c(n) - 3c(n-1) + c(n-2) \\ &= 3(n^2 - n + 1) - 3((n-1)^2 - (n-1) + 1) + (n-2)^2 - (n-2) + 1 \\ &= 3n^2 - 3n + 3 - 3n^2 + 9n - 9 + n^2 - 5n + 7 \\ &= n^2 + n + 1 \\ &= (n^2 + 2n + 1) - (n+1) + 1 \\ &= (n+1)^2 - (n+1) + 1. \end{aligned}$$

  We have the result above by using the definition of $c(n+1)$ and the hypothesis, and the result agrees with the given closed-form formula for $c(n+1)$. **[The Inductive Step Holds.]**

This completes the proof. □

Solution 25: Please be careful to adjust the domain of n as shown in the

following.

$$\begin{aligned}\forall n \geq 0[b(n+2) + 2b(n+1) + b(n) = 0] \\ \equiv\ \forall n \geq 0[b(n+2) = -2b(n+1) - b(n)] \\ \equiv\ \forall n \geq 2[b(n) = -2b(n-1) - b(n-2)].\end{aligned}$$

That's why this problem has to state that $b(n)$ is defined by the equation after first two values. Please compare this problem to the previous one[7].

Define $b(0) = b(1) = 1$. Let $D_n = \mathbf{N}^0$ and

$$P(n) : b(n) = (1-2n)(-1)^n.$$

- **Inductive Basis:** $n = 0$, and $n = 1$.

  We have to take $P(0)$ and $P(1)$ as our basis, because both $b(-1)$ and $b(-2)$ are undefined, and hence $b(0)$ and $b(1)$ cannot be obtained by using the equation $b(n) = -2b(n-1) - b(n-2)$ in the inductive step. [Same reason for the next problem.]

  $$b(0) = 1 = (1-0)(-1)^0.$$
  $$b(1) = 1 = (1-2)(-1)^1.$$

  $P(0) = P(1) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n$, and $1 \leq i$.
  Suppose, if $n \leq i$, then $P(n) = T$, i.e.,

  $$\forall n \in D_n, (n \leq i) \Rightarrow (b(n) = (1-2n)(-1)^n).$$

- **Inductive Step:** Let $n = i + 1$.

$$\begin{aligned}b(n) &= b(i+1) \\ &= -2b((i+1)-1) - b((i+1)-2) \\ &= -2b(i) - b(i-1) \\ &= -2(1-2i)(-1)^i - (1-2(i-1))(-1)^{i-1} \\ &= -2(1-2i)(-1)^i - (3-2i)(-1)^{i-1} \\ &= (-1)^{i-1}(-2(1-2i)(-1) - (3-2i)) \\ &= (-1)^{i-1}(-1-2i) \\ &= (-1)^2(-1)^{i-1}(1-2-2i) \\ &= (1-2(i+1))(-1)^{i+1} \\ &= (1-2n)(-1)^n.\end{aligned}$$

[7] One may ask why we don't define $b(n)$ as

$$\forall n \geq 0[b(n) = -b(n+2) - 2b(n+1)]$$

by using the given equation directly without adjusting the domain of n. Can we define a function based on its future values instead of its previous values? Theoretically, the answer is yes, but that's beyond the scope of our interest of using mathematical induction.

$P(i+1) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \in D_n, P(n)$ is true. □

Solution 26: Define $b(0) = 1, b(1) = -3$. Let $D_n = \mathbf{N}^0$, and

$$P(n) : b(n) = (1+2n)(-1)^n.$$

- **Inductive Basis:** $n = 0$, and $n = 1$.

$$b(0) = 1 = (1+0)(-1)^0.$$
$$b(1) = -3 = (1+2)(-1)^1.$$

$P(0) = P(1) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n$, and $1 \leq i$.
Suppose, if $n \leq i$, then $P(n) = T$, i.e.

$$\forall n \in D_n, (n \leq i) \Rightarrow (b(n) = (1+2n)(-1)^n).$$

- **Inductive Step:** Let $n = i+1$.

$$\begin{aligned} b(n) &= b(i+1) \\ &= -2b((i+1)-1) - b((i+1)-2) \\ &= -2b(i) - b(i-1) \\ &= -2(1+2i)(-1)^i - (1+2(i-1))(-1)^{i-1} \\ &= -2(1+2i)(-1)^i - (2i-1)(-1)^{i-1} \\ &= (-1)^{i-1}(-2(1+2i)(-1) - (2i-1)) \\ &= (-1)^{i-1}(3+2i) \\ &= (-1)^2(-1)^{i-1}(1+2+2i) \\ &= (1+2(i+1))(-1)^{i+1} \\ &= (1+2n)(-1)^n. \end{aligned}$$

$P(i+1) = T$. **[The Inductive Step Holds.]**

Therefore, $\forall n \in D_n, P(n)$ is true. □

Solution 27: Given

$$f_0 = 0, f_1 = 1,$$
$$f_n = f_{n-1} + f_{n-2}, \text{ for } n \geq 2.$$

We want to prove that, for all $n \geq 0$,

$$f_n = \frac{1}{\sqrt{5}} \times \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

- **Inductive Basis:** $n = 0$:

$$\begin{aligned} \tfrac{1}{\sqrt{5}} \times \left(\left(\tfrac{1+\sqrt{5}}{2} \right)^0 - \left(\tfrac{1-\sqrt{5}}{2} \right)^0 \right) &= \tfrac{1}{\sqrt{5}} \times (1-1) \\ &= 0 \ = \ f_0. \end{aligned}$$

$n = 1$:

$$\begin{aligned} \tfrac{1}{\sqrt{5}} \times \left(\left(\tfrac{1+\sqrt{5}}{2} \right)^1 - \left(\tfrac{1-\sqrt{5}}{2} \right)^1 \right) &= \tfrac{1}{\sqrt{5}} \times \left(\tfrac{1+\sqrt{5}}{2} - \tfrac{1-\sqrt{5}}{2} \right) \\ &= \tfrac{1}{\sqrt{5}} \times \left(\tfrac{1+\sqrt{5}-1+\sqrt{5}}{2} \right) \\ &= 1 \ = \ f_1 \end{aligned}$$

[The Basis Holds.]

- **Inductive Hypothesis:** Assume that, for $1 \leq k \leq n$,

$$f_k = \frac{1}{\sqrt{5}} \times \left(\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right).$$

- **Inductive Step:** In the following simplification we combine the two positive terms and the two negative terms, and use

$$\left(\tfrac{1+\sqrt{5}}{2} \right)^2 = \tfrac{3+\sqrt{5}}{2}, \text{ and } \left(\tfrac{1-\sqrt{5}}{2} \right)^2 = \tfrac{3-\sqrt{5}}{2}.$$

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &= \tfrac{1}{\sqrt{5}} \left(\left(\tfrac{1+\sqrt{5}}{2} \right)^n - \left(\tfrac{1-\sqrt{5}}{2} \right)^n \right) + \tfrac{1}{\sqrt{5}} \left(\left(\tfrac{1+\sqrt{5}}{2} \right)^{n-1} - \left(\tfrac{1-\sqrt{5}}{2} \right)^{n-1} \right) \\ &= \tfrac{1}{\sqrt{5}} \times \left[\left(\tfrac{1+\sqrt{5}}{2} \right)^n + \left(\tfrac{1+\sqrt{5}}{2} \right)^{n-1} - \left(\tfrac{1-\sqrt{5}}{2} \right)^n - \left(\tfrac{1-\sqrt{5}}{2} \right)^{n-1} \right] \\ &= \tfrac{1}{\sqrt{5}} \times \left[\left(\tfrac{1+\sqrt{5}}{2} \right)^{n-1} \times \left(\tfrac{3+\sqrt{5}}{2} \right) - \left(\tfrac{1-\sqrt{5}}{2} \right)^{n-1} \times \left(\tfrac{3-\sqrt{5}}{2} \right) \right] \\ &= \tfrac{1}{\sqrt{5}} \times \left[\left(\tfrac{1+\sqrt{5}}{2} \right)^{n-1} \times \left(\tfrac{1+\sqrt{5}}{2} \right)^2 - \left(\tfrac{1-\sqrt{5}}{2} \right)^{n-1} \times \left(\tfrac{1-\sqrt{5}}{2} \right)^2 \right] \\ &= \tfrac{1}{\sqrt{5}} \times \left[\left(\tfrac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\tfrac{1-\sqrt{5}}{2} \right)^{n+1} \right] \end{aligned}$$

[The Inductive Step Holds.]

□

Solution 28: Prove by induction that the total number of subsets having exactly two elements in a set of n elements is $n(n-1)/2$.

It is clear that if A is a set of 2 elements, the only subset of A with two elements is A itself. And since $1 = 2(2-1)/2$, the basis holds.

Suppose we have a set A with elements, and let $n \geq 2$. And suppose we already know by the inductive hypothesis that there are $n(n-1)/2$ many subsets of A with 2 elements. Now, we add a new element a into A, and examine the power set of the new A. What are those subsets with 2 elements? They are the old subsets with 2 elements plus every singleton subset of the old A union with $\{a\}$. Apparently, the old A has n-many singleton subsets. Therefore, the new A has $(n(n-1)/2 + n)$-many subsets with 2 elements, where the new size of A is $n+1$. And

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

This proves the inductive step and completes the proof of this problem. □

One may also want to define a recurrent relation according to the discussion above, and prove the result by induction more formally. The following is a proof.

Let t(n) be the number of subsets with 2 elements of a set with n elements. Apparently, $t(0) = 0$. If $n \geq 1$, we can recursively define t(n) as follows. For $n \geq 1$,

$$t(n) = t(n-1) + (n-1).$$

Now, let's prove the claim that for all $n \geq 0$, $t(n) = n(n-1)/2$. Define $D_n = \mathbf{N}^0$, and

$$P(n) \quad : \quad t(n) = \frac{1}{2}n(n-1).$$

- **Inductive Basis:** $n = 0$.

  $$t(0) = 0 = \frac{1}{2} \times 0 \times (0-1).$$

  Therefore, $P(0) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n$.
  Suppose, if $n \leq i$, then $P(n) = T$, i.e.

  $$t(n) = \frac{1}{2}n(n-1).$$

- **Inductive Step:** Let $n = i + 1$.

$$\begin{aligned} t(n) &= t(i+1) = t(i) + i \\ &= \frac{1}{2}i(i-1) + i = \frac{1}{2}i(i-1+2) \\ &= \frac{1}{2}(i+1)((i+1)-1) = \frac{1}{2}n(n-1). \end{aligned}$$

$P(i+1) = T$. **[The Inductive Step Holds.]**

Therefore, for any set with n elements, the set has $n(n-1)/2$-many subsets having exactly 2 elements. □

Solution 29: Prove by induction that for all integers $n \geq 2$ the set of all points of intersection of n distinct lines in the plane has no more than $n(n-1)/2$ elements. Give examples showing exactly that many, and also fewer.

Suppose we already have n lines on the plane with the maximum number of intersection points. If we draw a new line on the plane, we cannot introduce more than n new intersection points. Therefore, if $p(n)$ is the maximum number of the intersection points of n distinct lines, the recurrent relation will be

$$p(n) = p(n-1) + (n-1).$$

This is exactly the same as the recurrence relation in the previous problem. We skip the proof here. □

Solution 30: Define $P(n)$ for all $n \geq 1$ as

$$P(n) : 1 \leq x_n \leq \sqrt{n}.$$

- **Inductive Basis:** $n = 1$. $x_1 = 1$, and

$$1 \leq x_1 \leq \sqrt{1}.$$

Therefore, $P(1)$ is true. **[The Basis Holds.]**

- **Inductive Hypothesis:** Assume $P(n)$ is true, i.e.,

$$1 \leq x_n \leq \sqrt{n}.$$

- **Inductive Step:** To prove $P(n+1)$ is true.

From the hypothesis, we know that $1 \le x_n \le \sqrt{n}$. Thus,

$$\begin{aligned} 1 \le x_n \le \sqrt{n} \Rightarrow\ & 1 \le x_n^2 \le n \\ \Rightarrow\ & 1 + \frac{1}{x_n^2} \le x_n^2 + \frac{1}{x_n^2} \le n + \frac{1}{x_n^2}. \end{aligned}$$

Because $1 \le x_n^2 \Rightarrow \frac{1}{x_n^2} \le 1$, we have

$$1 \le 1 + \frac{1}{x_n^2} \quad \text{and} \quad n + \frac{1}{x_n^2} \le n + 1.$$

Therefore,

$$\begin{aligned} & 1 \le 1 + \frac{1}{x_n^2} \le x_n^2 + \frac{1}{x_n^2} \le n + \frac{1}{x_n^2} \le n + 1 \\ & \Rightarrow 1 \le x_n^2 + \frac{1}{x_n^2} \le n + 1 \\ & \Rightarrow 1 \le x_{n+1}^2 \le n + 1 \\ & \Rightarrow 1 \le x_{n+1} \le \sqrt{n+1}. \end{aligned}$$

$P(n+1)$ is true. **[The Inductive Step Holds.]**

Method 2: There is another way to prove the inductive step.

- **Inductive Step:** To prove $P(n+1)$ is true.
  From the hypothesis we know $1 \le x_n \le \sqrt{n}$, and $\frac{1}{\sqrt{n}} \le \frac{1}{x_n} \le 1$. Moreover, we know $0 \le \frac{1}{\sqrt{n}}$, thus

$$1 \le x_n^2 \le n \tag{3.11}$$

$$\frac{1}{n} \le \frac{1}{x_n^2} \le 1 \tag{3.12}$$

  By adding (3.11) and (3.12), we get

$$1 + \frac{1}{n} \le x_n^2 + \frac{1}{x_n^2} \le n + 1.$$

  Because $1 \le 1 + \frac{1}{n}$, we have

$$\begin{aligned} & 1 \le x_n^2 + \frac{1}{x_n^2} \le n + 1 \\ & \Rightarrow 1 \le x_n^2 + \frac{1}{x_n^2} \le n + 1 \\ & \Rightarrow 1 \le x_{n+1}^2 \le n + 1 \\ & \Rightarrow 1 \le x_{n+1} \le \sqrt{n+1}. \end{aligned}$$

  $P(n+1)$ is true. **[The Inductive Step Holds.]**

□

Solution 31:

- **Inductive Basis:** $n = 0$.

$$H_{2^n} = H_1 = \sum_{1 \le i \le 1} \frac{1}{i} = \frac{1}{1} \ge 1 + \frac{0}{2}.$$

[The Basis Holds.]

- **Inductive Hypothesis:** Assume $H_{2^n} \ge \left(1 + \frac{n}{2}\right)$.
- **Inductive Step:**

$$\begin{aligned}
H_{2^{n+1}} &= H_{2 \cdot 2^n} \\
&= \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{2^n} + \frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \cdots + \frac{1}{2^n + 2^n} \\
&= H_{2^n} + \frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \cdots + \frac{1}{2^n + 2^n} \\
&\ge 1 + \frac{n}{2} + \frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \cdots + \frac{1}{2^n + 2^n} \\
&\ge 1 + \frac{n}{2} + \overbrace{\frac{1}{2^n + 2^n} + \frac{1}{2^n + 2^n} + \cdots + \frac{1}{2^n + 2^n}}^{2^n} \\
&= 1 + \frac{n}{2} + \frac{2^n}{2^n + 2^n} \\
&= 1 + \frac{n+1}{2}
\end{aligned}$$

[The Inductive Step Holds.]

