MEERUT INSTITUTE OF ENGINEERING & TECHNOLOGY

Department of Computer Science Engineering

(ODD SEMESTER, 2022)

Discrete Structures & Theory of Logic

Compact Notes[1]

(with solutions to problems and some additional comments)

[1] Technical errors, if any found, may be communicated at *atul.kumar@miet.ac.in* Please ignore minor typos.

Subject Code: KCS-303 **Subject Name**: DSTL

Session: 2022-23 **Weightage**: Full TA

Contents

Important Instructions

- This document is compiled to provides you a quick review of all important definitions, comments, and statements of some crucial facts, to maximise on your performance in all examinations, including the *semester end examination*.

- This document includes the solutions of assignments problems.

- Some additional comments are also included to help you do a focussed preparation.

- The core idea is to facilitate time-efficient *self-study*, and reinforce concepts discussed during lecture classes.

- It is very important you prepare at least what is covered in this document.

- Prepare thoroughly all topics appearing in Sections 1.1, 1.2; Section 2 (all topics); Sections 3.3, 3.4; Sections 4.2; Sections 5.2; Sections 6 (all topics); Sections 8 (all topics); Sections 9 (all topics); Sections 11 (all topic); Sections 12 (all topic); Sections 13 (all topic); Sections 14 (all topic); Sections 15.1; Sections 16 (all topic); Sections 17.2.

1 Sets and Operations

A **set** is an unordered collection of dissimilar objects, which are also called the **elements** of the set. We usually express a *set* as $\{\ \dots\ \}$, where $\dots$ stands for the *elements* it contains[2]. It is common practice to use upper-case English alphabets

$$A, B, C, \dots \qquad \text{or} \qquad X, Y, Z, \dots,$$

to write a set, and lower-case English alphabets

$$a, b, c, \dots \quad \text{or} \quad x, y, z, \dots .$$

to write its elements. However, we use "standard notations" for certain special type of sets such the **number sets**, as listed below:

Natural Numbers $\mathbb{N} := \{1, 2, 3, \dots\}$;

Integers $\mathbb{Z} := \{\ \dots, -2, -1, 0, 1, 2, \dots\}$;

Rational Numbers $\mathbb{Q} := \{\frac{a}{b} \mid a, b \text{ are integers, with } b \neq 0\}$;

Irrational Numbers $\mathbb{I} := \{\text{a non-rational number such as } \sqrt{2}, e, \pi, e^{\pi}, \dots\}$;

Real Numbers $\mathbb{R} := \{\text{a rational or an irrational number}\}$;

Complex Numbers $\mathbb{C} := \{a + ib \mid a, b \text{ are real numbers, and } i = \sqrt{-1}\}$;

Also, $\mathbb{Z}^+$ denotes the set of *positive integers*, $\mathbb{Q}^*$ denotes the set of **non-zero** rational numbers, $2\mathbb{N}$ denotes the set of *even integers*, D_n denotes the *set of divisors* of a positive integer n, and so on. In general, in two types of *representations*, we can list the elements of a set X explicitly or the set is specified by a *property* shared by all its elements. In later case, if P is such a property, then we write the set X as

$$X = \{x \mid x \text{ satisfies } P\}. \tag{1.1}$$

The central idea of the set theory is to view a "collection of objects" as a *single entity*. In most part of mathematics, our goal is how to express a complex mathematical structures in terms of similar structures involving only simplest possible sets.

Definition 1.1. *A set having no element is called the* empty set*. It is denoted by* $\varnothing$*.*

In view of notation (1.1), we can write $\varnothing := \{x \mid x \neq x\}$.

[2] Unlike a *multiset*, the elements of a set are listed without repetition, and the order of listing is unimportant (see Definition 1.7).

Definition 1.2. *If X is a set, and x is an element of X, we write $x \in X$, which is read as x **belong to** (or is a **member of**) the set X. Otherwise, when an object x is not an element of a set X, we write $x \notin X$, which is read as x is **not a member of** the set X.*

Notice that $-2 \in \mathbb{Z}$, but $-2 \notin \mathbb{N}$. Also, $x \notin \mathbb{Q}$ is an **irrational numbers** such as $\sqrt{2}$, e, π, and also e^{π}, where e denotes the **Euler constant**. In this course, we are discussing *constructive approach* of such types of number sets.

Definition 1.3. *A set A is called a **subset**[3] of a set B if we have*

$$x \in A \qquad \Rightarrow \qquad x \in B. \tag{1.2}$$

That is, every element of the set A is also an element of the set B. In this case, we write $A \subseteq B$, which is read as A is contained in *B. Also, when $A \subseteq B$, and the set B has an element that is not in A, we call A a **proper subset** of the set B. In this case, we write $A \subset B$. If the set A has an element that is not in B, then A is **not a subset** of B. In this case, we write $A \not\subseteq B$.*

It follows from the relation (1.2) that the two sets A and B are **equal** if and only if $A \subseteq B$ and $B \subseteq A$. Symbolically, we write

$$A = B \quad \Leftrightarrow \quad (x \in A \Rightarrow x \in B) \text{ and } (x \in B \Rightarrow x \in A). \tag{1.3}$$

When A and B are **not equal**, we write $A \neq B$. In this case, we have either the set A has an element that is not in B or the set B has an element that is not in A. Clearly, we have

$$\mathbb{N} \subset \mathbb{Z} \qquad \text{and} \qquad E \subset \mathbb{N},$$

where E is the set of positive even integers.

Definition 1.4. *Let X be a nonempty set. The set of all subsets of X is called the* power set *of the set X. It is denoted by $\mathscr{P}(X)$.*

Since $X \subseteq X$, we have $X \in \mathscr{P}(X)$. Also, since $\varnothing \subset X$ is *vacuously true*, we have $\varnothing \in \mathscr{P}(X)$. These two subsets are called the *trivial subsets* of the set X. Therefore, for a non-trivial subset A of the set X, we have $\varnothing \neq A \neq X$. In particular, we have $\mathscr{P}(\varnothing) = \{\varnothing\}$.

Q 1 (2019)**.** *Find the* power set *of the sets (i) $\{a\}$; (ii) $\{a,b\}$; (iii) $\big\{\varnothing, \{\varnothing\}\big\}$; and, (iv) $\big\{a, \{a\}\big\}$.*

Sol. For (i), the power set is given by $\mathscr{P}(\{a\}) = \big\{\varnothing, \{a\}\big\}$; for (ii), the power set is given by

$$\mathscr{P}\big(\{a,b\}\big) = \big\{\varnothing, \{a\}, \{b\}, \{a,b\}\big\};$$

[3] In this case, we also say B is a **superset** of the set A, and write $B \supseteq A$, which is read as B is *a superset of* the set A.

for (iii), the power set is given by

$$\mathscr{P}\big(\{\varnothing,\{\varnothing\}\}\big)=\big\{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\big\};$$

for (iv), the power set is given by

$$\mathscr{P}\big(\{a,\{a\}\}\big)=\big\{\varnothing,\{a\},\{\{a\}\},\{a,\{a\}\}\big\}.$$

This completes the solution. ♢

Definition 1.5. *The number of elements a contains is called the* ***cardinality*** *of the set X, which is usually written as $|X|$ or $\#X$. A set X is said to be a* ***finite set*** *if it contains a finite number of elements, i. e., $|X|<\infty$. Otherwise, we say X is an* ***infinite set****.*

In the next question, we find the *cardinality* of the *power set* of a finite set.

Q 2. *Let a set A has n elements. Prove that its* power set *$\mathscr{P}(A)$ has 2^n elements.*

Sol. For $0\le k\le n$, there are $\binom{n}{k}$ ways to select a subset having k elements of the set A. Therefore, in total, power set $\mathscr{P}(A)$ contains

$$\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n-1}+\binom{n}{n}=2^n$$

sets, as asserted. ♢

1.1 Set Operations

We are assuming the reader is familiar with three fundamental *set operations*: the **union** of two sets A and B, denoted by $A\cup B$; the **intersection** of two sets A and B, denoted by $A\cap B$; and, the **complement** of a set A relative to a set B, denoted by $A-B$. In particular, the *complement* of a set A relative to a universal set U is denoted by A^c (or A'). These operations are used to do mathematics with sets, and also to make new sets from any given collection of sets. Moreover, the concept of *relative complement* also help introduce another interesting type of set operation, which is known as the *symmetric difference*.

Definition 1.6. *Let $X\neq\varnothing$, and $A,B\in\mathscr{P}(X)$. The set*

$$\big(A-B\big)\cup\big(B-A\big)=\big\{x\in X\mid x\in(A\cup B)-(A\cap B)\big\}. \tag{1.4}$$

is called the ***symmetric difference*** *of the sets A and B. It is denoted by $\vee$.*

It follows directly from the above definition that $\vee$ satisfies the following properties:

$$A\vee B=B\vee A,\qquad A\vee A=\varnothing;$$
$$A\vee\varnothing=A,\quad A\vee X=A',\quad A\vee A'=X.$$

Q 3. *Let $U = \{1,2,\ldots,8,9\}$ be a* universal set*, and consider the six sets given by*

$$A = \big\{1,2,3,4,5\big\}, \qquad B = \big\{4,5,6,7\big\}, \qquad C = \big\{5,6,7,8,9\big\},$$
$$D = \big\{1,3,5,7,9\big\}, \qquad E = \big\{2,4,6,8\big\}, \qquad F = \big\{1,5,9\big\}$$

Find the sets (a) $A\cup B, D\cup F$; (b) B^c, E^c, D^c; (c) $A-B, D-E, E-D$; (d) $C\vee D, E\vee F, A\vee B$; and (e) $\big(A\cup C\big)-B$, $\big(B\vee C\big)-A$.

Sol. For part (a), we have

$$A\cup B = \big\{1,2,3,4,5,6,7\big\} \quad \text{and} \quad D\cup F = \big\{1,3,5,7,9\big\}.$$

For part (b), we have

$$B^c = \big\{1,2,3,8,9\big\}, \quad E^c = \big\{1,3,5,7,9\big\}, \quad D^c = \big\{2,4,6,8\big\}.$$

For (c), we have

$$D-E = \big\{1,3,5,7,9\big\} \quad \text{and} \quad E-D = \big\{2,4,6,8\big\}.$$

For part (d), we have

$$C\vee D = \big\{1,3,6,8\big\}, \quad E\vee F = \big\{1,2,4,5,6,8,9\big\}, \quad A\vee B = \big\{1,2,3,6,7\big\}.$$

For part (e), we have

$$\big(A\cup C\big)-B = \big\{1,2,3,8,9\big\} \quad \text{and} \quad \big(B\vee C\big)-A = \big\{6,7,8,9\big\}.$$

This completes the solution. ♢

Let $X \neq \varnothing$. The next theorem proves that, with respect to set operations, the power set $\mathscr{P}(X)$ satisfy the fundamental algebraic properties such as *idempotent laws*, *associative laws*, *commutative laws*, *distributive laws*, *identity laws*, and *complementation laws*. Together with these laws, $\mathscr{P}(X)$ is called the *algebra of sets* defined on the set X, which is an interesting object of study.

Theorem 4. *Suppose $A,B,C \in \mathscr{P}(X)$. Then, we have*

1. *(Idempotency)* $A\cup A = A, \quad A\cap A = A$;
2. *(Associativity)* $A\cap(B\cap C) = (A\cap B)\cap C; \quad A\cup(B\cup C) = (A\cup B)\cup C$;
3. *(Commutativity)* $A\cup B = B\cup A; \quad A\cap B = B\cap A$;
4. *(Distributivity)* $A\cup(B\cap C) = (A\cup B)\cap(A\cup C); \quad A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$;
5. *(Identity Laws)* $A\cup\varnothing = A, \quad A\cap U = A$;

6. *(Complementation Laws)* $(A^c)^c = A$;

7. *(Involution Law)* $(A^c)^c = A$;

8. *(Dominance Laws)* $A \cup U = U, \quad A \cap \varnothing = \varnothing$;

9. *(Absorption Laws)* $A \cup (A \cap B) = A, \quad A \cap (A \cup B) = A$;

10. *(DeMorgan Laws)* $(A \cap B)^c = A^c \cup B^c; \quad (A \cup B)^c = A^c \cap B^c$.

Proof. In each of the above assertions, the “equality of sets" is taken in the sense of (1.3). Therefore, it is easy to prove any of these. However, as a simple illustration, we include here proof of the first of the two “DeMorgan Laws" stated in (10). That is, we show that

$$(A \cap B)^c \subseteq (A^c \cup B^c) \quad \text{and} \quad A^c \cup B^c \subseteq (A \cap B)^c.$$

For, let $x \in X$. Then, by the definitions of involved set operations, we have

$$\begin{aligned} x \in \big(A \cap B\big)^c &\Leftrightarrow \ x \notin A \cap B \\ &\Leftrightarrow \ x \notin A \quad \text{or} \quad x \notin B \\ &\Leftrightarrow \ x \in A^c \quad \text{or} \quad x \in B^c \\ &\Leftrightarrow \ x \in A^c \cup B^c \end{aligned}$$

Similarly, we can prove the other equality. □

Q 5. *Let A, B, C be three nonempty sets. Prove the following, both analytically and graphically:*

1. $\big(A - C\big) \cap \big(C - B\big) = \varnothing$;

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

3. $\big(A^c \cup B^c\big)^c \cup \big(A^c \cup B\big)^c = A$.

Sol. For (1), if the LHS is nonempty, let $x \in (A - C) \cap (C - B)$. Then, we have $x \in A - C$ and $x \in C - B$. However, the two conditions cannot hold simultaneously simply because

$$x \in A - C \quad \Rightarrow \quad x \notin C \quad \text{and} \quad x \in C - B \quad \Rightarrow \quad x \in C.$$

For (2), recall that $X - Y = X \cap Y^c$. Therefore, we have

$$\begin{aligned} A - \big(B \cap C\big) &= A \cap \big(B \cap C\big)^c \\ &= A \cap \big(B^c \cup C^c\big) && \text{(by DeMorgan Law)} \\ &= \big(A \cap B^c\big) \cup \big(A \cap C^c\big) && \text{(by Distributive Law)} \\ &= \big(A - B\big) \cup \big(A - C\big). \end{aligned}$$

For (3), we have.

$$\begin{aligned}
\left(A^c \cup B^c\right)^c \cup \left(A^c \cup B\right)^c &= \left(A \cap B\right) \cup \left(A \cap B^c\right) && \text{(by DeMorgan Law)}\\
&= A \cap \left(B^c \cup C^c\right) && \text{(by DeMorgan and Involution Laws)}\\
&= A \cap \left(B \cup B^c\right) && \text{(by Distributive Law)}\\
&= A \cap \left(U\right) && \text{(by Complementation Law)}\\
&= A.
\end{aligned}$$

In each case, a proof by Venn diagram[4] is simple. ♢

1.2 Multisets & Operations

We introduce here *multiset*, which is a *generalisation* of the concept of a set in the sense that we are now allowing “duplication of objects". The Indian mathematician *Bhaskaracharya* first applied multisets in 1150 to study their permutations. However, the term “multiset" was first coined by Nicolas de Bruijn.

Definition 1.7. *A **multiset** (or simply **mset**[5]) is an unordered collection having multiple instances of the same object, where the multiplicity of an object may be zero, one, or more than one. We usually write a multiset M as*

$$M := \left[k_1 \cdot a_1, k_2 \cdot a_2, \dots\right], \qquad \text{where} \quad k_i \in \mathbb{Z}^+, \tag{1.5}$$

*where the multiplicity k_i of an object a_i in the multiset M is the number of times it appears in the collection. The set $\left\{a_1, a_2, \dots\right\}$ is called the **base set** of the multiset M.*

For example, the two multisets A and B given by

$$A = \left[1,\, 1,\, 2,\, 2,\, 3,\, 4,\, 6,\, 6,\, 6\right] \quad \text{and} \quad B = \left[1,\, 2,\, 2,\, 2,\, 3,\, 3,\, 4,\, 4,\, 6\right].$$

have the same *base set* $\{1,2,3,4,6\}$. In the multiset A, object 1 has the multiplicity *two*; object 2 has the multiplicity *two*; object 3 has the multiplicity *one*; object 4 has the multiplicity *one*; and, object 6 has the multiplicity *three*. Similarly, we can read the multiplicities of objects in B, so that we can also write

$$A = \left[2 \cdot \mathbf{1},\, 2 \cdot \mathbf{2},\, \mathbf{3},\, \mathbf{4},\, 3 \cdot \mathbf{6}\right] \quad \text{and} \quad B = \left[\mathbf{1},\, 3 \cdot \mathbf{2},\, 2 \cdot \mathbf{3},\, 2 \cdot \mathbf{4},\, \mathbf{6}\right]. \tag{1.6}$$

More generally, in view of (1.5), there could be infinite number of multisets with base set $\{a,b\}$, but with varying multiplicities of these two objects. In the multiset $[a,a,b,b,b]$, the element a has multiplicity 2, and b has multiplicity 3. In the multiset $[a,a,b,b]$, both a and b have multiplicity 2. These two multisets are viewed different. However, as with sets, *order* of listing elements of a multiset is not important.

[4] Recall that a **Venn Diagram** is a graphical representation in which the *related* universal set is shown as the interior of a rectangle and its subsets as interiors of circles that lie inside the rectangle.

[5] Other terminologies in use are such as a **bag** (due to Peter Deutsch, 1972), an *aggregate, heap, bunch, sample, weighted set, occurrence set*, and *fireset* (acronym for “finitely repeated element set").

Definition 1.8. *The **cardinality** of a multiset is the sum of the multiplicities of all its elements.*

Remark 1.1. *There are numerous applications wherein we use* multisets. *For example, in a typical dataset of the form $(name, age)$ concerning a collection of people, the multiset of ages counts the number of people of a specific age in the list. In all such cases, major concern is to treat objects "equal" with respect to an equivalence relation, yet "distinct" with respect to some other relation. Also, in the context of elementary number theory, the* multiset of prime factors *of a natural number $n > 1$ is an example. A related example is that of the* multiset of solutions *of an algebraic equation.*

Therefore, the next three definitions are significant for their applications.

Definition 1.9. *Let M and N be two multisets, with the same base set $\{a_1, \dots, a_p\}$, given by*

$$M = \left[k_1 \cdot a_1, \dots, k_p \cdot a_p\right], \quad \text{and} \quad N = \left[\ell_1 \cdot a_1, \dots \ell_p \cdot a_p\right] \tag{1.7}$$

*The **union** $M \cup N$ of these two multisets is the multiset given by*

$$M \cup N := \left[\max(k_1, \ell_1) \cdot a_1, \dots \max(k_p, \ell_p) \cdot a_p\right]. \tag{1.8}$$

That is, in the case of union of multisets, maximum of the two multiplicities *is taken into the consideration.*

For example, the union of two multisets given in (1.6) is the multiset $A \cup B = \left[2 \cdot \mathbf{1}, 3 \cdot \mathbf{2}, 2 \cdot \mathbf{3}, 2 \cdot \mathbf{4}, 3 \cdot \mathbf{6}\right]$.

Definition 1.10. *Let M and N be two multisets, with the same base set $\{a_1, \dots, a_p\}$, given by*

$$M = \left[k_1 \cdot a_1, \dots, k_p \cdot a_p\right], \quad \text{and} \quad N = \left[\ell_1 \cdot a_1, \dots \ell_p \cdot a_p\right] \tag{1.9}$$

*The **intersection** $M \cap N$ of these two multisets is the multiset given by*

$$M \cap N := \left[\min(k_1, \ell_1) \cdot a_1, \dots \min(k_p, \ell_p) \cdot a_p\right]. \tag{1.10}$$

That is, in the case of intersection of multisets, minimum of the two multiplicities *is taken into the consideration.*

For example, the intersection of two multisets given in (1.6) is the multiset $A \cap B = A = \left[\mathbf{1}, 2 \cdot \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{6}\right]$.

Definition 1.11. *Let M and N be two multisets, with the same base set $\{a_1, \dots, a_p\}$, given by*

$$M = \left[k_1 \cdot a_1, \dots, k_p \cdot a_p\right], \quad \text{and} \quad N = \left[\ell_1 \cdot a_1, \dots \ell_p \cdot a_p\right] \tag{1.11}$$

*The **difference** of these two multisets is the multiset such that the multiplicity of an element equals difference of the multiplicities of elements in the two multisets, if the difference is positive. When the difference is zero* *or negative, we take the multiplicity as* 0. *That is, the* differences $M-N$ *and* $N-M$ *are respectively given by*

$$M-N := \big[(k_1-\ell_1)\cdot a_1, \dots (k_p-\ell_p)\cdot a_p\big]; \tag{1.12a}$$

$$N-M := \big[(\ell_1-k_1)\cdot a_1, \dots (\ell_p-k_p)\cdot a_p\big]. \tag{1.12b}$$

That is, in the case of difference of multisets, non-negative difference of the two multiplicities *is taken into the consideration.*

For example, the two differences of the multisets given in (1.6) are the multisets

$$A-B = \big[\mathbf{1}, 2\cdot\mathbf{6}\big] \quad \text{and} \quad B-A = \big[\mathbf{2}, \mathbf{3}, \mathbf{4}\big].$$

Definition 1.12. *Let* M *and* N *be two multisets, with the same base set* $\{a_1,\dots,a_p\}$*, given by*

$$M = \big[k_1\cdot a_1, \dots, k_p\cdot a_p\big], \quad \textit{and} \quad N = \big[\ell_1\cdot a_1, \dots \ell_p\cdot a_p\big] \tag{1.13}$$

The ***sum*** $M+N$ *of these two multisets is the multiset given by*

$$M+N := \big[(k_1+\ell_1)\cdot a_1, \dots (k_p+\ell_p)\cdot a_p\big]. \tag{1.14}$$

That is, in the case of the sum of two multisets, the multiplicities of the two multisets are added.

For example, the sum of the two multisets given in (1.6) is the multiset

$$A+B = \big[3\cdot\mathbf{1}, 5, 3\cdot\mathbf{3}, 3\cdot\mathbf{4}, 4\cdot\mathbf{6}\big].$$

Q 6 (2018)**.** *Define union and intersection of multisets, and find the same for the multisets* $A = \big[1, 1, 4, 2, 2, 3\big]$ *and* $B = \big[1, 2, 2, 6, 3, 3\big]$.

Sol. For the first part of the question see Definition 1.9 and Definition 1.10. For the second part, in view of (1.8) and (1.9), the union and intersection of multisets

$$A = \big[2\cdot 1, 4, 2\cdot 2, 3\big] \quad \text{and} \quad B = \big[1, 2\cdot 2, 6, 2\cdot 3\big]$$

are respectively given by

$$A\cup B = \big[2\cdot 1, 4, 2\cdot 2, 2\cdot 3, 6\big] \quad \text{and} \quad A\cap B = \big[1, 2\cdot 2, 3\big].$$

This completes the solution. ♢

1.3 Cartesian Product

The concept of *Cartesian product* (or simply the *product*) of sets is a fundamental set operation. It plays important role in various applications of modern mathematics. We start with the next definition.

Definition 1.13. *Let A and B two nonempty sets. The* ***Cartesian product*** *(or simply the* ***product****) of A and B, denoted by $A \times B$, is the set of* ordered pairs[6] *given by*

$$A \times B := \big\{(a,b) \mid a \in A \ \ and \ \ b \in B\big\}. \tag{1.15}$$

For a simple illustration, let $A = \{a,b\}$ and $B = \{1,2,3\}$. Then we have

$$A \times B = \big\{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\big\}.$$

More generally, if A and B are a finite set given by

$$A = \big\{a_1,\dots,a_m\big\} \quad \text{and} \quad A = \big\{b_1,\dots,n_n\big\},$$

then the set $A \times B$ contains mn elements, which can be written in matrix form as in Table 1.

Table 1: The product set $A \times B$ in matrix form.

	b_1	b_2	$\dots$	b_{n-1}	b_n
a_1	(a_1,b_1)	(a_1,b_2)	$\dots$	(a_1,b_{n-1})	(a_1,b_n)
a_2	(a_2,b_1)	(a_2,b_2)	$\dots$	(a_2,b_{n-1})	(a_2,b_n)
	$\vdots$	$\vdots$	$\dots$	$\vdots$	$\vdots$
a_{m-1}	(a_{m-1},b_1)	(a_{m-1},b_2)	$\dots$	(a_{m-1},b_{n-1})	(a_{m-1},b_n)
a_m	(a_m,b_1)	(a_m,b_2)	$\dots$	(a_m,b_{n-1})	(a_m,b_n)

Q 7. *Let A,B,C be three nonempty sets. Prove or disprove the following:*

1. $A \cap C = B \cap C$ *and* $A \cup C = B \cup C \quad \Rightarrow \quad A = B$*;*
2. $A \times \big(B \cup C\big) = \big(A \times B\big) \cup \big(A \times C\big)$*;*
3. $A \times \big(B \cap C\big) = \big(A \times B\big) \cap \big(A \times C\big)$.

[6] In 1921, *Kazimierz Kuratowski* defined an **ordered pair** (a,b) as the set $\big\{\{a\},\{a,b\}\big\}$. The element $a \in A$ is called the *first coordinate* of the ordered pair (a,b) and b is called the *second coordinate*.

Sol. For (1), we have

$$\begin{aligned} A &= A\cap\left(A\cup C\right) && \text{(by absorption)}\\ &= A\cap\left(B\cup C\right) && \text{(by given condition)}\\ &= \left(A\cap B\right)\cup\left(A\cap C\right) && \text{(by distributivity)}\\ &= \left(A\cap B\right)\cup\left(B\cap C\right) && \text{(by given condition)}\\ &= \left(A\cap B\right)\cup\left(C\cap B\right) && \text{(by commutativity)}\\ &= \left(A\cup C\right)\cap B && \text{(by distributivity)}\\ &= \left(B\cup C\right)\cap B && \text{(by given condition)}\\ &= B && \text{(by absorption)} \end{aligned}$$

For (2), we have

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

For (3), we have

$$\begin{aligned} A\times\left(B\cap C\right) &= \left\{(x,y)\mid\ x\in A \quad\text{and}\quad \left(y\in B\cap C\right)\right\}\\ &= \left\{(x,y)\mid\ x\in A \quad\text{and}\quad \left(y\in B \text{ and } y\in C\right)\right\}\\ &= \left\{(x,y)\mid\ \left(x\in A \text{ and } y\in B\right) \quad\text{and}\quad \left(x\in A \text{ and } y\in C\right)\right\}\\ &= \left\{(x,y)\mid\ (x,y)\in A\times B \quad\text{and}\quad (x,y)\in A\times C\right\}\\ &= \left(A\times B\right)\cap\left(A\times C\right). \end{aligned}$$

This completes the proof. ♢

2 Relations and Properties

We start with the next definition.

Definition 2.1. *Consider a finite set $A = \{a_1,\dots,a_n\}$. A **relation** on A is a set $R \subseteq A \times A$. When $R = \varnothing$, it called the **null relation**; and, when $R = A \times A$, it is called the **full relation**.*

In what follows, we shall work with relation that is neither the *null relation* nor the *full relation*. An important relation Δ_A on the set A is given by

$$\Delta_A := \{(a_1,a_1),(a_2,a_2),\dots,(a_n,a_n)\}$$

which is called the **diagonal relation** on A. Also, for a relation R on a set A, the relation

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

is called the **inverse relation** of the relation R. We are mainly interested in studying four important properties of a relation R on the set A.

1. A relation R on a set A is said to be **reflexive** if $\Delta_A \subseteq R$, where Δ_A is the *diagonal relation* on A. That is, $(a,a) \in R$, for all $a \in A$.

2. A relation R on a set A is said to be **symmetric** if $R = R^{-1}$. That is, $(a,,b) \in R$ implies that $(b,a) \in R$.

3. A relation R on a set A is said to be **antisymmetric** if

$$(a,b),\,(b,a) \in R \quad \Rightarrow \quad a = b.$$

Said differently, for a pair of <u>distinct</u> points $a,b \in A$, $(a,b) \in R$ or $(b,a) \in R$, but not both. Of course, neither (a,b) nor (b,a) may be in R.

4. A relation R on a set A is said to be **transitive** if

$$(a,b) \in R \text{ and } (b,c) \in R \quad \Rightarrow \quad (a,c) \in R.$$

We also say the triplet (a,b,c) satisfies the **triangle property**.

Also, a relation R on a set A is said to be **irreflexive** if $\Delta_A \cap R = \varnothing$.

Definition 2.2. *A relation R on a set A is called **partial order** if it is reflexive, antisymmetric, and transitive. A relation R on a set A is called **equivalence** if it is reflexive, symmetric, and transitive.*

Our focus in this course is to discuss the above two types of relations on a set.

2.1 Digraph & Relation Matrix

We start with the next definition.

Definition 2.3. *Let R be a relation on a set $A = \{a_1, \ldots, a_n\}$. The* ***digraph*** *of R is a graphical representation of R, denoted by D_R, wherein elements $a_i \in A$ are plotted as points in the plane and, for each pair $(a_i, a_j) \in R$ (possibly same), there is a* directed edge *from a_i to a_j. We also call elements $a_i \in A$* nodes *(or* vertices*) of the digraph D_R.*

We first describe below how to use the geometry of the *digraph D_R* of a relation R such that R satisfies certain specified properties. For example,

1. the relation R with the digraph shown in Fig. 8 is not reflexive, because D_R doesn't has a *self-loop* at d;

2. the relation R is not symmetric, because it contains *one-way edges*;

3. the relation R is antisymmetric, because D_R only contains *one-way edges* between pair of distinct nodes;

4. the relation R is not transitive, because some triplets (a, b, c) don't satisfy the *triangle property*.

Notice that, if a relation R is symmetric, then its digraph D_R cannot have any *single-edge* between two distinct points represented by the elements of the set A. On the other hand, if a relation R is antisymmetric, then its digraph D_R must satisfy this same property. These observations are used to answer some parts of the next question.

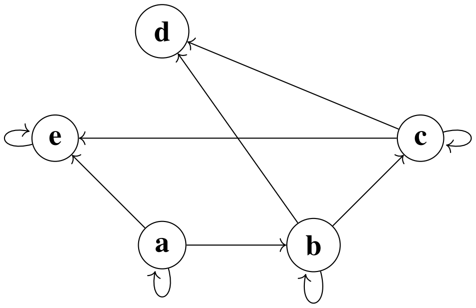


Figure 1: Digraph of a relation on the set $A = \{a, b, c, d, e\}$.

Q 8. *Let $A = \{a, b, c, d, e\}$. Give an example of a relation R on A such that*

1. R is both symmetric and antisymmetric;

2. R is antisymmetric, but not reflexive;

3. R is neither symmetric not antisymmetric;

4. *R is both irreflexive and antisymmetric.*

Sol. For (1), if a relation R on a set A is both symmetric and antisymmetric, then we must have $R \subseteq \Delta_A$. In particular, we may take $\{(a,a),(b,b),(d,d),(e,e)\}$. The same argument can be applied to answer (2). We may take a relation R containing some *single-edges* between distinct points represented by the elements of $A = \{a,b,c,d,e\}$, together with some elements of Δ_A. For (3), think along similar lines. For (4), we may take R containing some *single-edges* between distinct points represented by the elements of $A = \{a,b,c,d,e\}$ such that $R \cap \Delta_A = \varnothing$. ♢

Q 9. *Let R be a relation on a set $A = \{a,b,c\}$ with relation matrix M_R given by $\begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix}$. Find the relation matrices for the relations R^{-1}, R^2, and R^c. Also, draw their digraphs.*

Sol. It can be read from the matrix M_R that we have

$$R = \big\{(a,a),(b,c),(c,b),(c,c)\big\}.$$

Therefore, it follows that

$$\begin{aligned} R^{-1} &= \big\{(a,a),(b,c),(c,b),(c,c)\big\}; \\ R^2 = R\circ R &= \big\{(a,a),(b,b),(b,c),(c,b),(c,c)\big\}; \\ R^c &= \big\{(a,b),(a,c),(b,a),(b,b),(c,a)\big\}. \end{aligned}$$

Hence, the relation matrices for the relations R^{-1}, R^2, and R^c are respectively given by

$$\begin{aligned} M_{R^{-1}} &= \begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix}; \\ M_{R^2} &= \begin{pmatrix}1&0&0\\0&1&1\\0&1&0\end{pmatrix} = \begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix} \bullet \begin{pmatrix}1&0&0\\0&0&1\\0&1&1\end{pmatrix}; \\ M_{R^c} &= \begin{pmatrix}0&1&1\\1&1&0\\1&0&0\end{pmatrix}. \end{aligned}$$

The digraphs are as shown in Fig. 18. ♢

2.2 Equivalence Relation

Q 10. *On the set of integers $\mathbb{Z}$, define*

$$a \sim b \qquad \Leftrightarrow \qquad 6 \ \textit{divides} \ a-b.$$

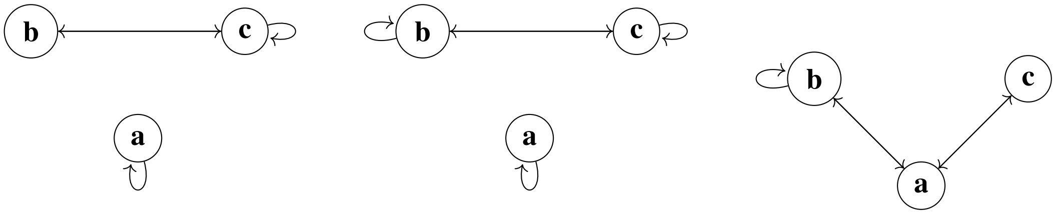


Figure 2: Digraph of R^{-1}, R^2, and R^c.

Show that $\sim$ is an equivalence relation, and also write all elements of the set $\mathbb{Z}_6$.

Sol. Since 6 divides $a-a=0$, for any $a \in \mathbb{Z}$, it follows that $a \sim a$ so that $\sim$ is a reflexive relation. Next, suppose $a \sim b$ so that we have $a-b=6k$, for some integer k. But then, we also have $b-a=6(-k)$, which implies $b \sim a$. So, $\sim$ is a symmetric relation. To prove transitivity of $\sim$, let $a \sim b$ and $b \sim c$. We thus have

$$a-b=6k_1 \quad \text{and} \quad b-c=6k_2, \qquad \text{for some} \quad k_1,k_2 \in \mathbb{Z}.$$

Adding the above two equations, we obtain

$$a-c=\big(a-b\big)+\big(b-c\big)=6\big(k_1+k_2\big), \qquad \text{where} \quad k_1,k_2 \in \mathbb{Z},$$

which shows that $a \sim c$. Therefore, $\sim$ is an equivalence relation. Finally, recall that the set $\mathbb{Z}_6$ consists of associated equivalence classes. That is, we have

$$\mathbb{Z}_6=\big\{\big[0\big],\big[1\big],\ldots,\big[5\big]\big\}, \quad \text{where} \quad \big[k\big]:=k+6\mathbb{Z}, \;\; \text{for} \;\; k=0,1,\ldots,5.$$

This completes the solution. $\diamondsuit$

2.3 Closures of Relations

In general, let $\mathscr{P}$ be a property of a relation R on a set A. By the $\mathscr{P}$ **- closure** of R we mean a relation S on the set A such that

(i) S has the property $\mathscr{P}$;

(ii) $R \subseteq S$; and,

(iii) S is the *smallest* that satisfies (i) and (ii).

Now, replacing $\mathscr{P}$ by a property such as reflexive, symmetric, or transitive, we obtain respectively the concept of the *reflexive closure, symmetric closure*, and *transitive closure* of R. Further, since a relation R is reflexive if and only if $\Delta_R \subseteq R$, it follows that **reflexive closure** of R is given by $S_{ref}=R \cup \Delta_R$. Also, since a relation R is symmetric if and only if $R=R^{-1}$, it follows that **symmetric closure** of R is given by $S_{sym}=R \cup R^{-1}$.

Q 11. *Let R be a relation on a set A. Describe what do you mean by the* reflexive, symmetric*, and* transitive closures *of R. Find all the three types of closures of the relation* $R = \big\{(1,2),(1,3),(2,4),(5,6)\big\}$ *on the set* $A = \{1,2,3,4,5,6\}$.

Sol. The *reflexive closure* S_{ref} and the *symmetric closure* S_{sym} of the relation $R = \big\{(1,2),(1,3),(2,4),(5,6)\big\}$ are respectively given by

$$\begin{aligned} S_{ref} &:= R \cup \Delta_R = \big\{(1,1),(1,2),(1,3),(2,2),(2,4),(3,3),(4,4),(5,5,)(5,6),(6,6)\big\}; \\ S_{sym} &:= R \cup R^{-1} = \big\{(1,2),(2,1),(1,3),(3,1),(2,4),(4,2),(5,6),(6,5)\big\} \end{aligned}$$

A complex way of getting the *transitive closure* S_{tran} of R is given by

$$S_{tran} := R \circ R \circ \cdots \circ R \text{ (6 times)}.$$

However, it is far more convenient to do so by using the *Warshall's algorithm.* ♢

Q 12. *Use Warshall's algorithm to compute the transitive closure of the relation R on the set* $A = \{1,2,3,4\}$ *given by* $R = \big\{(1,1),(1,3),(2,1),(2,2),(3,3),(3,4)\big\}$.

Sol. As illustrated during lecture classes (or see the supplemental shared). ♢

2.4 Warshall Algorithm

Let R be a relation on a finite set A with n elements. To find the *transitive closure* $T = R_{tran}$ of the relation R, we need to compute *n-fold composition* given by

$$R^n := R \circ \cdots \circ R \ \ (n\text{-times}).$$

This is not a convenient way of finding the *transitive closure*, especially when the given relation R has five or more elements. On the other hand, as we shall see, the *Warshall algorithm* provides a far more efficient procedure. It takes the relation matrix M_R of the relation R as input. So, we write

$$W^{[0]} := M_R = \big(a_{ij}\big), \qquad \text{wth} \ \ a_{ij} = \begin{cases} 1, & \text{if } \ a_{ij} \in R \\ 0, & \text{otherwise} \end{cases}.$$

Notice that the central idea of *Warshall algorithm* is to replace a 0-*entry* by a 1-*entry* in M_R; it does not change any 1-*entry*. For an illustration, we consider the relation R on the set $A = \{1,2,3,4\}$ with 4×4 relation matrix M_R given by

$$M_R = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

We write $= W^{[0]} = M_R$. To compute the matrix $W^{[1]}$ from the matrix $W^{[0]}$, we write

$$W^{[1]} = \begin{bmatrix} 1 & 1 & & 1 \\ 1 & & 1 & \\ 1 & 1 & & \\ & 1 & & 1 \end{bmatrix}$$

Next, we use *row-indices* of first Column C_1 that contains entry 1, which are called **row numbers** of the column C_1, and *column-indices* of the frst Row R_1 that contains entry 1, which are called the **colum numbers** of the row R_1. It is important to do so **in that order only**. Subsequently, we form ordered pairs taking *row numbers* as the first coordinate and the *colum numbers* as the second coordinate. Finally, to obtain $W^{[1]}$, we replace an entry 0 by 1 at respective position in $W^{[1]}$ if it has a 0 there.

In the above example, the *row numbers* of column C_1 are $1,2,3$, and the *column numbers* of row R_1 are $1,2,4$. Accordingly, in the above matrix $W^{[1]}$, we replace a 0 by a 1 at the positions

$$(1,1),\ (1,2),\ (1,4),\ (2,1),\ (\mathbf{2},\mathbf{2}),\ (\mathbf{2},\mathbf{4}),\ (3,1),\ (3,2),\ (\mathbf{3},\mathbf{4})$$

if there is a 0 at that position in the matrix $W^{[0]}$. Therefore, from the first application of the algorithm, we obtain

$$W^{[1]} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & \mathbf{1} & 1 & \mathbf{1} \\ 1 & 1 & 0 & \mathbf{1} \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

We also say pairs $(2,2), (2,4)$ and $(3,4)$ have created the **new edges** in the digraph D_R of the relation R. Similarly, for $W^{[2]}$, we write

$$W^{[2]} = \begin{bmatrix} 1 & 1 & & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & & 1 \\ & 1 & & 1 \end{bmatrix}$$

Next, we find the *row numbers* in column C_2 that have a 1 are $1,2,3,4$, and the *column numbers* in row R_2 that have 1 are $1,2,3,4$. Accordingly, we replace a 0 by a 1 at the positions

$$\begin{array}{llllll} (1,1), & (1,2), & (\mathbf{1},\mathbf{3}), & (1,4), & (2,1), & (2,2) \\ (2,3), & (2,4), & (3,1), & (3,2),(\mathbf{3},\mathbf{3}), & (3,4), & \\ (\mathbf{4},\mathbf{1}), & (4,2), & (\mathbf{4},\mathbf{3}), & (4,4) & & \end{array}$$

if there is a 0 at that position in the matrix $W^{[1]}$. Therefore, we obtain

$$W^{[2]} = \begin{bmatrix} 1 & 1 & \mathbf{1} & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & \mathbf{1} & 1 \\ \mathbf{1} & 1 & \mathbf{1} & 1 \end{bmatrix}$$

Notice that, at this stage of the algorithm, only the pairs $(1,3),(3,3),(4,1)$ and $(4,3)$ have created *new edges* in D_R. Hence, the transitive closure $T = R_{tran}$ of the relation R is the full set $A \times A$.

In general, For $k \geq 1$, the algorithm uses **row numbers** of kth column C_k and **colum numbers** of kth row R_k of the $W^{[k-1]}$ (in that order) to compute the matrix $W^{[k]}$, by using the same procedure. The stepwise procedure of getting $W^{[k]}$ from $W^{[k-1]}$ is as follows:

(STEP - 1) All the 1's in $W^{[k-1]}$ would retain their respective paces in $W^{[k]}$.

(STEP - 2) List separately the *row numbers* that have 1's in C_k, and the *column numbers* that have 1's in R_k.

(STEP - 3) Pair each of the *row number* with each of the *column number* (*in that order only*), and put a 1 in the corresponding place in $W^{[k]}$ if there in not a 1 already at that place. Let the remaining 0's stay put.

Example 2.1. *Let we use **Warshall's algorithm** to find the* transitive closure *of a relation R on a set $A = \{1,2,3,4\}$ whose 4×4 matrix M_R is given by*

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

*We may take $M_R = W^{[0]}$, and use above three steps to compute $W^{[1]}$. Firstly, according to **Step-1**,*

$$W^{[1]} = \begin{bmatrix} & 1 & & 1 \\ 1 & & 1 & \\ 1 & & & \\ & & & \end{bmatrix}$$

*Next, according to **Step-2**, the* row numbers *that have 1's in C_1 are 2,3, and the* column numbers *that have 1's in R_1 are 2,4. Finally, according to **Step-3**, we shall put a 1 in $W^{[1]}$ at the places*

$$(\mathbf{2},\mathbf{2}),\ (\mathbf{2},\mathbf{4}),\ (\mathbf{3},\mathbf{2}),\ (\mathbf{3},\mathbf{4}),$$

if there in not a 1 already at that place in $W^{[0]}$. Therefore, we obtain

$$W^{[1]} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & \mathbf{1} & 1 & \mathbf{1} \\ 1 & \mathbf{1} & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

*Note that these four pairs have created the new edges in D_R at this stage of the algorithm. For $W^{[2]}$, according to **Step-1**,*

$$W^{[2]} = \begin{bmatrix} & 1 & & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & & 1 \\ & & & \end{bmatrix}$$

*Next, according to **Step-2**, the* row numbers *that have 1's in C_2 are $1,2,3$, and the* column numbers *that have 1's in R_2 are $1,2,3,4$. Finally, according to **Step-3**, we shall put a 1 in $W^{[1]}$ at the places*

$$(\mathbf{1},\mathbf{1}),(1,2),(\mathbf{1},\mathbf{3}),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),(\mathbf{3},\mathbf{3}),(3,4)$$

if there in not a 1 already at that place in $W^{[0]}$. Therefore, we obtain

$$W^{[2]} = \begin{bmatrix} \mathbf{1} & 1 & \mathbf{1} & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & \mathbf{1} & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Note that only the pairs $(1,1)$, $(1,3)$ and $(3,3)$ have created the new edges in D_R at the second stage of the algorithm. Another application of the algorithm gives $W^{[3]} = W^{[2]}$. Hence, the transitive closure *T of the relation R is $\{(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4),(3,1),(3,2),(3,3),(3,4)\}$.*

Q 13. *Use Warshall algorithm to compute the transitive closure of the relation $R = \{(1,3),(2,1)(2,4),(4,2)\}$. [**Ans.** Edges for $(2,2),(2,3),(4,1),(4,3),(4,4)$ are created]*

Q 14. *Use Warshall algorithm to compute the transitive closure of the relation $R = \{(2,1)(2,4),(4,1),(4,3)\}$. [**Ans.** All edges for the first three rows are created]*

Q 15. *Use Warshall algorithm to compute the transitive closure of the relation R on the set $A = \{1,2,3,4\}$ given by $R = \big\{(1,1),(1,3),(2,1),(2,2),(3,3),(3,4)\big\}$.*

Sol. As illustrated during lecture classes (or see the supplemental shared). ♢

3 Functions and Properties

A *function* between two nonempty sets is a rule that associate with each element of one set to a unique element of the other set. Therefore, sets and functions are important to understand modern mathematics, and also some aspects of the *theory of computation*. In particular, the *polynomial functions, trigonometric functions*, and *exponential functions* are the most basic types of functions that hold vast geometric significance for applications. We study “properties of functions" to understand how elements of various types of sets are related to each other. Some simple examples include use of bijective functions to *compare the sizes* of sets, study *control objects* as in control theory, measure *computational complexity* of an algorithm, and so on.

3.1 Functions

An abstract definition of a function is as given below.

Definition 3.1. *Let X and Y be two nonempty sets (not necessarily distinct). A **function** f from X to Y is a relation $f \subseteq X \times Y$ such that, for each $x \in X$, we have*

(a) *there is some $y \in Y$ such that $(x,y) \in f$;*

(b) $(x,y_1), (x,y_2) \in f \;\Rightarrow\; y_1 = y_2$.

In this case, we write the function $f : X \to Y$ as

$$f = \big\{(x,y) \in X \times Y \mid y = f(x), \text{ for } x \in X\big\}. \tag{3.1}$$

*The set X is called the **domain**, and the set Y is called the **codomain**, of the function f. We usually write $X := \mathrm{Dom}\,(f)$. For $x \in X$, the set of* image elements *$f(x) \in Y$ is called the **range** of the function f, which is denoted by* $\mathrm{Ran}(f)$. *That is, we have*

$$\mathrm{Ran}\,(f) := \big\{y = f(x) \in Y \mid x \in X\big\} \tag{3.2}$$

We also write $y = f(x)$ as $f : x \mapsto y$ (read as f maps element x to element y).

Clearly, *not every relation is a function*. For example, in Fig. 3, R violates condition (a), and S violates condition (b). In general, we can define at least as many functions $f : X \to Y$ as there are elements in the set Y. For, let y_0 be any fixed element of the set Y, and define $f_{y_0} : X \to Y$ as $f_{y_0}(x) = y_0$, for $x \in X$. This is called the *constant function* at y_0 given on the set X. Next, we may choose two or more elements in the set Y, and define functions $f : X \to Y$ by mapping elements of X to some of these elements of Y (Fig. 4).

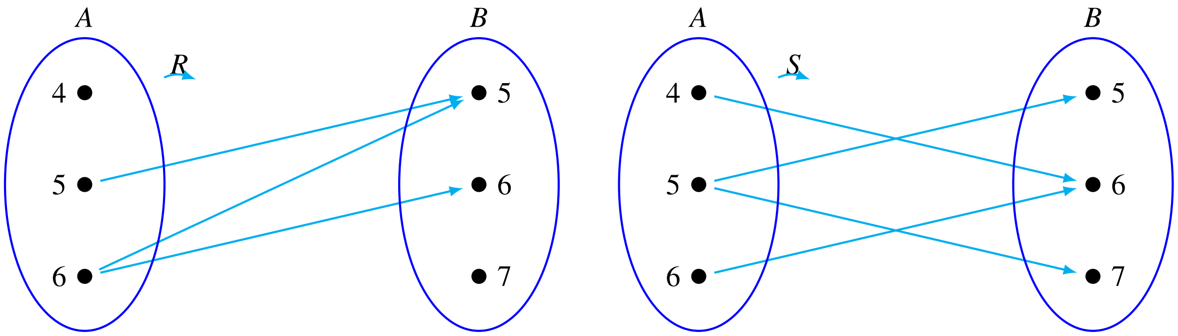


Figure 3: Two relations $R,S:A\to B$ that are not functions.

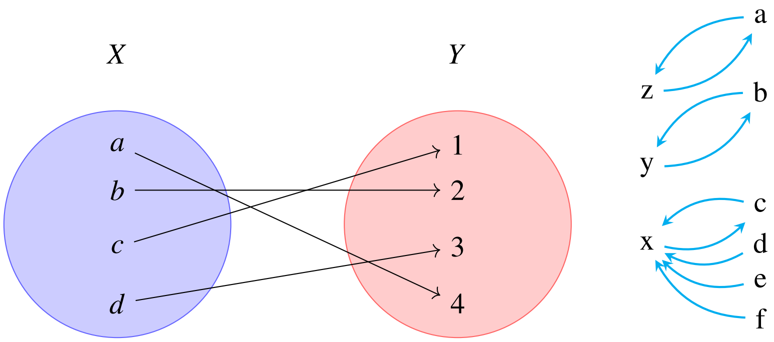


Figure 4: Graphs of some simple functions.

Definition 3.2. *Two functions $f:X\to Y$ and $g:U\to V$ are said to be* equal *if $X=U$, $Y=V$, and*

$$f(x)=g(x), \quad \textit{for all} \quad x\in X(=U). \tag{3.3}$$

Let $f:X\to Y$ be a function. We also call an element $x\in \mathrm{Dom}(f)$ an *argument* of the function f, and the element $y=f(x)\in Y$ is called the *image* of $x\in X$ under f. On the other hand, for $y\in Y$, the elements in the set $\{x\in X \mid f(x)=y\}$ are called the **preimages** of the element y. We write the set of preimages of an element $y\in Y$ as

$$f^{-1}(y):=\{x\in X \mid f(x)=y\} \tag{3.4}$$

More precisely, the notation f^{-1} is used later to write the *inverse of a function* f, which correspond to the case when $f^{-1}(y)$ contains exactly one element of X, for every $y\in Y$. Notice that it is possible that $f^{-1}(y)=\varnothing$, for some $y\in Y$.

3.2 Important Functions

Two related functions given in the next definition use archimedean property of the set $\mathbb{R}$.

Definition 3.3. *An integer-valued function* $\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z}$ *given by*

$$\lfloor x \rfloor = n, \quad \textit{if} \ \ x \geq n, \quad x \in \mathbb{R}, \tag{3.5}$$

is called the floor function, *and* $\lceil\ \rceil : \mathbb{R} \to \mathbb{Z}$ *given by*

$$\lceil x \rceil = n, \quad \textit{where} \ \ x \leq n, \quad x \in \mathbb{R}, \tag{3.6}$$

is called the ceiling function. *The floor function* $\lfloor\ \rfloor$ *is also known as the greatest integer function.*

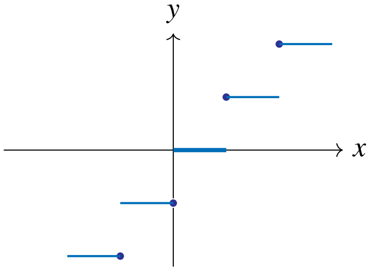


Figure 5: Graph of the greatest integer function $f(x) = \lfloor x \rfloor$.

The graph of each one of these two functions is like a *stair* (see Fig. 7). So, such types of functions are also known as the *stair functions*. Any assertion concerning the floor functions $\lfloor\ \rfloor$ is dealt with by taking $x = n + \varepsilon$, where $n = \lfloor x \rfloor \in \mathbb{Z}$ and $0 \leq \varepsilon < 1$. Similarly, while dealing with any assertion concerning the *ceiling functions*, we take $x = n - \varepsilon$, where $n = \lceil x \rceil \in \mathbb{Z}$ and $0 \leq \varepsilon < 1$. For example, we can apply these arguments to prove some interesting properties of the *stair functions* such as given in the next theorem. These relations are used very extensively in computer science.

Theorem 16. *For any* $x \in \mathbb{R}$,

1. $\lfloor x \rfloor = n \ \Leftrightarrow \ n \leq x < n+1$; $\lceil x \rceil = n \ \Leftrightarrow \ n-1 < x \leq n$.
2. $\lfloor x \rfloor = n \ \Leftrightarrow \ x-1 < n \leq x$; $\lceil x \rceil = n \ \Leftrightarrow \ x \leq n < x+1$.
3. $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$.
4. $\lfloor -x \rfloor = -\lceil x \rceil$ *and* $\lceil -x \rceil = -\lfloor x \rfloor$.
5. $\lfloor x+n \rfloor = \lfloor x \rfloor + n$ *and* $\lceil x+n \rceil = \lceil x \rceil + n$.

Also, *sequences* and *strings* are two special type of functions that find numerous applications in computer science and its allied branches. A *sequence* over a nonempty set X is an ordered list of elements of X, where the set of natural numbers $\mathbb{N}$ is used to order the *terms of the sequence*. More precisely, a **sequence** of elements of X is a function $s : \mathbb{N} \to X$ so that if

$$s(1) = x_1, \ \ s(2) = x_2, \ \ s(3) = x_3, \ldots \tag{3.7}$$

then we write the sequence s simply as $\big(x_n\big)$, where $x_n = s(n)$ is called the n-term of the sequence. As for functions, two sequences $s = \big(x_n\big)$ and $t = \big(y_n\big)$ are **equal** if $x_n = y_n$, for all $n \in \mathbb{N}$. In particular, when $X = \mathbb{R}$, we call s a *real sequence*; when $X = \mathbb{R}^2$, we call s a sequence of 2-dimensional vectors; when $X = \mathbb{R}^3$, we call s a sequence of 3-dimensional vectors; and, so on.

Example 3.1. *The following are some simple real sequences:*

1. $s_n = 2n+1$ *gives the sequence* $\big(3,5,7,\dots\big)$*;*

2. $s_n = (-1)^n \dfrac{n^2-1}{n}$ *gives the sequence* $\big(0,-3/2,8/3,\dots\big)$*;*

3. $s_n = \begin{cases} \dfrac{1-n}{2}, & \textit{if } n \textit{ is odd} \\ \dfrac{n}{2}\ , & \textit{if } n \textit{ is even} \end{cases}$ *gives the sequence* $\big(0,1,-1,2,-2,\dots\big)$*;*

4. $s_n = cos\, n\pi = (-1)^n$ *gives the sequence* $\big(-1,1,-1,\dots\big)$*;*

5. $s_n = \ln n$*.*

Notice that the sequence in (3) *gives a* listing *of elements of the set of integers* $\mathbb{Z}$ *as* $0,\ 1,\ -1,\ 2,\ -2,\ \dots$*. Also, the sequence in* (4) *lists* discrete values *of the continuous function* $f(x) = \cos(\pi x)$*,* $x \in \mathbb{R}$*, at the points* $n = 1,2,3,\dots$*. Such a process in certain applications is called* sampling*.*

On the other hand, **strings** over a finite set of alphabets is a special type of finite sequence that find applications in computer science and also in some other fields such as *genomics* (see Example 6.4).

Notice that the function in next definition is not *formula based.*

Definition 3.4 (Characteristic Function)**.** *Let X be a nonempty set, and $A \subseteq X$. The* characteristic function[7] *of the set A, denoted by χ_A, is a function $\chi_A : X \to \{0,1\}$ given by*

$$\chi_A(x) = \begin{cases} 1, & \textit{if } x \in A \\ 0, & \textit{if } x \in X - A \end{cases}, \tag{3.8}$$

It is also known as the indicator function *of the set A.*

The next theorem proves useful in several interesting situations.

Theorem 17. *Let X be a nonempty set, and $A,B \subseteq X$. The following relations hold:*

1. $\chi_{A\cap B} = \chi_A \cdot \chi_B$*;*

2. $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$*;*

[7] Such type of function plays an important role in Lebesgue's theory of integration.

3. $\chi_{A^c} = 1 - \chi_A$*;*

4. $\chi_{A \vee B} = \chi_A + \chi_B - 2\chi_A \cdot \chi_B$*;*

5. $a\chi_A + b\chi_B = a\chi_{A-B} + (a+b)\chi_{A\cup B} + b\chi_{B-A}$*, for any real numbers a and b.*

3.3 Important Properties

Let X and Y be two nonempty sets. The definitions given below are important.

1. A function $f : X \to Y$ is called an **injective function** (or a **one-one function**) if each pair of distinct elements in the set $X := \mathrm{Dom}(f)$ has distinct images in the set Y. That is, for any $x_1, x_2 \in X$,

$$x_1 \neq x_2 \qquad \Rightarrow \qquad f(x_1) \neq f(x_2). \tag{3.9}$$

2. A function $f : X \to Y$ is called a **surjective function** (or an **onto function**) if every element of the set Y has a preimage in X. That is, $\mathrm{Ran}(f) = Y$. We call a function $f : X \to Y$ an *into function* when it is not an onto function. Notice that, in this case, we have $\mathrm{Ran}(f) \subset Y$.

3. A function $f : X \to Y$ is called a **bijective function** (or simply a **bijection**) if f is both an injective and a surjective function.

4. Two sets X and Y are said to be in **bijective correspondence** if there is a bijection $f : X \to Y$.

In actual practice, while showing that a function is injective , we use the following contrapositive statement of the implication given in (3.9): For $x_1, x_2 \in X$,

$$f(x_1) = f(x_2) \qquad \Rightarrow \qquad x_1 = x_2. \tag{3.10}$$

For illustration, see the next example, and solution of Q. **??**. Also, when both X and Y are finite sets, (4) implies that $|X| = |Y|$. In particular, it follows that an injective function $f : X \to Y$ can not be an surjective function if Y has at least one more element than the set X. Therefore, there are many injective functions that are not surjective, and vice-versa. The function defined in the next example is an important *bijective function*.

Q 18. *Let A and B be two sets such that* $|A| = |B|$*. Prove that a function* $f : A \to B$ *is an injective function if and only if it is a surjective function.*

Sol. In general, if $f : A \to B$ is injective, we have $|A| \leq |B|$. However, since $|A| = |B|$, we have $\mathrm{Ran}(f) = B$. Thus, f is a surjective function. Conversely, if $f : A \to B$ is surjective, we have $\mathrm{Ran}(f) = B$ so that $|A| \geq |B|$. However, since $|A| = |B|$, no element $b \in B$ has more than one pre-image. Hence, f is an injective function. ♢

Q 19. *Let $f : A \to B$ and $g : B \to C$ be two functions such that the composite function $g \circ f : A \to C$ is a bijective function. Prove that f is injective, and g is surjective. Give an example to show that converse may not be true.*

Sol. We first prove that f is injective. For, let $f(a_1) = f(a_2)$, for $a_1, a_2 \in A$. Then we have

$$g\big(f(a_1)\big) = g\big(f(a_2)\big) \quad \Rightarrow \quad \big(g \circ f\big)(a_1) = \big(g \circ f\big)(a_2) \quad \Rightarrow \quad a_1 = a_2,$$

because $g \circ f$ is injective. To complete the solution, we show that g is surjective. For, let $c \in C$. Now, as $g \circ f : A \to C$ is surjective, there is some $a \in A$ such that $g \circ f(a) = c$. Finally, taking $b = f(a)$, we have $g(b) = c$. For a counter-example to disprove the converse, take $A = B$, $f = I_A$, $C = \{c\}$, and $g : A \to C$ the constant function. ♢

Q 20. *Show that the function $f : \mathbb{N} \to \mathbb{Z}$ given by*

$$f(n) = \begin{cases} n/2, & \text{if } n \text{ is even} \\ (1-n)/2, & \text{if } n \text{ is odd} \end{cases}$$

is a one-one and onto function.

Sol. We first show that f is one-one. Clearly, when integers n and m are of opposite parity, we have $f(n) \neq f(m)$. Next, let $f(n) = f(m)$, when n and m have the same parity. Now, if both n and m are even, then we obtain $n/2 = m/2$, and so $n = m$. The same conclusion is obtained when both n and m are odd. To prove f is onto, we have $2m \in \mathbb{N}$ when $m \in \mathbb{Z}$ is positive, and so $f(2m) = m$. We also have $1 - 2m \in \mathbb{N}$ when $m \in \mathbb{Z}$ is zero or negative, and so $f(1-2m) = m$, because $1 - 2m$ is odd. Notice that odd natural numbers $1, 3, 5, 7, \ldots$ are respectively mapped to non-positive integers $0, -1, -2, -3, \ldots$, whereas even natural numbers $2, 4, 6, 8, \ldots$ are respectively mapped to positive integers $1, 2, 3, 4, \ldots$. Hence, f is a bijective function. ♢

3.4 Composition & Inverse

We start with the next definition.

Definition 3.5. *The **composition** of two functions $f : X \to Y$ and $g : Y \to Z$, denoted by $g \circ f : X \to Z$ (see Fig. 6), is the function given by*

$$\big(g \circ f\big)(x) = g\big(f(x)\big), \quad \textit{for all} \quad x \in X. \tag{3.11}$$

Example 3.2. *The* composition *of functions $f : \mathbb{N} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ respectively given by*

$$f(n) = n - 2 \qquad \textit{and} \qquad g(n) = n^2,$$

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "g\circ f"'] & & Y \arrow[dl, "g"] \\
& Z &
\end{tikzcd}$$

Figure 6: Composition of functions.

is given by

$$\big(g\circ f\big)(n) = g\big(f(n)\big) = g(n-2) = (n-2)^2 = n^2-4n+4.$$

On the other hand, though the codomain of the function g is the set $\mathbb{Z}$, yet we can compute the composition $f\circ g$ (in reverse order) because we have

$$\text{Ran}\,\big(g\big) = \big\{n^2 \mid n\in\mathbb{Z}\big\} \subset \mathbb{N}.$$

In this case, we have

$$\big(f\circ g\big)(n) = f\big(g(n)\big) = f(n^2) = n^2-2.$$

Incidently, it is found that $f\circ g \neq g\circ f$, mainly due to the following two reasons:

(a) their values are different;

(b) the domains of $f\circ g$ and $g\circ f$ are not the same set.

In general, while verifying that the composition of two functions is same, we must ensure none of the above two conditions hold.

Theorem 21. *Let $f : X \to Y$ and $g : Y \to Z$ be any two functions.*

1. *If both f and g are injective then so is the composition $g\circ f$.*

2. *If both f and g are surjective then so is the composition $g\circ f$.*

3. *If both f and g are bijections,, then so is the composition $g\circ f$.*

We next consider the following general question: *Given a function $f : X \to Y$, does there exists a function $g : Y \to X$ that will undo the effect of the function f?*

Definition 3.6. *Let X and Y be two nonempty sets, and $f : X \to Y$ be a function. We say $g : Y \to X$ is an* inverse function *of f if*

$$g\circ f = I_X \quad \textit{and} \quad f\circ g = I_Y. \tag{3.12}$$

In this case, we write $g = f^{-1}$. We say a function $f : X \to Y$ is invertible *if it has an inverse.*

We remark that if a function $f : X \to Y$ is invertible, with $g : Y \to X$ as an inverse, then g is necessarily *unique*. For, suppose there are two functions $g_1, g_2 : Y \to X$ satisfying the conditions as in (3.12). That is,

$$f \circ g_1 = I_Y,\ \ g_1 \circ f = I_X \quad \text{and} \quad f \circ g_2 = I_Y,\ \ g_2 \circ f = I_X.$$

Then, we have

$$g_1 = g_1 \circ I_Y = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = I_X \circ g_2 = g_2.$$

This proves our assertion.

Example 3.3. *By the reasoning given earlier in Q. 20, it follows that the function g given by*

$$g(m) := \begin{cases} 2m, & \text{if } m \geq 1 \\ 1 - 2m, & \text{if } m \leq 0 \end{cases}$$

is the inverse of the function f.

The next theorem proves that, in general, a function is invertible if and only if it is bijective.

Theorem 22. *Let X and Y be two nonempty sets. A function $f : X \to Y$ has an inverse if and only if f is a bijective function.*

Proof. First, let there exists a function $g : Y \to X$ such that $g \circ f = I_X$ and $f \circ g = I_Y$. It then follows that f is bijective (see (a) of Exercise **??**). To prove the converse, suppose f is a bijective function. Then, for every $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$. We define $g : Y \to X$ by $g(y) = x$. It follows from the definition that g satisfies the conditions as in (3.12). Hence, g is the inverse of the function f. □

It follows easily that if $f : X \to Y$ is a bijective function then so is its inverse $f^{-1} : Y \to X$ (see (b) of Exercise **??**). The next theorem proves that the set operations are more well behaved with respect to inverse functions.

Theorem 23. *Let $f : X \to Y$ be an invertible function. Then*

1. $f^{-1}(A^c) = [f^{-1}(A)]^c$*; for all* $A \subseteq X$*;*
2. $\bigcup_\alpha f^{-1}(A_\alpha) = f^{-1}\left[\bigcup_\alpha A_\alpha\right]$*, for every class* $\{A_\alpha \subseteq X :\ \alpha \in I\}$*;*
3. $\bigcap_\alpha f^{-1}(A_\alpha) = f^{-1}\left[\bigcap_\alpha A_\alpha\right]$*, for every class* $\{A_\alpha \subseteq X :\ \alpha \in I\}$*.*

Q 24 (2021)**.** *Consider the three functions $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$, and $h : \mathbb{R}^* \to \mathbb{R}$ given by*

$$f(x) = 3x^2 + 2, \qquad g(x) = 7x - 5, \qquad h(x) = 1/x.$$

Compute the composite functions $f \circ g \circ h$, $g \circ g$, $g \circ h$, and $h \circ g \circ f$.

Definition 3.7. *The **Ackermann's function** $A(x,y)$ is the total function given by*

$$\begin{aligned} A\big(0,y\big) &= y+1, \\ A\big(x+1,0\big) &= A\big(x,1\big) \\ A\big(x+1,y+1\big) &= A\big(x,A(x+1,y)\big). \end{aligned}$$

The *Ackermann function* is an example of a recursive function that is not primitive recursive.

Q 25. *Compute the* Ackermann function $A(2,2)$.

Sol. For, by using the relation $A(0,y) = y+1$, we have

$$A(0,0) = 1, \quad A(0,1) = 2, \quad A(0,2) = 3,$$

$$A(0,3) = 4, \quad A(0,4) = 5, \quad A(0,5) = 6.$$

Next, by using the two relations given by

$$A(x+1,0) = A(x,1) \quad \text{and} \quad A(x+1,y+1) = A(x,A(x+1,y)),$$

it follows that

$$\begin{aligned} &A(1,0) = A(0,1) = 2; \\ &A(1,1) = A(0,A(1,0)) = A(0,2) = 3; \\ &A(1,2) = A(0,A(1,1)) = A(0,3) = 4; \\ &A(1,3) = A(0,A(1,2)) = A(0,4) = 5; \\ &A(1,4) = A(0,A(1,3)) = A(0,5) = 6; \\ &A(1,5) = A(0,A(1,4)) = A(0,6) = 7. \end{aligned}$$

Finally, by using the relation

$$A(x+1,y+1) = A(x,A(x+1,y)),$$

we obtain

$$\begin{aligned} &A(2,0) = A(1,1) = 3; \\ &A(2,1) = A(1,A(2,0)) = A(1,3) = 5; \\ &A(2,2) = A(1,A(2,1)) = A(1,5) = 7. \end{aligned}$$

Hence, we have $A(2,2) = 7$. ♢

4 Methods of Proof

As we shall see in a later section, the deductive reasoning based on Aristotle's syllogisms is central to a proof of a theorem. There are mainly two ways to establish the truth of a theorem of the form $p \Rightarrow q$. These are known as the method of *direct proof* and the method of *indirect proof*. The concepts we introduce in this part find applications to many situations discussed in the later parts of the course. The primary focus is to develop skills that help the reader know how to write and communicate a concise, clear, and complete proof of a theorem.

Definition 4.1. *We say $p \Rightarrow q$ is* trivially true *if the conclusion q holds regardless of the truth value of the premise p. In terms of symbolic logic discussed later in Section* **??***, we say*

$$q \rightarrow \big(p \rightarrow q\big)$$

is a tautology. Further, when premise p is a conjunction of premises $p_1, \ldots, p_n$ such that one or more p_i is false, the falsity of p implies that the implication $p \Rightarrow q$ is vacuously true*, mainly because the implication holds regardless of the truth value of q. In terms of symbolic logic, we say*

$$\neg p \;\rightarrow\; \big(p \rightarrow q\big)$$

is a tautology.