Therefore, for all $n \ge 0$, $H_{2^n} \ge \left(1 + \frac{n}{2}\right)$. □

Solution 32: Let A^* denote the set of all possible strings made from A, where $\lambda \in A^*$. Let μ range over A^*, and let $|\mu|$ denote the length of μ. We will prove the theorem by mathematical induction *on the length of strings.* Let us first define the domain and the predicate $P(n)$.

$$\begin{aligned}
D_n &: \{0, 1, 2, 3, \ldots\}, \\
P(n) &: \forall \mu \in A^*, [(|\mu| = n) \Rightarrow (\mu \in S \leftrightarrow \mu \text{ is a } \textit{palindrome})].
\end{aligned}$$

- **Inductive Basis:** $n = 0$ and $n = 1$.
  By the definition of S, $\lambda \in S$, and by the definition of palindrome, λ is also a palindrome. Therefore, $P(0) = T$.

  If $|\mu| = 1$, then by rule 2 any single character from A is in P, and it is also a palindrome over A. $P(1) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $i \in D_n$, and $1 \leq i$.
  Suppose if $n \leq i$, then $P(n) = T$, i.e.,

$$\forall \mu \in A^*, [(|\mu| \leq i) \Rightarrow (\mu \in S \leftrightarrow \mu \text{ is a } \textit{palindrome})].$$

- **Inductive Step:** Let $n = i + 1$. Because we assume that $1 \leq i$ in the hypothesis, we have $2 \leq n$. This will simplify our discussion because, as you will see, we don't have to consider rules 1 and 2 in the course of the inductive step. Please note that this is valid, because the cases when $n = 0$ and $n = 1$ were proved in the basis step.

  Let $\mu \in A^*$ and $|\mu| = i + 1$.

  1. If $\mu \in S$, then μ must satisfy rule 3. Rules 1 and 2 are ruled out because $2 \leq |\mu|$. Thus, μ must be a string like $a\nu a$, where $a \in A$ and $\nu \in S$. We also know that $|\nu| = i - 1$, and by the strong inductive hypothesis, $\nu \in S$ if and only if ν is a palindrome. Therefore, ν is a palindrome over A, and $a\nu a$ is also a palindrome over A. Therefore,

$$\mu \in S \rightarrow \mu \text{ is a } \textit{palindrome}.$$

  2. If μ is a palindrome over A and $2 \leq |\mu|$, μ must be a string like $a\nu a$, where $a \in A$ and ν is a palindrome over A. Since $|\nu| = i - 1$, and by the strong inductive hypothesis, $\nu \in S$ if and only if ν is a palindrome. Therefore, $\nu \in S$, and by rule 3, $a\nu a \in P$. Therefore,

$$\mu \text{ is a } \textit{palindrome} \rightarrow \mu \in S.$$

  $P(i + 1) = T$. **[The Inductive Step Holds.]**

For any length n, $P(n)$ is true, which means that S is the set of palindromes over A.

Note: The proof given above uses the original form of mathematical induction. We haven't seen the power of structural induction yet. Please compare the following proof with the previous one. We will see the full power of structural induction in the last two problems of this chapter.

Method 2: Structural induction

$$\begin{aligned} D_s &: A^*, \\ P(s) &: (s \in S \leftrightarrow s \text{ is a } \textit{palindrome}). \end{aligned}$$

- **Inductive Basis:** By the definitions of S and palindrome, $\lambda \in S$ and it is a palindrome. Thus, $P(\lambda) = T$. **[The Basis Holds.]**

- **Inductive Hypothesis:** Let $s \in A^*$, and assume $P(s) = T$, i.e.,

$$s \in S \ \leftrightarrow \ s \text{ is a } palindrome.$$

- **Inductive Step:** Our task is to prove

$$asa \in S \ \leftrightarrow \ asa \text{ is a } palindrome.$$

We have two cases about s: (1) $s \in S$, and (2) $s \notin S$.

case 1: $s \in S$. By the definition of S, $asa \in S$. By the hypothesis, s is a palindrome, and hence asa is also a palindrome. Thus,

$$[asa \in S \ \rightarrow \ asa \text{ is a } palindrome] = T.$$

case 2: $s \notin S$. By the definition of S, $asa \notin S$. By the hypothesis, s is not a palindrome, and hence asa is not a palindrome. Thus,

$$[asa \notin S \ \rightarrow \ asa \text{ is not a } palindrome] = T.$$

By contrapositive, we have

$$[asa \text{ is a } palindrome \ \rightarrow \ asa \in S] = T.$$

Together, we have $asa \in S \ \leftrightarrow \ asa$ is a $palindrome$.

[The Inductive Step Holds.]

Therefore, for any string s, $s \in S$ if and only if s is a palindrome. □

Solution 33: Let $D_s = S$, and define two variables predicate $P(\mu, \nu)$ as: for all $\mu, \nu \in S$,

$$P(\mu, \nu) : R(\mu\nu) = R(\nu)R(\mu).$$

- **Inductive Basis:** $\mu = a$, and $\mu = b$.

For $\mu = a$, let $\nu \in S$. We have

$$R(\mu\nu) = R(a\nu) = R(\nu)a = R(\nu)R(a) = R(\nu)R(\mu).$$

Same as $\mu = b$. Thus, for all $\nu \in S$, $P(a, \nu) = T$ and $P(b, \nu) = T$.

[The Basis Holds.]

- **Inductive Hypothesis:** Let $\mu, \nu \in S$. Assume that for all $\xi \in S$, $P(\mu, \xi) = P(\nu, \xi) = T$, i.e.,

$$R(\mu\xi) = R(\xi)R(\mu) \ \ \& \ \ R(\nu\xi) = R(\xi)R(\nu).$$

- **Inductive Step:** Our task is to prove that for all $\xi \in S$, $P(\mu\nu, \xi)$ is true, i.e., $R(\mu\nu\xi) = R(\xi)R(\mu\nu)$. Let $\xi \in S$,

$$\begin{array}{rcll} R(\mu\nu\xi) & = & R(\mu(\nu\xi)) & \\ & = & R(\nu\xi)R(\mu) & [\textbf{by IH}] \\ & = & R(\xi)R(\nu)R(\mu) & [\textbf{by IH}] \\ & = & R(\xi)(R(\nu)R(\mu)) & \\ & = & R(\xi)R(\mu\nu) & [\textbf{by IH}] \end{array}$$

Therefore, for all $\mu, \nu \in S$, $R(\mu\nu) = R(\nu)R(\mu)$. □

Solution 34: Let $D_s = S$, and define predicate $P(\mu)$ as: for all $\mu \in S$,

$$P(\mu) : R(R(\mu)) = \mu.$$

We will use the result proved in the previous problem: for all $\mu, \nu \in S$,

$$R(\mu\nu) = R(\nu)R(\mu). \tag{3.13}$$

- **Inductive Basis:** $\mu = a$, and $\mu = b$. It is clear that $P(a) = P(b) = T$, because

$$R(R(a)) = R(a) = a, \text{ and } R(R(b)) = R(b) = b.$$

[The Basis Holds.]

- **Inductive Hypothesis:** Let $\mu, \nu \in S$. Assume that

$$R(R(\mu)) = \mu, \text{ and } R(R(\nu)) = \nu.$$

- **Inductive Step:** We want to prove that $R(R(\mu\nu)) = \mu\nu$.

$$\begin{array}{rcll} R(R(\mu\nu)) & = & R(R(\nu)R(\mu)) & \text{by (3.13)} \\ & = & R(R(\mu))R(R(\nu)) & \text{by (3.13)} \\ & = & \mu\nu & [\textbf{by IH}] \end{array}$$

[The Inductive Step Holds.]

Therefore, for all $\mu \in S$, $R(R(\mu)) = \mu$. □

Solution 35:

We will prove this problem by structural mathematical induction. For convenience, let $\alpha(\omega)$ denote the number of a's in ω, and $\beta(\omega)$ the number of b's in ω. We shall prove that, for every $\omega \in A$, $\alpha(\omega) = \beta(\omega)$.

- **Inductive Basis:** $\omega = \Lambda$. It is clear that $\alpha(\omega) = \beta(\omega) = 0$. **[The Basis Holds.]**
- **Inductive Hypothesis:** Let $\mu, \nu \in A$, and $\alpha(\mu) = \beta(\mu) = m$, and $\alpha(\omega) = \beta(\omega) = n$.
- **Inductive Step:**

  By rule 2: $\omega = a\mu b$. Clearly, $\alpha(\omega) = \beta(\omega) = m + 1$.

  By rule 3: $\omega = \mu\nu$. Thus, $\alpha(\omega) = \alpha(\mu\nu) = m + n$ and $\beta(\omega) = \beta(\mu\nu) = m + n$.

  Thus, $\alpha(\omega) = \beta(\omega)$ in all cases. **[The Inductive Step Holds.]**

Therefore, if $\omega \in A$, then $\alpha(\omega) = \beta(\omega)$. □

Solution 36: As with the previous problem, let $\alpha(\omega)$ denote the number of a's in ω, and $\beta(\omega)$ the number of b's in ω. We shall prove that, if $\omega \in A$, then for any prefix σ of ω we have $\alpha(\sigma) \geq \beta(\sigma)$.

- **Inductive Basis:** $\omega = \Lambda$. The only prefix of Λ is Λ itself. It is clear that $\alpha(\omega) = \beta(\omega) = 0$. Thus, the inductive basis holds. **[The Basis Holds.]**
- **Inductive Hypothesis:** Fix $\mu, \nu \in A$, and assume that, for any σ, if σ is a prefix of μ or ν, then $\alpha(\sigma) \geq \beta(\sigma)$.
- **Inductive Step:**

  By rule 2: We obtain a new string $\omega = a\mu b$. Given σ a prefix of ω, we have the following cases.

  1. $\sigma = \Lambda$. In this case, it is clear that $\alpha(\sigma) \geq \beta(\sigma)$.
  2. $\sigma = a\sigma'$, where σ' is a prefix of μ. Thus, $\alpha(\sigma) = \alpha(a\sigma') = \alpha(\sigma') + 1$ and $\beta(\sigma) = \beta(a\sigma') = \beta(\sigma')$. By the inductive hypothesis, $\alpha(\sigma') \geq \beta(\sigma')$. Thus, $\alpha(\sigma') + 1 \geq \beta(\sigma')$, and hence $\alpha(\sigma) \geq \beta(\sigma)$.
  3. $\sigma = \omega = a\mu b$. In this case, $\alpha(\sigma) = \alpha(\mu) + 1$ and $\beta(\sigma) = \beta(\mu) + 1$. By the inductive hypothesis, $\alpha(\mu) \geq \beta(\mu)$. Thus, $\alpha(\sigma) \geq \beta(\sigma)$.

By rule 3: We obtain a new string $\omega = \mu\nu$. Given σ a prefix of ω, we have the following cases.

1. σ is a prefix of μ. By the inductive hypothesis, $\alpha(\sigma) \geq \beta(\sigma)$.
2. $\sigma = \mu\xi$, where ξ is a prefix of ν. By the inductive hypothesis, we have $\alpha(\mu) \geq \beta(\mu)$ and $\alpha(\xi) \geq \beta(\xi)$. Thus, $\alpha(\mu) + \alpha(\xi) \geq \beta(\mu) + \beta(\xi)$. Since $\alpha(\sigma) = \alpha(\mu) + \alpha(\xi)$ and $\beta(\sigma) = \beta(\mu) + \beta(\xi)$, it follow that $\alpha(\sigma) \geq \beta(\sigma)$.

[The Inductive Step Holds.]

This completes the proof. □

Chapter 4

Relations

I wanted certainty in the kind of way in which
people want religious faith.
I thought that certainty is more likely to be found in
mathematics than elsewhere.

– Bertrand Russell

4.1 Definitions, Theorems, and Comments

The concept of relation is widely used in everyday life. For example, "Sean and Leon are brothers" carries the concept of relation "brother" that Sean and Leon have. Or, "Dennis is the father of Sean" carries the concept of relation "father". For some relations, we can exchange the subject and object in the English sentences that represent some relations; while for some others we cannot. For example, if "Sean is a brother of Leon", then we also have the fact that "Leon is a brother of Sean" (presumably that both Sean and Leon are boys), whereas "Dennis is the father of Sean" shows that exchanging subject and object of the sentence is not allowed.

In this chapter, we will study some widely used relations in mathematics and give them mathematical characterizations.

4.1.1 Definitions

Definition 4.1: A *relation* R on sets S and T is a subset of the Cartesian product $S \times T$. That is, R is a *binary relation* if $R \subseteq S \times T$.

Comment: A relation R can be a subset of the Cartesian product of more than two sets, i.e., $R \subseteq S_1 \times S_2 \times \cdots \times S_n$, where $n \leq 2$. In this chapter, we are interested in binary relations.

Definition 4.2: If $R \subseteq S \times S$, we call R a *binary relation* on S.

Definition 4.3: If $R = S \times T$, then R is called the *complete relation*.

Notations for relations

There are many methods to express a relation:

1. ***Ordered pairs notation:*** We have used this notation in the definitions above. This notation directly comes from the definition of the Cartesian product of sets.

   Example 4.1 Let $S = \{a, b, c, d\}$, and

   $$R = \{(a, a), (b, a), (b, c), (c, d)\}.$$

   R is a relation on S. We say, b has relation R to a because $(b, a) \in R$, but a does not have relation R to b because $(a, b) \notin R$

2. ***Infix notation:*** In this notation the property $(x, y) \in R$ is written as xRy. This is also the method of expressing a relation in everyday life.

For example, note the similarity in the infix notation and a typical everyday real-life relation "x 'is a brother of' y", or a typical mathematical statement "x 'is divisible by' y".

Example 4.2 Consider the relation in Example 4.1. We have bRa because $(b, a) \in R$, but we don't have aRb because $(a, b) \notin R$.

3. ***Matrix notation:*** When R is a finite relation, it can be written as a matrix (also denoted by R) $R = (r_{i,j})$ where

$$r_{i,j} = \begin{cases} 1 & \text{if } i, j \in S \text{ and } (i, j) \in R \\ 0 & \text{if } i, j \in S \text{ and } (i, j) \notin R \end{cases}$$

Example 4.3 Let $S = \{x, y, z\}$, $T = \{a, b, c, d\}$. We represent a relation $R \subseteq S \times T$ in the following 3×4 matrix r.

$$R = \begin{array}{c|cccc} & a & b & c & d \\ \hline x & 1 & 0 & 1 & 0 \\ y & 0 & 1 & 0 & 0 \\ z & 1 & 0 & 1 & 1 \end{array}$$

For examples, $(x, c) \in R$ because $r_{x,c} = 1$, and $(z, b) \notin R$ because $r_{z,b} = 0$. Altogether, we have

$$R = \{(x, a), (x, c), (y, b), (z, a), (z, c), (z, d)\}.$$

4. ***Directed graph representation:*** In this representation the relation R is a directed graph with nodes as all elements of the set S, and for $x, y \in S$ the graph contains a directed edge from x to y if and only if $(x, y) \in R$.

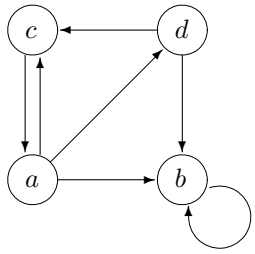
Example 4.4 Let $S = \{a, b, c, d\}$, and

$$R = \{(a, b), (a, c), (a, d), (b, b), (c, a), (d.b), (d, c)\}.$$

The following figure shows two different representations of the same relation R.

	a	b	c	d
a	0	1	1	1
b	0	1	0	0
c	1	0	0	0
d	0	1	1	0

Matrix



Directed Graph

Definition 4.4: Let S be a non-empty set and $R \subseteq S \times S$ a relation.

1. R is called a *reflexive* relation if and only if

$$\text{for all } x \text{ in } S, \text{ we have } (x, x) \in R.$$

2. R is called a *symmetric* relation if and only if

$$\text{for all } x, y \in S, \text{ if } (x, y) \in R, \text{ then } (y, x) \in R.$$

3. R is called a *transitive* relation if and only if

$$\text{for all } x, y, z, \in S, \text{ if } (x, y) \in R \text{ and } (y, z) \in R, \text{ then } (x, z) \in R.$$

Comment: The above definition can be extended to include the case $S = \emptyset$. In this special case, the only possible relation on S would be $\emptyset$. The empty relation, $\emptyset$, satisfies all three properties stated above.