4.1 Methods of Direct Proof

Our first preference in all other situations must be to find a *direct proof*, based on axioms, related definitions, some known facts, and the *rules of inference*. It is convenient to write a direct proof of an implication $p \Rightarrow q$ especially when the hypotheses p can be translated into an expressions involving equations or inequalities so as to facilitate some further algebraic manipulations. We start with a well known fact as stated in the next theorem. Recall that two integers are said to have the same *parity* if both are odd or both are even. Otherwise, we say integers have the *opposite parity*.

Theorem 26. *The sum of any two integers of the same parity is an even integer, and the sum of any two integers of opposite parity is odd.*

Proof. We first suppose a and b are odd integers so that we can write

$$a = 2m+1 \qquad \text{and} \qquad b = 2n+1, \quad \text{for some} \quad m,n \in \mathbb{Z}.$$

Then, by associativity and commutativity of addition, we have

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

which is an even integer. We can prove other two assertions by similar argument. □

In the above proof, we mainly used the definitions when an integer to said to be odd or even. Further, we can also write the assertion of Theorem 26 as a *quantified statement* involving three single-variable predicates, each having the set of integers $\mathbb{Z}$ as universe of discourse.

Q 27. *Prove by the method of* direct proof *that, for any odd integers n, we have*

$$\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right),$$

where $\lfloor\ \rfloor$ *denotes the* floor function.

Sol. We can write $n = 2k+1$, for some integer k, so that

$$n^2 = 4k^2+4k+1 \qquad \Rightarrow \qquad \left\lfloor \frac{n^2}{4} \right\rfloor = \left\lfloor \frac{4k^2+4k+1}{4} \right\rfloor = k^2+k.$$

We also have

$$\frac{n-1}{2} = k \quad \text{and} \quad \frac{n+1}{2} = k+1 \qquad \Rightarrow \qquad \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right) = k^2+k.$$

Hence, the equality, as asserted. ♢

4.2 Mathematical Induction

The *principle of mathematical induction* is a typical *direct method* that helps verify the truth of a universal statement involving a set of non-negative integers. Other interesting method of direct proof is known as the *proof by cases*, which we shall discuss in the next section.

Principle of Mathematical Induction: If $p(n)$ is a proposition involving an integer n such that

1. $p(n)$ is true for some fixed positive integer $n = n_0$; and

2. $p(k) \Rightarrow p(k+1)$, for $k \geq n_0$.

Then $p(n)$ is true, for all $n \geq n_0$. We call (1) the **base step** of mathematical induction, and (2) is known as the **induction hypotheses**.

Q 28 (2020)**.** *Show that, for all $n \geq 2$,*

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}.$$

Sol. Let $P(n)$ be the predicate given by

$$P(n)\ :\quad \frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\cdots+\frac{1}{\sqrt{n}}>\sqrt{n}.$$

For the *base case*, since $\sqrt{1}<\sqrt{2}\ \Rightarrow\ \big(1/\sqrt{1}\big)>\big(1/\sqrt{2}\big)$, we have

$$P(2)\ :\quad \frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}>\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}=\frac{2}{\sqrt{2}}=\sqrt{2}.$$

Therefore, $P(2)$ is true. Now, suppose $P(n)$ holds for $n=k$. That is, we have

$$\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\cdots+\frac{1}{\sqrt{k}}>\sqrt{k}. \tag{4.1}$$

Next, we show that $P(n)$ holds for $n=k+1$. For, by (4.1), we have

$$\begin{aligned}
&\Big(\frac{1}{\sqrt{1}}+\cdots+\frac{1}{\sqrt{k}}\Big)+\frac{1}{\sqrt{k+1}}\\
&\qquad>\sqrt{k}+\frac{1}{\sqrt{k+1}}\\
&\qquad=\frac{k}{\sqrt{k}}+\frac{1}{\sqrt{k+1}}\\
&\qquad>\frac{k}{\sqrt{k+1}}+\frac{1}{\sqrt{k+1}} &&\text{(using } \sqrt{k}<\sqrt{k+1}\text{)}\\
&\qquad=\frac{k+1}{\sqrt{k+1}}=\sqrt{k+1}.
\end{aligned}$$

It thus follows that $P(n)$ also holds for $n=k+1$. Hence, $P(n)$ is true for all $n\geq 2$. ♢

Q 29 (2018)**.** *Show that, for all $n\geq 1$, we have*

$$3+33+\cdots+33\cdots 3\,(n\text{ times})=\frac{10^{n+1}-9n-10}{27}.$$

Sol. Let $P(n)$ be the predicate given by

$$P(n)\ :\quad 3+33+\cdots+33\cdots 3\,(n\text{ times})=\frac{10^{n+1}-9n-10}{27}.$$

For the *base case*, we have

$$P(1)\ :\quad 3=\frac{10^2-9-10}{27},$$

which is true. Next, suppose $P(n)$ holds for $n=k$. That is, we have

$$3+33+\cdots+33\cdots 3\,(k\text{ times})=\frac{10^{k+1}-9k-10}{27}. \tag{4.2}$$

We need to show that $P(n)$ also holds for $n = k+1$. For, we have

$$\begin{aligned}
3+\cdots+33\cdots3\,(k\text{ times})+33\cdots3\,((k+1)\text{times}) \\
&= \frac{10^{k+1}-9k-10}{27}+33\cdots3\,((k+1)\text{ times}) \qquad \text{(by (4.2))}\\
&= \frac{10^{k+1}-9k-10}{27}+\frac{99\cdots9\,((k+1)\text{ times})}{3}\\
&= \frac{10^{k+1}-9k-10}{27}+\frac{10^{k+1}-1}{3}\\
&= \frac{10^{k+1}-9k-10+9[10^{k+1}-1]}{27}\\
&= \frac{10^{k+2}-9(k+1)-10}{27},
\end{aligned}$$

which proves that $P(n)$ is true for $n = k+1$. Hence, $P(n)$ is true for all $n \geq 1$. ♢

Q 30. *Use* principle of mathematical induction *to prove that*

$$\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}, \quad \textit{for} \quad n\geq 1.$$

Sol. Suppose $P(n)$ is the statement

$$\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}.$$

Now, for $n = 1$, $P(1)$ is the statement

$$\frac{1}{1\cdot3}=\frac{1}{3},$$

which holds trivially. Suppose $P(n)$ holds for $n = k$. That is, we have

$$\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2k-1)(2k+1)}=\frac{k}{2k+1}. \tag{4.3}$$

To complete the proof by induction, we shall show that $P(n)$ holds for $n = k+1$. For, we have

$$\begin{aligned}
\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\cdots+\frac{1}{(2k-1)(2k+1)}+\frac{1}{(2k+1)(2k+3)} \\
&= \frac{k}{2k+1}+\frac{1}{(2k+1)(2k+3)} \qquad \text{(by (4.3))}\\
&= \frac{1}{(2k+1)(2k+3)}\Big[k\big(2k+3\big)+1\Big]\\
&= \frac{1}{(2k+1)(2k+3)}\Big[k\big(2k+1\big)+2k+1\Big]\\
&= \frac{k+1}{2(k+1)+1}
\end{aligned}$$

Hence, $P(n)$ is true for all $n \geq 1$. ♢

Q 31. *Use* principle of mathematical induction *to prove that*

$$\frac{n^3}{3}+\frac{n^5}{5}+\frac{7n}{15} \quad \textit{is a natural number, for all} \quad n \geq 1.$$

Sol. Suppose $P(n)$ is the statement

$$\frac{n^3}{3}+\frac{n^5}{5}+\frac{7n}{15} \quad \text{is a natural number.}$$

Now, for $n=1$, $P(1)$ is the statement

$$\frac{1}{3}+\frac{1}{5}+\frac{7}{15}=1 \quad \text{is a natural number,}$$

which holds trivially. Suppose $P(n)$ holds for $n=k$. That is, we have

$$\frac{k^3}{3}+\frac{k^5}{5}+\frac{7k}{15} \quad \text{is a natural number, say N.}$$

To complete the proof by induction, we shall show that $P(n)$ holds for $n=k+1$. For, we have

$$\begin{aligned}
&\frac{(k+1)^3}{3}+\frac{(k+1)^5}{5}+\frac{7(k+1)}{15}\\
&\quad=\frac{k^3}{3}+\frac{3k^2+3k+1}{3}+\frac{k^5}{5}+\frac{5k^4+10k^3+10k^2+5k+1}{5}+\frac{7k}{15}+\frac{7}{15}\\
&\quad=\frac{k^3}{3}+\frac{k^5}{5}+\frac{7k}{15}+\left(k^2+k\right)+\left(k^4+2k^3+2k^2+k\right)+\frac{1}{3}+\frac{1}{5}+\frac{7}{15}\\
&\quad=N+\left(k^2+k\right)+\left(k^4+2k^3+2k^2+k\right)+1,
\end{aligned}$$

which is a natural number. Hence, $P(n)$ is true for all $n \geq 1$. ♢

Strong Mathematical Induction

While applying an inductive proof, a common difficulty is about finding an appropriate *induction hypothesis*. The illustrations given below show that it is important to strengthen our induction hypothesis to include all for non-negative integers $\geq n_0$ (base value) up to n. We start with the next statement.

Principle of Strong Mathematical Induction: If $p(n)$ is a statement about non-negative integers $n \geq n_0$ such that

$$p(n_0),\, p(n_0+1),\, \ldots,\, p(n) \quad \Rightarrow \quad p(n+1),$$

then $p(n)$ is true, for all $n \geq n_0$.

We first use *strong mathematical induction* to prove the next theorem, which is known as the **fundamental theorem of arithmetic**.

Theorem 32. *Every integer $n > 1$ is a prime*[8] *or a product of the form*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t},$$

where each p_i is a prime divisor of n, and integers $k_i \geq 0$, for $i = 1, \ldots, t$. Further, since it can always be arranged to assume $p_1 < p_2 < \cdots < p_t$, the above representation of n is unique.

Proof. Since 2 is a prime number, the assertion holds trivially for $n = 2$. To complete the proof by applying above stated *strong induction*, we may assume that every integer $2 \leq k < n+1$ is a prime or a product of prime numbers. Next, if $n+1$ is a prime number, we are done. Otherwise, suppose we can write $n+1 = ab$, where a and b are integers satisfying the condition $1 < a, b \leq n$. Therefore, by our (strong) induction hypothesis, it follows that both a and b are prime numbers or a product of prime numbers. Hence, so is their product $ab = n+1$. □

4.3 Proof by Cases

A method of *direct proof* of a mathematical implications $P \Rightarrow Q$, also known as *proof by exhaustion*, is based on the idea that if $P = P_1 \vee \cdots \vee P_n$ (exhaustively), then the conclusion Q follows by proving all the implications $P_i \Rightarrow Q$ separately. As each implication $P_i \Rightarrow Q$ is called a *case*, hence the terminology *proof by cases*. The validity of a proof by this method is guaranteed by the logical equivalence such as given below:

$$\big[\big(P_1 \vee \cdots \vee P_n\big) \to Q\big] \quad \Leftrightarrow \quad \big[\big(p_1 \to Q\big) \vee \cdots \vee \big(p_n \to Q\big)\big].$$

Clearly, the method of *proof by cases* is manageable only when we have relatively smaller number of cases to deal with (also see Remark **??**). However, in some complex situations, it is possible that we may also have to apply other methods of proof such as *principle of mathematical induction* or even a *computer-aided proof*[9].

Q 33. *Use the method of proof* by cases *to show that*

$$n \textit{ is an odd integers} \qquad \Rightarrow \qquad n^4 \equiv 1\,(mod\ 16).$$

Sol. Let $n = 2k+1$, for some integer k. Then we have

$$n^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1 \equiv 24k^2 + 8k + 1\,(\text{mod } 16).$$

It thus suffices to show that, for any integer k, we have

$$3k^2 + k \equiv 0\,(\text{mod } 2),$$

[8] Recall that an integer $n > 1$ is a *prime number* if its only divisors are 1 and itself. Otherwise, we say n is a *composite number*.

[9] In artificial intelligence, an **expert system** refers to a program specifically designed to emulate the decision-making ability of a human on the basis of reasoning through bodies of knowledge, which help solve complex problems represented as an implication.

which follows directly because we can write $3k^2+k=k(3k+1)$. Notice that, for k odd, $3k+1$ is even. Hence $n^4 \equiv 1 \pmod{16}$. ♢

4.4 Methods of Indirect Proof

In most cases, whenever a direct proof of a statement is easy to obtain, it is more convenient to prove the *contrapositive statement*.

Method of Contrapositive

To begin with, in the next theorem, we prove a known assertion that is analogous to the statement of Theorem 26.

Theorem 34. *For all integers a and b, if the product ab is an even integer, then a or b is an even integer.*

Proof. We prove here the *contrapositive statement*: If a and b are two odd integers, then their product ab is also an odd integer. For, suppose a and b are two odd integers. Then, we can write

$$a=2m+1 \qquad \text{and} \qquad b=2n+1, \quad \text{for some} \quad m,n\in\mathbb{Z}.$$

By using the associativity and commutativity of addition, and also the fact that distributive property holds for integers, it follows that

$$ab=\big(2m+1\big)\big(2n+1\big)=2\,\big(2mn+m+n\big)+1,$$

which is an odd integer. □

By an argument same as above, it is easy to show that if x^2 is an even integer then so is the integer x.

In general, a *proof by contrapositive* is an interesting case of the method of *indirect proof*. In this case, we prove the contrapositive $\neg q \Rightarrow \neg p$ of an implication $p \Rightarrow q$. That is, we give a direct proof of the contrapositive statement

$$\neg q \quad \Rightarrow \quad \neg p.$$

The validity of proof by contrapositive follows from the fact that

$$p \Rightarrow q \;\equiv\; \neg q \Rightarrow \neg p.$$

The simplest such a case is as given in the next theorem.

Theorem 35. *For an integer n, we have n^2 is even implies n is even.*

Proof. Refer to class notes. □

Method of Contradiction

The *method of contradiction* is yet another interesting case of an *indirect method*, which assumes P and $\neg Q$ to be true, and derives a contradiction. In some cases, the only known proof of an implication is by contradiction. Such It is also known as the method of *reduction to absurdity* (or *reductio-ad-absurdum*, in Latin).

A *proof by contradiction* may be given when we don't succeed in finding a direct proof of a statement or its contrapositive. In this case, the hypotheses p is taken to be true and the conclusion q false, then we try to arrive at a contradiction. The validity of proof by contradiction follows from the fact that two propositions $\neg(P \wedge \neg Q)$ and $P \Rightarrow Q$ are equivalent. More precisely, if we show that $P \wedge \neg Q$ is false, then $\neg(P \wedge \neg Q)$ is true so that the proposition $P \Rightarrow Q$ is true too. We first give a proof of a classical result of Euclid by *method of contradiction*.

Theorem 36 (Euclid)**.** *There are infinitely many prime numbers.*

Proof. On the contrary, suppose there are only finitely many prime numbers, say $p_1, p_2, \dots, p_n$. Consider the integer

$$N = p_1 p_2 \cdots p_n + 1.$$

Clearly, $N > 1$. However, none of n prime numbers p_i divides N, which contradicts Theorem 32. This completes the proof. □

We next prove the well known fact that $\sqrt{2}$ is an irrational number.

Theorem 37. *$\sqrt{2}$ is not a rational number.*

Proof. If possible, suppose $\sqrt{2}$ is a rational number. That is, we may assume that

$$\sqrt{2} = \frac{p}{q}, \quad \text{with } p, q \in \mathbb{Z},\ q \neq 0,$$

such that p and q have no common factor. Squaring both sides of the above equation, we obtain $p^2 = 2q^2$. Thus, p^2 is even, and so p is even (Theorem 35). Let $p = 2k$, for some integer k. Therefore,

$$p^2 = 2q^2 \quad \Rightarrow \quad 4k^2 = 2q^2 \quad \Rightarrow \quad q^2 = 2k^2.$$

Once again, we can conclude that q is even, which contradicts the assumption that p and q have no common factor. Hence, $\sqrt{2}$ is an irrational number. □

We can also use method of contradiction to prove a number of known facts. The next theorem proves the weak form of the principle of mathematical induction.

Theorem 38. *If $p(n)$ is a proposition involving natural number n such that*

1. *$p(1)$ is true; and*

2. *$p(k) \Rightarrow p(k+1)$, for $k \geq 1$.*

Then we have $p(n)$ is true, for all $n \geq 1$.

`Proof.` For a contradiction, suppose n_0 is the first natural number such that $p(n_0)$ is not true. We may consider the set $S \subset \mathbb{N}$ consisting of all natural number m such that $p(m)$ is not true. As $n_0 \in S$, it is a nonempty subset of $\mathbb{N}$. Therefore, by *well ordering principle*, S contains a least natural number, say m_0. Notice that, by (1), we have $m_0 \geq 2$, and so $m_0 - 1 \in \mathbb{N} \setminus S$. That is, $p(m_0 - 1)$ is true. But then, by (2), $p(m_0)$ is true, which contradicts our choice of m_0. Hence, $p(n)$ is true for all $n \geq 1$. □

In the next theorem, we prove *division algorithm.*

Theorem 39 (Division Algorithm)**.** *For any two integers a and b, with $b > 0$, there exist unique integers q and r such that*

$$a = bq + r, \qquad \textit{where} \quad 0 \leq r < b.$$

`Proof.` More generally, consider the set

$$S := \big\{a + bx \mid x \in \mathbb{Z}\big\} \cap \mathbb{N}.$$

Since $b \in S$, it follows by *well ordering principle* that it contains its least element, say n_0. We may write $n_0 = a + bx_0$, for $x_0 \in \mathbb{Z}$. For a contradiction, suppose $n_0 \geq b$. But then, we have

$$n_0 - b \geq 0 \qquad \Rightarrow \qquad n_0 - b = a + b\big(x_0 - 1\big) \in S,$$

which contradicts the minimality of n_0. Therefore, we conclude that $0 \leq n_0 < b$. Hence, we may take $q = -x_0$ and $r = n_0$. Uniqueness follows easily. □

Corollary 40 (*Euclid Algorithm*)**.** *For any two* nonzero *integers a and b, there exist an integers d such that*

1. *$d = \mathrm{hcf}(a,b)$; and*

2. *for some integers x, y, we have $d = ax + by$.*

`Proof.` Notice that, as a or $-a$ is positive, we have that the set

$$S := \big\{ax + by \mid x, y \in \mathbb{Z}\big\} \cap \mathbb{N}$$

is nonempty. Therefore, by *well ordering principle*, S contains its least element, say d. Let $d = ax_0 + by_0$, with $x_0, y_0 \in \mathbb{Z}$. It remains to show that $d = \mathrm{hcf}(a,b)$. For, by Theorem 39, we can find integers q, r such that

$$a = dq + r, \qquad \text{with} \quad 0 \leq r < d.$$

However, if $r \neq 0$, then $r = a - d\,q \in S$ contradicts our choice of $d \in S$. So, we must have $r = 0$ so that $d\big|a$. Similarly, it can be shown that $d\big|b$. Finally, for any integer c,

$$c \;\text{ divides both } a \text{ and } b \quad \Rightarrow \quad c \;\text{ divides }\; a\,x_0 + b\,y_0 = d,$$

which completes the proof. □

The next fact due to Euclid will prove useful in the sequel.

Lemma 4.1 (*Euclid Lemma*)**.** *For any two integers a and b, and a prime number p,* $p\big|ab$ *implies* $p\big|a$ *or* $p\big|b$.

Remark 4.1. *A typical idea that comes very handy in many situations is called the* pigeon-hole principle*, which is also known as the* Dirichlet box principle*. It is an interesting special case of the method of* non-constructive *indirect proof. We will discuss this principle later in Section* **??**.

Proof by Counterexamples

5 Binary Operations, Groups, Rings, & Fields

5.1 Semigroup and Monoid

Q 41. *On the set of rational elements $\mathbb{Q}$, define a binary operation $*$ as*

$$a*b := a+b+ab, \qquad \textit{for} \quad a,b \in \mathbb{Q}.$$

Show that $(\mathbb{Q},*)$ is an Abelian monoid. Also, find all its invertible elements.

Sol. Clearly, operation $*$ satisfies the *closure property* because $a+b+ab \in \mathbb{Q}$, for all $a,b \in \mathbb{Q}$. We also have

$$a*b = a+b+ab = b+a+ba = b*a, \qquad \text{for} \quad a,b \in \mathbb{Q}.$$

That is, the operation $*$ is commutative. Next, to prove that $*$ is *associative*, let $a,b,c \in \mathbb{Q}$. Then, by definition of $*$, we have

$$\begin{aligned}
\big(a*b\big)*c &= \big(a+b+ab\big)*c \\
&= a+b+ab+c+\big(a+b+ab\big)c \\
&= a+b+c+ab+bc+ac+abc; \\
a*\big(b*c\big) &= a*\big(b+c+bc\big) \\
&= a+b+c+bc+a\big(b+c+bc\big)c \\
&= a+b+c+ab+bc+ac+abc,
\end{aligned}$$

which proves associativity of the operation $*$. Further, if $e \in \mathbb{Q}$ is the identity for the operation $*$, we must have

$$a*e = e*a = a, \qquad \text{for} \quad a \in \mathbb{Q}.$$

That is, we have

$$a = a*e = a+e+ae \qquad \Rightarrow \qquad e(1+a) = 0, \;\; \text{for} \quad a \in \mathbb{Q}.$$

The only way the above condition holds is when $e = 0$. Therefore, $(\mathbb{Q},*)$ is an Abelian monoid, with 0 as the *identity element*. Finally, if $a \in \mathbb{Q}$ is invertible element with respect to the operation $*$, then there is some $b \in \mathbb{Q}$ such that $a*b = b*a = 0$. That is,

$$a+b+ab = 0 \qquad \Rightarrow \qquad b = -\frac{a}{1+a}.$$

Therefore, every rational number $a \neq -1$ is *invertible* with respect to the operation $*$. ♢

Q 42. *On the set $M = \mathbb{Q}\times\mathbb{Q}$, define a binary operation $*$ as*

$$(a,b)*(x,y) := (ax, ay+b), \qquad \textit{for} \quad a,b,x,y \in \mathbb{Q}.$$

Show that $(M,*)$ is a ***non-commutative*** *monoid. Also, find all its invertible elements.*

Sol. As $ax, ay+b \in \mathbb{Q}$, for all $a,b,x,y \in \mathbb{Q}$, it follows that operation $*$ satisfies the *closure property*. Further, since

$$[(1,1)*(2,1) = (2,2) \neq (2,3) = (2,1)*(1,1),$$

we have that $*$ is *non-commutative*. Next, to prove that $*$ is *associative*, let $a,b,x,y,u,v \in \mathbb{Q}$. Then, by definition of $*$, we have

$$\begin{aligned} \big((a,b)*(x,y)\big)*(u,v) &= (ax, ay+b)*(u,v) \\ &= \big(axu, axv+ay+b\big); \\ (a,b)*\big((x,y)*(u,v)\big) &= (a,b)*(xu, xv+y) \\ &= \big(axu, axv+ay+b\big), \end{aligned}$$

which shows $*$ is an associativity operation. Now, suppose $(e_1,e_2) \in M$ is the identity for the operation $*$ so that we have

$$(a,b)*(e_1,e_2) = (e_1,e_2)*(a,b) = (a,b), \qquad \text{for all} \quad a,b \in \mathbb{Q}.$$

That is, for all $a,b \in \mathbb{Q}$, we have

$$a = ae_1 \ \text{ and } \ b = ae_2 + b \qquad \Rightarrow \qquad e_1 = 1 \ \text{ and } \ e_2 = 0.$$

Therefore, $(M,*)$ is a non-commutative monoid, with $(1,0) \in M$ as the *identity element*. Finally, when $(a,b) \in M$ is invertible element with respect to the operation $*$, we can find some $(x,y) \in M$ such that

$$(a,b)*(x,y) = (x,y)*(a,b) = (1,0).$$

That is, $ax = 1$ and $ay+b = 0$, which implies $x = 1/a$ and $y = -b/a$. Therefore, every element $(a,b) \in M$ is *invertible* with respect to the operation $*$, provided $a \neq 0$. ♢

5.2 Groups, Examples, and Properties

Q 43. *On the set of positive rational numbers $\mathbb{Q}^+$, define a binary operation $*$ as*

$$a*b := \frac{ab}{3}, \qquad \textit{for} \quad a,b \in \mathbb{Q}^+.$$

Show that $(\mathbb{Q}^+,*)$ is an Abelian group.

Sol. Clearly, operation $*$ satisfies the *closure property* because $ab/3 \in \mathbb{Q}^+$, for all $a,b \in \mathbb{Q}^+$. We also have

$$a*b = \frac{ab}{3} = \frac{ba}{3} = b*a, \qquad \text{for} \quad a,b \in \mathbb{Q}^+.$$

That is, the operation $*$ is commutative. Next, to prove that $*$ is *associative*, let $a,b,c \in \mathbb{Q}^+$. Then, by definition of $*$, we have

$$\begin{aligned}(a*b)*c &= \left(\frac{ab}{3}\right)*c \\ &= \frac{abc}{9}; \\ a*(b*c) &= a*\left(\frac{bc}{3}\right) \\ &= \frac{abc}{9},\end{aligned}$$

which proves associativity of the operation $*$. Further, if $e \in \mathbb{Q}^+$ is the identity for the operation $*$, we must have

$$a*e = e*a = a, \qquad \text{for} \quad a \in \mathbb{Q}^+.$$

That is, we have

$$a = a*e = \frac{ae}{3} \qquad \Rightarrow \qquad a\left(1-\frac{e}{3}\right) = 0, \ \text{ for } \ a \in \mathbb{Q}^+.$$

The only way the above condition holds is when $e = 3$. Therefore, $(\mathbb{Q},*)$ is an Abelian monoid, with 3 as the *identity element*. Finally, if $a \in \mathbb{Q}^+$ is invertible element with respect to the operation $*$, then there is some $b \in \mathbb{Q}^+$ such that $a*b = b*a = 3$. That is,

$$\frac{ab}{3} = 3 \qquad \Rightarrow \qquad b = \frac{9}{a}.$$

Therefore, every rational number $a \in \mathbb{Q}^+$ is *invertible* with respect to the operation $*$. Hence, $(\mathbb{Q}^+,*)$ is an Abelian group. ♢

$+_4$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{3}$	$\underline{0}$	$\underline{1}$
$\underline{3}$	$\underline{3}$	$\underline{0}$	$\underline{1}$	$\underline{2}$

$\times_4$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$
$\underline{2}$	$\underline{0}$	$\underline{2}$	$\underline{0}$	$\underline{2}$
$\underline{3}$	$\underline{0}$	$\underline{3}$	$\underline{2}$	$\underline{1}$

Table 2: Multiplication Table for the operations $+_4$ and $\times_4$ on the set $\mathbb{Z}_4$.

Q 44. *Write* <u>*multiplication tables*</u> *for the set of congruence classes* $\mathbb{Z}_4$ *with respect to* addition modulo 4 *(denoted by* $+_4$*) and* multiplication modulo 4 *(denoted by* $\times_4$*).*

1. *Is* $(\mathbb{Z}_4,+_4)$ *a group ? Justify your answer.*

2. *Show that* $(\mathbb{Z}_4\setminus\{0\},\times_4)$ *is not a group.*

Sol. The two *multiplication tables* are as given in Table 2. Yes, $\big(\mathbb{Z}_4, +_4\big)$ is a group, with identity $\underline{0}$. As we can see from the left side table, the inverse of elements $\underline{1}, \underline{2}, \underline{3}$ with respect to the operation $+_4$ are respectively the elements $\underline{3}, \underline{2}, \underline{1}$. However, the set of *nonzero* congruence classes $\mathbb{Z}_4 \setminus \{0\}$ is not a group with respect to the operation $\times_4$. For, as we can see from the right side table, inverse of $\underline{2}$ doesn't exists. ♢

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Table 3: Multiplication Table for the group C_4.

Q 45. *Let $i := \sqrt{-1}$. Show that the set $C_4 = \big\{1, -1, i, -i\big\}$ is a cyclic group with respect to usual multiplication of complex numbers. What are all generators of C_4.*

Sol. The *multiplication table* of the set $C_4 = \big\{1, -1, i, -i\big\}$ with respect to usual multiplication $(\cdot)$ of complex numbers is as shown in Table 3. It is clear from the table that $\big(C_4, \cdot\big)$ is a group, with identity element 1 and

$$(-1)^{-1} = -1, \qquad (i)^{-1} = -i, \quad \text{and} \quad (-i)^{-1} = i.$$

Further, since we have

$$i^1 = i, \qquad i^2 = -1, \qquad i^3 = -i, \quad \text{and} \quad i^4 = 1;$$
$$\big(-i\big)^1 = -i, \qquad \big(-i\big)^2 = -1, \qquad \big(-i\big)^3 = i, \quad \text{and} \quad \big(-i\big)^4 = 1,$$

it follows that $\big(C_4, \cdot\big)$ is a cyclic group with each i and $-i$ as a generator. ♢

Q 46. *Let $(G, *)$ be a group. Prove that, for all $a, b \in G$, we have*

1. $\big(a^{-1}\big)^{-1} = a$;
2. $\big(a * b\big)^{-1} = b^{-1} * a^{-1}$.

Sol. Let $e \in G$ denotes the identity element. For (1), we know that an element $x \in G$ is the inverse of a if we have

$$a * x = x * a = e$$

In this case, we write $x = a^{-1}$. Also, the same condition says that a is the inverse of x. That is, $a = x^{-1}$. It thus follows that $a = x^{-1} = \big(a^{-1}\big)^{-1}$, as asserted. For (2), we have

$$\big(a * b\big) * \big(b^{-1} * a^{-1}\big) = a * \big(b * b^{-1}\big) * a^{-1} = a * \big(e\big) * a^{-1} = a * a^{-1} = e.$$

Similarly, we can see that $\big(b^{-1} * a^{-1}\big) * \big(a * b\big) = e$. Therefore, inverse of the element $a * b \in G$ is given by $b^{-1} * a^{-1}$. This completes the solution. ♢

Subgroups, Cosets, Lagrange Theorem

Q 47. *Show that the intersection of any two subgroups of a group is also a subgroup of the group. Give an example of a group that has two subgroups whose union is* not *a subgroup.*

Sol. Let H and K be two subgroups of a group G, and $x,y \in H \cap K$. Then $x,y \in H$, and also $x,y \in K$, so that we have

$$x * y^{-1} \in H \qquad \text{and} \qquad x * y^{-1} \in K,$$

because both H and K are subgroups. Therefore, $x * y^{-1} \in H \cap K$. Hence $H \cap K$ is a subgroup. For the second part of the question, take $G = (\mathbb{Z}, +)$ and consider the subgroups $2\mathbb{Z}$ and $3\mathbb{Z}$. Notice that $2,3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, but $2-3=-1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Therefore, the union $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subgroup of $(\mathbb{Z}, +)$. ♢

Q 48. *Compute all cosets of the subgroup $H = 5\mathbb{Z}$ in the group $(\mathbb{Z}, +)$. What is the* index $[G:H]$.

Sol. The *distinct cosets* of the subgroup $5\mathbb{Z}$ in the Abelain group $(\mathbb{Z}, +)$ are given by

$$\begin{aligned}
0+5\mathbb{Z} &= \{\,\dots,-15,-10,-5,0,5,10,15,\dots\,\} = 5+5\mathbb{Z} = 10+5\mathbb{Z} = \cdots;\\
1+5\mathbb{Z} &= \{\,\dots,-14,-9,-4,1,6,11,16,\dots\,\} = 6+5\mathbb{Z} = 11+5\mathbb{Z} = \cdots;\\
2+5\mathbb{Z} &= \{\,\dots,-13,-8,-3,2,7,12,17,\dots\,\} = 7+5\mathbb{Z} = 12+5\mathbb{Z} = \cdots;\\
3+5\mathbb{Z} &= \{\,\dots,-12,-7,-2,3,8,13,18,\dots\,\} = 8+5\mathbb{Z} = 13+5\mathbb{Z} = \cdots;\\
4+5\mathbb{Z} &= \{\,\dots,-11,-6,-1,4,9,14,19,\dots\,\} = 9+5\mathbb{Z} = 14+5\mathbb{Z} = \cdots.
\end{aligned}$$

It thus follows that the *index* $[G:H] = 5$. ♢

Q 49. *Consider the elements $\alpha = (13562)$ and $\beta = (1523)(46)$ of the permutation group S_6. Compute the elements $\alpha^{-1} \circ \beta \circ \alpha$ and $\beta^{-1} \circ \alpha \circ \beta$, where $\circ$ denotes the* composition *of functions.*

Sol. In *two-row* notation, the inverse of a permutation is obtained by reading pre-images of elements $1,2,\dots,6$ from the *second row*. For example, we have

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix} \qquad \Rightarrow \qquad \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix} = (12653);$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix} \qquad \Rightarrow \qquad \beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix} = (1325)(46)$$

It thus follows that we have

$$\begin{aligned}\alpha^{-1}\beta\alpha &= (12653)\circ\big[(1523)(46)\circ(13562)\big]\\ &= (12653)\circ(16425)\\ &= (1536)(24);\\ \beta^{-1}\alpha\beta &= (1325)(46)\circ\big[(13562)\circ(1523)(46)\big]\\ &= (1325)(46)\circ(25463)\\ &= (12435)\end{aligned}$$

This completes the solution. ♢

Q 50. *State and prove* Lagrange Theorem. *Hence deduce that every group of prime order is cyclic.*

Sol. The statement of the Lagrange Theorem is as follows: *Let G be a finite group, and H be a subgroup of G. Then $o(H)$ divides $o(G)$.* For a proof, we use H to define a relation $\sim$ on G as follows:

$$x\sim y \qquad \Leftrightarrow \qquad xy^{-1}\in H.$$

Now, as $e = xx^{-1}\in H$, for all $x\in G$, it follows that the relation $\sim$ is reflexive. Next, suppose $x\sim y$ so that we have $xy^{-1}\in H$. But then, since H is a subgroup, we also have $yx^{-1} = \big(xy^{-1}\big)^{-1}\in H$. So, $y\sim x$. That is, the relation $\sim$ is symmetric. To show that the relation $\sim$ is transitive, let $x\sim y$ and $y\sim z$, for $x,y,z\in G$. Then we have $xy^{-1}\in H$ and also $yz^{-1}\in H$. Once again, since H is a subgroup, we have

$$xz = xez = x\big(yy^{-1}\big)z = \big(xy^{-1}\big)\big(yz^{-1}\big)\in H.$$

Therefore, $x\sim z$. Hence, $\sim$ is an equivalence relation on G. Further, for any $x\in G$, we have

$$\big[x\big] := \big\{y\in G \mid\ y\sim x\big\} = \big\{y\in G \mid\ yx^{-1}\in H\big\} = Hx.$$

That is, the *disjoint* equivalence class of G with respect to the relation $\sim$ are precisely the *distinct* right cosets of the subgroup H in G. It thus follows that

$$o(G) = \sum_{i=1}^{k} o(Hx_i), \qquad \text{where} \quad k = \big[G:H\big].$$

Finally, using the fact that each right coset Hx_i contains exactly the same number of elements as there are in the subgroup H, we conclude that

$$o(G) = o(H)+o(H)+\cdots+o(H)\ (k \text{ times}) = o(H)\big[G:H\big].$$

Hence, we have shown that $o(H)$ divides $o(G)$.