Definition 4.5: A relation R on S is called an *equivalence relation* if it satisfies the following three properties:

1. R is a reflexive relation,
2. R is a symmetric relation, and
3. R is a transitive relation.

Example 4.5 Let $S = \{v_0, v_1, v_2, \ldots, v_n\}$ be the set of variables in a certain computer program. If $v_i = v_j$ means the values of v_i and v_j are the same, then at any moment during the course of running the program "=" is an equivalence relation on S.

Definition 4.6: Let S be a non-empty set. A *partition* P of S is a set of subsets of S,

$$P = \{A_1, A_2, \ldots, A_k\},$$

such that,

1. $\bigcup_{i=1}^{k} A_i = S$, and
2. for all i, $1 \leq i \leq k$, (a) $A_i \subseteq S$,

   (b) $A_i \neq \emptyset$,

   (c) $A_i \cap A_j = \emptyset$, where $1 \leq j \leq k$ and $i \neq j$.

The elements of the set P, $A_1, A_2, \ldots, A_k$ are called *cells*.

Definition 4.7: Let $P = \{A_1, A_2, \ldots, A_k\}$ and let $Q = \{B_1, B_2, \ldots, B_l\}$ be two partitions of a nonempty set S. The partition Q is called a *refinement* of P if and only if for any $B_j \in Q$ there exists one and only one $A_i \in P$ such that $B_j \subset A_i$.

Definition 4.8: Suppose that $R \subseteq S \times S$ is an equivalence relation, and $x \in S$ is a fixed element. The set $[x]_R = \{y : xRy, y \in S\}$ is known as the *equivalence class* of x.

Definition 4.9: Let $R \subseteq S \times S$ be an equivalence relation. It can be seen that the set of equivalence classes produced by R is a partition of S, i.e., $\{[x]_R : x \in S\}$ is a partition of S. This set is also known as *the quotient set* and is often denoted as S/R.

Example 4.6 Let $S = \{1, 2, 3, 4, 5, 6\}$. Consider the relation R given in the following matrix.

$R =$

	1	2	3	4	5	6
1	1	1	0	0	0	1
2	1	1	0	0	0	1
3	0	0	1	0	0	0
4	0	0	0	1	1	0
5	0	0	0	1	1	0
6	1	1	0	0	0	1

We have the following facts:

1. R is an equivalence relation on S because it is reflexive, symmetric, and transitive.
2. Let
$$P = \{\{1, 2, 6\}, \{3\}, \{4, 5\}\}.$$
Then P is a partition of S. In fact, P is the quotient set S/R given by the relation R because
$$[1]_R = [2]_R = [6]_R = \{1, 2, 6\},$$
$$[3]_R = \{3\},$$
$$[4]_R = [5]_R = \{4, 5\}.$$
3. Let
$$Q = \{\{1, 2\}, \{3\}, \{4, 5\}, \{6\}\}.$$
Then Q is a refinement of P.

Definition 4.10: A relation R on S is called an *irreflexive* relation if and only if for all $x \in S$, $(x, x) \notin R$.

Definition 4.11: A relation R on S is called an *asymmetric* relation if and only if for all $x, y \in S$, if $(x, y) \in R$ then $(y, x) \notin R$.

Definition 4.12: A relation R on S is called an *antisymmetric* relation if and only if for all $x, y \in S$, if $(x, y) \in R$, then either $x = y$ or $(y, x) \notin R$. In another words, if both (x, y) and (y, x) are in R, then $x = y$.

Definition 4.13: A relation R on S is called a *partial order relation* if it satisfies the following three properties:

1. R is a reflexive relation,
2. R is an antisymmetric relation, and
3. R is a transitive relation.

Should we push the transitive closure here?

Comment: In some occasions, we allow a partial order relation to be irreflexive. The reflexivity or irreflexivity of a partial order relation will not affect some major properties of the partial order relation we are interested in.

Example 4.7 Let $S = \{0, 1, 2, 3 \ldots\}$. The relation $\leq$ is a partial order relation on S. In fact, if S is any collection of real numbers, then $\leq$ is a partial order relation on S.

4.1.2 Theorems

There is an intimate relation between an equivalence relation $R \subseteq S \times S$ and a partition P of S. This relation is precisely stated below:

Theorem 4.1 Let $R \subseteq S \times S$ be an equivalence relation. Then R generates a unique partition of $P_R = \{A_1, A_2, \ldots, A_k\}$ of S such that, for all x, y

$$\exists i, 1 \leq i \leq k, (x, y) \in A_i \text{ if and only if } (x, y) \in R.$$

Conversely given a partition $P = \{A_1, A_2, \ldots, A_k\}$ of S, a unique equivalence relation R_P is defined as follows:

$$(x, y) \in R_P \text{ if and only if } \exists i, 1 \leq i \leq k, (x, y) \in A_i.$$

Theorem 4.2 Let $R \subseteq S \times S$ be an equivalence relation and $x, y \in S$. Then the following property holds: Either $[x]_R = [y]_R$ or $[x]_R \cap [y]_R = \emptyset$.

Comment: Given an equivalence relation on S, the above theorem shows that the collection of all possible equivalence classes give a partition of S.

4.2 Problems

Problem 1: Let S be a set, and R be a relation on S. Rewrite the definitions of reflexive, symmetric, and transitive relations into quantified predicates.

Problem 2: Same as above, rewrite the definitions of irreflexive, asymmetric, and antisymmetric relations into quantified predicates.

Problem 3:

1. Write the inclusion relation $\subseteq$ on the power set $\mathcal{P}(\{a, b, c\})$ in the matrix notation.
2. Is $\subseteq$ an equivalence relation on $\mathcal{P}(\{a, b, c\})$?
3. Is $\subseteq$ a partial order relation on $\mathcal{P}(\{a, b, c\})$?

Problem 4: Define the relation R on the power set $\mathcal{P}(A)$ of a set A as,

$$\forall a, b \in \mathcal{P}(A)[(a, b) \in R \leftrightarrow a \cap b \neq \emptyset].$$

Is R reflexive, symmetric, or transitive? Why?

Problem 5: Let A be the set of all lines in the plane, and R_1, R_2 be two relations on A defined as follows:

1. Definition of R_1: For all L, $L' \in A$,

   $$(L, L') \in R_1 \text{ iff } L \text{ is perpendicular to } L'.$$

2. Definition of R_2: For all L, $L' \in A$,

   $$(L, L') \in R_2 \text{ iff } L \text{ is perpendicular or parallel to } L'.$$

Mark the following table properly to indicate the properties of the relations R_1 and R_2 have.

	reflexive / irreflexive	symmetric / asymmetric	antisymmetric	transitive
R_1				
R_2				

Problem 6: Let $\mathbf{N}$ be the set all positive integers, and R_1, R_2 be two relations on $\mathbf{N}$ defined as follows:

1. Definition of R_1: For all $a, b \in \mathbf{N}$,

   $$(a, b) \in R_1 \text{ iff } a \neq b.$$

2. Definition of R_2: For all $a, b \in \mathbf{N}$,

   $$(a, b) \in R_2 \text{ iff } \frac{a}{b} = 2^i \text{ for some integer } i \geq 0.$$

Mark the following table properly to indicate the properties of the relations R_1 and R_2 have.

	reflexive	irreflexive	symmetric	asymmetric	antisymmetric	transitive
R_1						
R_2						

Problem 7: Define the relation R on $\mathbf{N}$ as

$$\forall\ c, d\ \in \mathbf{N} \quad (c, d) \in R \ \text{ iff } \ c + d \text{ is even.}$$

1. Prove that R is an equivalence relation.
2. How many equivalence classes does R have?

Problem 8: Let S be the set of all students at a school. Define the relation R as: For all students x and y in S,

$$xRy \ \text{ iff } \ x \text{ and } y \text{ are taking the same class.}$$

Is R an equivalence relation?

Problem 9: Let R be a reflexive and transitive relation on a set S. Define a relation Y on S as follows:

$$\forall a, b \in S\ [(a, b) \in Y \ \leftrightarrow\ ((a, b) \in R \wedge (b, a) \in R.)]$$

Prove that Y is an equivalence relation.

Problem 10:
1. Give an example of a relation that is symmetric and transitive, but not reflexive.
2. What is wrong with the following "proof" that every symmetric and transitive relation R is reflexive? If $(a, b) \in R$ then $(b, a) \in R$ by symmetry. By transitivity, $(a, a) \in R$. Therefore R is reflexive.

Problem 11: Let S be a set, $P(x)$ and $Q(x)$ be two predicates in one variable $x \in S$, and L be a binary equivalence relation on S. Suppose

$$\forall x \in S[P(x) \longrightarrow \neg Q(x)].$$

Define a binary relation R on S as follows:

$$(x, y) \in R \leftrightarrow [((x, y) \in L) \wedge P(x) \wedge Q(y)].$$

Is the relation R reflexive, symmetric, or transitive? Why?

Problem 12: An *isolated point* for a relation R on a set A is an element a, where $a \in A$ and $(a, x) \notin R$ and $(x, a) \notin R$ for any $x \in A$.

1. Given R and A as above, write a predicate to define the *isolated point*.
2. Suppose R is a binary relation on A such that, R is symmetric and transitive, and R has no isolated points. Prove that R is an equivalence relation.

Problem 13: Let A be a set having a total of n elements, where $n \geq 1$. Let R be any equivalence relation on A. Prove that the total number of ordered pairs in R is odd if n is odd, even if n is even.

[Hint: Consider the matrix notation for relations.]

Problem 14: Let R and S be two relations both on A.

1. If R and S are both reflexive, is $R \cap S$ also reflexive?
2. If R and S are both symmetric, is $R \cap S$ also symmetric?
3. If R and S are both transitive, is $R \cap S$ also transitive?

Problem 15: Let R and S be two relations both on A.

1. If R and S are both reflexive, is $R \cup S$ also reflexive?
2. If R and S are both symmetric, is $R \cup S$ also symmetric?
3. If R and S are both transitive, is $R \cup S$ also transitive?

Problem 16: Let $A,\ B,\ C$ be any three sets. And let

$$\begin{aligned} D =& (A - (B \cup C)), \\ E =& ((A - C) \cap B), \\ F =& (A \cap C). \end{aligned}$$

Suppose each of D, E and F is nonempty. Prove that $\{D, E, F\}$ is a partition of A.

[Hint: Use an epsilon argument, but first draw a Venn diagram to help yourself see what's going on.]

Problem 17: Define R to be the following relation on $\mathbf{N} \times \mathbf{N}$:

For all a, b, x, y in $\mathbf{N}$,

$$(a, b)R(x, y) \ \text{ iff } \ ay = bx.$$

Prove that R is an equivalence relation.

Problem 18: Let $A = \{1, 2, 3, 4\}$. For each of the following three relations on A, prove or disprove that it is an equivalence relation and, if it is one, write down its equivalence classes.

$$\begin{aligned} R_1 &= \{(1,1),(2,2),(3,4),(3,3),(4,4)\} \\ R_2 &= \left\{ \begin{array}{l} (1,1),(2,2),(3,4),(4,4),(1,2),(2,1), \\ (3,3),(4,3),(1,3),(1,4),(3,1),(4,1) \end{array} \right\} \\ R_3 &= \{(1,1),(2,2),(3,4),(3,3),(4,4),(1,2),(2,1),(4,2),(2,3)\}. \end{aligned}$$

Problem 19: List all the partitions of $\{a, b, c\}$.

Problem 20: Given any set S, is $\{S\}$ a partition of S?

Problem 21: Let $\mathbf{Z}$ be the set of all integers. Define relation R on $\mathbf{N}$ as follows:

$$\forall a, b \in \mathbf{N},\ (a, b) \in R \ \text{ iff } \ \exists i \in \mathbf{Z}\ \frac{a}{b} = 2^i.$$

1. Prove that R is an equivalence relation.
2. List the cells of the partition given by R.

Problem 22: How many equivalence relations are there on $A = \{1, 2, 3\}$?

Problem 23: Let R_1 and R_2 be equivalence relations on a set S. Prove or disprove that $R_1 \cup R_2$ is also an equivalence relation on S.

Problem 24: Let R_1 and R_2 be partial order relations on a set S. Prove or disprove that $R_1 \cup R_2$ is also a partial order relation on S.

Problem 25: Let $\mathcal{P}(\mathbf{N})$ be the power set of natural numbers. Prove that the subset relation $\subseteq$ is a partial order relation on $\mathcal{P}(\mathbf{N})$.

Problem 26: Let $S = \{1, 2, \ldots, 10\}$. Define the following four sets as:

$$\begin{aligned}
P_1 =& \{\{1, 3, 8\},\ \{2, 4, 6\},\ \{5, 7, 10\},\ \{9\}\}.\\
P_2 =& \{\{7, 4, 3, 8\},\ \{1, 5, 10, 3\},\ \{2, 6\}\}.\\
P_3 =& \{\{1, 5, 9\},\ \{2, 10, 4, 7\},\ \{8, 3, 6\}\}.\\
P_4 =& \{\{4, 2\},\ \{3, 8\},\ \{6\},\ \{10, 7\},\ \{1\}, \{5\},\ \{9\}\}.
\end{aligned}$$

1. Which of the sets above is a partition of S?
2. Which of the partitions is a refinement of which other partitions?

Problem 27: The set $\{1, 2, 3, 4, 5, 6\}$ is partitioned as

$$P = \{\{1, 2, 3\}, \{4, 5\}, \{6\}\}.$$

How many refinements does P have?

Problem 28: Let S be any non-empty set and suppose that

$$P_1 = \{C_1, \ldots, C_m\} \ \text{ and } \ P_2 = \{D_1, \ldots, D_n\}$$

are two partitions of S. Define set Q as:

$$Q = \{C_i \cap D_j\ ;\ 1 \le i \le m,\ 1 \le j \le n\} - \{\emptyset\}$$

1. Prove that Q is a is a partition of S.
2. Prove that Q is a refinement of both P_1 and P_2.

4.3 Solutions

Solution 1: Let S be a set, and R be a relation on S.

R is reflexive iff $\forall a \in S, (a, a) \in R$.

R is symmetric iff $\forall a, b \in S[(a, b) \in R \leftrightarrow (b, a) \in R]$.

R is transitive iff $\forall a, b, c \in S, [(a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R]$.

Note: For the definition of symmetry, we can also rewrite as:

$$R \text{ is symmetric iff } \forall a, b \in S[(a, b) \in R \rightarrow (b, a) \in R].$$

□

Solution 2: Let S be a set, and R be a relation on S.

R is irreflexive iff $\forall a \in S, (a, a) \notin R$.

R is asymmetric iff $\forall a, b \in S[(a, b) \in R \rightarrow (b, a) \notin R]$.

R is antisymmetric iff $\forall a, b \in S, [(a, b) \in R \wedge (b, a) \in R \rightarrow a = b]$.

□

Solution 3:

1. Relation matrix of $\subseteq$ on the power set $\mathcal{P}(\{a, b, c\})$:

$\subseteq$	$\emptyset$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{b, c\}$	$\{a, c\}$	$\{a, b, c\}$
$\emptyset$	1	1	1	1	1	1	1	1
$\{a\}$	0	1	0	0	1	0	1	1
$\{b\}$	0	0	1	0	1	1	0	1
$\{c\}$	0	0	0	1	0	1	1	1
$\{a, b\}$	0	0	0	0	1	0	0	1
$\{b, c\}$	0	0	0	0	0	1	0	1
$\{a, c\}$	0	0	0	0	0	0	1	1
$\{a, b, c\}$	0	0	0	0	0	0	0	1

2. $\subseteq$ is not an equivalence relation because it is not symmetric. For example, $\{a\} \subseteq \{a, b\}$, whereas $\{a, b\} \not\subseteq \{a\}$.