For the second part, let $o(G) = p$, where p is prime number. As $p \geq 2$, choose some $e \neq x \in G$, and consider the cyclic subgroup

$$H = \langle x \rangle = \{e, x, x^2, \dots\}.$$

By Lagrange Theorem, we have $o(H)$ divides $o(G) = p$. That is, $o(H) = 1$ or p. However, as $x \neq e$, we must have $o(H) = p$. Hence, $G = H$ is itself a cyclic group. ♢

Normal Subgroups and Homomorphisms

Q 51. *Let H be a subgroup of a group G. Show that H is a normal subgroup if and only if $g^{-1}hg \in H$, for all $h \in H$ and $g \in G$.*

Sol. We first assume that H is a normal subgroup. That is, by definition, we have

$$gH = Hg \quad \text{or, equivalently,} \quad H = g^{-1}Hg, \qquad \text{for all} \quad g \in G.$$

In particular, $g^{-1}Hg \subseteq H$ implies that $g^{-1}hg \in H$, for all $h \in H$ and $g \in G$. Therefore, the condition holds. Conversely, suppose we have

$$g^{-1}hg \in H, \qquad \text{for all} \quad h \in H \ \text{ and } \ g \in G.$$

In particular, if follows that $g^{-1}Hg \subseteq H$, and so $Hg \subseteq gH$, for all $g \in G$. Now, let $x = gh \in gH$. Then, we have $x = \left(g^{-1}\right)^{-1}hg^{-1}g = h_1 g \in Hg$, where $h_1 = \left(g^{-1}\right)^{-1}hg^{-1} \in H$, by the given condition. We have thus shown that $gH = Hg$, for all $g \in G$. Hence, H is a normal subgroup. ♢

Q 52. *Consider the subgroup $H = \{e, (2\,3)\}$ of the permutation group S_3 given by*

$$S_3 := \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

Show that H is <u>not</u> a normal subgroup of S_3. Futher, show that the subgroup

$$K := \{e, (1\,2\,3), (1\,3\,2)\}$$

is a normal subgroup of the group S_3.

Sol. Recall that $e = \big(1\big)\big(2\big)\big(3\big)$ is the identity function of the set $\{1, 2, 3\}$. Also, we may use the notations as given below:

$$\rho_1 = \big(132\big), \quad \rho_2 = \big(123\big), \quad \tau_1 = \big(23\big), \quad \tau_2 = \big(13\big), \quad \tau_3 = \big(12\big).$$

Then the *multiplication table* for the group $(S_3, \circ)$ is as show in Table 4, where $\circ$ denotes the *composition* of functions. Now, it follows directly from the table that we have

$$\rho_1 \circ H = \{\rho_1, \tau_3\} \quad \text{and} \quad H \circ \rho_1 = \{\rho_1, \tau_2\}.$$

Therefore, $\rho_1 \circ H \neq H \circ \rho_1$ implies that H is not a normal subgroup of S_3. However, for the subgroup K, we have

$$\begin{aligned} \tau_1 \circ K &= \{\tau_1, \tau_2, \tau_3\} \quad \text{and} \quad K \circ \tau_1 = \{\tau_1, \tau_3, \tau_2\}; \\ \tau_2 \circ K &= \{\tau_2, \tau_3, \tau_1\} \quad \text{and} \quad K \circ \tau_2 = \{\tau_2, \tau_1, \tau_3\}; \\ \tau_3 \circ K &= \{\tau_3, \tau_1, \tau_2\} \quad \text{and} \quad K \circ \tau_3 = \{\tau_3, \tau_2, \tau_1\}. \end{aligned}$$

It thus follows that K is a normal subgroup of the group S_3. ♢

$\circ$	e	ρ_1	ρ_2	τ_1	τ_2	τ_3
e	e	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	e	τ_3	τ_1	τ_2
ρ_2	ρ_2	e	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	e	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	e

Table 4: Multiplication Table for S_3 with respect to composition $\circ$ as operation.

5.3 Rings and Fields

Try to memorise all *definitions* and *examples* given in this section.

Q 53. *Define* ring*, and give an example.*

Sol. A **ring** is a nonempty set R, together with two binary operations $+$ (sum) and $\cdot$ (product), such that

1. $(R,+)$ is an Abelian group, where the additive identity $0 \in R$ is called the **zero element** of the ring R;
2. $(R,\cdot)$ is a semigroup ;
3. the product $(\cdot)$ distributes over sum $(+)$. That is, for all $a,b,c \in R$, we have

$$a \cdot (b+c) = a \cdot b + a \cdot c; \qquad (a+b) \cdot c = a \cdot c + b \cdot c.$$

Since the set of integers $\mathbb{Z}$ satisfies all above properties with respect to usual addition $(+)$ and usual multiplication $(\times)$ of integers. So, $(\mathbb{Z},+,\cdot)$ is an example of a ring, which is called the **ring of integers**. (In general, we write a ring as $(R,+,\cdot)$) ♢

In fact, there are several other examples of rings of interest in computer science.

1. Each number set $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are rings with respect to usual addition $(+)$ and usual multiplication $(\times)$. These are collectively called **number rings**. In particular, we have the *ring of rational numbers, ring of real numbers*, and *ring of complex numbers*, which are written respectively as $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, and $(\mathbb{C}, +, \times)$.

2. The set of *integer modulo n* $\mathbb{Z}_n$ is a ring with respect to two binary operations $+_n$ (*addition modulo n*) and $\times_n$ (*multiplication modulo n*), as defined in an earlier section. In this case, $\big(\mathbb{Z}_n, +_n, \times_n\big)$ is called the **ring of integer modulo n**.

3. The set of all polynomials with coefficients drawn from a ring $(R, +, \cdot)$ is a ring with respect to two binary operations given by usual addition and multiplication of polynomials. This is called the **polynomial ring** over the ring R, and is denoted by $P\big[R\big]$. In particular, when R is any of the *ring of numbers* as mentioned in (1), we obtain concepts such as ring of *integer polynomials*, *rational polynomials*, *real polynomials*, and *complex polynomials*. Of course, in some applications such as related to coding theory and cryptography, we also use the polynomials over the *ring of integer modulo n*, especially when n is an integer power of a prime.

4. For any integer $m \geq 1$, the set of square matrices of order m with entries in some ring $(R, +, \cdot)$ is a ring with respect to two binary operations given by usual addition and multiplication of such matrices. This is called the **matrix ring** over the ring R, and is denoted by $M_m(R)$. In particular, when R is any of the *ring of numbers* as mentioned in (1), we obtain concepts such as *integer matrix ring*, *rational matrix ring*, *real matrix ring*, and *complex matrix ring*. Of course, in some advance applications, we also use the matrix ring over the ring of integer modulo n.

Definition 5.1. *A ring $(R, +, \cdot)$ is said to be **commutative** if the product $\cdot$ is commutative. That is, we have*

$$a \cdot b = b \cdot a, \qquad \textit{for all} \quad a, b \in R.$$

*A ring $(R, +, \cdot)$ is **non-commutative** if there is a pair of elements $x, y \in R$ such that $x \cdot y \neq y \cdot x$.*

All the number rings, ring of integer modulo n, and a polynomial ring over any number ring, are all examples of a *commutative ring*. On the other hand, for example, the ring of 2×2 real matrices is a non-commutative ring. For, we have

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \qquad \Rightarrow \qquad AB \neq BA.$$

Definition 5.2. *An element 1 in a ring $(R, +, \cdot)$ is called the **unity** if $(R, \cdot, 1)$ is a monoid. That is, we have*

$$1 \cdot a = a \cdot 1 = a, \qquad \textit{for all} \quad a \in R.$$

In this case, we also say that R is a ring with unity 1.

For example, since integer 1 is the multiplicative identity for each *number ring*, it follows that $1 \in \mathbb{Z}$ is the unity of each such types of rings. Similarly, $1 \in \mathbb{Z}_n$ is the unity of the *ring of integer modulo n*; the constant polynomial $1 \in P\big[\mathbb{R}\big]$ is the unity of the ring of *real polynomials*; and, the identity matrix $I \in M_m\big[\mathbb{R}\big]$ is the unity of the ring of *real matrices*.

Definition 5.3. *Let $(R,+,\cdot)$ be a commutative ring. A* nonzero element *$a \in R$ is called a **zero divisor** if for some* nonzero element *$b \in R$ we have $a \cdot b = 0$.*

For example, in the ring $(\mathbb{Z}_6, +_6, \times_6)$, we have

$$\underline{2} \cdot \underline{3} = \underline{0} \qquad \text{and also} \qquad \underline{3} \cdot \underline{4} = \underline{0}.$$

Therefore, the commutative ring $(\mathbb{Z}_6, +_6, \times_6)$ has three *zero divisors*, namely, $\underline{2}, \underline{3}$, and $\underline{4}$ (see Table 5).

Table 5: Multiplication Table for the operation $\times_6$ on the set $\mathbb{Z}_6$.

$\times_6$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{5}$
$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$	$\underline{0}$
$\underline{1}$	$\underline{0}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{4}$	$\underline{5}$
$\underline{2}$	$\underline{0}$	$\underline{2}$	$\underline{4}$	$\underline{0}$	$\underline{2}$	$\underline{4}$
$\underline{3}$	$\underline{0}$	$\underline{3}$	$\underline{0}$	$\underline{3}$	$\underline{0}$	$\underline{3}$
$\underline{4}$	$\underline{0}$	$\underline{4}$	$\underline{2}$	$\underline{0}$	$\underline{4}$	$\underline{2}$
$\underline{5}$	$\underline{0}$	$\underline{5}$	$\underline{4}$	$\underline{3}$	$\underline{2}$	$\underline{1}$

Definition 5.4. *Let $(R,+,\cdot)$ be a ring with unity 1. An element $u \in R$ is called a **unit** if there is some $v \in R$ such that*

$$u \cdot v = v \cdot u = 1.$$

Said differently, u is invertible with respect to the product $\cdot$. Clearly, $u \neq 0$.

For example, every nonzero element in any number rings such as $(\mathbb{Q},+,\times), (\mathbb{R},+,\times)$, or $(\mathbb{C},+,\times)$ is a unit. Also, every matrix in the ring of 2×2 real matrices with nonzero determinant is a unit.

Definition 5.5. *A commutative ring $(R,+,\cdot)$ with unity 1 is called a **field** if every nonzero element in F is a unit.*

For example, number rings such as $(\mathbb{Q},+,\times), (\mathbb{R},+,\times)$, or $(\mathbb{C},+,\times)$, are all examples of a field. Also, the ring $(\mathbb{Z}_n, +_n, \times_n)$ of integer modulo n is a field if n is a prime.

Q 54. *Find the zero divisors and units of the ring $(\mathbb{Z}_6, +_6, \times_6)$.*

Sol. The *multiplication table* for the operation $\times_6$ on the set $\mathbb{Z}_6$ is as shown in Table 5. It follows from this table that $\underline{2}, \underline{3}$, and $\underline{4}$ are *zero divisors*, and $\underline{5}$ is the only unit, with respect to the operation $\times_6$. $\diamondsuit$

Q 55. *Prove that every finite integral domain is a field.*

Sol. Let R be a finite integral domain so that we can write

$$R = \{0 = a_1, 1_R = a_2, a_3, \ldots, a_n\},$$

where 1_R is the *unit element* of R. Now, for any $i \neq 1$, we have $a_i a_j \neq 0$, for any $j = 2, \ldots, n$, because R has no zero divisors. Therefore, we must have

$$a_i a_j = 1_R, \qquad \text{for some} \quad j = 2, \ldots, n.$$

Hence, every nonzero element of R is a unit. That is, R is a field. $\diamondsuit$

6 Posets and Hasse Diagram

We discuss here a special type of binary relation that helps decide when some element in a set precedes (or succeeds) the other according to some specified criterion. For example, in a collection of items such as books, foods, etc., each having certain number of attributes, two items a and b are considered related if every attribute of a is also an attribute of b. Any such type of reflexive, antisymmetric, and transitive relation is called a *partial order* on the set. An *order* on a nonempty set is defined in terms of a *partial order*. In general, in any situation wherein certain processes need to be done before others is nicely modeled by using the idea of *partial ordering*. The term *partial* indicates that not every pair of elements in the underlying set may be related with respect to a given partial order.

6.1 Posets

A *partial order* on a nonempty set A is a relation that help decide when for some pair of elements one precedes (or succeeds) the other. In Example 6.2, the usual inclusion relation $\subseteq$ on the power set P is a partial order. We may write $S \leq T$ when $S \subseteq T$. Notice that, replacing $\subseteq$ by $\supseteq$ reverses the ordering on the set P, which we write as $\succeq$. We begin our discussion here by first brushing up some terminologies introduced earlier in section dealing with properties of binary relations on a set. Let A be a nonempty set. Recall that

$$\Delta_A := \big\{(a,a) mid \text{ for all } \; a \in A\big\}, \tag{6.1}$$

denotes the **diagonal relation** on the set A. Also, a relation R on a nonempty set A is said to be *reflexive* if it contains the *diagonal relation* Δ_A, and R is **symmetric** if $R = R^{-1}$, where

$$R^{-1} := \big\{(b,a) : \text{ for each } \; (a,b) \in R\big\}. \tag{6.2}$$

On the other hand, a relation R on a set A is said to be **antisymmetric** if we have

$$(a,b) \in R \quad \text{and} \quad (b,a) \in R \qquad \Rightarrow \qquad a = b. \tag{6.3}$$

In particular, we have the diagonal relation Δ_A is both symmetric and antisymmetric.

Definition 6.1. *A **pre-order** on a nonempty set P is a reflexive and transitive relation on the set P. An irreflexive and transitive relation on P is called a **quasiorder**. A **partial order** on a nonempty set P is an antisymmetric pre-order on P. We usually write a partial order on a set P as $\leq$, and the pair $(P,\leq)$ is called a **partial ordered set** (or simply a* poset*). Therefore, we write $a \leq b$ when $(a,b) \in \leq$.*

The notation $\leq$ used above is a generic symbol that should not be confused with usual *less than or equal to* $(\leq)$. That is, for $a,b \in P$, we write $a \leq b$ to say a precedes b. In this case, we also say b succeeds a and write $b \succeq a$. Also, $a \prec b$ means $a \neq b$ and a precedes b. We also say *a strictly precedes b*. Similarly, $a \succ b$ means *a strictly succeeds b*.

Example 6.1 (Poset of Divisor). *Let $A \subseteq \mathbb{N}$ be a set of natural numbers. Consider the relation R given by*

$$(a,b) \in R \qquad \Leftrightarrow \qquad a \text{ divides } b. \tag{6.4}$$

Since each $a \in A$ divides itself, it follows that R is reflexive. *Next, suppose both (a,b) and (b,a) belongs to R. That is,*

$$b = k_1 a \quad \text{and} \quad a = k_2 b, \qquad \text{for some} \quad k_1, k_2 \in \mathbb{N}.$$

Then, we have

$$a = \big(k_1 k_2\big) a \quad \Rightarrow \quad k_1 k_2 = 1 \quad \Rightarrow \quad k_1 = k_2 = 1.$$

Therefore, $a = b$. It thus follows that R is antisymmetric. *Finally, suppose (a,b), $(b,c) \in R$. That is,*

$$b = k_1 a \quad \text{and} \quad c = k_2 a, \qquad \text{for some} \quad k_1, k_2 \in \mathbb{N}.$$

Then, $c = \big(k_1 k_2\big) a$ implies that $(a,c) \in R$. Therefore, R is transitive. *Hence, A is a poset with respect to the relation "divides". In particular, the set D_n of divisors of n is a poset with respect to "divides" relation. We call D_n the* poset of divisors *of n. Notice that D_n contains only two elements* 1 *and n when n is a prime number. We thus always assume that $n \geq 2$.*

Example 6.2 (Poset of Sets). *Let X be a nonempty set, and $A = \mathscr{P}(X)$. Consider the usual* inclusion relation $\subseteq$ *on the power set of . That is, for $S, T \in P$, take*

$$S \sim T \qquad \Longleftrightarrow \qquad S \subseteq T.$$

As $S \subseteq S$, for any $S \in P$, it follows that the relation $\sim$ is reflexive. *Also,*

$$S \subseteq T \quad \text{and} \quad T \subseteq S \qquad \Rightarrow \qquad S = T,$$

by the definition of equality of sets. Therefore, the relation $\sim$ is antisymmetric. *Finally, as*

$$S \subseteq T \quad \text{and} \quad T \subseteq U \qquad \Rightarrow \qquad S \subseteq U,$$

we conclude that the relation $\sim$ is transitive. Hence, usual inclusion relation $\subseteq$ on the set P is reflexive, antisymmetric and transitive. Hence, the power set of a nonempty set is a poset with respect to the inclusion relation. *We usually call this the* poset of sets.

Definition 6.2. *A relation R on a set A is called **irreflexive** if there is no $a \in A$ such that $(a,a) \in R$. That is, $R \cap \Delta_A = \varnothing$.*

For example, the proper inclusion $\subset$ on a collection of subsets of a set is an irreflexive relation (Example 6.2). Also, the usual order $<$ on the set $\mathbb{N}$ is an irreflexive relation. Notice that a relation that is not reflexive may not be irreflexive, and vice-versa. On the other hand, a relation R on a set X is said to be *connected* if it satisfies the condition

$$x \neq y \;\text{ in }\; P \qquad \Rightarrow \qquad (x,y) \in R \;\text{ or }\; (y,x) \in R.$$

Remark 6.1. *In a poset $(P,\leq)$, we write $a \leq b$ if either $a = b$ or $a \prec b$. Notice that $a \succeq b$ in $(P,\leq)$ is same as $b \leq a$. We say a* strictly precedes *b when $a \prec b$. In this case, we may also write $b \succ a$ to say that b* strictly succeeds *a. Notice that a strict order can never have a* closed loops*. That is, there is no $a \in P$ such that $a < a$. Further, $a \neq b$ in $P \;\Rightarrow\;$ either $a \leq b$ or $b \leq a$. It can be shown that for a transitive relation $\sim$ on a set X, the above conditions are equivalent to the* trichotomy condition*.*

Example 6.3. *The relation $\sim$ on the set $P = \{a,b,c,d,e\}$ given by*

$$\sim = \Delta_P \bigcup \big\{(a,b),(a,c),(b,c),(b,d),(c,d),(c,e),(d,e),(d,a),(e,a),(e,b)\big\}$$

is a partial order. Also, the relation $\sim$ on the set

$$D_{60} = \big\{1,2,3,4,5,6,10,12,15,20,30,60\big\}$$

of divisors of the integer 60 *given by*

$$a \sim b \qquad \Longleftrightarrow \qquad a \;\text{ divides }\; b$$

is a partial order. The partial order given by inclusion relation *on the collection of all subsets of set $\{a,b,c\}$ is another interesting case of a poset (see Example 6.2). However, the usual order on the set of integers $\mathbb{Z}$ is not a partial order.*

Definition 6.3. *Let $(X,\leq)$ be a poset. Two element $x,y \in X$ are said to be* comparable *if $x \leq y$ or $y \leq x$. Otherwise, we say x and y are* incomparable *with respect to the partial order $\leq$. A subset C of a poset $(X,\leq)$ is called a* chain *if each pair of elements in C are comparable with respect to* induced ordering.

In Example 6.2, not every pair of sets in the collection P are *comparable* with respect to the *inclusion relation*. However, it does contain many *chains*. Therefore, the term partial used earlier refers to the fact that not every pair of elements in a poset $(X,\leq)$ are comparable.

Definition 6.4. *A poset $(X,\leq)$ in which each pair of elements in X are comparable is called* linearly ordered *(or* totally ordered*). In this case, we say $\leq$ is a* linear order *(or a* total order*) on the set X.*

The *usual order* $\leq$ on any number set such as $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ is a linear order. A simple construction described in the next example gives an interesting linearly order on product set. It is called *Lexicographic Ordering*, which is very useful in computer science. For example, it applies in sorting the character data.

Example 6.4. *The construction of a linearly ordered set described in this example is very useful in computer science. Let $\mathscr{A} = \{a_1,\ldots,a_n\}$ be a finite set of* alphabets *for a natural language. Suppose $\mathscr{A}$ has a linear order given by $\prec$ so that $a_1 \prec a_2 \prec \cdots \prec a_n$. A* string of alphabets *a_i of length m is a juxtaposed expression given by $x_1x_2\cdots x_m$, with $x_i \in \mathscr{A}$. That is, strings of different lengths over the set $\mathscr{A}$ are formed by putting*

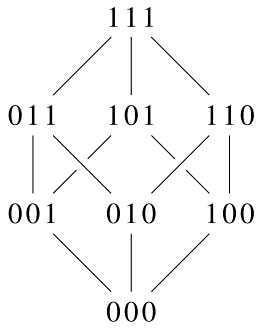


Figure 7: Lexicographic ordering on strings of length 3 on two alphabets.

together alphabets a_i in any order, possibly with repetitions. For instance, the two strings given below are respectively of length 5 *and* 7*:*

$$a_1a_1a_4a_3a_1 \qquad\qquad a_5a_2a_2a_2a_3a_1a_1.$$

We may write the set of strings of length m over alphabets $\mathscr{A}$ as $\mathscr{A}^m$. Therefore, the set $\mathscr{S}$ given by

$$\mathscr{S} = \mathscr{A}^1 \cup \mathscr{A}^2 \cup \cdots \cup \mathscr{A}^n \cup \cdots \tag{6.5}$$

is the collection of strings of all possible lengths defined over the alphabets $a_1,\ldots,a_n$. We extend the linear order $\prec$ on $\mathscr{A}$ to the collection $\mathscr{S}$ by ordering two strings lexicographically. *That is, in the* dictionary order. *For, if*

$$s = x_1x_2\cdots x_p \quad \textit{and} \quad t = y_1y_2\cdots y_q$$

are two strings of lengths p and q, then we say $s \prec t$ if

1. $x_1 \prec y_1$ *in* $(\mathscr{A},\prec)$*; or,*

2. $x_1 = y_1, x_2 = y_2, \ldots, x_k = y_k$*, but* $x_{k+1} \prec y_{k+1}$ *in* $(\mathscr{A},\prec)$*, for some* $1 \le k < r = min(p,q)$.

It follows easily that $\prec$ defines a linear order on $\mathscr{S}$. In algebraic terms, $\mathscr{S}$ is called a free monoid *on the set $\mathscr{A}$, where binary operation is defined by* juxtaposition *and* empty string *(of length* 0*) correspond to the identity element. A practical aspect of the above construction can be given in terms of human gene, which is a finite string of four* alphabets *that are actually initial letters of certain amino acids. Also, it applies in sorting the character data.*

Remark 6.2. *Recall that some programming languages are defined by using strings based upon an unlimited number of alphabets (characters), with a limit on the number of characters actually used to determines if the two words are same or different, as checked by a* compiler. *For example, in traditional C language, only the first eight characters of a string are checked by the compiler. So, if two words of any length agree in their first eight characters then the compiler treats the two same. This is where the concept of equivalence classes come into the play.*

6.2 Hasse Diagram

Every relation on a finite set A can be represented graphically as a *digraph*.

Definition 6.5. *Let $\sim$ be a relation on a set $A = \{a_1, \ldots, a_n\}$. A **directed graph** (or simply* digraph*) $D_\sim$ of the relation $\sim$ has the elements a_i's as the* vertices *plotted as points in the plain, and each ordered pairs $(a,b) \in \sim$ is represented by a directed edge drawn as an arrow from the vertices a to b. The arrows from a vertex a_i back to itself in $D_\sim$ is called a **loop*** at the vertex a_i.

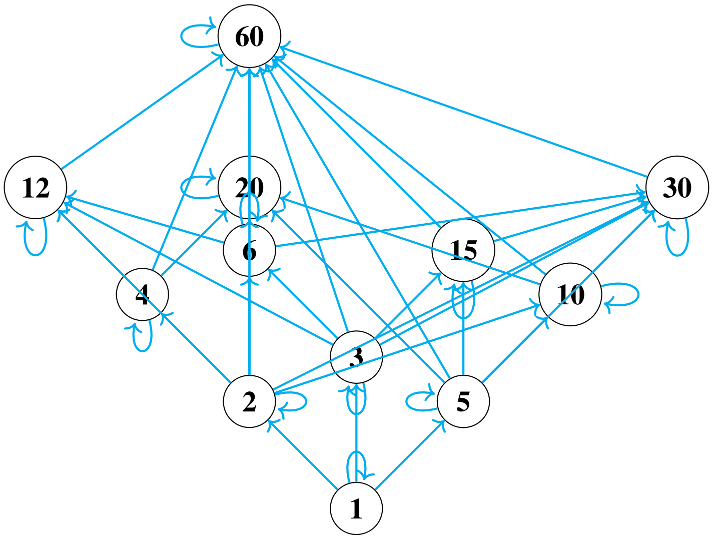


Figure 8: Digraph of the poset $(D_{60}, |\ )$.

For example, the relation on the set $\{a,b,c,d,e\}$ as given in Example 6.3 is represented graphically by the digraph as shown in Fig. 9. Also, the digraph of the poset $(D_{60}, |\ )$ is as shown in Fig. 8. As said earlier, a relation $\sim$ on a finite set A can be represented graphically as a *digraph* $D_\sim$, where the elements of A are *vertices* and each ordered pair in $\sim$ correspond to a *directed edge*. However, a poset $(P, \leq)$ has a much simpler graphical representation, which is known as the *Hasse diagram* of the poset. The simple procedure to obtain the Hasse diagram of a poset is as given below.

1. Draw the digraph $D_\leq$ of the poset P.

2. Omit *loops* at each vertex in D_P. Notice that we don't lose any information because $\leq$ is reflexive.

3. Omit arrows between points that are connected by sequences of arrows. Notice that we don't lose any information because $\leq$ is transitive.

4. Finally, the *Hasse diagram* of the poset is obtained by removing arrows on edges assuming that they are *oriented upwards*, i.e., all arrowheads are understood to be pointing upward.

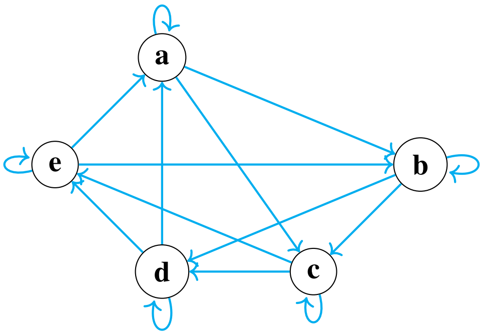


Figure 9: Digraph of first poset in Example 6.3.

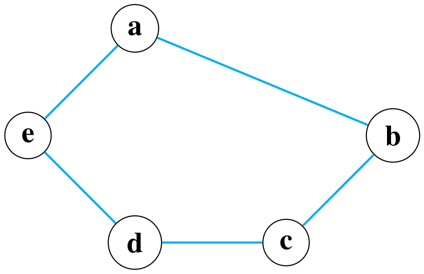


Figure 10: Hasse diagram of first poset in Example 6.3.

Therefore, *Hasse diagram* is a convenient way to visualise a poset $(P, \leq)$. For example, the Hasse diagram of the first poset in Example 6.3 is as shown in Fig. 10, which is known as the *pentagon lattice*. Notice that, in this case, the edges are *oriented downwards*, i.e., all arrowheads are understood to be pointing downward.

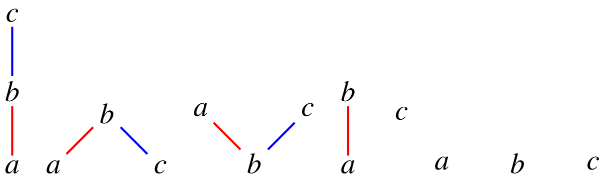


Figure 11: Hasse diagram of all possible posets on three elements.

Also, the Hasse diagram of the second poset in Example 6.3 is as shown in Fig. 12. Further, the Hasse diagram of third poset on the set $\{a,b,c\}$ as in Example 6.3 is as shown in Fig. 13. Fig. 19 shows the Hasse diagrams of all possible posets on three elements.

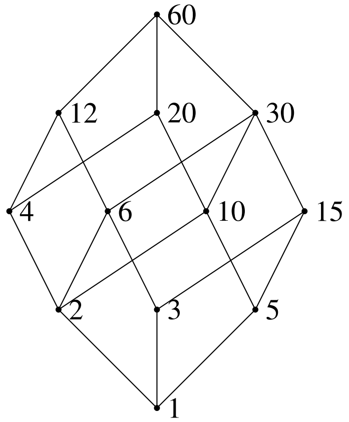


Figure 12: Hasse diagram of the poset D_{60}.

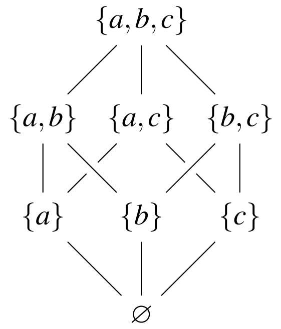


Figure 13: Hasse diagram of the poset $(\{a,b,c\}, \subseteq)$.

6.3 Extremal Elements

In simple terms, a *maximal element* in a poset $(P, \leq)$ is the one that has no successor, and a *minimal element* is the one that has no predecessor in $(P, \leq)$. Very roughly, a unique maximal element of a poset is called the *greatest element* (or *maximum element*), and a unique minimal element is called the *least element* (or *minimum element*) of a poset. We also introduce important concepts such as the greatest lower bound and the least upper bound element of a subset of a poset. Let us begin with the next definition.

Definition 6.6. *Let $(P, \leq)$ be a poset. An element $x \in P$ is called a **maximal** if there is no $y \in P$ such that $x \prec y$. An element $x \in P$ is called a **minimal** if there is no $y \in P$ such that $x \succ y$.*

It is clear from the Hasse diagram shown in Fig. 14 that the related poset has *a* and *b* as maximal elements, whereas *c*, *d* are its minimal elements.

Q 56. *In this question, assume the partial order $\leq$ is the relation "*divides*":*

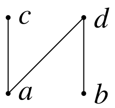


Figure 14: Hasse diagram of $\Delta_A \cup \{(a,c),(a,d),(a,d)\}$.

(i) Draw the Hasse diagram of the posets $\big(P_1, \leq\big)$ *and* $\big(P_2, \leq\big)$*, where*

$$P_1 = \big\{2,3,6,12,24,36\big\} \qquad \textit{and} \qquad P_2 = \big\{3,6,12,24,48\big\}.$$

(ii) Find the maximal and minimal elements of the poset $\big(P, \leq\big)$*, where*

$$P = \big\{2,4,5,10,12,20,25\big\}.$$

(iii) With $P = \{1,2,3,4,5,6,7,8\}$*,* $A = \{1,2\}$*, and* $B = \{3,4,5\}$*, find the lower and upper bounds of the subsets A and B of the poset* $(P, \leq)$*. Also, find the* $\sup(A)$*,* $\inf(A)$*,* $\sup(B)$*, and* $\inf(B)$*.*

Sol. The Hasse diagrams of posets $\big(P_1, \leq\big)$ and $\big(P_2, \leq\big)$ are respectively as in Fig. 15.

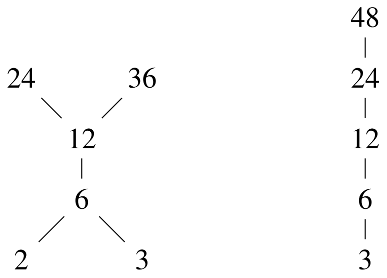


Figure 15: Hasse diagrams of posets the P_1 and P_2 in Q. 56(i).

For (ii), the Hasse diagram of the poset $\big(P, \text{"}\textit{divides}\text{"}\big)$ is the left side picture in Fig. 16.

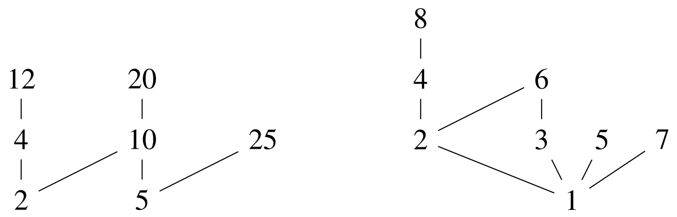


Figure 16: Hasse diagrams of posets in Q. $56(ii)$ (left) and Q. $56(iii)$ (right).

Clearly, maximal elements of the left side poset are $12, 20, 25$, and minimal elements are $2, 5$.

For (iii), the Hasse diagram of the poset $\big(P, \leq\big)$ is shown on the right side of Fig. 16. Therefore, the lower and upper bounds for the subsets $A = \{1,2\}$ and $B = \{3,4,5\}$ of P are given by

$$\begin{array}{lcl} \text{Lower bound of } A = \big\{1\big\}; & \text{and} & \text{Lower bound of } B = \big\{1\big\}; \\ \text{Upper bound of } A = \big\{2,4,6,8\big\}; & \text{and} & \text{Upper bound of } B = \varnothing. \end{array}$$

It thus follows that we have

$$\sup(A) = 2, \qquad \inf(A) = 1, \qquad \inf(B) = 1,$$

but $\sup(B)$ does not exists. ♢

Q 57. *In each of the following cases, use the* Hasse diagram *to construct a suitable example of a poset* $\big(P, \leq\big)$ *satisfying the conditions as stated below:*

(i) P has precisely three maximal elements and two minimal elements.

(ii) P has minimal elements, but no maximal element.

(iii) P neither has a minimal element nor a maximal element.

(iv) P has a subset A with more than one upper bounds, but $\sup(A)$ *doesn't exist.*

(v) P has a subset A with more than one lower bounds, but $\inf(A)$ *doesn't exist.*

Sol. For (i), we have the poset $\big(P, \text{"}divides\text{"}\big)$ with the Hasse diagram as on the left of Fig. 16. Notice that it has precisely three maximal elements and two minimal elements. Next, for (ii), we may use *well ordering property* of the set of natural numbers $\mathbb{N}$, and choose any infinite subset of $\mathbb{N}$ with respect to natural order. Also, for (iii), we may take the set of real number $\mathbb{R}$ with respect to natural order. Finally, for parts (iv) and (v), consider the poset P with the Hasse diagram as in Fig. 17.

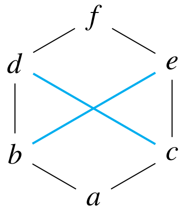


Figure 17: The Hasse diagram of poset P in Q. $57(iv)\&(v)$.

In this case, we have $P = \{a,b,c,d,e,f\}$. Notice that the set $A = \{b,c\} \subset P$ has elements d,e,f as upper bounds, but $\sup(A)$ doesn't exist. Also, the set $A = \{d,e\} \subset P$ has elements a,b,c as lower bounds, but $\inf(A)$ doesn't exist. ♢

With reference to $Q.2(iii)$, recall that every finite poset has a minimal and a maximal elements. However, with $A = \{a,b,c,d,e\}$, if we consider the partial order R on A given by

$$R = A_\Delta \cup \{(a,b),(a,c),(b,c),(b,d),(c,d),(c,e),(d,e),(d,a),(e,a),(e,b)\},$$

then (A,R) is a *finite poset* that neither has a maximal nor a minimal element. The related digraph and the Hasse diagram (with arrows) is shown in Fig. 18. We ask: *Why this particular example doesn't contradict the afore mentioned standard fact about finite posets*? We would appreciate a comment to help us find the answer! Interestingly, every step of computation of *transitive closure* breaks down the anti-symmetry property of R.

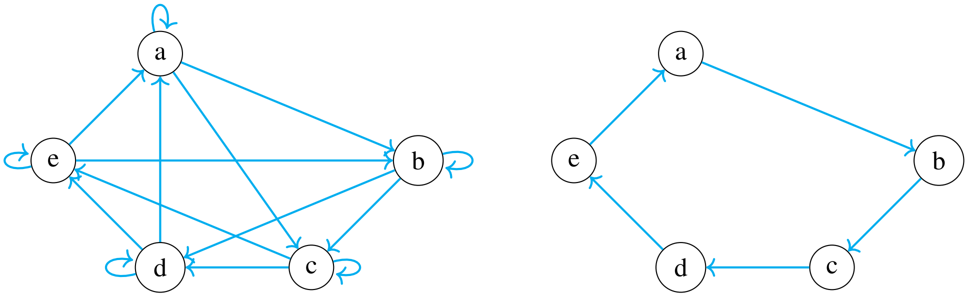


Figure 18: Digraph and Hasse diagram of poset in Q. $57(iii)$.

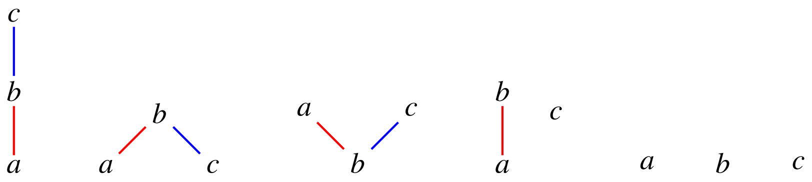


Figure 19: Hasse diagram of all possible posets with three elements.

Q 58. *Let $P = \{a,b,c\}$ be a poset with respect to some partial order. Draw all Hasse diagrams that P possibly can have. Also, discuss their maximal, minimal, maximum (or greatest), minimum (or least) elements.*

Sol. All the Hasse diagrams of the poset structures of $P = \{a,b,c\}$ are shown in Fig. 19. Starting from the Hasse diagram on the left side of this figure, notice that

1. the first poset has c as a unique maximum element (and so it is the greatest element) and a as a unique minimum element (and so it is the least element);

2. the second poset has b as a unique maximum element (and so it is the greatest element), and a,c as minimal elements;

3. the third poset has a, c as maximal elements, and b as a unique minimum element (and so it is the least element);

4. the fourth poset has both b, c as maximal elements and both a, c as minimal elements;

5. the fifth poset has the three elements a, b, c as maximal elements and also as minimal elements.

Clearly, in latter the two cases, maximum (or greatest) or minimum (or least) elements don't exists. $\diamondsuit$

7 Lattices and Properties

The concept of a **lattice** is an abstraction that is the part of the mathematical discipline known as the *order theory*. Definitions of some related terminologies are as given below.

Definition 7.1. *A poset $(L,\leq)$ is called a* ***lattice*** *if, for every pair of elements $a,b\in L$, both the* supremum $\sup\{a,b\}$ *and the* infimum $\inf\{a,b\}$ *exist.*

For $a,b\in L$, we also write

$$a\vee b := \sup\big\{a,b\big\} \quad \text{and} \quad a\wedge b := \inf\big\{a,b\big\},$$

where $\vee$ is called the **join operation** and $\wedge$ is called the **meet operation**. In general, for emphasis, a lattice is also denoted by $(L,\leq,\vee,\wedge)$. For example, in the case of a poset of sets $L=\mathscr{P}(X)\,(X\neq\varnothing)$ partially ordered by the “*inclusion relation*" $\subseteq$, we have

$$A\vee B := \sup\{A,B\} = A\cup B \qquad \text{and} \qquad A\wedge B := \inf\{A,B\} = A\cap B,$$

always exist, for every pair of elements A and B in L. We call this a **lattice of sets** given on the set X. Also, in the case of any poset $L\subseteq\mathbb{N}$ partially ordered by the relation “*divides*",

$$a\vee b := \sup\{a,b\} = \operatorname{lcm}\big\{a,b\big\} \quad \text{and} \quad a\wedge b := \inf\{a,b\} = \operatorname{hcf}\big\{a,b\big\},$$

always exist, for every pair of elements a and b in L. In particular, the same is true for the **divisor lattice** $(D_n,$“*divides*”$)$, where D_n is the set of divisors of the positive integer $n\geq 2$.

Definition 7.2. *A lattice $(L,\leq)$ is called a* ***complete lattice*** *if both the* supremum *and the* infimum *exist for every finite subset of L.*

The good way to find extremal elements of a poset is to use its Hasse diagram. In geometrical terms, to find the join $a\vee b$, move up along the two chains in the Hasse diagram that contain these two elements, and look for the element where the two join for the first instance. Similarly, to find the meet $a\wedge b$, move down along the chains in the Hasse diagram that contain these two elements, and look for the element where the two meet for the first instance. Also, this geometric interpretation explains the terminology *join* and *meet*.

Definition 7.3. *A lattice $\big(L,\leq,\vee,\wedge,\big)$ is called a* ***distributive lattice*** *if we have:*

$$a\wedge\big(b\vee c\big) = \big(a\wedge b\big)\vee\big(a\wedge c\big), \qquad \textit{for all} \quad a,b,c\in L. \tag{7.1}$$

If L is a *distributive lattice*, then we also have the following inequality:

$$a\vee\big(b\wedge c\big) = \big(a\vee b\big)\wedge\big(a\vee c\big), \tag{7.2}$$

which holds by the *duality principle* for lattices.

Definition 7.4. *A lattice* $\big(L,\leq,\vee,\wedge,\big)$ *is called a **modular lattice** if we have*

$$a\leq c \qquad \Rightarrow \qquad a\vee\big(b\wedge c\big)=\big(a\vee b\big)\wedge c, \qquad \textit{for} \quad a,b,c\in L. \tag{7.3}$$

If L is a *modular lattice*, then we also have the following:

$$a\leq c \qquad \Rightarrow \qquad a\wedge\big(b\vee c\big)=\big(a\wedge b\big)\vee c, \qquad \text{for} \quad a,b,c\in L, \tag{7.4}$$

which holds by the *duality principle* for lattices.

Definition 7.5. *A lattice* $\big(L,\leq,\vee,\wedge,\big)$ *is called a **bounded lattice** if it has both maximum and minimum elements, which are usually denoted by* 0 *and* 1. *Equivalently, L is a* bounded lattice *if it contains two elements* 0 *and* 1 *such that we have*

$$a\wedge 0=0 \quad \textit{and} \quad 1\vee a=1, \qquad \textit{for all} \quad a\in L. \tag{7.5}$$

Notice that every finite lattice is bounded, because the meet of all its element is the greatest element 1, and the join of all its element is the least element 0.

Definition 7.6. *A bounded lattice* $\big(L,\leq,\vee,\wedge,0,1\big)$ *is called a **complemented lattice** if each* $a\in L$ *is* complemented *with respect to bounds* 1 *and* 0. *That is, there is some* $b\in L$ *such that we have*

$$a\vee b=1 \qquad \textit{and} \qquad a\wedge b=0. \tag{7.6}$$

*In this case, we say b is a **complement** of a, and write* $b=a'$.

Theorem 59. *In a bounded distributive lattice* $\big(L,\leq,\vee,\wedge,0,1\big)$, *complement of an element is unique, if it exists.*

`Proof.` Let $a\in L$ be complemented. Suppose $b,c\in L$ are two complements of a. Then, by definition,

$$a\vee b=1 \qquad \text{and} \qquad a\wedge b=0; \tag{7.7}$$

$$a\vee c=1 \qquad \text{and} \qquad a\wedge c=0. \tag{7.8}$$

Now, we have

$$\begin{aligned} b&=1\wedge b && \text{(by identity law)}\\ &=\big(a\vee c\big)\wedge b && \text{(by (7.8))}\\ &=\big(a\wedge b\big)\vee\big(c\wedge b\big) && \text{(by distributivity)}\\ &=0\vee\big(b\wedge c\big) && \text{(by (7.7))}\\ &=b\wedge c. && \text{(by identity law)} \end{aligned}$$

Similarly, we also have

$$\begin{aligned} c &= 1 \wedge c && \text{(by identity law)} \\ &= \big(a \vee b\big) \wedge c && \text{(by (7.7))} \\ &= \big(a \wedge c\big) \vee \big(b \wedge c\big) && \text{(by distributivity)} \\ &= 0 \vee \big(b \wedge c\big) && \text{(by (7.8))} \\ &= b \wedge c. && \text{(by identity law)} \end{aligned}$$

Therefore, $b = c$, which proves uniqueness. □

As stated in the next question, the **cancellation property** holds in general for distributive lattices. You may imitate the proof of this property given earlier for sets, as in Assignment-1. In that proof, we need to view a, x, y as elements of a lattice, and accordingly replace $\cup$ by $\vee$ and $\cap$ by $\wedge$. However, an alternative proof is as given below.

Q 60 (*Cancellation property*)**.** *Let $\big(L, \leq, \vee, \wedge\big)$ be a distributive lattice, and $a, x, y \in L$ such that we have*

$$a \wedge x = a \wedge y \qquad \text{and} \qquad a \vee x = a \vee y.$$

Show that $x = y$.

Sol. The idea is to show that the element $y \wedge (a \vee x)$ equals both x and y. For, we have

$$\begin{aligned} y \wedge \big(a \vee x\big) &= y \wedge \big(a \vee y\big) && \text{(given condition)} \\ &= y \wedge \big(y \vee a\big) && \text{(commutativity)} \\ &= y && \text{(absorption)} \end{aligned}$$

We also have that

$$\begin{aligned} y \wedge \big(a \vee x\big) &= \big(y \wedge a\big) \vee \big(y \wedge x\big) && \text{(distributivity)} \\ &= \big(a \wedge y\big) \vee \big(y \wedge x\big) && \text{(commutativity)} \\ &= \big(a \wedge x\big) \vee \big(y \wedge x\big) && \text{(given condition)} \\ &= \big(a \vee y\big) \wedge x && \text{(distributivity)} \\ &= \big(a \vee x\big) \wedge x && \text{(given condition)} \\ &= x \wedge \big(x \vee a\big) && \text{(commutativity)} \\ &= x && \text{(absorption)} \end{aligned}$$

Hence $x = y$. This completes the solution. ♢

Q 61 (*Distributive Inequality*)**.** *Let $\big(L,\leq,\vee,\wedge\big)$ be a lattice. Prove that we always have*

$$a\wedge\big(b\vee c\big)\geq\big(a\wedge b\big)\vee\big(a\wedge c\big),\qquad \textit{for all}\quad a,b,c\in L. \tag{7.9}$$

Give an example of a lattice wherein equality *holds.*

Sol. By definition of inf, we have $a\wedge b:=\inf\{a,b\}\leq a$, and also

$$a\wedge b\leq b\leq\sup\{b,c\}:=b\vee c.$$

Therefore, $a\wedge b$ is a lower bound of the set $\{a,b\vee c\}$. It thus follows that

$$a\wedge b\leq\sup\big\{a,b\vee c\big\}:=a\wedge\big(b\vee c\big). \tag{7.10}$$

Similarly, since $a\wedge c:=\inf\{a,c\}\leq c$, and also

$$a\wedge c\leq c\leq\sup\{b,c\}:=b\vee c,$$

it follows that $a\wedge c$ is a lower bound of the set $\{a,b\vee c\}$. Therefore, we have

$$a\wedge c\leq\sup\big\{a,b\vee c\big\}:=a\wedge\big(b\vee c\big). \tag{7.11}$$

Hence, (7.10) and (7.10) implies that the inequality (7.9) holds. For the second part of the question, notice that the equality holds for both a *lattice of sets* (on any nonempty set) and a *divisor lattice* $D_n\,(n\geq 2)$. ♢

Q 62. *Define the terms* distributive lattice, modular lattice, bounded lattice*, and* complemented lattice.

(i) Prove that every distributive lattice is modular. Give an example of a lattice to show that the converse is not true.

(ii) Give an example of a finite lattice L such that at least one element of L has no complement.

(iii) Give an example of a finite lattice L such that at least one element of L has more that one complements.

(iv) Find the complements of elements of the lattice D_{42}.

Sol. Definitions are as given above. For (i), notice that the implication (7.3) follows directly from (7.1) because $a\leq c\ \Rightarrow\ a\wedge c=a$. Also, notice that the lattice L with the Hasse diagram shown in Fig. 20 is a modular lattice because the condition $a\leq c$ in this case would mean that a or c is a bound. However, in view of Theorem 59 it is not a distributive lattice. More precisely, each has the other two elements as complements.

For (ii), consider bounded lattice with Hasse diagram as on the left side of Fig. 21. Notice that a and e are complements of each other; and, b and d are complements of each other. However, complement of c doesn't

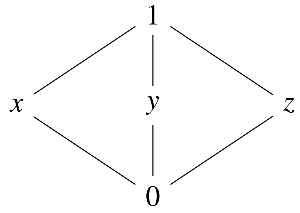


Figure 20: A non-distributive modular lattices.

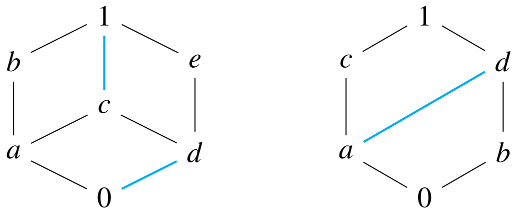


Figure 21: The Hasse diagram of poset in $Q.7(ii)$.

exist. Further, we ask do the elements a,d in the lattice with Hasse diagram as shown on right side of Fig. 21 have complements?

For (iii), the finite bounded lattice with Hasse diagram as in Fig. 20 is such that any of the elements a,b,c has the other two as its complements. For (iv), notice that two elements $a,b \in D_{42}$ are complements of each other with respect to relation “divides" if we have

$$a \vee b := \operatorname{lcm}\{a,b\} = 42 \qquad \text{and} \qquad a\wedge := \operatorname{hcf}\{a,b\} = 1.$$

Now, we can see from the Hasse diagram of lattice D_{42} (Fig. 22) that such pair of elements $\{a,b\}$ are precisely the *diagonally opposite* elements. It thus follows that we have

$$1' = 42, \qquad 2' = 21, \qquad 6' = 7, \qquad 3' = 14.$$

This completes the solution. ♢

7.1 Sublattices & Isomorphism

Definition 7.7. *Let $(L, \leq, \vee, \wedge)$ be a lattice. A nonempty set $S \subseteq L$ is called a **sublattice** of the lattice L if, for all $a,b \in S$, we have $a \vee b$, $a \wedge b \in S$.*

Q 63. *Define sublattice of a lattice. Draw the Hasse diagram of the lattice D_{24}, and find its sublattices with $4,5,6,$ and 7 elements. Does D_{24} contains a sublattice with 3 elements? Explain.*

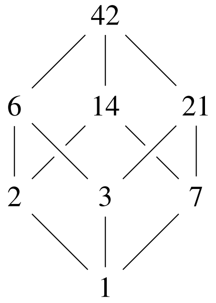


Figure 22: Hasse diagram of the divisor lattice $(D_{42}, \text{"}divides\text{"})$.

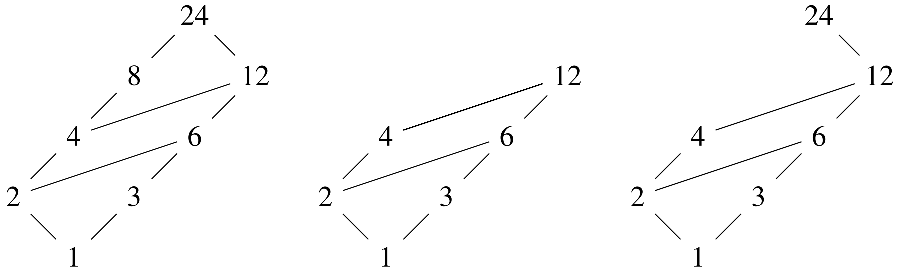


Figure 23: Hasse diagrams of lattice $(D_{24}, \text{"}divides\text{"})$ and some sublattices.

Sol. The definition is as given above. The Hasse diagram of the divisor lattice $(D_{24}, \text{"}divides\text{"})$ is shown on the left side of Fig.23. We may take the two sublattices as $\{2,4,8,24\}$ and $\{1,3,6,12\}$, which are actually **chains** of length 4. Next, we may take the two sublattices as $\{1,2,4,8,24\}$ and $\{1,3,6,12,24\}$, which are actually **chains** of length 4. The sublattices with 6 and 7 elements respectively are as shown on right of the first picture in Fig.23. Clearly, this lattice has many sublattices with 3 elements. May be you can specify some! ♢

Definition 7.8. *Let $(L_1, \leq_1, \vee_1, \wedge_1)$ and $(L_2, \leq_2, \vee_2, \wedge_2)$ be two lattices. A function $f : L_1 \to L_2$ is called a*

1. ***join homomorphism*** *if $f\big(a \vee_1 b\big) = f(a) \vee_2 f(b)$, for all $a, b \in L_1$.*
2. ***meet homomorphism*** *if $f\big(a \wedge_1 b\big) = f(a) \wedge_2 f(b)$, for all $a, b \in L_1$.*

Further, f is called a ***lattice isomorphism*** *if it is a bijective function.*

In actual practice, we need to make two **operation tables** each for L_1 and its image $f(L_1) \subseteq L_2$.

Q 64. *Show that D_{12} and D_{18} are isomorphic lattices. Further, show that none is isomophic to the lattice D_{20}.*

Sol. The Hasse diagrams of lattices D_{12} and D_{18} are as in Fig. 24. Therefore, we define the *order-preserving* bijective function $f : D_{12} \to D_{18}$ as follows:

$$f\big(1\big) = 1, \quad f\big(2\big) = 3, \quad f\big(3\big) = 2, \quad f\big(4\big) = 9, \quad f\big(6\big) = 6, \quad f\big(12\big) = 18.$$

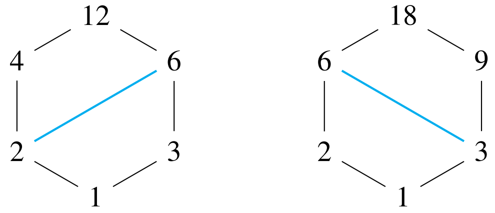


Figure 24: The Hasse diagrams of divisor lattices D_{12} and D_{18}.

It is easy to see that *join table* and *meet table* of elements of $1,2,3,6,12$ and their images under f are exactly the same, and so f is both a *join homomorphism* and a *meet homomorphism*. That is, f is a lattice isomorphism. ♢

Q 65. *For the two lattices* L_1 *and* L_2 *with Hasse diagrams as shown on the left and middle pictures of Fig 25, draw the Hasse diagram of the product lattice* $L_1 \times L_2$ *with respect to lexicographic ordering.*

Sol. The Hasse diagrams of lattices L_1 and L_2 are left and middle pictures of Fig 25.

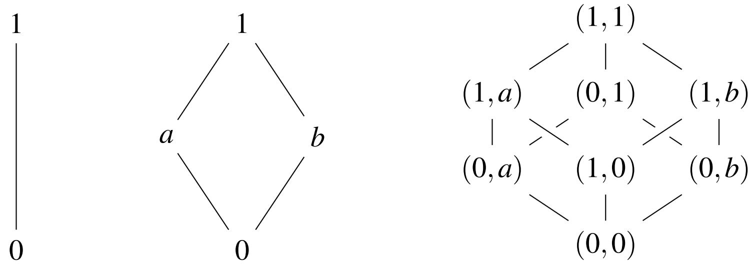


Figure 25: Hasse diagrams of lattices L_1, L_2, and $L_1 \times L_2$.

Now, since we have

$$L_1 \times L_2 = \{(0,0),(0,a),(0,b),(0,1),(1,0),(1,a),(1,b),(1,1)\}$$

it follows that with respect to *lexicographic ordering* the Hasse diagram of the product lattice $L_1 \times L_2$ is the last picture in Fig. 25. ♢

8 Boolean Algebras and Applications

In all that follows, the next definition is important.

Definition 8.1. *A **Boolean algebra** is a set with two special elements* 0 *and* 1*; two binary operations denoted by* $+$ *(sum) and* $\cdot$ *(product); and, a unary operation denoted by* $'$ *(complementation) such that, for all* $a,b,c \in B$*, the following five axioms hold:*

B1. ***(Identity Laws)*** $a+0=a$ *and* $a\cdot 1=a$*;*

B2. ***(Commutative Laws)*** $a+b=b+a$ *and* $a\cdot b=b\cdot a$*;*

B3. ***(Associative Laws)*** $a+(b+c)=(a+b)+c$ *and* $a\cdot(b\cdot c)=(a\cdot b)\cdot c$*;*

B4. ***(Distributive Laws)*** $a\cdot(b+c)=a\cdot b+a\cdot c$ *and* $a+(b\cdot c)=(a+b)\cdot(a+c)$*;*

B5. ***(Complement Laws)*** $a+a'=1$ *and* $a\cdot a'=0$*.*

We write a Boolean algebra as $(B,+,\cdot,{}',0,1)$*, where* 0 *is called the **zero element** and* 1 *is called the **identity element**. Also, for* $a\in B$*, the element* $a'\in B$ *is called the **complement** of* a*.*

8.1 Important Boolean Algebras

The *algebra of sets* $\mathscr{P}(X)$ defined on a nonempty set X is a Boolean algebra, with respect to binary operations $\cup$ and $\cap$; usual "set complementation" as unary operation; and, by taking $0\equiv\varnothing$, $1\equiv X$. This is known as the **Boolean algebra of sets**[10] given by the set X.

Example 8.1 (Lattice Boolean Algebra). *Let* $\big(L,\leq,\vee,\wedge\big)$ *be a complemented distributive lattice, with bounds denoted by* 0 *and* 1*, and* $a,b\in L$*. Since the* join *and* meet *of every pair of elements in* L *are unique, it follows that* $\vee$ *and* $\wedge$ *are binary operations on the set* L*. Since* L *is complemented distributive lattice, the mapping* $a\mapsto a' : L\to L$ *is well defined, where* a' *denotes the complement of the element* a*. Now, taking* $\vee$ *as the sum* $+$ *and* $\wedge$ *as the product* $\cdot$*, it follows from the problems solved in the previous section that all the five axioms* $(B1)$ – $(B5)$ *hold, with the least element* 0 *of* L *as the* zero element*, and the greatest element* 1 *of* L *as the* identity element*. Therefore,* every complemented distributive lattice is a Boolean algebra*, which is called the* lattice Boolean algebra*. For emphasis, we may this Boolean algebra as* B_L*.*

Example 8.2. *We see here why a* 3*-point or a* 5*-point lattice cannot be a Boolean algebra. For, let* $\big(L,\leq,\vee,\wedge\big)$ *be a complemented distributive lattice with* 3 *or* 5 *elements. We know that a boolean algebra has at*

[10] By Stone's representation theorem, every finite Boolean algebra is essentially a *Boolean algebra of sets* on some set, and so has 2^n elements, for some $n\geq 1$.

least two elements, 0 *and* 1*, which are respectively the minimum and maximum elements of* L*. Let* $x \in L$ *be the third element. Since* $0 \neq x \neq 1$*, by unique complement property, we have* $0 \neq x' \neq 1$*. Therefore,* x' *is the fourth element of* L*. A similar argument applies if* L *has an additional element* $y \neq x$*.*

Q 66. *Show that the set* $B = \{1,2,3,6\}$ *is a Boolean algebra with respect to operations as given below:*

$$a+b = \operatorname{lcm}\{a,b\}, \qquad a \cdot b = \operatorname{hcf}\{a,b\}, \qquad a\prime = \frac{6}{a}.$$

Further, show that the set $B = \{1,2,4,8\}$ *is a not a Boolean algebra with respect to* $+$ *and* $\cdot$ *as above, and* $x\prime = \frac{8}{x}$*.*

Sol. We first show that the set $B = \{1,2,3,6\}$ is a Boolean algebra with respect to operations as given below:

$$a+b = \operatorname{lcm}\{a,b\}, \qquad a \cdot b = \operatorname{hcf}\{a,b\}, \qquad a' = \frac{6}{a}.$$

The three operations $+$, $\cdot$, and $'$, on the set $B = \{1,2,3,6\}$ are as given in Table 6.

$+$	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

$\cdot$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

a	a'
1	6
2	3
3	2
6	1

Table 6: Tables of operations $+$, $\cdot$, and $'$ on $B = \{1,2,3,6\}$.

It follows from the first two tables that $+$ and $\cdot$ are associative and commutative binary operations. Also, each operation distributes over the other. Further, for any $a \in \{1,2,3,6\}$, we have

$$\operatorname{lcm}\{a,1\} = a \quad \text{and} \quad \operatorname{hcf}\{a,6\} = a.$$

Therefore, the *zero element* **0** is given by the element 1, and the *identity element* **1** is given by the element 6. Further, the third table on the right side shows that the *complementation laws* hold. Notice that, for $a \in \{1,2,3,6\}$, we have

$$a + a' = \operatorname{lcm}\{a, 6/a\} = 6 \equiv \mathbf{1} \quad \text{and} \quad a \cdot a' = \operatorname{hcf}\{a, 6/a\} = 1 \equiv \mathbf{0}$$

Therefore, the set $B = \{1,2,3,6\}$ is a Boolean algebra with operations as given in the question.

Finally,we show that the set $B = \{1,2,4,8\}$ is a *not* a Boolean algebra with respect to $+$ and $\cdot$ as defined in the previous case. However, we now have $x' = 8/x$. The three tables of operations $+$, $\cdot$, and $'$ on the set $B = \{1,2,4,8\}$ are given in Table 7. As in the previous case, we have that $+$ and $\cdot$ are associative and commutative binary operations. Also, each operation distributes over the other. Further, the *zero element* **0**

$+$	1	2	4	8
1	1	2	4	8
2	2	2	4	8
4	4	4	4	8
8	8	8	8	8

$\cdot$	1	2	4	8
1	1	1	1	1
2	1	2	2	2
4	1	2	4	4
8	1	2	4	8

a	a'
1	8
2	4
4	2
8	1

Table 7: Tables of operations $+$, $\cdot$, and $'$ on $B = \{1,2,4,8\}$.

is given by the element 1, and the *identity element* **1** is given by the element 8. However, the third table on the right side shows that the complementation laws *doesn't* hold. For example, with $a = 2$, we have

$$a + a' = \text{lcm}\{2, 8/2\} = 4 \neq 8 \equiv \mathbf{1} \quad \text{and} \quad a \cdot a' = \text{hcf}\{2, 8/2\} = 2 \neq 1 \equiv \mathbf{0}.$$

Therefore, the set $B = \{1,2,4,8\}$ is <u>not</u> a Boolean algebra. ◇

Q 67. *Let $\big(B, +, \cdot, ', 0, 1\big)$ be a Boolean algebra, and $a, b \in B$. Show that*

(i) $a + 1 = 1$ *and* $a \cdot 0 = 0$.

(ii) $a \cdot \big(a + b\big) = a$ *and* $a + \big(a \cdot b\big) = a$.

(iii) $\big(a'\big)' = a$.

(iv) $0' = 1$ *and* $1' = 0$.

(v) $a + b = b \quad \Leftrightarrow \quad a \cdot b = a \quad \Leftrightarrow \quad a \cdot b' = 0 \quad \Leftrightarrow \quad a' + b = 1$.

(vi) $ab' + a'b = 0 \quad \Leftrightarrow \quad a = b$.

Sol. To prove the **Idempotent Laws**[11] given by

$$a + a = a \qquad \text{and} \qquad a \cdot a = a,$$

we have

$$\begin{aligned} a &= a + 0 && \text{(by B1)} \\ &= a + (a \cdot a') && \text{(by B5)} \\ &= (a + a) \cdot (a + a') && \text{(by B4)} \\ &= (a + a) \cdot 1 && \text{(by B5)} \\ &= a + a && \text{(by B1);} \end{aligned}$$

[11] The part (i) of the next question is modified in view of axiom B1.

and also

$$\begin{aligned} a &= a\cdot 1 && \text{(by B1)}\\ &= a\cdot(a+a') && \text{(by B5)}\\ &= (a\cdot a)+(a\cdot a') && \text{(by B4)}\\ &= (a\cdot a)+0 && \text{(by B5)}\\ &= a\cdot a && \text{(by B1)} \end{aligned}$$

Next, to prove the **Absorption Laws** given by

$$a\cdot\big(a+b\big)=a \qquad \text{and} \qquad a+\big(a\cdot b\big)=a,$$

we have

$$\begin{aligned} a\cdot\big(a+b\big) &= (a+0)\cdot\big(a+b\big) && \text{(by B1)}\\ &= a\cdot(0+b) && \text{(by B4)}\\ &= a+0 && \text{(by dominance Law)}\\ &= a && \text{(by B1)} \end{aligned}$$

Similarly, we can prove the other equality. Also, to prove the **Involution Law** given by $\big(a'\big)'=a$, recall that we have

$$a+a'=1 \quad \text{and} \quad a\cdot a'=0,$$

, by B5, which also says that a is the complement of a', i. e., $a=(a')'$. Further, to prove the **0 - 1 Law** given by $0'=1$ and $1'=0$, recall that $a\cdot a'=0$, by B5, so that

$$\begin{aligned} 0' &= (a\cdot a')' && \text{(by B5)}\\ &= a'+(a')' && \text{(by DeMorgan Law)}\\ &= a'+a && \text{(by part } (iii))\\ &= 1 && \text{(by B5)} \end{aligned}$$

Once again, applying involution law, we obtain $0=(0')'=1'$. We now prove the following equivalences

$$a+b=b \quad \Leftrightarrow \quad a\cdot b=a \quad \Leftrightarrow \quad a\cdot b'=0 \quad \Leftrightarrow \quad a'+b=1$$

First notice that both ways proof of the equivalence given below follows directly from the DeMorgan Laws, and the previous part:

$$a\cdot b'=0 \qquad \Leftrightarrow \qquad a'+b=1.$$

Now, suppose we have $a+b=b$. Then, we have

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

where the second equality is given by absorption law. To prove the reverse implication, suppose we have $a \cdot b = a$. Then, we have

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

where the second equality is given by absorption law. It thus follows that

$$a + b = b \qquad \Leftrightarrow \qquad a \cdot b = a.$$

To conclude the solution of part (v), we show that

$$a + b = b \qquad \Leftrightarrow \qquad a + b' = 1.$$

First, suppose $a + b = b$. Then we have

$$a' + b = a' + (a + b) = (a' + a) + b = 1 + b = 1,$$

where the last equality is given by dominance law. To prove other way implication, suppose $a' + b = 1$. Then we have

$$a + b = (a + b) \cdot 1 = (a + b) \cdot (a' + b) = (a \cdot a') + b = 0 + b = b.$$

Notice that we trivially have

$$a = b \qquad \Rightarrow \qquad a \cdot b' + a' \cdot b = 0.$$

Finally, to conclude the solution, suppose $a \cdot b' + a' \cdot b = 0$. Then we have

$$\begin{aligned} & a + (a \cdot b' + a' \cdot b) = a + 0 = a & \\ \Rightarrow \quad & a + a' \cdot b = a & \text{(by absorption Law)} \\ \Rightarrow \quad & (a + a') \cdot (a + b) = a & \text{(by B4)} \\ \Rightarrow \quad & 1 \cdot (a + b) = a & \text{(by B5)} \\ \Rightarrow \quad & a + b = a & \text{(by B1)} \end{aligned}$$

We also have

$$\begin{aligned} & b + (a \cdot b' + a' \cdot b) = b + 0 = b & \\ \Rightarrow \quad & b + a \cdot b' = b & \text{(by absorption Law)} \\ \Rightarrow \quad & (b + a) \cdot (b + b') = b & \text{(by B4)} \\ \Rightarrow \quad & (b + a) \cdot 1 = b & \text{(by B5)} \\ \Rightarrow \quad & a + b = b & \text{(by B1 and B2)} \end{aligned}$$

Hence, we have $a = b$. This completes the solution of the question. ♢

8.2 Boolean Expressions & Boolean Functions

Let $B = \{0,1\}$, and $\big(B,+,\cdot,',0,1\big)$ be the **2-point Boolean algebra**, where the three operations are defined as in Table 8. Recall that the product set

$$B^n := \big\{(x_1,\ldots,x_n) \mid \text{ each } x_i \in B\big\}$$

Table 8: Tables of operations $+$, $\cdot$, and $'$ on $B = \{0,1\}$.

$+$	0	1
0	0	1
1	1	1

$+$	0	1
0	0	0
1	0	1

a	a'
0	1
1	0

has *natural* Boolean algebra structure with respect to operations defined pointwise. Also, the identity **1** and the zero element **0** of B^n are respectively given by

$$\mathbf{1} := \big(1,1\ldots,1\big) \qquad \text{and} \qquad \mathbf{0} := \big(0,0,\ldots,0\big).$$

However, we now follow the convention of writing the elements of B^n as strings $x_1\cdots x_n$ of length n. In this case, we say x_i's are Boolean variables taking values in the set $B = \{0,1\}$. In all that follows, we take $n \leq 5$. Also, let F_e denotes the function : $B^n \to B$ obtained by evaluating a Boolean expression $E(x_1,\ldots,x_n)$ at 2^n values in the Boolean algebra B^n. We call F_e (or simply F) the **Boolean function** associated with the expression E.