3. $\subseteq$ is a partial order relation. From the relation matrix, it is easy to verify that $\subseteq$ is reflexive and antisymmetric. In general, the transitivity is not obvious to be seen from the relation matrix. But in this particular problem, we can see the property directly from the basic theorems in set. That is, for any sets $A, B, C \in \mathcal{P}(\{a, b, c\})$, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$. Therefore, $\subseteq$ is transitive.

□

Solution 4: Given any set A, the relation R on the power set $\mathcal{P}(A)$ is defined as,

$$\forall a, b \in \mathcal{P}(A)\ [(a, b) \in R \leftrightarrow a \cap b \neq \emptyset].$$

1. R is not reflexive because $\emptyset$ is an element of the power set of any set A, and $\emptyset \cap \emptyset = \emptyset$. By the definition, $(\emptyset, \emptyset) \notin R$.

2. R is symmetric because the intersection operator $\cap$ is commutative, thus, if $a \cap b \neq \emptyset$, then $b \cap a \neq \emptyset$.

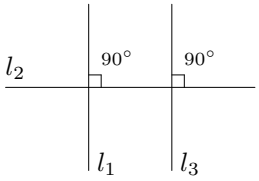
3. R is not transitive, because if $a \cap b \neq \emptyset$ and $b \cap c \neq \emptyset$ doesn't mean that $a \cap c \neq \emptyset$. Here is a counter example: let $a = \{1, 2\}, b = \{2, 3\}$, and $c = \{3, 4\}$.

□

Solution 5: Answers:

	reflexive	irreflexive	symmetric	asymmetric	antisymmetric	transitive
R_1		√	√			
R_2	√		√		√	

Explanation: Let $l_1 \perp l_2$ denote line l_1 is perpendicular to line l_2, and $l_1 \parallel l_2$ denote l_1 is parallel to l_2. Consider the following figure.



R_1:

1. It is clear that $\perp$ is not reflexive because any line is not perpendicular to itself. In another words, $\perp$ is irreflexive.
2. $\perp$ is symmetric because
$$l_1 \perp l_2 \;\Rightarrow\; l_2 \perp l_1.$$
3. $\perp$ is not asymmetric because
$$l_1 \perp l_2 \;\text{ and }\; l_2 \perp l_1.$$
4. $\perp$ is not antisymmetric because
$$(l_1 \perp l_2 \;\wedge\; l_2 \perp l_1) \;\not\Rightarrow\; l_1 = l_2.$$
5. $\perp$ is not transitive because
$$(l_1 \perp l_2 \;\wedge\; l_2 \perp l_3) \;\not\Rightarrow\; l_1 \perp l_3.$$

R_2:

1. R_2 is reflexive because for all l, we know that $l \parallel l$, thus
$$l \parallel l \;\Rightarrow\; (l \parallel l) \vee (l \perp l) \;\Rightarrow\; (l, l) \in R_2.$$
2. R_2 is symmetric because,
$$\begin{aligned}(l_1, l_2) \in R_2 \Rightarrow\; & (l_1 \parallel l_2) \vee (l_1 \perp l_2) \\ \Rightarrow\; & (l_2 \parallel l_1) \vee (l_2 \perp l_1) \\ \Rightarrow\; & (l_2, l_1) \in R_2.\end{aligned}$$
3. R_2 is not asymmetric. As shown in the example above, both (l_1, l_2) and (l_2, l_1) are in R_2.
4. R_2 is not antisymmetric. As shown in the example above both (l_1, l_2) and (l_2, l_1) are in R_2, and $l_1 \neq l_2$.
5. R_2 is transitive, because, for all l_1, l_2 and l_3, if $(l_1, l_2) \in R_2$ and $(l_2, l_3) \in R_2$, we have four cases:

   case 1: $l_1 \parallel l_2$ and $l_2 \parallel l_3$, $\Rightarrow\;\; l_1 \parallel l_3 \;\;\Rightarrow\;\; (l_1, l_3) \in R_2$.
   case 2: $l_1 \parallel l_2$ and $l_2 \perp l_3$, $\Rightarrow\;\; l_1 \perp l_3 \;\;\Rightarrow\;\; (l_1, l_3) \in R_2$.
   case 3: $l_1 \perp l_2$ and $l_2 \parallel l_3$, $\Rightarrow\;\; l_1 \perp l_3 \;\;\Rightarrow\;\; (l_1, l_3) \in R_2$.
   case 4: If $l_1 \perp l_2$ and $l_2 \perp l_3$, $\Rightarrow\;\; l_1 \parallel l_3 \;\;\Rightarrow\;\; (l_1, l_3) \in R_2$.

   In each cases, we have $(l_1, l_3) \in R_2$.

□

Solution 6: Answers:

	reflexive	irreflexive	symmetric	asymmetric	antisymmetric	transitive
R_1		$\surd$	$\surd$			
R_2	$\surd$				$\surd$	$\surd$

Explanation:

R_1:

1. R_1 is not reflexive because for all $a \in \mathbf{N}$, $a = a$.
2. R_1 is irreflexive because for all $a \in \mathbf{N}$, $a = a$, thus $(a, a) \notin R_1$.
3. R_1 is symmetric because for all $a, b \in \mathbf{N}$, if $a \neq b$ then $b \neq a$, i.e., if $(a, b) \in R_1$, then $(b, a) \in R_1$.
4. R_1 is not asymmetric because there exist $a, b \in \mathbf{N}$, $a \neq b$ and $b \neq a$.

   Note: We must not say that R_1 is not asymmetric because R_1 is symmetric. Consider the empty relation, it is symmetric, asymmetric, and antisymmetric!!
5. R_1 is not antisymmetric because there exist different a and b in $\mathbf{N}$ such that, $a \neq b$ and $b \neq a$.
6. R_1 is not transitive because, for example, $(1, 2), (2, 1) \in R_1$ but $(1, 1) \notin R_1$.

R_2:

1. R_2 is reflexive because for all $a \in \mathbf{N}$, $\frac{a}{a} = 1 = 2^0$, this $(a, a) \in R_4$.
2. R_2 is not symmetric because if $(a, b) \in R_2$, then $\frac{a}{b} = 2^i$, where $i \geq 0$, but $\frac{b}{a} = 2^{-i}$, where $-i \leq 0$. Therefore, $(b, a) \notin R_2$.
3. R_2 is not asymmetric. Because, if we let $a = b$, we can have both (a, b) and (b, a) in R_2.
4. R_2 is antisymmetric. If $(a, b) \in R_2$ and $(b, a) \in R_2$, we have $\frac{a}{b} = 2^i$ and $\frac{b}{a} = 2^j$, where $i, j \geq 0$. Then

   $$\frac{a}{b} \times \frac{b}{a} = 1 = 2^{i+j}.$$

   Thus, $i + j = 0$. Since $i, j \geq 0$, we have $i = j = 0$. Therefore, $\frac{a}{b} = 1$, and hence $a = b$.
5. R_2 is transitive because, if $(a, b), (b, c) \in R_2$, then $\frac{a}{b} = 2^i$ and $\frac{b}{c} = 2^j$, where $i, j \geq 0$.

   $$\frac{a}{c} = \frac{a}{b} \times \frac{b}{c} = 2^{i+j}, \text{ where } i + j \geq 0.$$

   Therefore, $(a, c) \in R_2$.

□

Solution 7: If $c+d$ is even, then we can find an integer i such that, $c+d = 2i$.

1. R is an equivalence relation because,

   Reflexive: For all $a \in \mathbf{N}$, $a+a = 2a$, which is even. Therefore, $(a, a) \in R$.

   Symmetric: If $a+b$ is even, then $b+a$ is even. Therefore, for all $a, b \in \mathbf{N}$, if $(a, b) \in R$, then $(b, a) \in R$.

   Transitive: Let $(a, b) \in R$ and $(b, c) \in R$. Then,

   $$a + b = 2i \tag{4.1}$$
   $$b + c = 2j \tag{4.2}$$

   where, i and j are integers. Take (1)+(2), we have $a+2b+c = 2i+2j$. Thus, $a + c = 2(i + j - b)$. Since $i + j - b$ is an integer, we know that $a + c$ is even. Therefore, $(a, c) \in R$.

2. There are two equivalence classes of R:

   $$E := \{x : x \in \mathbf{N}, x \text{ is even}\}.$$
   $$O := \{x : x \in \mathbf{N}, x \text{ is odd}\}.$$

   Because, if $x \in E$ and $(x, y) \in R$, that means $x + y$ is even. If x and $x + y$ are even, y must be even. Therefore, $y \in E$. Likewise, if $x \in O$ and $(x, y) \in R$, that means $x + y$ is even. Therefore, y must be odd, hence $y \in O$. And since $E \cup O = \mathbf{N}$, no other equivalence class is possible.

□

Solution 8: R is not an equivalence relation due to the lack of transitivity. Let $x, y, z \in B$. Suppose x and y taking discrete mathematics, y and z taking programming languages. That means $(x, y) \in R$ and $(y, z) \in R$. But, that does not mean x takes programming languages, nor z takes discrete mathematics. Therefore, $(x, z) \in R$ is not necessarily true. □

Solution 9: Given a reflexive and transitive relation R on S.

Reflexivity: For all $a \in S$, $(a, a) \in R$, because R is reflexive.

$$\begin{aligned}(a, a) \in R &\Rightarrow (a, a) \in R \text{ and } (a, a) \in R \\ &\Rightarrow (a, a) \in Y.\end{aligned}$$

Symmetry: For all $a, b \in S$, from the definition of Y, we have

$$\begin{aligned}(a,b) \in Y &\Rightarrow (a,b) \in R \text{ and } (b,a) \in R \\ &\Rightarrow (b,a) \in R \text{ and } (a,b) \in R \\ &\Rightarrow (b,a) \in Y.\end{aligned}$$

Transitivity: For all $a, b, c \in S$, we have

$$\begin{aligned}(a,b),(b,c) \in Y \;&\Rightarrow\; [(a,b) \in R \wedge (b,a) \in R] \wedge [(b,c) \in R \wedge (c,b) \in R] \\ &\Rightarrow\; [(a,b) \in R \wedge (b,c) \in R] \wedge [(c,b) \in R \wedge (b,a) \in R] \\ &\Rightarrow\; (a,c) \in R \wedge (c,a) \in R \quad \text{because } R \text{ is transitive.} \\ &\Rightarrow\; (a,c) \in Y.\end{aligned}$$

Therefore, Y is an equivalence relations. □

Solution 10:

1. Let $S = \{1, 2, 3\}$, and define R on S as:

   $$R = \{(1,1), (2,2), (1,2), (2,1)\}.$$

   This is an example of a relation that is symmetric and transitive, but not reflexive.

2. If R is reflexive, we require that for every element $a \in A$, (a, a) has to be in R. But, if R is symmetric and transitive, given any a in A, (a, b) may not be in R. Therefore, we can't assure that $(b, a) \in R$, and apply the transitivity to conclude that (a, a) is in R. In the above example, if $a = 3$, we don't have any relation (3,b) in R. Thus, in no way we can apply symmetric and transitive properties of R to conclude that $(3, 3) \in R$.

□

Solution 11: Let $P(x)$ and $Q(x)$ be two predicates such that,

$$\forall x \in S[P(x) \longrightarrow \neg Q(x)], \tag{4.3}$$

and L be an equivalence relation on S. Define the relation R on S as follows:

$$(x,y) \in R \leftrightarrow [((x,y) \in L) \wedge P(x) \wedge Q(y)].$$

1. R is not reflexive, because for all x in S,

$$\begin{aligned} P(x) \longrightarrow \neg Q(x) \ &\Rightarrow \neg P(x) \vee \neg Q(x) \\ &\Rightarrow \neg(P(x) \wedge Q(x)). \end{aligned}$$

That means $(P(x) \wedge Q(x))$ is false, hence, $(x, x) \notin R$.

2. R is not symmetric. Assume $(x, y) \in R$. From the definition of R, we know that

$$((x, y) \in L) \wedge P(x) \wedge Q(y),$$

$P(x)$ is true. From (4.3), $Q(x)$ is false. Thus, $((y, x) \in L) \wedge P(y) \wedge Q(x)$, is false. Therefore, $(y, x) \notin R$.

3. R is transitive. Suppose $(x, y) \in R$ and $(y, z) \in R$. From the definition of R, we know that

$$\begin{aligned} &[(x, y) \in L) \wedge P(x) \wedge Q(y)] \wedge [(y, z) \in L \wedge P(y) \wedge Q(z)] \\ &\quad \Rightarrow \ [(x, y) \in L \wedge (y, z) \in L] \wedge P(x) \wedge Q(z) \\ &\quad \Rightarrow \ (x, z) \in L \wedge P(x) \wedge Q(z) \ \text{ because } L \text{ is transitive.} \\ &\quad \Rightarrow \ (x, z) \in R. \end{aligned}$$

□

Solution 12: Let R be a binary relation on A.

1. The predicate P that defines the isolated points is: For all $a \in A$,

$$P(a) = (a \in A) \ \wedge \ [\forall x \in A((a, x) \notin R \wedge (x, a) \notin R)].$$

a is an isolated point of R if and only if $p(a)$ is true. □

2. We want to prove that if a symmetric and transitive relation without any isolated points, then it is also reflexive.

Given such a relation R on A. For any $a \in A$, because a is not an isolated point, there must exist $b \in A$ such that, $(a, b) \in R$ or $(b, a) \in R$. If $(a, b) \in R$, we know that $(b, a) \in R$ because R is symmetric. Likewise, if $(b, a) \in R$, we know that $(a, b) \in R$. In either case, by the transitivity of R, we have $(a, a) \in R$. Therefore, R is reflexive.

□

Solution 13: Consider the relation matrix of a equivalence relation on a set A with n elements.

	1	2	3	$\cdots$	$\cdots$	n
1	1	·	·	$\cdots$	$\cdots$	·
2	·	1				·
3	·		1			·
$\vdots$	$\vdots$			$\ddots$		$\vdots$
$\vdots$	$\vdots$				$\ddots$	$\vdots$
n	·	·	·	$\cdots$	$\cdots$	1

Because R is symmetric, the number of 1s in the upper right corner must be equal to the number of 1's in the lower left corner. Therefore, the total number of 1's in both corners is an even number. Let it be $2k$.

Because R is reflexive, all entries on the diagonal must be 1, and the total number is n. Thus, the total number of ordered pairs in R is $2k + n$.

Therefore, if n is even, then $2k + n$ is even, and if n is odd, then $2k + n$ is odd. □

Solution 14: Given two binary relations R and S on A.

1. Suppose both R and S are reflexive.

   Given any $a \in A$, we know that

   $$(a, a) \in R \wedge (a, a) \in S \;\Rightarrow\; (a, a) \in (R \cap S).$$

   Therefore, if both R and S are reflexive, so is $R \cap S$.

2. Suppose both R and S are symmetric.
   Assume $(x, y) \in (R \cap S)$.

   $$\begin{aligned}(x, y) \in (R \cap S) &\Rightarrow (x, y) \in R \wedge (x, y) \in S \\ &\Rightarrow (y, x) \in R \wedge (y, x) \in S \\ &\Rightarrow (y, x) \in (R \cap S).\end{aligned}$$

   Therefore, if both R and S are symmetric, so is $R \cap S$.