Q 68. *Simplify the following Boolean expresions by algebraic manipulation:*

(i) $x\cdot\big[y+z\cdot\big(xy+xz\big)\prime\big].$

(ii) $a+a\prime\cdot b\cdot c\prime+\big(b+c\big)\prime.$

Sol. We simplify the following two Boolean expressions by algebraic manipulation:

(i) $\quad x\cdot\big[y+z\cdot\big(x\cdot y+x\cdot z\big)'\big].$

(ii) $\quad a+a'\cdot b\cdot c'+\big(b+c\big)'.$

For (i), we have

$$\begin{aligned}
x\cdot\big[y+z\cdot\big(xy+xz\big)'\big] &= x\cdot\big[y+z\cdot\big((xy)'\cdot(xz)'\big)\big] \quad \text{(by DeMorgan Law)}\\
&= x\cdot\big[y+z\cdot\big((x'+y')\cdot(x'+z')\big)\big] \quad \text{(by DeMorgan Law)}\\
&= x\cdot\big[y+(x'+y')\cdot\big(z\cdot(x'+z')\big)\big] \quad \text{(by B2 and B3)}\\
&= x\cdot\big[y+(x'+y')\cdot\big(z\cdot x'+z\cdot z'\big)\big] \quad \text{(by B4)}\\
&= x\cdot\big[y+(x'+y')\cdot\big(z\cdot x'+0\big)\big] \quad \text{(by B5)}\\
&= x\cdot\big[y+(x'+y')\cdot(z\cdot x')\big] \quad \text{(by B5)}\\
&= x\cdot\big[y+x'\cdot(z\cdot x')+y'\cdot(z\cdot x')\big] \quad \text{(by B4)}\\
&= x\cdot y+x\cdot x'\cdot(z\cdot x')+x\cdot y'\cdot(z\cdot x') \quad \text{(by B4)}\\
&= x\cdot y+0\cdot(z\cdot x')+y'\cdot z\cdot 0 \quad \text{(by B5 and B2)}\\
&= x\cdot y+0+0 = x\cdot y \quad \text{(by Dominance Law and B5)}
\end{aligned}$$

Next, for (ii), we have

$$\begin{aligned}
a+a'\cdot b\cdot c'+\big(b+c\big)' &= a+a'\cdot b\cdot c'+b'\cdot c' \quad \text{(by DeMorgan Law)}\\
&= a+(a'\cdot b+1)\cdot c' \quad \text{(by B4)}\\
&= a+1\cdot c' \quad \text{(by Dominance Law)}\\
&= a+c' \quad \text{(by B1)}
\end{aligned}$$

This completes the solution. ♢

Q 69. *Obtain the DNF associated with the Boolean expressions given by*

$$f\big(x,y,z\big) = \big(yz+xz\prime\big)\big(xy\prime+z\prime\big)\prime \qquad \textit{and} \qquad g\big(x_1,x_2,x_3\big) = x_1x_2\prime+x_3,$$

by using truth table method, and also by applying algebraic methods.

Sol. We have to obtain the DNF of the expressions given by

$$f\big(x,y,z\big) = \big(y\cdot z+x\cdot z'\big)\cdot\big(x\cdot y'+z'\big)' \qquad \text{and} \qquad g\big(x_1,x_2,x_3\big) = x_1\cdot x_2'+x_3,$$

by using *truth table method*, and also by *algebraic method*. The truth tables of Boolean expressions f and g are obtained as in Table 9. Now, since only two entries in the last column of the left side table are 1's, with associated maxterms $x'\cdot y\cdot z$ and $x\cdot y\cdot z$, it thus follows that the DNF of f is given by $x'\cdot y\cdot z+x\cdot y\cdot z$. Next, considering 1 entries in the last column of the right side table, we find that the maxterms are

$$x_1'\cdot x_2'\cdot x_3,\;\; x_1'\cdot x_2\cdot x_3,\;\; x_1\cdot x_2'\cdot x_3',\;\; x_1\cdot x_2'\cdot x_3,\;\; \text{and}\;\; x_1\cdot x_2\cdot x_3.$$

Table 9: Truth Tables for Boolean functions of Q.13.

x	y	z	$(y\cdot z+x\cdot z')\cdot(x\cdot y'+z')'$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

x_1	x_2	x_3	$x_1\cdot x_2'+x_3$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Therefore, the DNF of g is given by

$$x_1'\cdot x_2'\cdot x_3+x_1'\cdot x_2\cdot x_3+x_1\cdot x_2'\cdot x_3'+x_1\cdot x_2'\cdot x_3+x_1\cdot x_2\cdot x_3.$$

For the second part, recall that the *algebraic method* involves inserting *missing literals* using the identity $a\cdot 1=a$. However, we first need to clear *complementation* (if any involved) by using DeMorgan laws. For the given f, this is the case. Therefore, by applying the DeMorgan laws, we obtain

$$\begin{aligned}
f(x,y,z) &= (y\cdot z+x\cdot z')\cdot(x\cdot y'+z')' \\
&= (y\cdot z+x\cdot z')\cdot((x\cdot y')'\cdot(z')') \\
&= (y\cdot z+x\cdot z')\cdot((x'+(y')')\cdot z) \\
&= (y\cdot z+x\cdot z')\cdot(x'\cdot z+y\cdot z) \\
&= (y\cdot z)\cdot(x'\cdot z)+(x\cdot z')\cdot(x'\cdot z)+(y\cdot z)\cdot(y\cdot z)+(x\cdot z')\cdot(y\cdot z) \\
&= x'\cdot y\cdot z+y\cdot z
\end{aligned}$$

It thus follows from the identity

$$y\cdot z=1\cdot y\cdot z=(x+x')\cdot y\cdot z=x\cdot y\cdot z+x'\cdot y\cdot z$$

that the DNF of f is given by

$$x'\cdot y\cdot z+x\cdot y\cdot z+x'\cdot y\cdot z=x'\cdot y\cdot z+x\cdot y\cdot z.$$

Similarly, the DNF of the expression g by the *algebraic method* is obtained as follows:

$$\begin{aligned}
g(x_1,x_2,x_3) &= x_1\cdot x_2'+x_3\\
&= (x_1\cdot x_2')\cdot 1+1\cdot x_3\\
&= x_1\cdot x_2'\cdot(x_3+x_3')+(x_1+x_1')\cdot x_3\\
&= x_1\cdot x_2'\cdot x_3+x_1\cdot x_2'\cdot x_3'+x_1\cdot x_3+x_1'\cdot x_3\\
&= x_1\cdot x_2'\cdot x_3+x_1\cdot x_2'\cdot x_3'+x_1\cdot 1\cdot x_3+x_1'\cdot 1\cdot x_3\\
&= x_1\cdot x_2'\cdot x_3+x_1\cdot x_2'\cdot x_3'+x_1\cdot(x_2+x_2')\cdot x_3+x_1'\cdot(x_2+x_2')\cdot x_3\\
&= x_1\cdot x_2'\cdot x_3+x_1\cdot x_2'\cdot x_3'+x_1\cdot x_2\cdot x_3+x_1\cdot x_2'\cdot x_3+x_1'\cdot x_2\cdot x_3+x_1'\cdot x_2'\cdot x_3\\
&= x_1\cdot x_2'\cdot x_3+x_1\cdot x_2'\cdot x_3'+x_1\cdot x_2\cdot x_3+x_1'\cdot x_2\cdot x_3+x_1'\cdot x_2'\cdot x_3,
\end{aligned}$$

by using the identity $a+a=a$ to obtain the last equality. This completes the solution. ♢

Q 70. *Obtain the CNF associated with the Boolean expressions given by*

$$f(x,y,z)=(x+z)\cdot y \qquad \textit{and} \qquad g(x_1,x_2,x_3)=(x_2x_3+x_1x_3\prime)(x_1x_2\prime+x_3)\prime,$$

by using truth table method, and also by applying algebraic methods.

Sol. We have to obtain the CNF of the expressions given by

$$f(x,y,z)=(x+z)\cdot y \qquad \text{and} \qquad g(x_1,x_2,x_3)=(x_2x_3+x_1x_3')\cdot(x_1x_2'+x_3)',$$

by using *truth table method*, and also by *algebraic method*. The truth tables of Boolean expressions f and g are obtained as in Table 10. Now, since five entries in the last column of the left side table are 0's, with associated minterms $x'+y'+z'$, $x'+y'+z$, $x'+y+z'$, $x+y'+z'$, and $x'+y'+z$, it thus follows that the CNF of f is obtained as

Table 10: Truth Tables for Boolean functions of Q.14.

x	y	z	$(x+z)\cdot y$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

x_1	x_2	x_3	$(x_2x_3+x_1x_3')\cdot(x_1x_2'+x_3)'$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

$$(x'+y'+z')\cdot(x'+y'+z)\cdot(x'+y+z')\cdot(x+y'+z')\cdot(x'+y'+z).$$

Next, considering 0 entries in the last column of the right side table, we find that the minterms are

$$x_1'+x_2'+x_3',\quad x_1'+x_2'+x_3,\quad x_1'+x_2+x_3',\quad x_1'+x_2+x_3,$$
$$x_1+x_2'+x_3',\quad x_1+x_2'+x_3,\quad \text{and}\quad x_1+x_2+x_3$$

Therefore, the CNF of g is given by the product of the above seven terms. For the second part, recall that the *algebraic method* involves inserting *missing literals* using the identity $a+0=a$. Therefore, in this case, we have

$$\begin{aligned}
f(x,y,z) =&(x+z)\cdot y\\
&= (x+0+z)\cdot(0+y)\\
&= (x+y\cdot y'+z)\cdot(x\cdot x'+y)\\
&= (x+y+z)\cdot(x+y'+z)\cdot(x+y)\cdot(x'+y)\\
&= (x+y+z)\cdot(x+y'+z)\cdot(x+y+0)\cdot(x'+y+0)\\
&= (x+y+z)\cdot(x+y'+z)\cdot(x+y+z\cdot z')\cdot(x'+y+z\cdot z')\\
&= (x+y+z)\cdot(x+y'+z)\cdot(x+y+z)\cdot(x+y+z')\cdot(x'+y+z)\cdot(x'+y+z')\\
&= (x+y+z)\cdot(x+y'+z)\cdot(x+y+z')\cdot(x'+y+z)\cdot(x'+y+z'),
\end{aligned}$$

by using the identity $a\cdot a=a$ to obtain the last equality. This is the CNF of the expression f. Finally, to obtain the CNF of the expression g by *algebraic method*, we first clear the *complementation* by using DeMorgan laws. For, we have

$$\begin{aligned}
g(x_1,x_2,x_3) &= (x_2\cdot x_3+x_1\cdot x_3')\cdot(x_1\cdot x_2'+x_3)'\\
&= (x_2\cdot x_3+x_1\cdot x_3')\cdot((x_1\cdot x_2')'\cdot x_3')\\
&= (x_2\cdot x_3+x_1\cdot x_3')\cdot((x_1'+x_2)\cdot x_3')\\
&= (x_2\cdot x_3+x_1\cdot x_3')\cdot(x_1'\cdot x_3'+x_2\cdot x_3')\\
&= (x_2\cdot x_3)\cdot(x_1'\cdot x_3')+(x_2\cdot x_3)\cdot(x_2\cdot x_3')+(x_1\cdot x_3')\cdot(x_1'\cdot x_3')+(x_1\cdot x_3')\cdot(x_2\cdot x_3')\\
&= x_1\cdot x_2\cdot x_3'.
\end{aligned}$$

Now, by using the identities $a+0=a$ and $a\cdot a'=0$ repeatedly, we have

$$\begin{aligned}
x_1 &= (x_1+x_2)\cdot(x_1+x_2')\\
&= (x_1+x_2+x_3)\cdot(x_1+x_2+x_3')\cdot(x_1+x_2'+x_3)\cdot(x_1+x_2'+x_3');\\
x_2 &= (x_1+x_2)\cdot(x_1'+x_2)\\
&= (x_1+x_2+x_3)\cdot(x_1+x_2+x_3')\cdot(x_1'+x_2+x_3)\cdot(x_1'+x_2+x_3');\\
x_3' &= (x_1+x_3')\cdot(x_1'+x_3')\\
&= (x_1+x_2+x_3')\cdot(x_1+x_2'+x_3')\cdot(x_1'+x_2+x_3')\cdot(x_1'+x_2'+x_3').
\end{aligned}$$

It thus follows that the CNF of g is given by the following product:

$$\left(x_1+x_2+x_3\right)\cdot\left(x_1'+x_2+x_3\right)\cdot\left(x_1+x_2'+x_3\right)\cdot\left(x_1+x_2+x_3'\right)\cdot\left(x_1+x_2'+x_3'\right)\cdot\left(x_1'+x_2+x_3'\right)\cdot\left(x_1'+x_2'+x_3'\right)$$

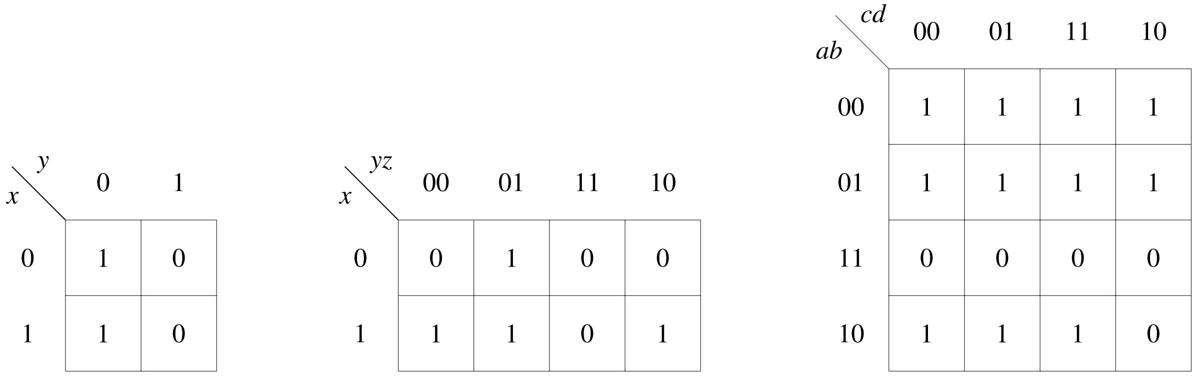
This completes the solution. ♢

8.3 Applications: Karnaugh Map

> A *Karnaugh map* is a $2D$ or a $3D$ geometric representation of the Boolean function associated with a Boolean expression representing some logic circuit. The main emphasis here is use this concept to obtain a minimal SOP or POS form of a Boolean expression.

A *minterm term* in the case of an SOP or a *maxterm term* in the case of a POS is called an **implicant**. Also, by **prime implicants** we mean all possible circles that can be formed in the K-Map. And, the prime implicants that always appear in the final minimal form is known as the **essential prime implicants**. We start with the next important definition.

Definition 8.2. *The **Karnaugh map** (or simply a **K-map**) is a geometric way to visualise the Boolean function $F : B^n \to B$ of a Boolean expression $E(x_1,\dots,x_n)$, with $n \leq 6$. It is a grid of 2^n squares such that each square has two adjacent squares, when $n = 2$; each square has three adjacent squares, when $n = 3$; each square has four adjacent squares, when $n = 4$; and, so on (see Fig 26). For each of the 2^n input values taken from the product algebra B^n, the corresponding square has 1 or 0 as the F-*value *of the expression E. A* minterm *is represented by a square with F-value 1, and a* maxterm *is represented by a square with F-value 0.*



$x \backslash y$	0	1
0	1	0
1	1	0

$x \backslash yz$	00	01	11	10
0	0	1	0	0
1	1	1	0	1

$ab \backslash cd$	00	01	11	10
00	1	1	1	1
01	1	1	1	1
11	0	0	0	0
10	1	1	1	0

Figure 26: K-maps of a Boolean functions in two and three variables.

In more precise geometric terms, , for $n = 3$, a K-map is a **cylinder** obtained by identifying the shorter edges of the 2^3-grid; and, , for $n = 4$, a K-map is a **torus** obtained by identifying opposite edges of the 2^4-grid.

To obtain a minimal *sum of products* (or simply SOP) form of a Boolean expression, we *circle together* squares with F-value 1 in powers of 2. Similarly, to obtain a minimal *product of sums* (or simply POS), we *circle together* squares with F-value 0 in powers of 2. Notice that **circling** (or **grouping**) two squares eliminates one variable; *circling* four squares eliminates two variables, and so on[12]. A minterm (or a maxterm) is said to be **covered** if it is included in at least one circle of 1's (or a circle of 0's). We need to remember the following five aspect of a K-map while computing a minimal form of a Boolean function, say an SOP:

1. Begin with *loneliest squares* to ensure *adjacencies* offer more possible combinations, which must be combined at a later stage of the process. By **adjacencies** we mean minterms with multiple adjacent minterms.

2. Circle together as many squares as possible. Of course, the larger the circle, fewer would be the number of literals in sought after SOP.

3. Cover all squares making as few circles as possible. Of course, lesser the number of circles, the fewer would be the number of product terms in minimised SOP.

4. In steps 2 and 3, a minterm can be used any number of times, subject to that it is being used at least once.

5. Stop when all the minterms are used at least once.

The algorithm given below helps to follow the above guidelines, and to ensure a high likelihood of finding the minimal SOP of a given Boolean expression. The aim is to find a minimum set of prime implicants that covers the associated Boolean function. The following algorithm generally finds a minimal solution in an easy way. However, as random choices are allowed in Step-1 and Step-2, no optimality is claimed in finding the minimum cover for the associated Boolean function.

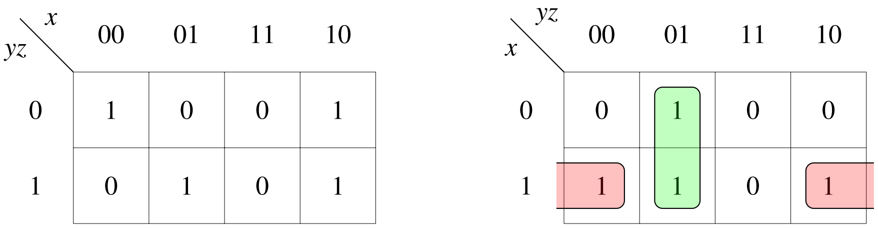
1. Count the number of *adjacencies* for each minterm of the K-map.

2. Select an uncovered minterm with lowest number of adjacencies. Choose randomly when more than one choices are available.

3. Generate a prime implicant for the chosen minterm and put it in the cover. In case it is covered by more than one prime implicant, select the one that covers the most uncovered minterms.

4. Keep repeating the previous two steps until all minterms are covered.

[12] Notice that *circling* 2^n squares eliminates all the n variables. This corresponds to the case when the Boolean expression is the constant 1 or the constant 0.



x \ yz	00	01	11	10
0	1	0	0	1
1	0	1	0	1

yz \ x	00	01	11	10
0	0	1	0	0
1	1	1	0	1

Figure 27: K-maps of a Boolean functions in three variables.

Q 71. *Use Karnaugh map to find the minimal SOP expression for the function*

$$F\left(x,y,z\right)=\sum\left(0,2,5,6\right).$$

Also draw the associated digital circuits.

Sol. We need to find a minimal SOP expression for the function

$$F\left(x,y,z\right)=\sum\left(0,2,5,6\right).$$

The associated K-map, and circling of 1's is as shown in the left and right side pictures of Fig. 27. Therefore, a minimal SOP expression is given by $y'z+xz'$. It is easy to draw the associated digital circuits. ♢

Q 72. *Use Karnaugh map to find the minimal SOP expression for the function*

$$F\left(u,v,w\right)=uv'w'+uvw'+uvw+u'v'w.$$

Also draw the associated digital circuits.

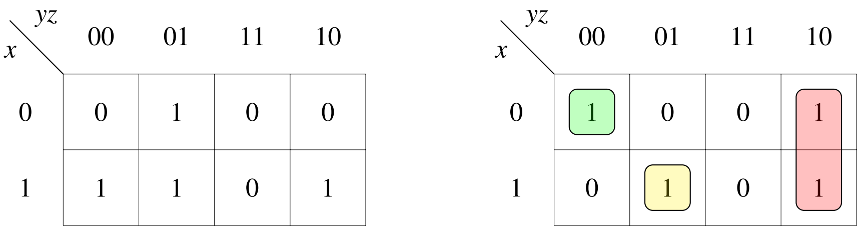
Sol. We need to find the minimal SOP expression for the function

$$F\left(u,v,w\right)=uv'w'+uvw'+uvw+u'v'w.$$

Notice that we have

$$\begin{aligned} F\left(u,v,w\right) &= uv'w'+uvw'+uvw+u'v'w \\ &= 100+110+111+001 \\ &= \sum\left(1,4,5,6\right) \end{aligned}$$

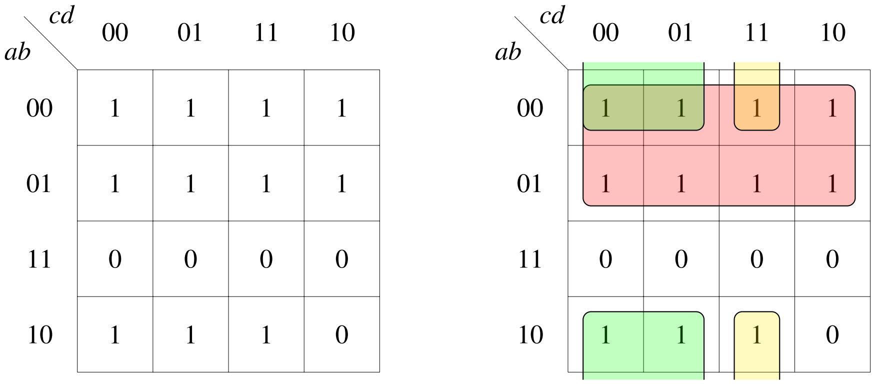
The associated K-map, and circling of 1's is as shown in the left and right side pictures of Fig. 28. Therefore, a minimal SOP expression is given by $yz'+x'y'z'+xy'z$. It is easy to draw the associated digital circuits. ♢



x \ yz	00	01	11	10
0	0	1	0	0
1	1	1	0	1

x \ yz	00	01	11	10
0	1	0	0	1
1	0	1	0	1

Figure 28: K-maps of a Boolean functions in three variables.



ab \ cd	00	01	11	10
00	1	1	1	1
01	1	1	1	1
11	0	0	0	0
10	1	1	1	0

ab \ cd	00	01	11	10
00	1	1	1	1
01	1	1	1	1
11	0	0	0	0
10	1	1	1	0

Figure 29: K-maps and circling for Q.17.

Q 73. *Use Karnaugh map to find the minimal SOP expression for the function*

$$F(a,b,c,d) = \sum(0,1,2,3,4,5,6,7,8,9,11).$$

Also draw the associated digital circuits.

Sol. We need to find the minimal SOP of the Boolean expression given by

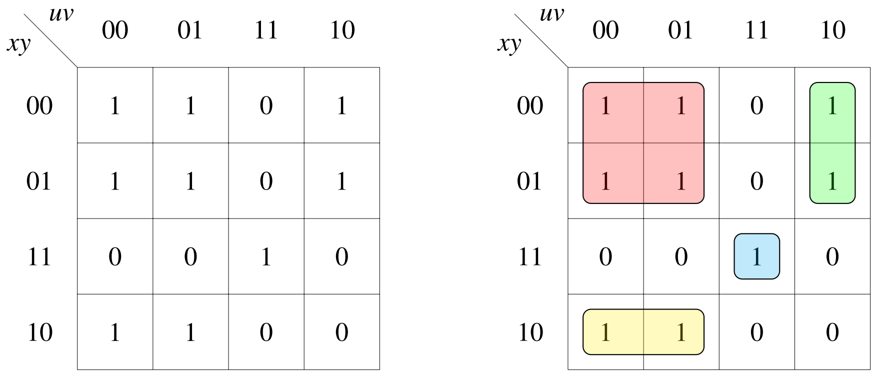
$$F(a,b,c,d) = \sum(0,1,2,3,4,5,6,7,8,9,11).$$

For the given Boolean expression, the K-map and circling of 1's are as shown in the left and right side pictures of Fig. 29. Therefore, a minimal SOP expression is given by $a' + b'c' + b'cd$. It is easy to draw the associated digital circuits. ♢

Q 74. *Use Karnaugh map to find the minimal SOP expression for the function*

$$F(x,y,u,v) = x'y'u'v' + x'y'u'v + x'y'uv' + x'yu'v' + x'yu'v + x'yuv' + xy'u'v' + xy'u'v + xyuv.$$

Also draw the associated digital circuits.



$xy \backslash uv$	00	01	11	10
00	1	1	0	1
01	1	1	0	1
11	0	0	1	0
10	1	1	0	0

$xy \backslash uv$	00	01	11	10
00	1	1	0	1
01	1	1	0	1
11	0	0	1	0
10	1	1	0	0

Figure 30: K-maps and circling for Q.18.

Sol. We need to find the minimal SOP expression for the function

$$F\left(x,y,u,v\right) = x'y'u'v' + x'y'u'v + x'y'uv' + x'yu'v' + x'yu'v + x'yuv' + xy'u'v' + xy'u'v + xyuv.$$

By simple conversion from binary to digits, it follows that we can write

$$F\left(x,y,u,v\right) = \sum\left(0,1,2,4,5,6,8,9,15\right).$$

For the above expression, the K-map and circling of 1's are as shown in the left and right side pictures of Fig. 30. Therefore, a minimal SOP expression is given by $a'c' + a'cd' + ab'c' + abcd$. It is easy to draw the associated digital circuits. ♢

9 Propositional Calculus

According to Greek philosopher Aristotle, *Thales of Miletus* was first to recognise the importance of both "what we know" and "how we know it". The ancient form of philosophical reasoning is based on five *syllogisms* introduced by Chrysippus. A symbolic treatment of these syllogisms, mainly due to George Boole, ultimately led to the development of important topics such as *propositional calculus, predicate logic*, and the *theory of inference*. In general, mathematical logic is a study of rules of *deductive reasoning* that help prove a statements of the form "if ... then ...". The related concepts as discussed in this and the next section find applications to core subjects of computer science such as data structure, algorithms, compilers design, computability, and complexity.

9.1 Propositions, Connectives, Truth Tables

Only a declarative sentence can be classified as *true* or *false*, which is called a *proposition*, and the two possible *truth values* that a proposition can take are usually denoted by T and F. We usually write a proposition as $p,q,r,\ldots$.

Definition 9.1. *A* ***compound proposition*** $P\big(p_1,\ldots,p_n\big)$ *is formed by using* **logical connectives** *such as AND ($\wedge$), OR ($\vee$), NOT ($\neg$ or ˜or ′), and also the* conditional connectives *such as* if ..., then ... $(\to)$ *and* ... if and only if ... ... $(\leftrightarrow)$*, to put together n-tuple of propositions* $\big(p_1,\ldots,p_n\big)$ *in any manner whatsoever.*

A proposition that involves no connectives is also called an *atomic proposition*. To process more involved conversation in any natural language, we combine atomic propositions using *connectives* to study *compound propositions*. The subject matter of *propositional logic* is to use propositions as variables, and describe ways to determine equivalence of various types of compound propositions by way of comparing their *truth tables* or by applying simple algebraic laws satisfied by the class of propositions with respect to two binary operations $\wedge$, $\vee$, and the unary operation $\neg$.

1. The *disjunction* of propositions p and q, denoted by $p \vee q$, is the proposition "*p or q*" with the truth value F if and only if both p and q have the truth value F. In algebraic terms, a disjunction corresponds to the *sum*;

2. The *conjunction* of propositions p and q, denoted by $p \wedge q$, is the proposition "*p and q*" with the truth value T if and only if both p and q have the truth value T. In algebraic terms, a conjunction corresponds to the *product*;

3. The negation of a proposition is the proposition with the truth value opposite to that of the given proposition. We write $\neg$ to denote "*not*". So, for any proposition p, $\neg p$ is the proposition whose truth value is the opposite to the truth value of p. In algebraic terms, $\neg$ corresponds to an involutory *unary operation*;

4. For propositions p and q, the *conditional connective*, denoted by $p \to q$, is the proposition "*if p, then q*" with the truth value F if and only if p has the truth value T and q has the truth value F. In the conditional statement $p \to q$, we call p a *hypothesis* (or *antecedent*) and q a *conclusion* (or *consequent*).

5. A *biconditional statement* "*p if and only if q*", denoted by $p \leftrightarrow q$, is the proposition whose truth value is T if and only if both p and q have the same truth value. The proposition $p \to q$ and $p \leftrightarrow q$ are usually expressed as follows:

$p \to q$	$p \leftrightarrow q$
if p, (then) q p implies q p only if q q is necessary for p p is sufficient for q	p if and only if q p is necessary and sufficient for q If p, (then) q and conversely

The first three types of connectives are *fundamental* in the sense that we can write propositions involving any other types of connectives in terms of these three connectives (also see Definition 9.8).

Example 9.1. *The sentence "*You can access the internet from campus only if you are a computer science student or you are not a freshman*" as a logical expression may be written by using the three propositions p, q, and r given by*

$$p: \text{"you are a computer science student"},$$
$$q: \text{"you are a freshman"},$$
$$r: \text{"you can access the internet from campus"}.$$

Therefore, the given sentence is a conditional statement*, with the hypothesis $p \vee \neg q$, and the conclusion r. So, the logical expression for the above sentence is $(p \vee \neg q) \to r$. Notice that its negation is the proposition $\neg((p \vee \neg q) \to r)$.*

Definition 9.2. *A tabular representation of the truth values of a compound proposition $P(p_1, \ldots, p_n)$ for 2^n truth values of its atomic propositions $p_1, \ldots, p_n$ is called a* ***truth table****.*

Q 75. *Suppose $p \to q$ is a false statement. Find the truth value of $(\neg p \vee \neg q) \to q$.*

Sol. We know that the truth value of $p \to q \equiv \neg p \vee q$ is F if and only if the truth value of p is T and the truth value of q is F. It thus follows from

$$(\neg p \vee \neg q) \to q = (\neg T \vee \neg F) \to F = F$$

that the truth value of $(\neg p \vee \neg q) \to q$ is F. $\diamondsuit$

Notice that we also have

$$\begin{aligned}(\neg p \vee \neg q) \to q &\equiv \neg(\neg p \vee \neg q) \vee q && \text{(implication as disjunction)}\\ &\equiv (p \wedge q) \vee q && \text{(DeMorgan)}\\ &\equiv q \vee (p \wedge q) && \text{(commutative)}\\ &\equiv q, && \text{(absorption)}\end{aligned}$$

which shows that, in general, the truth value of the statement $(\neg p \vee \neg q) \to q$ doesn't dependent on the truth value of the proposition p.

Q 76. *Write recursive definition of a well-formed formula, and give some examples. Also, write the following in symbolic form:* The crop will be destroyed if there is a flood.

Sol. By a *well-formed formula* (or a statement formula) we mean the following:

1. Each proposition is a statement formula, and so are the two symbols $\mathscr{T}$ and $\mathscr{F}$.
2. If P and Q are statement formulas, then so are $P \vee Q$, $P \wedge Q$, $P \to Q$, and $P \leftrightarrow Q$.
3. If P is a statement formula, then so is $\neg P$.

In general, a statement formula obtained by using the above recursive procedure finitely many times is called a *well-formed formula*. As simple illustrations, the following are some examples of statement formulas:

$$\big((p \vee q) \to r\big) \quad \text{and} \quad \big((p \wedge q) \leftrightarrow (\neg p)\big); \tag{9.1a}$$

$$\neg\big((\neg p) \vee (q \vee r)\big) \quad \text{and} \quad \neg(p \vee q) \vee \neg(\neg p \vee \neg q); \tag{9.1b}$$

$$(p \vee q) \to (p \wedge \neg q) \quad \text{and} \quad (p \to q) \to (q \to p). \tag{9.1c}$$

For the second part of the problem, we may write

$$p: \text{ There is a flood} \quad \text{and} \quad q: \text{ The crop will be destroyed,}$$

so that "*The crop will be destroyed if there is a flood*" can be expressed symbolically as $p \to q$. ◇

Notice that we can omit some parenthesis to obtain a simpler form of a statement formula. In particular, we may write the two formulas given in (9.1a) respectively as

$$(p \vee q) \to r \qquad \text{and} \qquad (p \wedge q) \leftrightarrow \neg p.$$

In general, the **order of precedence** for logical connectives is as given below:

1. The negation ($\neg$) takes precedence over all other connectives. For example, in statement formula $\neg p \vee (q \vee r)$, the negation is applied only to p. When we need to apply the negation to all the terms, we must write the statement formula $\neg p \vee (q \vee r)$ as $\neg(p \vee (q \vee r))$.
2. The conjunction ($\wedge$) takes precedence over the disjunction ($\vee$). For example, the statement formula $p \wedge q \vee r$ is read as $(p \wedge q) \vee r$, but not as $p \wedge (q \vee r)$.
3. Within a parenthesis, the conditional connective $\to$ takes precedence over the bi-conditional connective $\leftrightarrow$. In general, both $\to$ and $\leftrightarrow$ have lower precedence than all other logical connectives.

Q 77. *Construct the truth tables of the following two formulas:*

$$\neg\big(p \wedge q\big) \;\leftrightarrow \big(\neg p \vee \neg q\big) \quad \textit{and} \quad \big((p \to q) \vee r\big) \vee \big(p \to q \to r\big).$$

Sol. We write $P(p,q) := \neg\big(p \wedge q\big) \;\leftrightarrow \big(\neg p \vee \neg q\big)$. Recall the truth value of $r \leftrightarrow s$ is T if and only if r and s are both true or both false. It thus follows that the truth table for the statement formula $P(p,q)$ is given by Table 11. Notice that we used the above fact to write the truth values in the last column of this table.