3. Suppose both R and S are transitive.
   Assume $(x, y) \in (R \cap S)$ and $(y, z) \in (R \cap S)$.

   $$\begin{aligned}&(x, y) \in (R \cap S) \wedge (y, z) \in (R \cap S) \\ &\Rightarrow\quad (x, y) \in R \wedge (x, y) \in S \wedge (y, z) \in R \wedge (y, z) \in S \\ &\Rightarrow\quad (x, z) \in R \wedge (x, z) \in S \\ &\Rightarrow\quad (x, z) \in (R \cap S).\end{aligned}$$

   Therefore, if both R and S are transitive, so is $R \cap S$.

□

Solution 15: Given two binary relations R and S on A.

1. Suppose both R and S are reflexive.

   Given any $a \in A$, we know that

   $$(a, a) \in R \wedge (a, a) \in S \;\Rightarrow\; (a, a) \in (R \cup S).$$

   Therefore, if both R and S are reflexive, so is $R \cup S$.

2. Suppose both R and S are symmetric.
   Assume $(x, y) \in (R \cup S)$.

   $$\begin{aligned}(x, y) \in (R \cup S) &\Rightarrow (x, y) \in R \vee (x, y) \in S \\ &\Rightarrow (y, x) \in R \vee (y, x) \in S \\ &\Rightarrow (y, x) \in (R \cup S).\end{aligned}$$

   Therefore, if both R and S are symmetric, so is $R \cup S$.

3. If both R and S are transitive, $R \cup S$ is not necessary to be a transitive relation. We can see this in the following example. Let $A = \{a, b\}$, and define relations R and S on A as:

   $$R = \{(a, b)\}; \quad S = \{(b, a)\}.$$

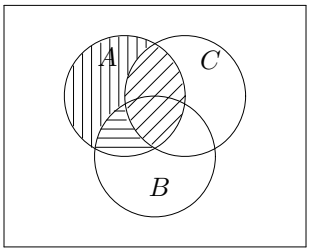
   Thus, we have $R \cup S = \{(a, b), (b, a)\}$, and it is not transitive. Because (a, b), $(b, a) \in R$, but $(a, a) \notin R$.

Note: Make sure you know why R and S are transitive. □

Solution 16: If we want to claim that a collection of sets is a partition of set A, we have to make sure 3 things.

1. None of the sets in the collection is empty.
2. The union of the sets in the collection is equal to A.
3. The sets in the collection are mutually disjointed, i.e., they are disjointed to each other.

For this problem, let's first draw a Venn diagram. It's not the only case, but it will help us to build up the feeling.



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

1. $A-(B\cup C), (A-C)\cap B$, and $A\cap C$ are given to be nonempty. Therefore, we only have to prove that 2. and 3. are satisfied.

2. To prove that $(A - (B \cup C)) \cup ((A - C) \cap B) \cup (A \cap C) = A$:

   Let $a \in (A - (B \cup C)) \cup ((A - C) \cap B) \cup (A \cap C)$. There are 3 cases:

   (a) $a \in (A - (B \cup C))$

   $$\begin{aligned} &\Rightarrow (a \in A) \wedge (a \notin (B \cup C)) \\ &\Rightarrow a \in A. \end{aligned}$$

   (b) $a \in ((A - C) \cap B)$

   $$\begin{aligned} &\Rightarrow (a \in (A - C)) \wedge (a \in B) \\ &\Rightarrow a \in (A - C) \\ &\Rightarrow (a \in A) \wedge (a \notin C) \\ &\Rightarrow a \in A. \end{aligned}$$

   (c) $a \in (A \cap C)$

   $$\begin{aligned} &\Rightarrow (a \in A) \wedge (a \in C) \\ &\Rightarrow a \in A. \end{aligned}$$

   Therefore,

   $$((A - (B \cup C)) \cup ((A - C) \cap B) \cup (A \cap C)) \subseteq A$$

   Let $a \in A$. Consider the following two cases:

   (a) $a \in C$. If so, $a \in (A \cap C)$.

   (b) $a \notin C$. There are two sub-cases:

   i. $a \in B$.

   $$(a \in A) \wedge (a \notin C) \;\Rightarrow\; (a \in (A - C)).$$

   Therefore, $a \in ((A - C) \cap B)$.

ii. $a \notin B$.

$$(a \notin B) \wedge (a \notin C) \;\Rightarrow\; (a \notin (B \cup C)).$$

Therefore, $a \in (A - (B \cup C))$.

From above, and the definition of union, we have

$$a \in ((A - (B \cup C)) \cup ((A - C) \cap B) \cup (A \cap C)).$$

Therefore,

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

That prove 2.

3. To prove that $(A-(B\cup C)), ((A-C)\cap B), (A\cap C)$ are mutually disjointed:

   Be careful, $X \cap Y \cap Z = \emptyset$ does not imply X, Y, Z are mutually disjointed. Therefore, it is not sufficient if we simply prove that

$$(A - (B \cup C)) \cap ((A - C) \cap B) \cap (A \cap C) = \emptyset.$$

   (a) $a \in (A - (B \cup C))$

$$\begin{aligned} &\Rightarrow a \in A \wedge a \notin (B \cup C) \\ &\Rightarrow a \in A \wedge a \notin B \wedge a \notin C \\ &\Rightarrow a \notin ((A - C) \cap B) \wedge a \notin (A \cap C). \end{aligned}$$

   (b) $a \in ((A - C) \cap B)$

$$\begin{aligned} &\Rightarrow a \in (A - C) \wedge a \in B \\ &\Rightarrow a \in A \wedge a \notin C \wedge a \in B \\ &\Rightarrow a \in A \wedge a \in (B \cup C) \wedge a \notin (A \cap C) \\ &\Rightarrow a \notin (A - (B \cup C)) \wedge a \notin (A \cap C). \end{aligned}$$

   (c) $a \in (A \cap C)$

$$\begin{aligned} &\Rightarrow a \in A \wedge a \in C \\ &\Rightarrow a \in A \wedge a \in (B \cup C) \wedge a \notin (A - C) \\ &\Rightarrow a \notin (A - (B \cup C)) \wedge a \notin ((A - C) \cap B). \end{aligned}$$

That proves the claim. □

Solution 17:

Note: Do not be confused by the notation $(a,b)R(c,d)$. $(a,b)R(c,d)$ means $((a,b),(c,d)) \in R$, in another words, (a,b) and (c,d) have R relation. And, another common mistake is to consider (a,b) as an instance of R. (a,b) is only an object in $\mathbf{N} \times \mathbf{N}$, and this object may or may not have R relation to other objects in $\mathbf{N} \times \mathbf{N}$. Therefore, if $(a,b) \in \mathbf{N} \times \mathbf{N}$, the statement $(a,b) \in R$ is nonsense.

Reflexivity: Given any $(a,b) \in \mathbf{N} \times \mathbf{N}$. $((a,b),(a,b)) \in R$ since $ab = ba$. Thus, R is reflexive.

Symmetry: Suppose $((a,b),(c,d)) \in R$,

$$\begin{aligned} &\Rightarrow ad = bc \\ &\Rightarrow cb = da \\ &\Rightarrow ((c,d),(a,b)) \in R. \end{aligned}$$

Therefore, R is symmetric.

Transitivity: Suppose $((a,b),(c,d)) \in R$ and $((c,d),(e,f)) \in R$,

$$\begin{aligned} &\Rightarrow ad = bc \wedge cf = de \\ &\Rightarrow adcf = bcde \\ &\Rightarrow (af)(dc) = (be)(dc) \\ &\Rightarrow af = be \\ &\Rightarrow ((a,b),(e,f)) \in R. \end{aligned}$$

R is transitive.

Therefore, R is an equivalence relation. □

Solution 18:

	reflexive	symmetric	transitive
R_1	√		√
R_2	√	√	
R_3	√		

None of them is an equivalence relation.

R_1: Not symmetric. $(3,4) \in R$ but $(4,3) \notin R$. Note that R_1 is transitive. Think why.

R_2: Not transitive. $(2,1) \in R_2, (1,3) \in R_2$ but $(2,3) \notin R_2$.

R_3: Not symmetric. $(3,4) \in R_3$ but $(4,3) \notin R_3$. R_3 is not transitive either, because $(1,2) \in R_3, (2,3) \in R_3$ but $(1,3) \notin R_3$.

□

Solution 19: The possible partitions of $\{a, b, c\}$:

$$\{\{a, b, c\}\},\ \{\{a\}, \{b, c\}\},\ \{\{a, b\}, \{c\}\},\ \{\{b\}, \{a, c\}\},\ \{\{a\}, \{b\}, \{c\}\}.$$

□

Solution 20: If S is a non-empty set, then $\{S\}$ is a partition of S. If $S = \emptyset$, the partition of S is not $\{\emptyset\}$. The partition of $\emptyset$ is $\emptyset$. □

Solution 21:

1. **Reflexivity:** For $a \in \mathbf{N}$, $\frac{a}{a} = 1 = 2^0$. Therefore, $(a, a) \in R$, and hence R is reflexive.

   Symmetry: Suppose $(a, b) \in R$.

   $$\begin{aligned}(a, b) \in R &\Rightarrow \exists i \in \mathbf{Z}, \frac{a}{b} = 2^i \\ &\Rightarrow \exists i \in \mathbf{Z}, \frac{b}{a} = 2^{-i} \\ &\Rightarrow (b, a) \in R \quad \text{because } -i \in \mathbf{Z}.\end{aligned}$$

   Transitive: Suppose $(a, b), (b, c) \in R$.

   $$\begin{aligned}(a, b) \in R &\Rightarrow \exists i \in \mathbf{Z}, \frac{a}{b} = 2^i \\ (b, c) \in R &\Rightarrow \exists j \in \mathbf{Z}, \frac{b}{c} = 2^i\end{aligned}$$

   $$\frac{a}{c} = \frac{a}{b} \times \frac{b}{c} = 2^{i+j}.$$

   Since $i + j \in \mathbf{Z}$, therefore, $(a, c) \in R$.

   Therefore, R is an equivalence relation.

2. Given any natural number x, there exist $k, i \in \mathbf{N}$ such that, k is not divisible by 2 and $x = k2^i$. For any natural number $y = k2^j$, we have $\frac{x}{y} = 2^{i-j}$, and $i - j$ is an integer. Thus $(x, y) \in R$, namely, x and y are in

the same cell. Therefore, the cells of R are as follows:

$$\{1 \cdot 2^i \mid i = 0, 1, 2, \ldots\},$$
$$\{3 \cdot 2^i \mid i = 0, 1, 2, \ldots\},$$
$$\{5 \cdot 2^i \mid i = 0, 1, 2, \ldots\},$$
$$\{7 \cdot 2^i \mid i = 0, 1, 2, \ldots\},$$
$$\vdots$$

□

Solution 22: By theorem 4.1, each partition determines an equivalence relation on A. Therefore, this problem is exactly same problem 19. We just have to list all possible partitions of A. They are:

$$\{\{1,2,3\}\},\ \{\{1\},\{2,3\}\},\ \{\{1,2\},\{3\}\},\ \{\{2\},\{1,3\}\},\ \{\{1\},\{2\},\{3\}\}.$$

□

Solution 23: Let $S = \{a, b, c\}$, and

$$R_1 = \{(a,a),(b,b),(c,c),(a,b),(b,a)\}$$
$$R_2 = \{(a,a),(b,b),(c,c),(a,c),(c,a)\}.$$

Both R_1 and R_2 are equivalence relations, but $R_1 \cup R_2$ is not. Because, $R_1 \cup R_2$ is not transitive, where $(b,a),(a,c) \in (R_1 \cup R_2)$, but $(b,c) \notin (R_1 \cup R_2)$.

Note: The results in problem 15 do not directly give us the answer to this problem. The two relations given in problem 15 are not equivalence relations.

□

Solution 24: Let R_1 and R_2 be two partial order relation on S. The union $R_1 \cup R_2$ may not be a partial order relation, because the union operation does not preserve antisymmetry and transitivity. Consider the following example. Let $S = \{a, b, c\}$, and

$$R_1 = \{(a,a),(b,b),(c,c),(a,b)\}$$
$$R_2 = \{(a,a),(b,b),(c,c),(b,a),(b,c)\}.$$

Both R_1 and R_2 are partial order relations, but $R_1 \cup R_2$ is not. Because both (a, b) and (b, a) are both in $R_1 \cup R_2$ but $a \neq b$, thus $R_1 \cup R_2$ is not antisymmetric. (a, b) and (b, c) are both in $R_1 \cup R_2$ but $(a, c) \notin R_1 \cup R_2$, thus $R_1 \cup R_2$ is not transitive.

Note: Although we have shown that both antisymmetry and transitivity cannot be preserved by the union operation, but one is enough for us to claim that partial order relations are not closed under union.

□

Solution 25: From the basic theorem for sets in chapter 1, it is easy to see that:

Reflexivity: For all $A \in \mathcal{P}(\mathbf{N})$, $A \subseteq S$.

Antisymmetry: For all $A, B \in \mathcal{P}(\mathbf{N})$, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Transitivity: For all $A, B, C \in \mathcal{P}(\mathbf{N})$, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Therefore, $\subseteq$ is a partial order relation on $\mathcal{P}(\mathbf{N})$. □

Solution 26:

1. P_2 is the only one that is not a partition of S, because, in which $\{7, 4, 3, 8\} \cap \{1, 5, 10, 3\} \neq \emptyset$.
2. P_4 is a refinement of both P_1 and P_3, because itself is a partition of S and every element of P_4 is a subset of one of the elements in P_1 and P_3.

□

Solution 27: The number of refinements of a partition P is the number of the ways to further partition cells in P. The cell $\{1, 2, 3\}$ has 5 ways, $\{4, 5\}$ has 2 ways, and $\{6\}$ has one way. Therefore, the total number of refinements of P is $5 \times 2 \times 1 = 10$. □

Solution 28: Since $\emptyset$ has been removed from Q by definition, we have to prove only that $\bigcup Q = A$ and, for any $p \in Q$ and $q \in Q$, if $p \neq q$, then $p \cap q = \emptyset$.

1. To prove $\bigcup Q = A$, consider

$$\begin{aligned} a \in \bigcup Q &\iff \exists i, j\ [a \in (C_i \cap D_j)] && \text{by the definition of } Q \\ &\iff \exists i, j\ [a \in C_i \text{ and } a \in D_j] && \text{by the definition of } \cap \\ &\iff a \in A \quad \text{since } P_1 \text{ and } P_2 \text{ are two partiontions on } A. \end{aligned}$$

2. To prove, for all $p, q \in Q$, if $p \neq q$ then $p \cap q = \emptyset$, let $p = (C_i \cap D_j)$ and $q = (C_k \cap D_l)$. Suppose $p \neq q$. If so, it must be the case that, $i \neq k$ or $j \neq l$. Since P_1 and P_2 are two partitions, we have if $i \neq k$ then $C_i \cap C_k = \emptyset$; if $j \neq l$ then $D_j \cap D_l = \emptyset$. Thus,

$$\begin{aligned} p \cap q &= (C_i \cap D_j) \cap (C_k \cap D_l) \\ &= (C_i \cap C_k) \cap (D_j \cap D_l) \\ &= (\emptyset \cap (D_j \cap D_l)) \text{ or } ((C_i \cap C_k) \cap \emptyset) \\ &= \emptyset. \end{aligned}$$

From 1. and 2., Q is a partition of A.

Moreover, given any $(C_i \cap D_j) \in Q$, since $(C_i \cap D_j) \subseteq C_i$, it follows that Q is a refinement of P_1. Likewise, $(C_i \cap D_j) \subseteq D_j$, and hence Q is a refinement of P_2. □

Chapter 5

Functions

A new problem ... is like a young rice plant,
which can only thrive and bear fruit when it is carefully
grafted onto an old stem according to
the rules of art of the gardener,
the stem here being the secure treasury of mathematical knowledge.

– David Hilbert

5.1 Definitions, Theorems, and Comments

"Function" is one of the most frequent used terms in mathematics. For example, $f(x) = x^2$, $g(x, y) = x^2 + y^2$, ... are typically functions we have studied since middle school. In general, f and g are the *names* of the functions, which are used to identify the functions. x^2 and $x^2 + y^2$ are the *bodies* of the functions f and g respectively, which show the "meanings" of the functions. x and y are called *arguments*.

In this chapter, we will introduce important formal terminologies and definitions for functions, and study some typical properties of functions.

5.1.1 Definitions

Definition 5.1: Let S and T be two sets. We formally write $f : S \longrightarrow T$ to say that f is a mapping of the elements of the set S to elements of the set T. The set S is known as the *domain* set, and the set T is known as the *codomain* set.

Let $x \in S$. $f(x) = y$ means that if we evaluate the function f at x, the "value" y will be obtained.

Definition 5.2: $f : S \longrightarrow T$ is a function stands for a mapping which takes **each** element of the set S and associates with it **one and only one element** of the set T. For $x \in S$ the value $f(x) \in T$ is also known as the *image* of x.

Comment: Most of the time, "function", "mapping", "correspondence", and "transformation" are different words that carry the same the same concept. We choose to use function in our discussion.

Definition 5.3: Let $f : S \longrightarrow T$ be a function and $x \in S$. If there is an $y \in T$ such that $f(x) = y$, we say that the function, f, is *defined* at x.

Definition 5.4: Let $f : S \longrightarrow T$ be a function. If f is *defined* at every $x \in S$, then such a function is called *total*. If there is an $x \in S$ such that, for every $y \in T$, $f(x) \neq y$, in another words, f is undefined at x, then such a function is called *partial*.

Comment: We only consider total functions in this chapter. Therefore, all "functions" in the following discussion refer to "total functions".

Comment: Function is a special case of relation. It is also possible to define the concept of function in terms of relation. A function f is a relation $f \subset S \times T$ that satisfies a very special property, namely, if $(x, y) \in f$ and $(x, z) \in f$, then $y = z$. This condition says that there is a unique value associated with each argument $x \in S$. One can observe that this condition is equivalent to Definition 2

Definition 5.5: Let $f : S \longrightarrow T$ be a function. As stated earlier, S is known as the *domain* of f, and T is known as the *codomain* of f. The set

$$\{y : \exists x \in S \text{ such that } f(x) = y \text{ and } y \in T\}$$

is known as the *range*.

Definition 5.6: Let $f : S \longrightarrow T$ be a function. If f satisfies the property,

$$\text{whenever } f(x_1) = y \text{ and } f(x_2) = y, \text{ then } x_1 = x_2,$$

then f is known as a *one-to-one* function. In logics,

$$\forall x_1, x_2 \in S\ [(f(x_1) = f(x_2)) \ \Rightarrow\ (x_1 = x_2)].$$

A one-to-one function is also known as an *injection*.

Definition 5.7: Let $f : S \longrightarrow T$ be a function. If the range of $f = T$, then f is known as an *onto* function. In logic,

$$\forall y \in T\ \exists x \in S\ [f(x) = y].$$

An onto function is also known as a *surjection*.

Definition 5.8: If $f : S \longrightarrow T$ is a function that is one-to-one and onto, then the function is also known as a *bijection*.

Definition 5.9: If $f : S \longrightarrow S$ is a bijection and S is finite, then such function f is also known as a *permutation* of S.

Definition 5.10: Consider a function $f : S \longrightarrow S$. (Note that the domain and codomain sets are the same.) The function defined such that $f(x) = x$ for all values of $x \in S$ is known as the *identity function*. It is customary to denote the identity function as i or i_S if we wish to remember the set on which the identity function is defined.

Definition 5.11: Suppose there are two functions $f : S \longrightarrow T$ and $g : T \longrightarrow U$, (Note that the codomain of f and the domain of g are the same.) Then we denote the *composition* of these two functions as $g \circ f : S \longrightarrow U$ and define it as follows:

$$\forall x \in S, (g \circ f)(x) = g(f(x)).$$

Definition 5.12: Suppose $f : S \longrightarrow T$ is a function. The *inverse* function of f is a function $g : T \longrightarrow S$ such that the following two properties are satisfied:

$$f \circ g = i_S \text{ and } g \circ f = i_T.$$

It is customary to denote the inverse function of f by f^{-1}.

Definition 5.13: Suppose that $f : S \longrightarrow T$ is a function. A new function defined using the properties of f is known as an *induced* function (induced by f). We define two such functions below. Let $\mathcal{P}(S)$ and $\mathcal{P}(S)$ denote the power sets of S and T, respectively.

1. The function $\widehat{f} : \mathcal{P}(S) \longrightarrow \mathcal{P}(T)$ is induced by f and is defined as: For all $A \subseteq S$,
$$\widehat{f}(A) = \{y : y = f(x) \text{ for } x \in A\}.$$

2. The function $\widehat{f}^{-1} : \mathcal{P}(T) \longrightarrow \mathcal{P}(S)$ is induced by f and is defined as: For all $B \subseteq T$,
$$\widehat{f}^{-1}(B) = \{x : x \in S \text{ such that } f(x) \in B\}.$$

Definition 5.14: Let S be a set, $A \subseteq S$, and f a function defined as follows:

$$f(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

Then f is known as the *characteristic* function of the set A. Typical notation for a characteristic function is χ_A.

5.1.2 Theorems

Theorem 5.1: The inverse of a function $f : S \longrightarrow T$ exists if and only if f is a bijection.

Theorem 5.2: If $f : S \longrightarrow S$ is a permutation, then $f^{-1} : S \longrightarrow S$ is also a permutation.

Theorem 5.3: If $f : S \longrightarrow S$ and $g : S \longrightarrow S$ are permutations, then $f \circ g$ and $g \circ f$ are both permutations.

Theorem 5.4: Let $f : X \to Y$, $A \subseteq X$ and $B \subseteq Y$. We have the following properties.

1. $\widehat{f}^{-1}(\widehat{f}(A)) \supseteq A$.
2. $\widehat{f}(\widehat{f}^{-1}(B)) \subseteq B$.
3. $\widehat{f}^{-1}(\widehat{f}(A)) = A$, when f is injective.
4. $\widehat{f}(\widehat{f}^{-1}(B)) = B$, when f is surjective.

5.2 The Pigeonhole Principle

The Pigeonhole Principle is an easy yet powerful tool in the study of combinatorial mathematics. For example, many difficult proofs of the theorem in Ramsey Theory are based on the principle. Consider the following intuitively understandable statement:

The Pigeonhole Principle: If we wish to distribute k pigeons to n pigeonholes and $k > n$, then there must exist a pigeonhole with at least two pigeons.

This principle is based on an important observation of the one-to-one functions. "Let S and T be two finite sets and $|S| < |T|$, i.e., the number of elements in S is less than the number in T. Then it is impossible to define a one to one function from s to T."

Theorem 5.5 Let $S = \{1, 2, \ldots, 9\}$. Any six-element-subset of S must have at least two elements with sum equal 10.

Proof: The set $S = \{1, 2, \ldots, 9\}$ can be partitioned into five cells as follows.

$$\{1, 9\},\ \{2, 8\},\ \{3, 7\},\ \{4, 6\},\ \{5\}.$$

By the Pigeonhole Principle, if 6 different numbers are picked from S, then at least one cell must contribute 2 numbers. Clearly, the sum of the two numbers is 10 according to our partition. □

Theorem 5.6 Let $x_0, x_1, x_2, \ldots, x_{n^2}$ be any sequence of n^2+1 distinct numbers. Then, there must exist a subsequence of $n+1$ numbers that is either increasing or decreasing. That is, there exists a sequence $x_{i_0}, x_{i_1}, \ldots, x_{i_n}$ such that, $i_0 < i_1 < \cdots < i_{i_n}$ and either $x_{i_0} < x_{i_1} < \ldots < x_{i_n}$ or $x_{i_0} > x_{i_1} > \ldots > x_{i_n}$.

Proof: For each x_i in the sequence, let (a_i, b_i) be the pair of numbers such that, a_i is the length of the longest increasing subsequence ending at x_i and b_i is the length of the longest decreasing subsequence ending at x_i. We observe that, if $0 \leq i, j \leq n$ and $i \neq j$, then $(a_i, b_i) \neq (a_j, b_j)$. Since we have $n^2 + 1$ numbers in the sequence, it is impossible to associate every number in the sequence a pair of numbers each is less than n. (Note: the number of possible pairs of two numbers from $\{1, 2, \ldots n\}$ is n^2.) Therefore, there must be an x_i that is the end of an increasing or decreasing subsequence of length at least $n + 1$. □

5.3 Asymptotic Notations

This is section, we introduce an important notation in computer science. It is about the set of functions that are considered equivalent in the context of computational complexity analysis.

We use the following conventions throughout this section. We use f, g, or h to denote a total function from $\mathbf{N}$ to $\mathbf{N}$. P and Q are one-place predicates over $\mathbf{N}$. m, n, x, y, and these with subscripts are variables range over $\mathbf{N}$. Let $\mathbf{R}^+$ be the set of all positive real numbers, and a, b, c, range over $\mathbf{R}^+$. In addition to the standard quantifier in predicate logic introduced in Chapter 2, we bring up the following notations for convenience.

Definition 5.15: $\overset{\infty}{\forall}\, xP(x) \quad \triangleq \quad \exists\, n \forall x[x \geq n \rightarrow P(x)].$

Definition 5.16: $\overset{\infty}{\exists}\, xP(x) \quad \triangleq \quad \forall n \exists x[(x \geq n) \wedge P(x)].$

Theorem 5.7

$$\overset{\infty}{\forall}\, x[P(x) \wedge Q(x)] \iff [\overset{\infty}{\forall}\, xP(x) \wedge \overset{\infty}{\forall}\, xQ(x)].$$

Proof: For ($\Rightarrow$) direction:

$$\begin{aligned}
&\overset{\infty}{\forall}\, x[P(x) \wedge Q(x)] \\
&\iff \exists n \forall x \left[(x \geq n) \rightarrow [P(x) \wedge Q(x)]\right] \\
&\iff \exists n \forall x \left[\neg(x \geq n) \vee [P(x) \wedge Q(x)]\right] \\
&\iff \exists n \forall x \left[[\neg(x \geq n) \vee P(x)] \wedge [\neg(x \geq n) \vee Q(x)]\right] \\
&\iff \exists n \left[\forall x[\neg(x \geq n) \vee P(x)] \wedge \forall x[\neg(x \geq n) \vee Q(x)]\right] \\
&\implies \exists n \forall x[\neg(x \geq n) \vee P(x)] \wedge \exists n \forall x[\neg(x \geq n) \vee Q(x)] \\
&\iff \exists n \forall x[(x \geq n) \rightarrow P(x)] \wedge \exists n \forall x[(x \geq n) \rightarrow Q(x)] \\
&\iff \overset{\infty}{\forall}\, xP(x) \wedge \overset{\infty}{\forall}\, xQ(x).
\end{aligned}$$

For ($\Leftarrow$) direction: We will use the following implication:

$$[(A \rightarrow C) \wedge (A \rightarrow B) \wedge (C \rightarrow D)] \Longrightarrow [A \rightarrow (B \wedge D)].$$

$$\begin{aligned}
&\overset{\infty}{\forall}\, xP(x) \wedge \overset{\infty}{\forall}\, xQ(x) \\
&\iff \exists n \forall x[(x \geq n) \rightarrow P(x)] \wedge \exists n \forall x[(x \geq n) \rightarrow Q(x)] \\
&\iff \forall x[(x \geq n_0) \rightarrow P(x)] \wedge \forall x[(x \geq n_1) \rightarrow Q(x)], \text{ where } n_0, n_1 \in \mathbf{N} \\
&\iff \forall x \left[[(x \geq n_0) \rightarrow P(x)] \wedge [(x \geq n_1) \rightarrow Q(x)]\right].
\end{aligned}$$

We have two cases: $n_0 \geq n_1$ and $n_0 < n_1$. We now consider the first case.

Suppose $n_0 \geq n_1$. In this case, we have $(x > n_0) \rightarrow (x > n_1)$. Thus,

$$\begin{aligned}
&\forall x \left[[(x \geq n_0) \rightarrow P(x)] \wedge [(x \geq n_1) \rightarrow Q(x)]\right] \\
&\quad \Longleftrightarrow \quad \forall x \left[[(x > n_0) \rightarrow (x > n_1)] \wedge [(x \geq n_0) \rightarrow P(x)] \wedge [(x \geq n_1) \rightarrow Q(x)]\right] \\
&\quad \Longrightarrow \quad \forall x[(x > n_0) \rightarrow (P(x) \wedge Q(x))] \\
&\quad \Longleftrightarrow \quad \exists n \forall x[(x > n) \rightarrow (P(x) \wedge Q(x))] \\
&\quad \Longleftrightarrow \quad \overset{\infty}{\forall}\, x[P(x) \wedge Q(x)].
\end{aligned}$$

For the other case, $n_0 < n_1$, the proof is similar. □

However, the distributive law of $\overset{\infty}{\forall}$ over $\vee$ does not hold. Consider the following properties. We leave the proofs to the reader as exercises.

Exercise:

1. Prove that $\neg \overset{\infty}{\forall}\, xP(x) \iff \overset{\infty}{\exists}\, x\neg P(x)$.
2. Prove that $\overset{\infty}{\forall}\, x[P(x) \vee Q(x)] \Longleftarrow [\overset{\infty}{\forall}\, xP(x) \vee \overset{\infty}{\forall}\, xQ(x)]$.
3. Disprove that $\overset{\infty}{\forall}\, x[P(x) \vee Q(x)] \Longrightarrow [\overset{\infty}{\forall}\, xP(x) \vee \overset{\infty}{\forall}\, xQ(x)]$.
4. Prove that $\overset{\infty}{\exists}\, x[P(x) \vee Q(x)] \iff [\overset{\infty}{\exists}\, xP(x) \vee \overset{\infty}{\exists}\, xQ(x)]$.
5. Prove that $\overset{\infty}{\exists}\, x[P(x) \wedge Q(x)] \Longrightarrow [\overset{\infty}{\exists}\, xP(x) \wedge \overset{\infty}{\exists}\, xQ(x)]$.
6. Disprove that $\overset{\infty}{\exists}\, x[P(x) \wedge Q(x)] \Longleftarrow [\overset{\infty}{\exists}\, xP(x) \wedge \overset{\infty}{\exists}\, xQ(x)]$.

Theoretically, we can modify a function at finitely many places in an efficient way. This viewpoint leads to the use of asymptotic notations where we neglect finitely many points at which the functions may violate some nice properties concerned. $O(g)$, $\Omega(g)$, and $\Theta(g)$ are sets of functions from $\mathbf{N}$ to $\mathbf{N}$ defined in the following.

Definition 5.17: $f \in O(g) \iff \exists\, c\, \overset{\infty}{\forall}\, n[f(n) \leq cg(n)]$.

Definition 5.18: $f \in \Omega(g) \iff \exists\, c\, \overset{\infty}{\forall}\, n[cg(n) \leq f(n)]$.

Definition 5.19: $f \in \Theta(g) \iff \exists\, c_1 \exists\, c_2\, \overset{\infty}{\forall}\, n[c_1 g(n) \leq f(n) \leq c_2 g(n)]$.