Table 11: Truth Table of $\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$.

p	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$P(p,q)$
T	T	F	F	T	F	F	T
T	F	F	T	F	T	T	T
F	T	T	F	F	T	T	T
F	F	T	T	F	T	T	T

Next, we write $Q(p,q,r) := \big((p \to q) \vee r\big) \vee \big(p \to q \to r\big)$. In this case, we shall repeatedly make use of the fact that the truth value of $r \to s$ is F if and only if the truth value of r is T and the truth value of s is F. It thus follows that the truth table for the statement formula $P(p,q)$ is given by Table 12. This completes the solution. ♢

Table 12: Truth Table of $((p \to q) \vee r) \vee (p \to q \to r)$.

p	q	r	$p \to q$	$(p \to q) \vee r$	$p \to q \to r$	$Q(p,q,r)$
T	T	T	F	T	T	T
T	T	F	T	T	F	T
T	F	T	F	T	T	T
T	F	F	F	F	T	T
F	T	T	T	T	T	T
F	T	F	T	T	F	T
F	F	T	T	T	T	T
F	F	F	T	T	F	T

9.2 Converse, Inverse, and Contrapositive

The *converse, contrapositive*, and the *inverse* of a statement $p \to q$ are respectively given by

$$\begin{aligned}\textbf{Converse}: &\quad q \to p;\\ \textbf{Contrapositive}: &\quad \neg q \to \neg p;\\ \textbf{inverse}: &\quad \neg p \to \neg q.\end{aligned}$$

Notice that we use symbols $p, q, r, \ldots$ only as an aid to write the above for any given statement written in a *natural language* such as English. The real emphasis must be on writing these as statements in the same *natural language*, which one can do without using symbols.

Q 78. *Write the* converse, contrapositive*, and* inverse *of the following statements:*

(i) If it rains, then I will not go to market.

(ii) I am in trouble if the work is not finished on time.

Sol. Let p : *It rains*, and q : *I will go to market*, so the statement (i) can be expressed symbolically as $p \to \neg q$. Therefore, the *converse, contrapositive*, and *inverse* are respectively given by

$$\begin{aligned}&\text{If I will not go to market, then it rains } (\neg q \to p);\\ &\text{If I will go to market, then it rains } (q \to \neg p);\\ &\text{If it doesn't rain, then I will go to market } (\neg p \to q).\end{aligned}$$

Next, let p : *The work is finished on time*, and q : *I am in trouble*, so the statement (ii) can be expressed symbolically as $\neg p \to q$. Therefore, the *converse, contrapositive*, and *inverse* are respectively given by

$$\begin{aligned}&\text{If I am in trouble, then the work is not finished on time } (q \to \neg p);\\ &\text{If am not in trouble, then the work is finished on time } (\neg q \to p);\\ &\text{If the work is finished on time, then I am not in trouble } (p \to \neg q).\end{aligned}$$

This completes the solution. ♢

9.3 Tautology, Contradiction or Contingency

We start with next definitions. We are using “statement" and “propositional formula" interchangeably.

Definition 9.3. *A* universally true *statement is called a **tautology**. We usually write a tautology as $\mathscr{T}$ (or simply* **T***).*

Therefore, a *tautology* is a propositional formula that has the truth value T, irrespective of the truth values assigned to the individual propositions involved. That is, each entry in the last column of the related truth table is T. For example, the statement "*the sum of an odd integer and an even integer is an odd integer*" is a tautology. In general, the propositional formula $p \vee \neg p$ is a tautology, and so is $(p \vee q) \vee \neg p$. Also, the propositional formula $(p \to q) \leftrightarrow (\neg p \vee q)$ is a tautology.

Definition 9.4. A universally false *statement is called a* ***contradiction***. *We usually write a contradiction as* $\mathscr{F}$ *(or simply* **F**).

Therefore, a *contradiction* is a propositional formula that has the truth value F, irrespective of the truth values assigned to the individual propositions involved. That is, each entry in the last column of the related truth table is F. For example, the statement "*there is no integral solution to the equation* $x^2 + y^2 = z^2$" is a contradiction. In general, the propositional formula $p \wedge \neg p$ is a contradiction, and so is $q \wedge (p \wedge \neg q)$.

Definition 9.5. *A propositional formula that is neither a tautology nor a contradiction is called a* ***contingency*** *(or a* ***satisfiable formula****).*

Q 79. *Use truth table to determine which of the following is a tautology or a contradiction:*

(i) $\neg\big(q \to r\big) \wedge r \wedge \big(p \to q\big)$.

(ii) $\big((p \vee q) \wedge (p \to r) \wedge (q \to r)\big) \to r$.

Sol. We may write $P(p,q,r) := \neg\big(q \to r\big) \wedge r \wedge \big(p \to q\big)$. Then, the truth table for the statement formula in (i) is as given by Table 13. Therefore, the statement formula in (i) is a contradiction. Next, we may write $Q(p,q,r) := \big((p \vee q) \wedge (p \to r) \wedge (q \to r)\big)$ and $R(p,q,r) := \big((p \vee q) \wedge (p \to r) \wedge (q \to r)\big) \to r$. Then, the truth table for the statement formula in (ii), the truth table is given by Table 14. Therefore, the statement formula in (ii) is a tautology. ♢

Table 13: Truth Table for $P(p,q,r)$ of $Q.5(i)$.

p	q	r	$q \to r$	$\neg(q \to r)$	$p \to q$	$P(p,q,r)$
T	T	T	T	F	T	F
T	T	F	F	T	T	F
T	F	T	T	F	F	F
T	F	F	T	F	F	F
F	T	T	T	F	T	F
F	T	F	F	T	T	F
F	F	T	T	F	T	F
F	F	F	T	F	T	F

Table 14: Truth Table for $Q(p,q,r)$ of $Q.5(ii)$.

p	q	r	$p\vee q$	$p\rightarrow r$	$q\rightarrow r$	$Q(p,q,r)$	$R(p,q,r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	T	T	T	T	T
T	F	F	T	F	T	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	F	F	T
F	F	T	F	T	T	F	T
F	F	F	F	T	T	F	T

9.4 Equivalences & Implications

We begin with the next definition.

Definition 9.6. *We say a proposition p (logically)* ***implies*** *q if and only if p $\Rightarrow$ q is a tautology. In this case, we write p $\rightarrow$ q. Further, we say two propositions p and q are (logically)* ***equivalent*** *if and only if p $\Leftrightarrow$ q is a tautology. In this case, we write p $\leftrightarrow$ q.*

Therefore, two propositions are treated *logically equivalent* if they have the same truth values irrespective of the truth values assigned to the individual propositions involved. We can use $\leftrightarrow$ to define equivalence relation on the collection of all propositions. Notice that $p\leftrightarrow q$ if and only if $p\Rightarrow q$ and $q\Rightarrow p$. In general, we can prove the equivalences and implications by constructing the truth tables or by using other equivalences.

Definition 9.7. *For a conditional statement p $\Rightarrow$ q, the proposition q $\Rightarrow$ p is called its* converse*; the proposition $\neg p\Rightarrow\neg q$ is called the inverse; and, the proposition $\neg q\Rightarrow\neg p$ is called its* contrapositive.

Notice that, for every pair p,q, the conditional proposition $p\Rightarrow q$ and its contrapositive $\neg q\Rightarrow\neg p$ are equivalent; also, the converse $q\Rightarrow p$ and inverse $\neg p\Rightarrow\neg q$ are equivalent. The detachment law (or *modus ponens*) states that

$$(p\Rightarrow q)\wedge p\Rightarrow q.$$

The contrapositive (or *modus tollens*) states that

$$(p\rightarrow q)\wedge\neg q\Rightarrow\neg p.$$

The chain rule (or *hypothetical syllogism*) states that

$$(p\rightarrow q)\wedge(q\rightarrow r)\Rightarrow(p\rightarrow r).$$

It follows easily that $p\Rightarrow(p\vee q)$. In general, we can prove implications by using truth tables or by using *known equivalences*. Recall that $p\rightarrow q$ if $p\Rightarrow q$ is a tautology. Now, when p is a conjunction of the propositions $p_1,p_2,\dots,p_n$ and q (logically) follows from $p_1,\dots,p_n$, we write

$$(p_1\wedge p_2\wedge\cdots\wedge p_n)\Rightarrow q,$$

where $p_1, p_2, \ldots, p_n$ are called the *premises* of the (valid) conclusion q. We can also show that p follows from $p_1, \ldots, p_n$ by constructing the truth table for the expression $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Rightarrow q$.

Theorem 80. *If $p_1, p_2, \ldots, p_n$ and p imply q, then $p_1, p_2, \ldots, p_n$ imply $p \to q$.*

Proof. As $(p_1 \wedge \cdots \wedge p_n \wedge p) \Rightarrow q$, so

$$(p_1 \wedge \cdots \wedge p_n \wedge p) \Rightarrow q$$

is a tautology. We also have that the following equivalence holds:

$$(r \wedge s) \to t \quad \leftrightarrow \quad r \to (s \to t.)$$

It thus follows that

$$(p_1 \wedge \cdots \wedge p_n) \Rightarrow (p \to q)$$

is a tautology, and hence

$$(p_1 \wedge \cdots \wedge p_n) \to (p \to q),$$

as asserted. □

Definition 9.8. *A set of connectives is called* functionally independent *if it is possible to write every proposition involving any other types of connectives in terms of such types of connectives.*

It follows from above discussion that the following three sets of connectives are *functionally independent*:

$$C_1 = \{\vee, \neg\}, \qquad C_2 = \{\wedge, \neg\}, \qquad C_3 = \{\to, \neg\}$$

Q 81. *Use truth table to show that $p \to q \equiv \neg p \vee q \equiv \neg q \to \neg p$.*

Sol. The truth tables for the three statement formulas $p \to q$, $\neg p \vee q$, and $\neg q \to \neg p$ are as given in Table 15. The third and fifth columns of this table proves the equivalence $p \to q \equiv \neg p \vee q$, and the fifth and seventh columns proves the equivalence $\neg p \vee q \equiv \neg q \to \neg p$. ♢

Table 15: Truth Table for *Q*.6.

p	q	$p \to q$	$\neg p$	$\neg p \vee q$	$\neg q$	$\neg q \to \neg p$
T	T	T	F	T	F	T
T	F	F	F	F	T	F
F	T	T	T	T	F	T
F	F	T	T	T	T	T

Q 82. *Use truth table to show that $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$.*

Table 16: Truth Table for *Q*.7.

p	q	$\neg p$	$\neg q$	$p\wedge q$	$\neg p\wedge\neg q$	$p\leftrightarrow q$	$p\to q$	$q\to p$	$(p\to q)\wedge(q\to p)$	$(p\wedge q)\vee(\neg p\wedge\neg q)$
T	T	F	F	T	F	T	T	T	T	T
T	F	F	T	F	F	F	F	T	F	F
F	T	T	F	F	F	F	T	F	F	F
F	F	T	T	F	T	T	T	T	T	T

Sol. Recall that the truth value of the bi-conditional $r\leftrightarrow s$ is T if and only if r and s are both true or both false.The truth tables for the three statement formulas $p\leftrightarrow q$, $\big(p\to q\big)\wedge\big(q\to p\big)$, and $\big(p\vee q\big)\vee\big(\neg p\wedge\neg q\big)$ are as given in Table 16. The seventh and tenth columns of this table proves the first equivalence, and the tenth and eleventh columns proves the second equivalence. ♢

Q 83. *Prove the following equivalences, without using truth tables:*

(i) $\big(p\to r\big)\wedge\big(q\to r\big)\;\equiv\;\big(p\vee q\big)\to r.$

(ii) $\big((p\wedge q\wedge a)\to r\big)\wedge\big(a\to(p\vee q\vee r)\big)\;\equiv\;\big((p\leftrightarrow q)\wedge a\big)\to r.$

Sol. For (i), we have

$$\begin{aligned}\big(p\to r\big)\wedge\big(q\to r\big) &\equiv \big(\neg p\vee r\big)\wedge\big(\neg q\vee r\big) && \text{(implication as disjunction)}\\ &\equiv \big(\neg p\wedge\neg q\big)\vee r && \text{(distributivity)}\\ &\equiv \neg(p\vee q)\vee r && \text{(DeMorgan)}\\ &\equiv \big(p\vee q\big)\to r && \text{(implication as disjunction)}\end{aligned}$$

For (ii), we start by using *implication as disjunction* so that we have

$$\begin{aligned}\big((p\wedge q\wedge a)\to r\big)\wedge\big(a\to(p\vee q\vee r)\big) &\equiv \big(\neg(p\wedge q\wedge a)\vee r\big)\wedge\big(\neg a\vee(p\vee q\vee r)\big)\\ &\equiv \big((\neg p\vee\neg q\vee\neg a)\vee r)\big)\wedge\big((\neg a\vee p\vee q)\vee r\big) && \text{(DeMorgan)}\\ &\equiv \big((\neg p\vee\neg q\vee\neg a)\vee r\big)\wedge\big((p\vee q\vee\neg a)\vee r)\big) && \text{(commutative)}\\ &\equiv \big((\neg p\vee\neg q\vee\neg a)\wedge(p\vee q\vee\neg a)\big)\vee r && \text{(distributivity)}\\ &\equiv \big(((\neg p\vee\neg q)\wedge(p\vee q))\vee\neg a\big)\vee r && \text{(distributivity)}\\ &\equiv \big(\neg\big[(p\wedge q)\vee(\neg p\wedge\neg q)\big]\vee\neg a\big)\vee r && \text{(DeMorgan)}\\ &\equiv \neg\big(\big[(p\wedge q)\vee(\neg p\wedge\neg q)\big]\wedge a\big)\vee r && \text{(DeMorgan)}\\ &\equiv \neg\big((p\leftrightarrow q)\wedge a\big)\vee r && \text{(equivalence in Q.7)}\\ &\equiv \big((p\leftrightarrow q)\wedge a\big)\to r && \text{(implication as disjunction)}\end{aligned}$$

This completes the solution. ♢

Q 84. *Without using truth tables, obtain an equivalent formula for the implication* $p \wedge \big(q \leftrightarrow r\big) \rightarrow q$ *that doesn't contain any conditional connectives.*

Sol. We first use the equivalence $q \leftrightarrow r \equiv (q \wedge r) \vee (\neg q \wedge \neg r)$ so that we have

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

It thus follows that

$$\begin{aligned} p \wedge \big(q \leftrightarrow r\big) \rightarrow q &\equiv \neg\big(p \wedge (q \leftrightarrow r)\big) \vee q \\ &\equiv \big(\neg(p \wedge q \wedge r) \wedge \neg(p \wedge \neg q \wedge \neg r)\big) \vee q \\ &\equiv \big((\neg p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee r)\big) \vee q \\ &\equiv (\neg p \vee \neg q \vee \neg r \vee q) \wedge (\neg p \vee q \vee r \vee q) \\ &\equiv (\neg p \vee \neg r \vee \mathscr{T}) \wedge (\neg p \vee q \vee r) \\ &\equiv \mathscr{T} \wedge (\neg p \vee q \vee r) \\ &\equiv \neg p \vee q \vee r, \end{aligned}$$

which is equivalent formula without any conditional connectives. ♢

Q 85. *Prove the following fundamental implications:*

*(i) (*Modus Ponens*)* $\big(p \rightarrow q\big) \wedge p \Rightarrow q.$

*(ii) (*Modus Tollens*)* $\big((p \rightarrow q\big) \wedge \neg q \Rightarrow \neg p.$

*(iii) (*Hypothetical Syllogism*)* $\big(p \rightarrow q\big) \wedge \big(q \rightarrow r\big) \Rightarrow \big(p \rightarrow r\big).$

*(iv) (*Disjunctive Syllogism*)* $\big(p \vee q\big) \wedge \neg p \Rightarrow q.$

Sol. For (i), we have

$$\begin{aligned} \big(p \rightarrow q\big) \wedge p \rightarrow q &\equiv \big(\neg p \vee q\big) \wedge p \rightarrow q && \text{(implication as disjunction)} \\ &\equiv \big((\neg p \wedge p) \vee (q \wedge p)\big) \rightarrow q && \text{(distributivity)} \\ &\equiv \big(\mathscr{F} \vee (q \wedge p)\big) \rightarrow q && \text{(complementation)} \\ &\equiv (q \wedge p) \rightarrow q && \text{(identity law)} \\ &\equiv \neg(q \wedge p) \vee q && \text{(implication as disjunction)} \\ &\equiv \big(\neg q \vee \neg p\big) \vee q && \text{(DeMorgan)} \\ &\equiv \big(\neg q \vee q\big) \vee \neg p && \text{(commutativity)} \\ &\equiv \mathscr{T} \vee \neg p && \text{(identity law)} \\ &\equiv \mathscr{T} && \text{(dominance)} \end{aligned}$$

We have thus shown that $\big(p \to q\big) \wedge p \to q$ is a tautology. Next, for (ii), we have

$$\begin{aligned}
\big(p \to q\big) \wedge \neg q \to \neg p &\equiv \big(\neg p \vee q\big) \wedge \neg q \ \to\ \neg p && \text{(implication as disjunction)}\\
&\equiv \big((\neg p \wedge \neg q) \vee (q \wedge \neg q)\big) \to \neg p && \text{(distributivity)}\\
&\equiv \big(\neg(p \vee q) \vee \mathscr{F}\big) \to \neg p && \text{(DeMorgan \& complementation)}\\
&\equiv \neg(p \vee q) \to \neg p && \text{(identity law)}\\
&\equiv p \vee q \vee \neg p && \text{(implication as disjunction)}\\
&\equiv \big(p \vee \neg p\big) \vee q && \text{(commutativity)}\\
&\equiv \mathscr{T} \vee q && \text{(complementation)}\\
&\equiv \mathscr{T} && \text{(dominance)}
\end{aligned}$$

We have thus shown that $\big((p \to q\big) \wedge \neg q \ \to\ \neg p$ is a tautology. Also, for (iii), we have

$$\begin{aligned}
\big(p \to q\big) \wedge \big(q \to r\big) &\equiv \big(\neg p \vee q\big) \wedge \big(\neg q \vee r\big) && \text{(implication as disjunction)}\\
&\equiv \big((\neg p \wedge \neg q) \vee (\neg p \wedge r)\big) \vee \big((q \wedge \neg q) \vee (q \wedge r)\big) && \text{(distributivity)}\\
&\equiv \big((\neg p \wedge \neg q) \vee (\neg p \wedge r)\big) \vee \big(\mathscr{F} \vee (q \wedge r)\big) && \text{(complementation)}\\
&\equiv \big((\neg p \wedge \neg q) \vee (\neg p \wedge r)\big) \vee (q \wedge r) && \text{(identity law)}\\
&\equiv \big((\neg p \wedge \neg q) \vee (q \wedge r)\big) \vee (\neg p \wedge r) && \text{(commutativity \& associativity)}\\
&\equiv \big(((\neg p \vee q) \wedge (\neg p \vee r)) \wedge ((\neg p \vee r) \wedge (\neg q \vee r))\big) \vee (\neg p \wedge r) && \text{(distributivity)}\\
&\equiv \big((\neg p \vee q) \wedge (\neg p \vee r) \wedge (\neg q \vee r)\big) \vee (\neg p \wedge r) && \text{(idempotent law)}\\
&\equiv \big((\neg p \vee q) \vee (\neg p \wedge r)\big) \wedge (\neg p \vee r) \wedge \big((\neg q \vee r) \vee (\neg p \wedge r)\big) && \text{(distributivity \& idempotent)}\\
&\equiv (\neg p \vee q) \wedge (\neg p \vee r) \wedge (\neg q \vee r) && \text{(see below)}\\
&\equiv (\neg p \vee q) \wedge \big((\neg p \wedge \neg q) \vee r)\big) && \text{(distributivity)}\\
&\equiv (\neg p \vee q) \wedge \big(\neg(p \vee q) \vee r)\big) && \text{(DeMorgan)}\\
&\equiv (p \to q) \wedge \big((p \vee q) \to r)\big) && \text{(implication as disjunction)}\\
&\equiv p \to r && \text{(by } (ii) \text{ and } (iv))
\end{aligned}$$

Above we have used the following equivalences:

$$(\neg p \vee q) \vee (\neg p \wedge r) \equiv \big((\neg p \vee q) \vee \neg p\big) \wedge \big((\neg p \vee q) \vee r\big) \equiv \big(\neg p \vee q\big) \wedge \big(\neg p \vee q \vee r\big) \equiv \neg p \vee q$$

$$(\neg q \vee r) \vee (\neg p \wedge r) \equiv \big((\neg q \vee r) \vee \neg p\big) \wedge \big((\neg q \vee r) \vee r\big) \equiv \big(\neg q \vee r \vee \neg p\big) \wedge \big(\neg q \vee r\big) \equiv \neg q \vee r$$

It thus follows that $\big(p \to q\big) \wedge \big(q \to r\big) \to \big(p \to r\big)$ is a tautology. Finally, for (iv), we have

$$\begin{aligned}\big(p \vee q\big) \wedge \neg p \to q &\equiv \big((p \wedge \neg p) \vee (q \wedge \neg p)\big) \to q && \text{(distributivity)}\\ &\equiv \big(\mathscr{F} \vee (q \wedge \neg p)\big) \to q && \text{(complementation)}\\ &\equiv (q \wedge \neg p) \to q && \text{(identity)}\\ &\equiv \neg(q \wedge \neg p) \vee q && \text{(implication as disjunction)}\\ &\equiv (\neg q \vee p) \vee q && \text{(DeMorgan)}\\ &\equiv (\neg q \vee q) \vee p && \text{(commutativity)}\\ &\equiv \mathscr{T} \vee p && \text{(complementation)}\\ &\equiv \mathscr{T} && \text{(dominance)}\end{aligned}$$

We have thus shown that $\big(p \vee q\big) \wedge \neg p \to q$ is a tautology. ♢

9.5 Rules of Inference

Q 86. *Describe Rule - P, Rule - T, and Rule - CP of logical deductive reasoning.*

Sol. *Rule - P* states that a premise may be introduced as an argument at any step. *Rule - T* states that a statement formula may be introduced as an argument at any step, subject to it is tautologically implied by one or more preceding formulas. *Rule - CP* states that if a formula s can be derived from another formula r, together with a set of premises p, then the statement $r \to s$ can be derived from the set of premises alone. That is, in symbolical terms, we have $p \to (r \to s) \equiv (p \wedge r) \to s$. ♢

Q 87. *What is a* consistent *and* inconsistent *premises? Show that the premises* $r \to \neg q,\ r \vee s,\ s \to \neg q,\ p \to q \ \Rightarrow\ \neg p$ *are consistent. Also, show that the premises* $p \to q,\ p \to r,\ q \to \neg r,\ p$ *are inconsistent.*

Sol. A set of premises $h_1, \ldots, h_n$ are said to be *inconsistent* if $h_1 \wedge \cdots \wedge h_n \to \mathscr{F}$, i.e., they lead to a contradiction. Otherwise, we say premises $h_1, \ldots, h_n$ are *consistent*. We first show that the premises given by

$$r \to \neg q, \quad r \vee s, \quad s \to \neg q, \quad p \to q, \quad \neg p$$

are consistent. That is, we show that the above premises don't lead to a contradiction.

(1)	$p \to q$	*Rule - P*
(2)	$r \to \neg q$	*Rule - P*
(3)	$q \to \neg r$	(2), *Rule - T* (contrapositive)
(4)	$p \to \neg r$	(1), (3), hypothetical syllogism
(5)	$s \to \neg q$	*Rule - P*

(6)	$q \to \neg s$	(5), *Rule - T* (contrapositive)
(7)	$p \to \neg s$	(1),(6), hypothetical syllogism
(8)	$\neg p$	(5), (7), modus ponens
(9)	$p \wedge \neg p \equiv \mathscr{F}$	(1), (8)

Next, we show that the premises given by

$$p \to q, \quad p \to r, \quad q \to \neg r, \quad p$$

are inconsistent. That is, we show that the above premises implies a contradiction.

(1)	p	*Rule - P*
(2)	$p \to q$	*Rule - P*
(3)	q	(1), (2), modus ponens
(4)	$q \to \neg r$	*Rule - P*
(5)	$\neg r$	(3), (4), modus ponens
(6)	$p \to r$	*Rule - P*
(7)	$\neg r \to \neg p$	(6), *Rule - T* (contrapositive)
(8)	$\neg p$	(5), (7), modus ponens
(9)	$p \wedge \neg p \equiv \mathscr{F}$	(1), (8)

This completes the solution. ♢

Q 88. *Check the validity of the argument:* If I try hard, and I have talent, then I will become a scientist. If I become a scientist, then I will be happy. Therefore, if I will not be happy, then I did not try hard or I do not have talent.

Sol. We may write

p : I try hard	q : I have talent
r : I will become a scientist	s : I will be happy

Then, in symbolic form, the given argument may be expressed as

$$p \wedge q \to r, \quad r \to s \qquad \Rightarrow \qquad \neg s \to \neg p \vee \neg q$$

We have

(1)	$p \wedge q \to r$	*Rule - P*
(2)	$r \to s$	*Rule - P*
(3)	$p \wedge q \to s$	(1), (2), hypothetical syllogism
(4)	$\neg s \to \neg(p \wedge q)$	(4), *Rule - T* (contrapositive)
(5)	$\neg s \to \neg p \vee \neg q$	(4), *Rule - T* (DeMorgan law)

Therefore, the argument is valid. ♢

Q 89. *Check the validity of the argument:* If the traffic is heavy, then travelling is difficult. If customers arrived on time, then travelling was not difficult. They arrived on time. Therefore, the traffic was not heavy.

Sol. We may write

p : the traffic is heavy	q : travelling is difficult
r : customers arrived on time	

Then, in symbolic form, the given argument may be expressed as

$$p \to q, \quad r \to \neg q, \quad r \qquad \Rightarrow \qquad \neg p$$

We have

(1)	$p \to q$	*Rule - P*
(2)	$\neg q \to \neg p$	(1), *Rule - T* (contrapositive)
(3)	$r \to \neg q$	*Rule - P*
(4)	$r \to \neg p$	(3), (2), hypothetical syllogism
(5)	r	*Rule - P*
(6)	$\neg p$	(4), (5), modus ponens

Therefore, the argument is valid. ♢

10 First Order Logic

As an improvement over propositional calculus, **first order logic** (or simply FOL) is used to express any types of mathematical relations or sentences written in a natural language such as English in terms of variables or subjects, predicates, standard logical connectivities, and logical quantifiers such as $\forall$ (“for all" or “every") and $\exists$ (“for some" or “there is one").

10.1 Predicate Logic & Quantifiers

Definition 10.1. *By a **predicate** P in certain finite number of variables (or subjects) $x_1, \dots, x_n$ we mean a property or a relation that these variables satisfy. In this case, we write the n-variable predicate as $P(x_1, \dots, x_n)$.*

For example, we can write the sentence “x is a bird" as the predicate $\text{Bird}(x)$, and the predicate $\text{Fly}(x)$ stands for the sentence “x can fly". Both these predicates involve a single variable x that takes values in the set of “all birds", which is a *universe of discourse* of the two predicates.

Definition 10.2. *Let $P(x_1, \dots, x_n)$ be an n-variable predicate. The set of “values" that the variables $x_1, \dots, x_n$ may take is called a **universe of discourse** (or simply a **universe** or a **domain**) of the predicate P. Any particular value in a universe of a predicate such as the name of an individual or a place or a thing is called a **constant**.*

For example, $\text{Love}(x,y)$ for the sentence “x loves y" is a two-variable predicate.

Remark 10.1. *In general, a predicate $P(x_1, \dots, x_n)$ may not be a proposition unless the variables $x_1, \dots, x_n$ are assigned “values" from the associated* universe of discourse*. For example, both $Bird(parrot)$ and $Fly(pigeon)$ are propositions with the truth value T. Whereas $Fly(ostrich)$ is also a proposition, but the truth value in this case is F.*

It is important to remember that we quantify over variables or subjects, but never over properties. For example, we can express the sentence “*All birds can fly*" as

$$\forall x \left[\text{Bird}(x) \to \text{Fly}(x)\right].$$

Also, to say that something is a cube and it is large we write

$$\exists x \left[\text{Cube}(x) \wedge \text{Large}(x)\right].$$

Further, in terms of the two-variable predicate $\text{Love}(x,y)$, we can express the sentence “*Everybody loves somebody*" as

$$\forall x \exists y \, \text{Love}(x,y),$$

with the set of people as a *domain* for both variables x and y.

Definition 10.3. *A statement or sentence is called a* ***nested predicate*** *if it involves predicates, standard logical connectives, and the two universal quantifiers.*

One of the most important aspect of first order logic is to transform mathematical statements or a sentences into machine compatible logical expressions involving *nested predicates*. Such a skill has enormous potential for applications in computer science related to fundamental topics such as *programming, artificial intelligence, software engineering*, and in many other allied disciplines. The purpose of the next question is to help you have some practice how to deal with *nested sentences*[13].

Q 90. *Transform the statements given below as expressions involving predicates, logical connectives, and, the two universal quantifiers:*

(i) Not all birds can fly.

(ii) Everybody loves somebody.

(iii) Some men are genius.

(iv) There is somebody whom no one loves.

(v) No student has done every problem in the assignment.

(vi) Every real number is either negative or has a square root.

(vii) There is a barber who shaves all men in the town who do not shave themselves.

Sol. We first consider the statement "*All birds can fly*". Take the predicates

$$B(x): \; x \text{ is a bird} \qquad F(x): \; x \text{ can fly}$$

Then, the statement *All birds can fly* may be expressed as

$$\forall x \left[B(x) \to F(x) \right].$$

Now, since (i) is the *negation* of the statement "*All birds can fly*", it follows that the statement "*Not all birds can fly*" may be expressed as

$$\neg\left\{ \forall x \left[B(x) \to F(x) \right] \right\} \equiv \exists x \left[B(x) \wedge \neg F(x) \right].$$

Notice that the statement "*Not all birds can fly*" may be expressed simply as $\exists x \neg F(x)$, provided the *universe* for the predicate variable x is taken as the set of all birds. For (ii), we take the two-variable predicate

$$L(x,y): \; x \text{ loves } y$$

[13] For compatibility, the notations used in the solution are same as in the prescribed book.

so that the statement “*Everybody loves somebody*" may be expressed as

$$\forall x \exists y\, L(x,y),$$

where the universe for both variables x and y consists of all people in the world. For (iii), take the predicates

$$M(x): \; x \text{ is a man} \qquad G(x): \; x \text{ is genius}$$

Then, the statement *Some men are genius* may be expressed as

$$\exists x \left[M(x) \to G(x)\right].$$

As said earlier, the same statement may be expressed simply as $\exists x\, G(x)$, provided the *universe* for x is taken as the set of all men. For (iv), once again, we take the two-variable predicate $L(x,y): \; x$ loves y so that the statement “*There is somebody whom no one loves*" may be expressed as

$$\neg\big\{[\forall x \exists y\, L(x,y)\big\} \equiv \exists x \forall y\; \neg L(x,y),$$

where the universe for both variables x and y consists of all people in the world. For (v), take the two-variable predicate

$$D(x,y): \; x \text{ has done the problem } y \text{ of the assignment}$$

so that the statement “*No student has done every problem in the assignment*" may be expressed as

$$\neg\left(\exists x \forall y\, D(x,y)\right),$$

where the universe for x are students and y consists of assignment problems. For (vi), take the predicates

$$N(x): \; x \text{ is negative} \qquad S(x): \; x \text{ has a square root}$$

Then, the statement *Every real number is either negative or has a square root* may be expressed as

$$\forall x \left[N(x) \vee S(x)\right],$$

where the universe for x are real numbers. For (vii), take the two-variable predicate

$$B(y): \; y \text{ is a barber} \qquad S(x,y): \; x \text{ shaves } y$$

so that the statement “*There is a barber who shaves all men in the town who do not shave themselves*" may be expressed as

$$\exists y \left(B(y) \wedge \forall \left[\neg S(x,x) \to S(y,x)\right]\right),$$

where the universe for both x and y are all men. In simple terms, taking $y = b$ (barber), the above statement may also be expressed as

$$\exists b \forall x \left[\neg S(x,x) \to S(b,x)\right]$$

This completes the solution. ♢

Remark 10.2. *Do remember that there is no “cookbook approach" to above types of problems. Each such problem has to be dealt with some level of ingenuity. Also, there may be more one ways to express a particular statement. More you practice, better would be the chances of you doing it right.*

10.2 Theory of Inference

Q 91. *Giving suitable example in each case, describe **rules of specification**: Rule - US and Rule - ES, and also **rules of generalisation**: Rule - UG, and Rule - EG that one applies to deal with predicate formulas involving quantifiers.*

Sol. Since $\forall x\, P(x)$ is true if and only if $P(x)$ is true for every x in the universe of discourse, the implication $(x)P(x) \;\Rightarrow\; P(y)$ holds. This is known as the **rule of universal specification** (or simply *Rule - US*). Notice that $P(y)$ is a proposition and y is in the universe. For example, consider

Similarly, when we have $P(x)$ is true for all x, it follows that $\forall x\; P(x)$ is true. That is, $P(x) \;\Rightarrow\; \forall y\; P(y)$ holds. This is known as the **rule of universal generalization** (or simply *Rule - UG*). For example, consider

Next, if $(\exists x)P(x)$ is true, then $P(x)$ is true for some a in the universe, and so we have the implication $(\exists x)P(x) \;\Rightarrow\; P(a)$. This is called as the **rule of existential specification** (or simply *Rule - ES*). For example, consider

Also, if $P(x)$ is true for at least one subject $x = a$ in the universe of discourse, then we have the conclusion $P(a) \;\Rightarrow\; (\exists x)P(x)$. This is known as the **rule of existential generalization** (or simple *Rule - EG*). For example, consider ♢

> Something that is true in all possible circumstances is called a **logical truth**, and an argument is **valid** if the conclusion is true in every possible circumstance in which its premises is true. In propositional logic, truth-tables are apt to express the notion of “possible circumstances", where a possible circumstance is represented as a row of the truth table. However, since there are valid arguments that are not truth table based valid, and also there are logical truths that are not tautologies, we need to make precise the idea of *possible circumstances* while dealing with statement functions involving quantifiers. Said differently, we must provide a more accurate account of what it means to be a FOL truth, a FOL consequence, or a FOL equivalence. The core idea is FOL validities (or consequences, or equivalences) are truths (or consequences, or equivalences) solely by virtue of the truth functional connectives, the quantifiers, and the identity symbol. That is, to determine whether a statement is an FOL valid (or an argument a case of FOL consequence, or a pair of statements FOL equivalent) we ignore the meanings of the names and predicates they contain.