Theorem 5.8

$$f \in \Theta(g) \iff [f \in O(g) \wedge f \in \Omega(g)].$$

Proof:

$$\begin{aligned}
f \in \Theta(g) &\iff \exists c_1 \exists c_2 \overset{\infty}{\forall} x[c_1 g(x) \leq f(x) \leq c_2 g(x)] \\
&\iff \exists c_1 \exists c_2 \overset{\infty}{\forall} x \left[[c_1 g(x) \leq f(x)] \wedge [f(x) \leq c_2 g(x)]\right] \\
&\iff \exists c_1 \exists c_2 \left[\overset{\infty}{\forall} x[c_1 g(x) \leq f(x)] \wedge \overset{\infty}{\forall} x[f(x) \leq c_2 g(x)]\right] \\
&\iff \exists c_1 \exists c_2 \overset{\infty}{\forall} x[c_1 g(x) \leq f(x)] \wedge \exists c_1 \exists c_2 \overset{\infty}{\forall} x[f(x) \leq c_2 g(x)] \\
&\iff \exists c \overset{\infty}{\forall} x[cg(x) \leq f(x)] \wedge \exists c \overset{\infty}{\forall} x[f(x) \leq cg(x)] \\
&\iff f \in \Omega(g) \wedge f \in O(g).
\end{aligned}$$

□

Theorem 5.9

$$[f_1 \in O(g) \wedge f_2 \in O(g)] \iff (f_1 + f_2) \in O(g).$$

Proof: For ($\Rightarrow$) direction:

$$\begin{aligned}
& f_1 \in O(g) \wedge f_2 \in O(g) \\
\iff & \exists c \overset{\infty}{\forall} x[f_1(x) \leq cg(x)] \wedge \exists c \overset{\infty}{\forall} x[f_2(x) \leq cg(x)] \\
\iff & \overset{\infty}{\forall} x[f_1(x) \leq c_1 g(x)] \wedge \overset{\infty}{\forall} x[f_2(x) \leq c_2 g(x)] \\
\iff & \overset{\infty}{\forall} x[f_1(x) \leq c_1 g(x) \wedge f_2(x) \leq c_2 g(x)] \\
\Longrightarrow & \overset{\infty}{\forall} x[(f_1(x) + f_2(x) \leq (c_1 + c_2) g(x)] \\
\iff & \exists c \overset{\infty}{\forall} x[(f_1(x) + f_2(x) \leq cg(x)] \\
\iff & (f_1 + f_2) \in O(g).
\end{aligned}$$

For ($\Leftarrow$) direction:

$$\begin{aligned}
& (f_1 + f_2) \in O(g) \\
\iff & \exists c \overset{\infty}{\forall} x[(f_1(x) + f_2(x) \leq cg(x)] \\
\iff & \exists c \overset{\infty}{\forall} x[f_1(x) \leq cg(x) \wedge f_2(x) \leq cg(x)] \\
\iff & \exists c \left[\overset{\infty}{\forall} x[f_1(x) \leq cg(x)] \wedge \overset{\infty}{\forall} x[f_2(x) \leq cg(x)]\right] \\
\Longrightarrow & \exists c \overset{\infty}{\forall} x[f_1(x) \leq cg(x)] \wedge \exists c \overset{\infty}{\forall} x[f_2(x) \leq cg(x)] \\
\iff & f_1 \in O(g) \wedge f_2 \in O(g).
\end{aligned}$$

□

Theorem 5.10

$$[f_1 \in \Theta(g) \wedge f_2 \in \Theta(g)] \Longrightarrow (f_1 + f_2) \in \Theta(g).$$

Proof:

$$
\begin{aligned}
& f_1 \in \Theta(g) \wedge f_2 \in \Theta(g) \\
\iff\ & \exists c_1 \exists c_2 \overset{\infty}{\forall} x[c_1 g(x) \leq f_1(x) \leq c_2 g(x)] \wedge \exists c_1 \exists c_2 \overset{\infty}{\forall} x[c_1 g(x) \leq f_2(x) \leq c_2 g(x)] \\
\iff\ & \overset{\infty}{\forall} x[a_1 g(x) \leq f_1(x) \leq b_1 g(x)] \wedge \overset{\infty}{\forall} x[a_2 g(x) \leq f_2(x) \leq b_2 g(x)] \\
\iff\ & \overset{\infty}{\forall} x[a_1 g(x) \leq f_1(x) \leq b_1 g(x) \wedge a_2 g(x) \leq f_2(x) \leq b_2 g(x)] \\
\iff\ & \overset{\infty}{\forall} x[(a_1 + a_2) g(x) \leq (f_1(x) + f_2(x)) \leq (b_1 + b_2) g(x)] \\
\iff\ & \exists c_1 \exists c_2 \overset{\infty}{\forall} x[c_1 g(x) \leq (f_1(x) + f_2(x)) \leq c_2 g(x)] \\
\iff\ & (f_1 + f_2) \in \Theta(g).
\end{aligned}
$$

□

Theorem 5.11

$$f \in \Theta(g) \iff g \in \Theta(f).$$

$$
\begin{aligned}
f \in \Theta(g) \iff & \overset{\infty}{\forall} x \left[c_1 g(x) \leq f(x) \leq c_2 g(x)\right] \\
\iff & \overset{\infty}{\forall} x \left[[c_1 g(x) \leq f(x)] \wedge [f(x) \leq c_2 g(x)]\right] \\
\iff & \overset{\infty}{\forall} x \left[[g(x) \leq \frac{1}{c_1} f(x)] \wedge [\frac{1}{c_2} f(x) \leq g(x)]\right] \\
\iff & \overset{\infty}{\forall} x \left[\frac{1}{c_2} f(x) \leq g(x) \leq \frac{1}{c_1} f(x)\right] \\
\iff & g \in \Theta(f).
\end{aligned}
$$

□

Exercise 1 *Prove:*

$$[f \in \Theta(g) \wedge g \in \Theta(h)] \implies f \in \Theta(h). \tag{5.1}$$

Theorem 5.12

$$f \in \Theta(g) \iff \Theta(f) = \Theta(g).$$

Proof: The proof of ($\Rightarrow$) direction is trivial.

For ($\Rightarrow$) direction, suppose $f \in \Theta(g)$. We shall prove $\Theta(f) \subseteq \Theta(g)$ and $\Theta(f) \supseteq \Theta(g)$.

1. Let $h \in \Theta(f)$. Since $h \in \Theta(f)$ and $f \in \Theta(g)$, by (5.1), we have $h \in \Theta(g)$. Thus, $\Theta(f) \subseteq \Theta(g)$.
2. Let $h \in \Theta(g)$. Since $f \in \Theta(g)$, by Theorem 11, we have $g \in \Theta(f)$. Then, by (5.1), $h \in \Theta(g)$ and $g \in \Theta(f)$ imply $h \in \Theta(f)$. Thus, $\Theta(g) \subseteq \Theta(f)$.

Therefore, $\Theta(g) = \Theta(f)$. □

Theorem 5.13 Let $a, b \in \mathbf{R}^+$. Then, $a^n \in \Theta(b^n) \iff a = b$.

Proof: The proof of ($\Rightarrow$) direction is trivial.

For ($\Rightarrow$) direction, suppose $a^n \in \Theta(b^n)$.

$$\begin{aligned}
a^n \in \Theta(b^n) &\implies \overset{\infty}{\forall}\, x\, [c_1 b^n \le a^n \le c_2 b^n] \\
&\implies \overset{\infty}{\forall}\, x\, [\log(c_1 b^n) \le \log a^n \le \log(c_2 b^n)] \\
&\implies \overset{\infty}{\forall}\, x\, [(\log c_1 + n \log b) \le n \log a \le (\log c_2 + n \log b)] \\
&\implies \overset{\infty}{\forall}\, x\, \left[\left(\frac{\log c_1}{n} + \log b\right) \le \log a \le \left(\frac{\log c_2}{n} + \log b\right)\right].
\end{aligned}$$

If $x \approx \infty$, then $\frac{\log c_1}{n} \approx 0$ and $\frac{\log c_2}{n} \approx 0$. Thus, when $x \approx \infty$, we have

$$\log b \le \log a \le \log b.$$

Therefore, $a = b$. □

5.4 Problems

Problem 1: List all total and partial functions with domain $\{1, 2\}$ and codomain $\{a, b\}$.

Problem 2: Which of the following functions are: injective, surjective?

1. $g:\ \mathbf{R} \to \mathbf{R}.\ g(x) := 2x + 1.$
2. $h:\ \mathbf{N} \to \mathbf{N}.\ h(x) := x^2 + 2.$

Problem 3: Let $D = \{1, 2, 3, 4\}$ be the domain and $\mathbf{N}$ be the codomain of the functions f_1 and f_2 defined as follows:

1. For all b in $D,\ f_1(b) := b^2$.
2. For all b in $D,\ f_2(b) :=$ the smallest prime that divides $3b + 1$.

Express f_1 and f_2 in two relations.

Problem 4: Let A be any set. Consider relations on A and functions from A to A as sets of ordered pairs. Find all equivalence relations on A which are also functions from A to A. Explain.

Problem 5: Let f and g be injective functions, $f : X \longrightarrow Y$ and $g : W \longrightarrow X$, for sets W, X, Y. Prove that the composition $f \circ g$ is injective.

Problem 6: Give an example of two functions $f : D \longrightarrow Y$ and $g : Y \longrightarrow W$ such that $D,\ Y$, and W are finite sets and $g \circ f$ is bijective, but neither f nor g is bijective.

Problem 7: Let f be a function $f : X \to Y$, and $A \subseteq X$, $B \subseteq X$. Prove that

$$\hat{f}(A \cap B) \ \subseteq\ \hat{f}(A) \cap \hat{f}(B).$$

Is the reverse inclusion true?

Problem 8: Let A and B be subsets of X such that $A \subseteq B$. Prove that $\hat{f}(A) \subseteq \hat{f}(B)$.

Problem 9: Let $B \subseteq Y$ and $A = \hat{f}^{-1}(B)$. Prove that

$$\hat{f}(A) \subseteq B$$

and that in some cases equality does not hold.

Problem 10: Let f be a function and let A be a subset of the domain of f. Assume that $\hat{f}^{-1}(\hat{f}(A)) \subseteq A$. Prove that $A = \hat{f}^{-1}(\hat{f}(A))$.

Problem 11: Let $f : X \to Y$ be a function.

1. Prove that if f is injective and $A \subseteq X$, then $\hat{f}^{-1}(\hat{f}(A)) = A$. Explain where you use the injectivity.

2. Prove that if f is surjective and $B \subseteq Y$, then $\hat{f}(\hat{f}^{-1}(B)) = B$. Explain where you use the surjectivity.

Problem 12: Let the function composition $\underbrace{f \circ f \overset{i}{\circ} \cdots f}$ be denoted as f^i. If $i = 0$, then f^i is the identity function. Let f be a permutation of a finite set X. For each $a \in X$ define $S(a) := \{f^i(a); i = 0, 1, 2, \ldots\}$. Define the relation R on X by the rule: for all $a, b \in X$, aRb iff $b \in S(a)$. Prove that R is an equivalence relation on X.

Problem 13: Suppose there are n people lined up in some order. Show that you can achieve any other ordering of them by successively having some two adjacent people trade places.

Problem 14: Prove that in a group of 700 people, there must be 2 people who have the same first and last initials.

Problem 15: Prove that at any party there must be two people who have shaken hands with the same number of others present.

5.5 Solutions

Solution 1:

$$\begin{array}{ll} f_0 = \emptyset, & f_5 = \{(1,a),(2,b)\} \\ f_1 = \{(1,a)\} & f_6 = \{(1,b),(2,a)\} \\ f_2 = \{(1,b)\} & f_7 = \{(1,a),(2,a)\} \\ f_3 = \{(2,a)\} & f_8 = \{(1,b),(2,b)\} \\ f_4 = \{(2,b)\} & \end{array}$$

Note that f_0, f_1, f_2, f_3, and f_4 are partial functions, and f_5, f_6, f_7 and f_8 are total functions. Don't forget that $\emptyset$ is a partial function. □

Solution 2:

1. $g: \mathbf{R} \to \mathbf{R}$. $\forall x \in \mathbf{R}, g(x) := 2x + 1$.

   (a) g is injective. Because, for all $x_1, x_2 \in \mathbf{R}$,

   $$\begin{aligned} x_1 \neq x_2 &\Rightarrow 2x_1 + 1 \neq 2x_2 + 2 \\ &\Rightarrow g(x_1) \neq g(x_2). \end{aligned}$$

   (b) g is surjective. Because, for all $y \in \mathbf{R}$,

   $$\begin{aligned} &\Rightarrow \exists x \in \mathbf{R}, x = (y-1)/2, \\ &\Rightarrow \exists x \in \mathbf{R}, f(x) = y. \end{aligned}$$

2. $h: \mathbf{N} \to \mathbf{N}$. $\forall x \in \mathbf{N}, h(x) := x^2 + 2$.

   (a) h is injective. Because, for all $x_1, x_2 \geq 0$,

   $$\begin{aligned} x_1 \neq x_2 &\Rightarrow x_1^2 + 2 \neq x_2^2 + 2 \\ &\Rightarrow h(x_1) \neq h(x_2). \end{aligned}$$

   and, $x_1, x_2 \in \mathbf{N} \Rightarrow x_1, x_2 \geq 0$.

   (b) h is not surjective. Because, given any $y \in \mathbf{N}$, we cannot always find $x \in \mathbf{N}$ such that, $f(x) = y$. For example, if $y = 1$, there is no $x \in \mathbf{N}$ such that $f(x) = x^2 + 2 = 1$.

□

Solution 3:

1. $f_1 = \{(1,1),(2,4),(3,9),(4,16)\}$.

b	1	2	3	4
b^2	1	4	9	16

2. $f_2 = \{(1,2),(2,7),(3,2),(4,13)\}$.

b	1	2	3	4
$3b+1$	4	7	10	13
f_2	2	7	2	13

Note: For many applications in computer science and mathematics, by convention, we consider 2 as the smallest prime number. But, if you examine the definition of prime numbers: p is a prime number iff p is a positive integer and p is divisible by 1 and p only, you may consider 1 as the smallest prime number. Then,

$$f_2 = \{(1,1),(2,1),(3,1),(4,1)\}.$$

□

Solution 4: Let A be any set $\{a,b,c,\ldots\}$. The only equivalence relation R on A which is also a function from A to A is,

$$\{(a,a),(b,b),(c,c),\ldots\}.$$

Why? The restriction of a relation being a function is that the relation has to be single valued, i.e., if (x,y) and (x,z) in the relation, then $y=z$. And, since R is an equivalence relation, we know that for each element $a \in A$, $(a,a) \in R$. Therefore, $(a,x) \notin R$ unless $a = x$. □

Solution 5: Let f and g be injective functions, $f : X \to Y$ and $g : W \to X$, for sets W, X, Y. We first prove that $f \circ g : W \to Y$ is well defined. The only thing we have to do is to prove that $f \circ g$ as a relation on $W \times Y$ is single valued.

Given $w_1, w_2 \in W$. If $w_1 = w_2$ and $g(w_1), g(w_2)$ are defined, then

$$g(w_1) = g(w_2),$$

because g is a well defined function. And, if $g(w_1) = g(w_2)$ and $f(g(w_1))$, $f(g(w_2))$ are defined, then

$$f(g(w_1)) = f(g(w_2)),$$

because f is a well defined function. Therefore, if $w_1 = w_2$ and $f \circ g(w_1)$, $f \circ g(w_2)$ are defined, then

$$f \circ g(w_1) = f \circ g(w_2).$$

That means $f \circ g$ is a well defined function from W to Y.

To prove that $f \circ g$ is injective, let $x, y \in W$, and suppose that $x \neq y$ and $f \circ g(x), f \circ g(y)$ are defined.

$$\begin{array}{ll} x \neq y \Rightarrow g(x) \neq g(y) & g \text{ is injective} \\ \Rightarrow f(g(x)) \neq f(g(y)) & f \text{ is injective.} \end{array}$$

Therefore, $f \circ g$ is injective. □

Solution 6: Let $D = \{1, 2\}, Y = \{a, b, c\}, W = \{\alpha, \beta\}$. Define

$$f : D \longrightarrow Y \quad \text{as} \quad \begin{array}{c|c|c} x & 1 & 2 \\ \hline f(x) & a & b \end{array}$$

$$g : Y \longrightarrow W \quad \text{as} \quad \begin{array}{c|c|c|c} x & a & b & c \\ \hline g(x) & \alpha & \beta & \beta \end{array}$$

Wh have

$$g \circ f : D \longrightarrow W \quad \text{as} \quad \begin{array}{c|c|c} x & 1 & 2 \\ \hline (g \circ f)(x) & \alpha & \beta \end{array}$$

f is not surjective, and g is not injective, but $g \circ f$ is bijective. □

Solution 7: Let $f : X \to Y$, and $A \subseteq X, B \subseteq X$.

$$\begin{array}{rl} y \in f(A \cap B) \Rightarrow & \exists x \in (A \cap B), f(x) = y \\ \Rightarrow & \exists x, x \in A, x \in B, f(x) = y \\ \Rightarrow & \exists x \in A, f(x) = y \text{ and } \exists x \in B, f(x) = y \\ \Rightarrow & y \in f(A) \text{ and } y \in f(B) \\ \Rightarrow & y \in (f(A) \cup f(B)) \end{array}$$

Therefore,

$$f(A \cap B) \ \subseteq \ f(A) \cap f(B).$$

However, the the reverse inclusion is not true. Here is a counter example.

Define $f : \mathbf{Z} \to \mathbf{Z}$, $f(x) = x^2$. Let, $A = \{-2\}, B = \{2\}$. We have

$$f(A) = \{4\}, \ f(B) = \{4\}, \ f(A) \cap f(B) = \{4\}, \ f(A \cap B) = \emptyset.$$

Therefore, in general, $f(A \cap B) \not\supseteq f(A) \cap f(B)$ □

Solution 8: Let $y \in \hat{f}(A)$.

$$\begin{array}{rcll} y \in \hat{f}(A) & \Rightarrow & \exists x \in A, f(x) = y & \\ & \Rightarrow & \exists x \in B, f(x) = y & \text{because } A \subseteq B \\ & \Rightarrow & y \in \hat{f}(B). & \end{array}$$

Therefore, $\hat{f}(A) \subseteq \hat{f}(B)$. □

Solution 9: The only thing having to do with this problem is the definitions of the sets $\hat{f}(A)$ and $\hat{f}^{-1}(B)$. We carefully write down the definitions as follows.

Let $f : X \to Y$, $A \subseteq X$ and $B \subseteq Y$.

$$\hat{f}(A) := \{b \mid \exists a \in A, f(a) = b\}. \tag{5.2}$$

$$\hat{f}^{-1}(B) := \{a \mid a \in X, f(a) \in B\}. \tag{5.3}$$

Given $A = \hat{f}^{-1}(B)$. To prove that $\hat{f}(A) \subseteq B$, let $b \in \hat{f}(A)$.

$$b \in \hat{f}(A) \;\Rightarrow\; \exists a \in A, f(a) = b. \quad \text{by def. (5.2)}$$

Fix this a. Because $A = \hat{f}^{-1}(B)$, we know that $a \in \hat{f}^{-1}(B)$. From the definition in (5.3),

$$a \in \hat{f}^{-1}(B) \;\Rightarrow\; f(a) \in B.$$

Therefore, $b \in B$.

If f is not surjective, then $\hat{f}(A) \supseteq B$ is not necessary to be true. For example, define

$$f : \{0, 1\} \to \{0, 1\},$$

$$\begin{aligned} f(0) &= 0, \\ f(1) &= 0. \end{aligned}$$

Let $B = \{0, 1\}, A = \hat{f}^{-1}(B)$. We have

$$\begin{aligned} A &= \{0, 1\}, \\ \hat{f}(A) &= \{0\}. \end{aligned}$$

Therefore, $B \not\subseteq \hat{f}(A)$. □

Solution 10: Let $f : X \to Y$, $A \subseteq X$. We first prove that

$$A \subseteq \hat{f}^{-1}(\hat{f}(A)). \tag{5.4}$$

$$\begin{aligned} a \in A &\Rightarrow f(a) \in \hat{f}(A) \\ &\Rightarrow a \in \hat{f}^{-1}(\hat{f}(A)) \qquad \text{by def. (5.3).} \end{aligned}$$

Therefore, $A \subseteq \hat{f}^{-1}(\hat{f}(A))$.

If $\hat{f}^{-1}(\hat{f}(A)) \subseteq A$ is given, then, with the fact (5.4) we just proved, we can conclude that $A = \hat{f}^{-1}(\hat{f}(A))$. □

Solution 11: Let $f : X \to Y$.

1. With the fact (5.4) that we have proven in the previous problem, this problem is in fact asking to prove that if f is injective, and A is any subset of X, then
$$\hat{f}^{-1}(\hat{f}(A)) \subseteq A.$$
Suppose f is injective.
$$\begin{aligned} a \in \hat{f}^{-1}(\hat{f}(A)) &\Rightarrow f(a) \in \hat{f}(A) \\ &\Rightarrow \exists x' \in A, f(a) = f(x') \\ &\Rightarrow x' \in A, a = x' \qquad f \text{ is injective} \\ &\Rightarrow a \in A. \end{aligned}$$
Therefore, $\hat{f}^{-1}(\hat{f}(A)) \subseteq A$, plus (5.4), gives
$$\hat{f}^{-1}(\hat{f}(A)) = A.$$

2. Let's first prove a result similar to (5.4).
$$\hat{f}(\hat{f}^{-1}(B)) \subseteq B. \tag{5.5}$$
$$\begin{aligned} b \in \hat{f}(\hat{f}^{-1}(B)) &\Rightarrow \exists a \in \hat{f}^{-1}(B), f(a) = b \\ &\Rightarrow \exists a \in X, f(a) \in B, f(a) = b \\ &\Rightarrow b \in B. \end{aligned}$$
That proves (5.5). Now, suppose f is surjective.
$$b \in B \;\Rightarrow\; \exists a \in X, f(a) = b.$$

Because f is surjective, given any b in the codomain, we are able to find such a in the domain and $f(a) = b$. Fix this a. From the definition in (5.2), we know that

$$\begin{aligned} a \in \hat{f}^{-1}(B) \wedge f(a) = b \quad &\Rightarrow\ f(a) \in \hat{f}(\hat{f}^{-1}(B)) \wedge f(a) = b \\ &\Rightarrow\ b \in \hat{f}(\hat{f}^{-1}(B)). \end{aligned}$$

Therefore, $B \subseteq \hat{f}(\hat{f}^{-1}(B))$, plus (5.5) and f is surjective, gives

$$\hat{f}(\hat{f}^{-1}(B)) = B.$$

□

Solution 12:

Reflexivity: By the definition, $f^0 = i_X$. Thus, for all $a \in X$.

$$a = f^0(a),\ a \in S(a).$$

Therefore, $(a, a) \in R$.

Symmetry: Given any $a, b \in X$, and $(a, b) \in R$, i.e., exists $i \geq 0, b = f^i(a)$. Consider the following sequence,

$$f^0(a), f^1(a), \ldots, f^i(a), \ldots, f^j(a), \ldots, f^{j+k}(a), \ldots,$$

where $f^0(a) = a$ and $f^i(a) = b$. Because f is a permutation on X, we are able to find j, k such that

$$i \leq j, 0 \leq k, f^j(a) = f^{j+k}(a) = c,$$

where $c \in X$.[1] Now, we want to prove that a is in the cycle

$$f^j(a), f^{j+1}(a), \ldots, f^{j+k}(a).$$

For any two sequences, let

$$a_0, a_1, \ldots, a_n \ \equiv\ b_0, b_1, \ldots, b_n \text{ iff } a_0 = b_0, a_1 = b_1, \ldots, \text{ and } a_n = b_n.$$

By way of contradiction, suppose that

$$a \notin \{f^j(a), f^{j+1}(a), \ldots, f^{j+k}(a)\}.$$

There are two cases:

[1] In fact, $i = j$ and $b = c$, but suppose we don't know this fact.

Case 1: $j \leq k$. Because f is injective, $f(a) = f(b)$ implies $a = b$. By the assumption that $f^j(a) = f^{j+k}(a) = c$, we have

$$\begin{aligned} f^j(a) = f^{j+k}(a) &\Rightarrow f(f^{j-1}(a)) = f(f^{k+j-1}(a)) \\ &\Rightarrow f^{j-1}(a) = f^{k+j-1}(a) \\ &\Rightarrow f^{j-2}(a) = f^{k+j-2}(a) \\ &\vdots \\ &\Rightarrow f^1(a) = f^{k+1}(a) \\ &\Rightarrow f^0(a) = f^k(a). \end{aligned}$$

Therefore, $f^k(a) = f^0(a) = a$, and

$$f^0(a), f^1(a), \ldots, f^j(a) \equiv f^k(a), f^{k+1}(a), \ldots f^{j+k}(a).$$

From the assumption in this case that $j \leq k \leq j + k$, we know

$$a \in \{f^j(a), f^{j+1}(a), \ldots, f^{j+k}(a)\}.$$

That leads a contradiction.

Case 2: $k < j$. With the same reason that f is injective, we can have the following deduction,

$$\begin{aligned} f^j(a) = f^{j+k}(a) = c &\Rightarrow f^{j-1}(a) = f^{j+k-1}(a) \\ &\Rightarrow f^{j-2}(a) = f^{j+k-2}(a) \\ &\vdots \\ &\Rightarrow f^{j-k}(a) = f^j(a). \end{aligned}$$

Therefore, we have

$$f^{j-k}(a), f^{j-k+1}(a), \ldots, f^j(a) \equiv f^j(a), f^{j+1}(a), \ldots f^{j+k}(a),$$

where $f^{j-k} = f^j(a) = c$ and $0 < j - k$. From the assumption,

$$\begin{aligned} & a \notin \{f^j(a), f^{j+1}(a), \ldots f^{j+k}(a)\} \\ \Rightarrow\ & a \notin \{f^{j-k}(a), f^{j-k+1}(a), \ldots, f^j(a)\}. \end{aligned}$$

Now, if $j - k$ is still greater than k, we repeat the above arguments, until, after n times, we have

$$\begin{aligned} f^{j-nk}(a), f^{j-nk+1}(a), \ldots, f^{j-nk+k}(a) \equiv \\ f^{j-nk+k}(a), f^{j-nk+1}(a), \ldots f^{j-nk+2k}(a), \end{aligned}$$

where $j - nk \leq k$. We also know that

$$\begin{aligned} & f^{j-nk}(a), f^{j-nk+1}(a), \ldots, f^{j-nk+k}(a) \\ \equiv \;& f^{j-nk+k}(a), f^{j-nk+k+1}(a), \ldots f^{j-nk+2k}(a) \\ \equiv \;& \cdots \\ \equiv \;& \cdots \\ \equiv \;& f^{j}(a), f^{j+1}(a), \ldots f^{j+k}(a), \end{aligned}$$

and,

$$a \notin \{f^{j-nk}(a), f^{j-nk+1}(a), \ldots, f^{j-nk+k}(a)\}.$$

Then, we use the similar argument in case 1. We will have

$$f^0(a), f^1(a), \ldots, f^{j-nk}(a) \;\equiv\; f^k(a), f^{k+1}(a), \ldots f^{j-nk+k}(a).$$

$$\begin{aligned} a \in \{f^{j-nk}(a), f^{j-nk+1}(a), \ldots, f^{j-nk+k}(a)\} \\ \Rightarrow\; a \in \{f^{j}(a), f^{j+1}(a), \ldots f^{j+k}(a)\}. \end{aligned}$$

That leads a contradiction.

In both cases, the assumption will lead a contradiction. Therefore, we can conclude that

$$a \in \{f^j(a), \ldots, f^{j+k}(a)\}. \tag{5.6}$$

Let $a = f^l(a)$, where $i \leq j \leq l \leq j + k$ and

$$a = f^l(a) = f^{l-i}(f^i(a)) = f^{l-i}(b).$$

Since $l - i \geq 0$, thus $a \in S(b)$, and $(b, a) \in R$. Therefore, R is symmetric.

Transitivity: For all $a, b, c \in X$,

$$\begin{aligned} (a,b),(b,c) \in R \;&\Rightarrow\; b \in S(a) \text{ and } c \in S(b) \\ &\Rightarrow\; \exists i, j \geq 0,\; b = f^i(a) \text{ and } c = f^j(b) \\ &\Rightarrow\; c = f^j(f^i(a)) \\ &\Rightarrow\; c = f^{i+j}(a) \\ &\Rightarrow\; (a,c) \in R. \end{aligned}$$

R is transitive.

Therefore, R is an equivalence relations. □

Solution 13: If we do some experiment, we will find that it is not so difficult to see that we are able to reorder a line of people by successively switching two adjacent people. The problem is, how to prove it formally. It is indeed what we try to learn in this class. As to conclude the homework solutions for this class, let me prove it by mathematical induction on the number of people lined up.

At first, let's define a class of functions as the following. For any x, y,

$$f_{x,y}(a) = \begin{cases} y & \text{if } a = x, \\ x & \text{if } a = y, \\ a & \text{otherwise.} \end{cases} \tag{5.7}$$

Apparently, if we restrict the domain X to a finite one that includes x and y, then $f_{x,y}$ is a permutation on X, which only exchanges x and y. Therefore, if we can prove that any order can be achieved from any other order by using the functions in this class, then we would have proved this problem.

Inductive Basis: $n = 2$. It is clear that $f_{1,2}$ can do the job.

[The Basis Holds.]

Inductive Hypothesis: If there are n people lined up, then any order of the line can be achieved from any other order by using the functions in the class defined in (5.7).

Inductive Step: Suppose there are $n + 1$ people lined up in the following order.

$$a_1, a_2, \ldots, a_n, a_{n+1}. \tag{5.8}$$

And, given any another order,

$$b_1, b_2, \ldots, b_n, b_{n+1}. \tag{5.9}$$

Suppose $b_1 = a_k$, where $1 \leq k \leq n + 1$. We can apply

$$f_{1,2} \circ f_{2,3} \circ \ \ldots \ f_{k-2,k-1} \circ f_{k-1,k} \tag{5.10}$$

to (5.8), and result in

$$a_k, a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_{n+1}. \tag{5.11}$$

Now, we have to permute (5.11) into (5.9). Since a_k is already in the first position required by the target order (5.9), we only have to permute

$$a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_{n+1} \tag{5.12}$$

into

$$b_2, \ldots, b_n, b_{n+1}. \tag{5.13}$$

From the inductive hypothesis, we can make a composition function g of the functions in (5.7) to do the job. Let f' denote the composition function (5.10). We have $g \circ f'$, which will perform the permutation from (5.8) into (5.9), and $g \circ f'$ is a composition of functions from the class defined in (5.7).

[The Inductive Step Holds.]

That completes the proof. □

Solution 14: The number of all possible combinations of the first and last initials are

$$26 \times 26 = 676.$$

Thus, by the Pigeonhole Principle, assigning 700 people to 676 different initials must introduce at least 2 people who have the same initials. □

Solution 15: Suppose there is a party with n people. We may consider the following two cases.

Case 1: Every body has shaken hands. Then, the possible numbers of people for each person who has shaken hands with are $1, 2, 3, \ldots, n-1$. Every body got a number from those possible numbers. We have n people, and $n-1$ numbers. By the Pigeonhole Principle, at least one number is assigned to two people.

Case 2: There is one person who does not shake hands with any others. In this case, the possible numbers become $0, 1, 2, \ldots, n-2$. Please note, $n-1$ is not allowed, otherwise, there is one person has shaken hands with everybody in the party, and that contradicts the assumption. Just like case 1, we have n people and $n-1$ numbers. By the Pigeonhole Principle, at least one number is assigned to two people.

□