Definition 10.4. *Let S and T be two statement functions involving predicates and quantifiers. We say S and T are **FOL equivalent**, denoted by $S \equiv T$, if they have the same truth value no matter which predicates are substituted for these statements, and which domain of discourse is used for the involved predicate variables.*

For an illustration, we prove below the fact that *universal quantifier distributes over conjunction*. That is,

$$\forall x \left[P(x) \wedge Q(x)\right] \equiv \forall x P(x) \wedge \forall x Q(x). \tag{10.1}$$

For, suppose P and Q are particular predicates with a common domain of discourse such that $\forall x\,\big[P(x)\wedge Q(x)\big]$ is true. Then, $P(a)\wedge Q(a)$ is true, for any a in the domain. Therefore, $P(a)$ is true for any a in the domain, and also $Q(a)$ is true for any a in the domain. Hence, $\forall x P(x)\wedge\forall x Q(x)$ is true. Similarly, we can prove the converse. Further, in the same way, it can be shown that *existential quantifier distributes over a disjunction*. That is,

$$\exists x\,\big[P(x)\vee Q(x)\big]\equiv\exists x P(x)\vee\exists x Q(x). \tag{10.2}$$

It is easy to find examples to prove that the equivalence given in (10.1) don't hold when the *conjunction* is replaced with *disjunction*. For example, with the set of integers $\mathbb{Z}$ as domain, let

$$P(x):\ x \text{ is even} \qquad \text{and} \qquad Q(x):\ x \text{ is odd}$$

Then $\forall x\,\big[P(x)\vee Q(x)\big]$ means every integer x is either even or odd, which is true, but $\forall x P(x)\vee\forall x Q(x)$ is absurd. Also the equivalence given in (10.2) don't hold when the *disjunction* is replaced with *conjunction*. For example, with $P(x)$ and $Q(x)$ as above, we have $\big(\exists x\, P(x)\big)\wedge\big(\exists y\, Q(y)\big)$ means there is an even integer x and there is an odd integer y, which is true, but $\exists x\ \big[P(x)\wedge Q(x)\big]$ is absurd because there is no integer that's both even and odd. In the next question, we prove which part of the two-way implications are stronger.

The purpose of the next two questions is to help you understand *logical equivalences involving quantifiers*. The main arguments used below are simple extensions of the concepts introduced earlier while discussing similar types of problems involving statement formulas.

Q 92. *Show that*

(i) $\big(\forall x\, P(x)\big)\vee\big(\forall x\, Q(x)\big)\ \Rightarrow\ \forall x\ \big[P(x)\vee Q(x)\big]$.

(ii) $\exists x\ \big[P(x)\wedge Q(x)\big]\ \Rightarrow\ \big(\exists x\, P(x)\big)\wedge\big(\exists y\, Q(y)\big)$.

Sol. For (i), suppose P and Q are two predicates with common domain of discourse such that $\big(\forall x\, P(x)\big)\vee\big(\forall x\, Q(x)\big)$ is true. Then $P(x)$ is true for every x or $Q(x)$ is true for every x. It is also possible to have some x in the domain for which both $P(x)$ and $Q(x)$ are true. In any case, all x must satisfy $P(x)$ or $Q(x)$ or both are true. Hence, $\forall x\ \big[P(x)\vee Q(x)\big]$ is true. For (ii), suppose P and Q are two predicates with common domain such that $\exists x\ \big[P(x)\wedge Q(x)\big]$ is true. That is, there is some x for which $P(x)$ is true and $Q(x)$ is true. Therefore, for some a in the domain, $P(a)\wedge Q(a)$ is true. Hence, by *Rule - EG*, $\big(\exists x\ P(x)\big)\wedge\big(\exists y\ Q(y)\big)$ is true. This completes the solution. ♢

Q 93. *Prove or disprove the following equivalence:*

(i) $\forall x\ \big[P(x)\ \to\ Q(x)\big]\quad\equiv\quad\exists\ x\, P(x)\ \to\ \forall\ x\, Q(x)$.

(ii) $\forall x\,\exists y\, P(x,y)\quad\equiv\quad\exists y\,\forall x\, P(x,y)$.

Sol. For (i), suppose P and Q are two predicates with a common domain such that $\forall x\ \big[P(x)\ \rightarrow\ Q(x)\big]$ is true. Now, since $P \rightarrow Q \equiv \neg P \vee Q$, it follows from the first part of Q. 92 that $\big(\forall x\ \neg P(x)\big) \vee \big(\forall x\ Q(x)\big)$ is true. Therefore, using the equivalence $\forall x\ \neg P(x) \equiv \neg\, \exists x\ P(x)$, we conclude that $\neg\ \big(\exists x\ P(x)\big) \vee \big(\forall x\ Q(x)\big)$ is true. Hence, $\exists\ x\ P(x)\ \rightarrow\ \forall\ x\ Q(x)$ is true. We ask: *Is the converse true?*. For (ii), notice that $\forall x\ \exists y\ P(x,y)$ is true when for every x there is a y for which $P(x,y)$ is true. In this case, y may depend on x. And, it is false when there is an x such that $P(x,y)$ is false for every y. On the other hand, $\exists y\ \forall x\ P(x,y)$ is true if f there is a y for which $P(x,y)$ is true for every x, i.e., true for a particular y regardless of x. And, it is false when for every y there is an x for which $P(x,y)$ is false. Therefore, order matters! In particular, we have if $\exists y\ \forall x\ P(x,y)$ is true, then $\forall x\ \exists y\ P(x,y)$ is also true. However, the converse may not hold. For example, consider the two-variable predicate Love(x,y) for the statement “x loves y". Then $\forall x \exists y$ Love(x,y) is the statement “*Everybody loves somebody*", whereas $\exists x \forall y$ Love(x,y) is the statement “*There is somebody whom everybody loves*". ♢

11 Graph Theory

The problems included here are based on some fundamental structures related to combinatorial graphs, some elementary enumeration techniques, and also two important methods of solving a linear recurrence relation that are known as the *method of characteristics* and *generating function method*.

11.1 Basic Concepts

Let $G = (V,E)$ be a finite simple graph. The number $|V|$ is called the **order** of G, and the number $|E|$ is called the **size** of G. If $|V| = n$ and $|E| = m$, we also say the G is an $(\mathbf{n},\mathbf{m})$**-graph**. The number of edges incident to a vertex $v \in V$ is called the **degree** of the vertex v. It is denoted by $\deg(v)$. A vertex of degree 1 is called a **pendant vertex**. For example, in the simple graph G shown in Fig. 31, we have

$$\deg(A) = 2, \quad \deg a = 3, \quad \deg(b) = 3, \quad \deg(c) = 3;$$
$$\deg(d) = 3, \quad \deg e = 3, \quad \deg(f) = 3, \quad \deg(B) = 2.$$

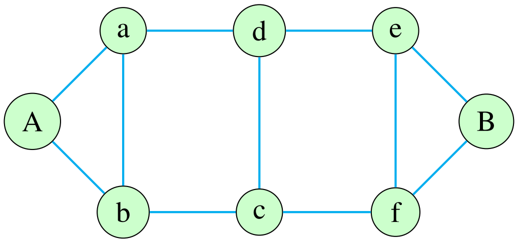


Figure 31: A simple graph G with 8 vertices and 11 edges.

In this case, finite monotonic nonincreasing sequence of degrees $(3,3,3,3,3,3,2,2)$ is called the **degree sequence** of the graph G. Conversely, such a finite sequence $(d_1,d_2,\ldots,d_{n-1})$ of non-negative integers is called **graphical** if there is a simple graph with this as a *degree sequence*.

Havel-Hakimi Theorem A finite sequence is graphical if and only if the sequence $(d_1-1,d_2-1,\ldots,d_k-1,d_{k+1},\ldots,d_{n-1})$ is also graphical.

To ensure first that a given sequence $(d_1,d_2,\ldots,d_{n-1})$ is indeed graphical, we start with using the two most important facts of graph theory, as stated in next two theorems.

Theorem 94 (Handshaking Theorem). *Let $G = (V,E)$ be a finite simple graph. Prove that*

$$\sum_{v\in V} \deg(v) = 2|E|. \tag{11.1}$$

In particular, the sum of degrees of all vertices of a graph is always an even number.

`Proof.` Since an edge $e \in E$ is incident with exactly two vertices of the graph G, it follows that each edge of G contributes 2 to the left side sum in (11.1). Hence, the assertion holds. This completes the proof. □

We will also use the following two notations:

$$\delta\big(G\big) := \min\big\{\deg(v) \mid \ v \in V\big\}; \tag{11.2a}$$

$$\Delta\big(G\big) := \max\big\{\deg(v) \mid \ v \in V\big\}. \tag{11.2b}$$

Notice that it follows from (11.1) that when G is an (n,m)-graph, we have

$$\delta\big(G\big) \leq \frac{2m}{n} \leq \Delta\big(G\big), \tag{11.3}$$

where $\delta\big(G\big)$ and $\Delta\big(G\big)$ are as defined in (11.2). The next theorem proves useful in various situations.

Theorem 95. *Let $G = (V,E)$ be a simple graph. Prove that the number of odd degree vertices in V is even.*

`Proof.` Let V_e and V_o denote the set of vertices of *even* and *odd* degrees, respectively. Clearly, we have $V = V_o \cup V_e$. It follows from the *handshaking theorem* that

$$\begin{aligned} 2\big|E\big| &= \sum_{v\in V} \deg\big(v\big) \\ &= \sum_{v\in V_e} \deg\big(v\big) + \sum_{v\in V_o} \deg\big(v\big). \end{aligned} \tag{11.4}$$

Since each number in the first sum of equation (11.4) is an even integers, and also $2\big|E\big|$ is even, it follows that the second sum must also be an even integer. It thus follows that the set V_o has even number of elements, because the sum of k odd numbers is even if and only if k itself is an even integer. This completes the proof. □

Q 96. *Consider the finite sequences as given below:*

(i) $\big(4,4,4,3,2\big)$; (ii) $\big(5,5,4,3,2,1\big)$; (iii) $\big(3,3,3,3,2\big)$;
(iv) $\big(3,3,3,3,3,3\big)$; (v) $\big(5,4,3,2,1,1\big)$; (vi) $\big(5,5,5,5,5,5,4,4,4,4\big)$.

Whenever possible, draw simple graphs with above as their degree sequences. *Otherwise, explain why such a graph doesn't exists.*

Sol. By handshaking theorem, we know that the sum of degrees of all vertices of a graph is always an even number. Therefore, there is no simple graph with *degree sequence* $\big(4,4,4,3,2\big)$. Next, suppose there is a simple graph G wth $\big(5,5,4,3,2,1\big)$ as the degree sequence. Among 6 vertices, each one of the two vertex of degree 5 in G have to be adjacent to remaining 5 vertices, which implies that the rest 4 vertices have degrees at least 2. However, as G has a *pendant vertex*, there doesn't exist such a graph G. A drawing of a graph with $\big(3,3,3,3,2\big)$ as the degree sequence is the left side picture shown in Fig. 32. A drawing of a graph with $\big(3,3,3,3,3,3\big)$ as the degree sequence is the right side pictureshown in Fig. 32. For the sequence in (v), you can use argument similar to given earlier for the part (ii). Also, draw the related graph. ♢

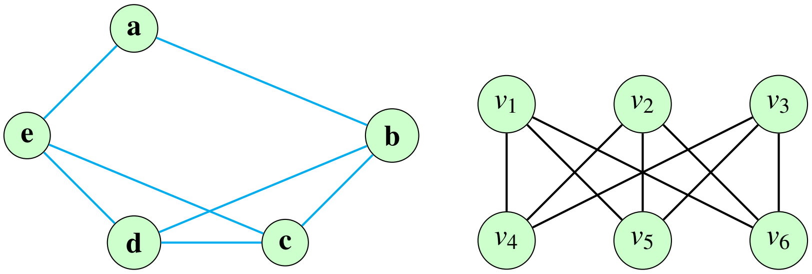


Figure 32: Drawings of two graphs with degree sequences as in parts (iv) and (v).

Let $G = (V,E)$ be a graph. For a subset $V' \subset V$, we may write $E[V']$ for the set of edges in G having their end vertices in the set V'. A **subgraph** of the graph G can be obtained by taking any $V' \subset V$ and $E' \subset E[V']$, and we denote this *subgraph* as $\big(V',E'\big)$. For example, if G is graph of order 11 shown on the left side of Fig. 33, then all the three graphs shown on the right side of Fig. 33, and both in Fig. 34, are subgarphs of the graph G. A simple way to obtain a subgraph of a graph is by deleting edges. However, in addition, *if a vertex is also deleted then we also need to delete all edges incident to this vertex.*

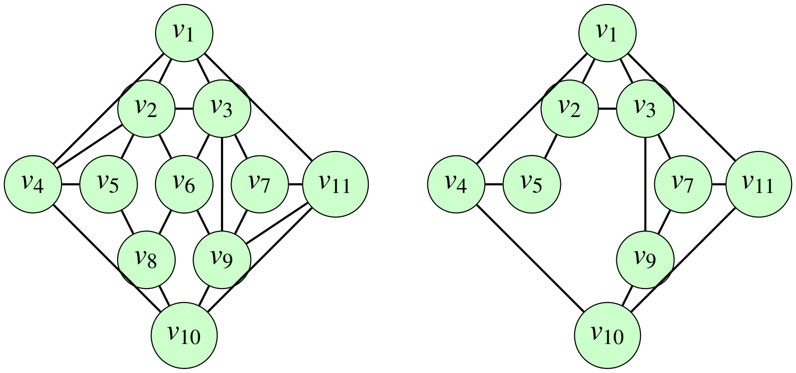


Figure 33: A graph and a vertex-deleted subgraph.

Q 97. *Giving one example in each case, define* (i) spanning subgraph*;* (ii) vertex deleted subgraph*; and,* (iii) induced subgraph.

Sol. A subgraph of a graph $G = (V,E)$ obtained by deleting some edges, but none of the vertices, is called a **spanning subgraph** of the graph. For example, the right side graph in Fig. 34 is a *spanning subgraph* of the the left side graph shown in Fig. 33. Next, a subgraph of a graph $G = (V,E)$ obtained by deleting some of the vertices, and hence also all edges incident to these vertices, is called a **vertex deleted subgraph**. For example, the right side graph in Fig. 33 is a *vertex deleted subgraph.* Finally, for any subset $V' \subset V$, the subgraph $G\big[V'\big] = \big(V',E[V']\big)$ is called the **induced subgraph** given by the vertices in the set V'. For example, the left side graph in Fig. 34 is an *induced subgraph* of the graph on the left side of Fig. 33. $\diamondsuit$

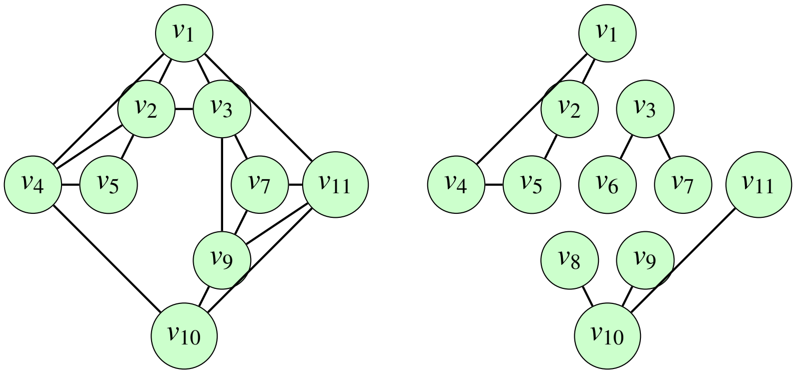


Figure 34: An induced subgraph and a spanning subgraph.

The *graph isomorphism* between two graphs G_1 and G_2 is bijection $\theta : V(G_1) \to V(G_2)$ that *preserves incidence* between the edge sets $E(G_1)$ and $E(G_2)$. That is, two vertices in G_1 are incident on an edge in G_1 if and only if their images under θ are incident vertices with the corresponding edge in G_2. It can be shown that two graphs G_1 and G_2 (without self-loops) are *isomorphic* if it possible to obtain the *incidence matrix* $I(G_1)$ from the incidence matrix $I(G_2)$, by *permuting its rows and columns*. Therefore, very roughly, the concept of *graph isomorphism* is about having different drawings of the same graph, without disturbing "incidence character" of edges.

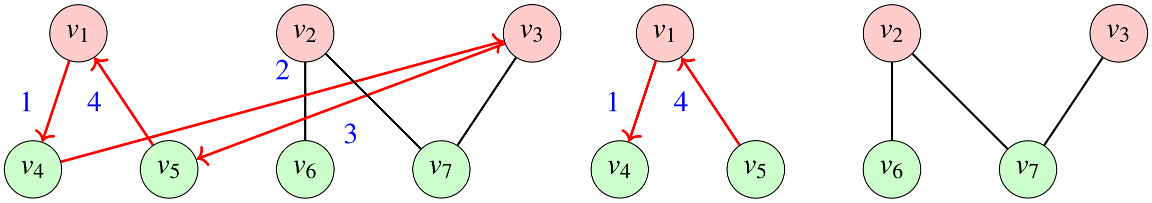


Figure 35: Two "different drawings" of the same graph known as $K_{2,7}$.

Q 98. *Giving one example in each case, define* (i) *graph isomorphism;* (ii) adjacency matrix*; and,* (iii) *incidence matrix.*

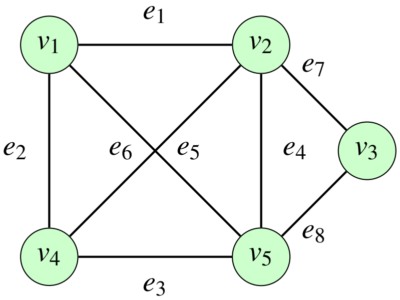
Sol. Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two graphs. We say G_1 and G_2 are **graph isomorphic** if there is a one-one, onto function $\theta : V_1 \to V_2$ such that the following *adjacency condition* holds for every pair of vertices $u, v \in V_1$:

$$e = uv \in E_1 \qquad \Longleftrightarrow \qquad f = \theta(u)\theta(v) \in E_2. \tag{11.5}$$

In this case, we say θ is a **graph isomorphism** between the graphs G_1 and G_2. Next, consider an (n,m)-graph G with vertices $v_1, v_2, \ldots, v_n$ and edges $e_1, e_2, \ldots, e_m$. The **adjacency matrix** of the graph G is a square matrix of order n, denoted by $A(G) = \big(a_{ij}\big)$, where the entry a_{ij} is given by

$$a_{ij} = \begin{cases} 1, & \text{if the vextex } v_i \text{ is adjacent to vertex } v_j \\ 0, & \text{otherwise.} \end{cases}$$

For example, a graph G and its adjacency matrix are as shown in Fig. 36. $\diamondsuit$



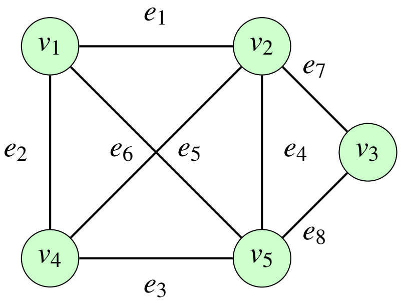
$$A(G) = \begin{array}{cccccc} & v_1 & v_2 & v_3 & v_4 & v_5 \\ v_1 & 0 & 1 & 0 & 1 & 1 \\ v_2 & 1 & 0 & 1 & 1 & 1 \\ v_3 & 0 & 1 & 0 & 0 & 1 \\ v_4 & 1 & 1 & 0 & 0 & 1 \\ v_5 & 1 & 1 & 1 & 1 & 0 \end{array}$$

Figure 36: A graph with associated adjacency matrix.

Finally, consider an (n,m)-graph G, with vertices $v_1, v_2, \ldots, v_n$ and edges $e_1, e_2, \ldots, e_m$. The **incidence matrix** of the graph G is a matrix of order $n \times m$, denoted by $I(G) = \big(a_{ij}\big)$, where the entry a_{ij} given by

$$a_{ij} = \begin{cases} 1, & \text{if } j\text{th edge } e_j \text{ is incident with } i\text{th vertex } v_i \\ 0, & \text{otherwise.} \end{cases}$$

For example, a graph G and its incidence matrix $I(G)$ are as shown in Fig. 37.



$$I(G) = \begin{array}{ccccccccc} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\ v_1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ v_2 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ v_3 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ v_4 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ v_5 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Figure 37: A graph with associated incidence matrix.

Remark 11.1. *Of course, two isomorphic graphs have the same* degree sequence. *However, the converse may not be true. As an important application of the* Havel-Hakimi Theorem *that we mentioned in the beginning, it follows that if the degree sequences of two graphs are different, then they cannot be isomorphic. It is an interesting fact that the adjacency matrix of a complete graph K_n is $J - I$, where J is a square matrix of order n with all entries equal to* 1 *and I is the $n \times n$ identity matrix. Further, since every edge in a simple graph is incident to two distinct vertices, each column of the incidence matrix $I(G)$ has exactly two* 1*'s. Also, the row-sum equals the degree of the corresponding vertex. Therefore, the total number of* 1*'s in $I(G)$ is twice the number of edges in the graph G. Identical columns corresponds to parallel edges. An isolated vertex is represented by a row all of whose entries are zero.*

Q 99. *Giving one example in each case, define* (i) *cycle of length n;* (ii) *complete graph of order n;* (iii) *bipartite graph of* (m,n) *type; and,* (iv) *an r-regular graph.*

Sol. For $n \geq 3$, a graph G with vertices $v_1, v_2, \ldots, v_n$ is called an **n - cycle** (or a *cycle of length* n) if the only edges in G are of form $v_i v_{i+1}$ (for $1 \leq i \leq n-1$) and the edge $v_1 v_n$. It is denoted by C_n. In particular, C_3 is a *triangle*; C_4 is a *square*; and, the left side drawing in Fig. 42 is the cycle graph C_5. A graph G is called a **complete graph** if any two vertices of G are adjacent. A *complete graph* on n vertices is denoted by K_n. For example, the middle and right side drawings in Fig. 42 are respectively the complete graphs K_4 and K_5.

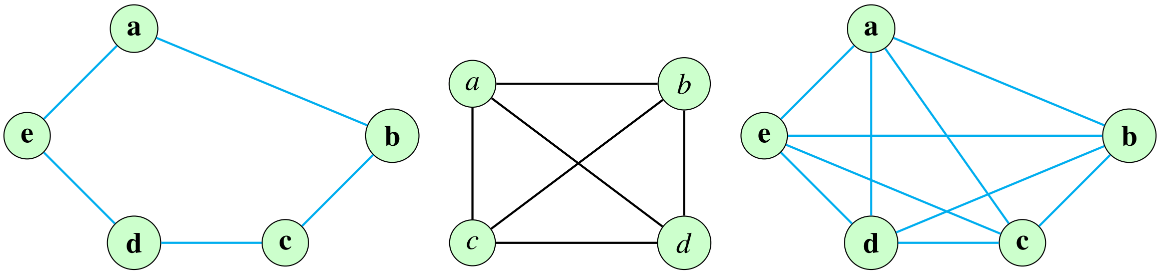


Figure 38: The cycle C_5, and the complete graphs K_4, K_5.

A simple graph $G = (V, E)$ is said to be a **bipartite graph** if the vertex set V has a bipartition $\big(V_1, V_2\big)$, where both V_1 and V_2 are independent set of vertices[14], and each edge $e \in E$ has its two end vertices in the sets V_1 and V_2. In this case, we may write $G = \big(V_1, V_2\big)$. A *bipartite graph* $G = \big(V_1, V_2\big)$ is called a **complete bipartite graph** if every vertex in V_1 is adjacent to each vertex of V_2. When $|V_1| = m$ and $|V_2| = n$, we write the complete bipartite $G = \big(V_1, V_2\big)$ simply as $K_{m,n}$. For example, the drawings in Fig. 39 are bipartite graphs; and, the right side drawing in Fig. 40 is the *complete bipartite graph* $K_{3,3}$.

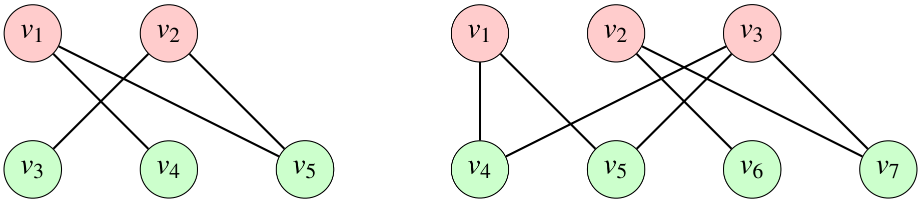


Figure 39: A $(2,3)$ - bipartite and $(3,4)$ - bipartite graphs.

A graph $G = (V, E)$ is called a *regular graph* of degree r (or simply an **r-regular**) if $\deg(v) = r$, for all $v \in V$. For example, each cycle C_n is a 2-regular graph; the complete graph K_n is a regular graph of degree $n-1$; and, the complete bipartite graph $K_{m,n}$ is a regular graph if and only if $m = n$. $\diamondsuit$

Remark 11.2. *Notice that the degree of each vertex of the cycle* C_n *is two, and the degree of each vertex of a complete graph* K_n *is* $n-1$. *In particular, it follows that* a graph on n vertices can have at most

[14] A set of vertices of a graph is said to be **independent** if every pair of vertices in this set are non-adjacent.

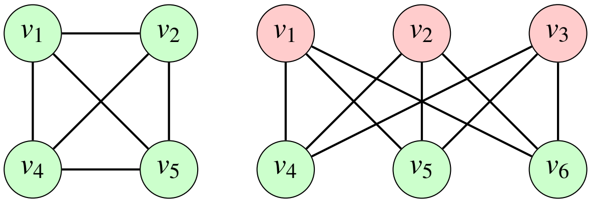


Figure 40: Two cubic graphs: K_4 and $K_{3,3}$.

$\binom{n}{2} = n(n-1)/2$ edges. *In the next problem, we show that this bound on the number of edges can be improved for a graph with k components. A* 3*-regular graph is also known as* ***cubic graph****. Two cubic graphs shown in Fig. 40 are cubic graphs. The Petersen graph is another interesting* cubic graph. *Notice that it follows from the* handshaking theorem *that an r-regular graph of order n and size m satisfies the condition $m = nr/2$. Therefore, the complete graph K_n has exactly $n(n-1)/2$ edges. In general,* every cubic graph has an even number of vertices. *More generally, a* k-regular spanning subgraph *of a graph is called an* **k*****-factor****. If the edge set of a graph can be divided into k - factors, such a decomposition is called a* **k*****- factorization*** *of the graph. In particular, a* 1 *- factorisation is called simply a* factorisation *(or a* resolution*).*

Q 100. *Let $G = (V,E)$ be a graph of order n, with k components. Show that $|E| \leq (n-k)(n-k+1)/2$.*

Sol. Let n_i and e_i respectively denote the number of vertices and edges in the ith component of the graph G, and e be the total number of edges of G. Then, we have

$$e = e_1 + e_2 + \cdots + e_k \qquad n = n_1 + n_2 + \cdots + n_k.$$

Now, as every component must have at least one vertex, the maximum number of vertices in any component is $n-(k-1) = n-k+1$. Therefore, $n_i \leq n-k+1$ for all $i = 1,2,\ldots,k$. Further, as each of the component is simple, the number of edges in the ith component can not be more than the number of edges in the complete graph with n_i vertices. It thus follows that $e_i \leq n_i(n_i-1)/2$. Hence, we have

$$\begin{aligned} e &= e_1 + e_2 + \cdots + e_k \\ &\leq \frac{n_1(n_1-1)}{2} + \frac{n_2(n_2-1)}{2} + \cdots + \frac{n_k(n_k-1)}{2} \\ &\leq \frac{(n-k+1)(n_1-1)}{2} + \frac{(n-k+1)(n_2-1)}{2} + \cdots + \frac{(n-k+1)(n_k-1)}{2} \\ &= (n-k+1)\left(\frac{n_1-1}{2} + \frac{n_2-1}{2} + \cdots + \frac{n_k-1}{2}\right) \\ &= \frac{(n-k+1)(n-k)}{2}. \end{aligned}$$

The graph consisting of a complete graph of degree $n-k+1$ and $k-1$ isolated vertices has k components and n vertices and also $(n-k+1)(n-k)/2$ edges. An example with $n = 11$ and $k = 3$ is given in Fig. 41. ♢

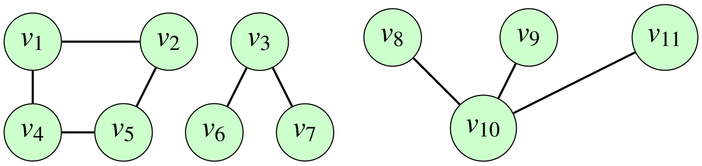


Figure 41: Example of a graph for Q. 100, with $n = 11$ and $k = 3$.

12 Eulerian & Hamiltonian Graphs

We start with the next definition.

Definition 12.1. *A cycle in a graph that goes through each edge exactly once is called an **eulerian cycle**. A graph containing an eulerian cycle is called an **eulerian graph**.*

Q 101. *For what values of n do the* complete graph K_n *and the* cycle C_n *would be eulerian graphs ?*

Sol. Since the degree of each vertex of a complete graph K_n is $n-1$, it follows from criterion proved in Q. 102 that K_n is an eulerian graph if and only if $n > 1$ is an odd integer. Since the cycle C_n is a 2-regular graph, for $n \geq 3$, it follows from criterion proved in Q. 102 that each cycle C_n is an eulerian graph. For example, we see drawings of two such graphs in Fig. 42, for $n = 5$. ♢

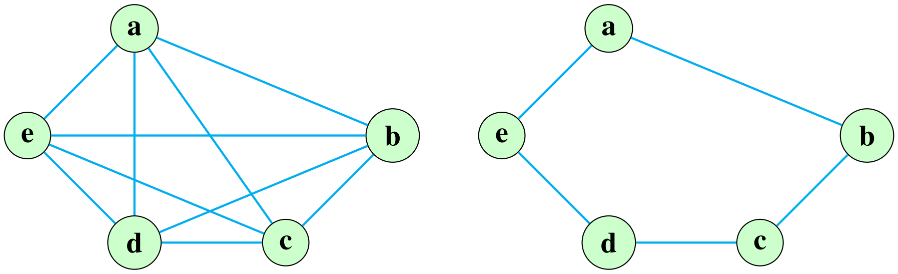


Figure 42: The complete graph K_5 and the cycle C_5.

Q 102. *Show that a connected graph G is eulerian if and only if the degree of each vertex of G is even.*

Sol. We first assume that a graph $G = (V,E)$ is eulerian, with an Euler circuit C, say starting at a vertex $v \in V$. As v is also the last vertex of the circuit C, it is an even vertex. Moreover, as all other edges on C are distinct, it follows that all other vertices on C are of even degrees. Therefore, each vertex of G is of even degree. Conversely, suppose $G = (V,E)$ is simple connected graph such that every vertex of G is of even degree. Starting from a vertex $v \in V$, we walk along as many distinct edges as possible. Now, as the degree of every vertex is even, the walk ends only at v. Let the closed walk so obtained be denoted by W. If W contains all the edges of G, then we are done. Otherwise, consider the graph $G' = G - W$, obtained by removing from G all the edges in W. Clearly the vertices of G' are of even degree, and there is at least one vertex $v' \in V$ that is common to both G' and W. Therefore, starting at v', we traverse as many distinct edges of G' as possible, and write W_1 for the closed walk so obtained. Then combining Γ and Γ_1 by traversing from v to v' in Γ, followed by Γ_1 and finally the portion of Γ from v' to v, we get new walk Γ' that contain more edges than Γ. If this walk contains all the edges of G, we have the required Eulerian line. Otherwise this process can be continued to get an Eulerian line. Note that the process will terminate as there are only a finite number of edges. ♢

Definition 12.2. *A path in a graph that visits each vertex exactly once is called a* ***Hamiltonian path****. A closed Hamiltonian path in a graph is called a* ***Hamiltonian cycle****. A graph containing a Hamiltonian cycle is called a* ***Hamiltonian graph****.*

Clearly, every graph of order n that contains the cycle C_n is a *Hamiltonian graph*. More generally, a graph is a Hamiltonian graph if it has spanning subgraph that is Hamiltonian.

Q 103. *Which of the graphs shown in Fig. 43 has a Hamiltonian cycle or at least a Hamiltonian path:*

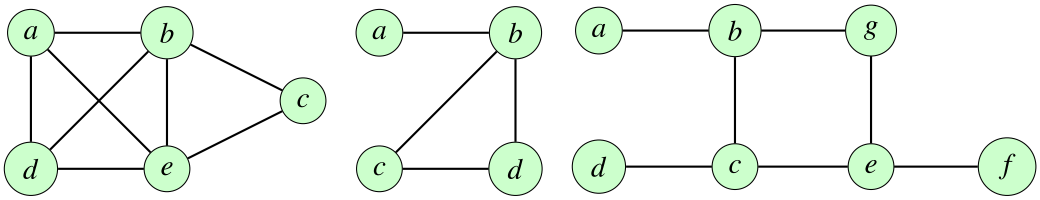


Figure 43: Examples of graphs for Q. 103.

Sol. Since the left side graph in Fig. 43 has 5 vertices, and it contains C_5, it is a Hamiltonian graph. However, the middle graph in Fig. 43 only contains a Hamiltonian path. Finally, the right side graph in Fig. 43 doesn't contain a Hamiltonian path. ♢

Q 104. *Use suitable examples to differentiate between an eulerian and a Hamiltonian graph. Further, give an example of a graph that is both eulerian and Hamiltonian. Is it true that a Hamiltonian graph necessarily has to have an eulerian circuit? Explain.*

Sol. For example, the graph with a drawing shown on the left side of Fig. 44 is a Hamiltonian graph, but it is not an eulerian graph because it has vertices of odd degrees (see also Q. 105). However, the graph with a drawing shown on the right side of Fig. 44 is both an eulerian graph and a Hamiltonian graph. Finally, an example of a graph that is an eulerian graph, but not a Hamiltonian graph, is provided by any K_n, for $n \geq 2$ even. This last example also shows that a Hamiltonian graph need not have any eulerian circuit. ♢

Q 105. *Suppose G is a $(11,53)$-type of connected graph. Explain why G is Hamiltonian, but not eulerian.*

Sol. Recall that the complete graph K_{11} has $11(11-1)/2 = 55$ edges, and the graph G has 53 edges. So, we can visualise G as K_{11} with two edges "missing". These two edges may be *adjacent edges* or *non-adjacent*

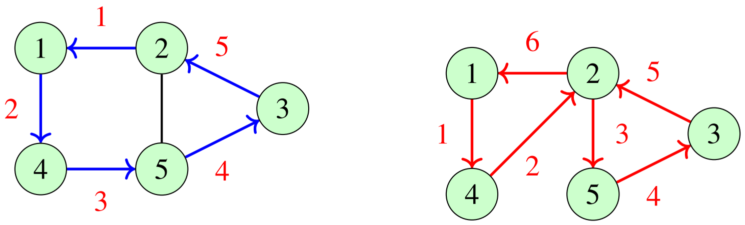


Figure 44: Examples of graphs for Q. 104.

edges. Therefore, the degree sequence of the graph G is given by

$$\big(10,10,10,10,10,10,10,10,9,9,8\big) \quad \text{or} \quad \big(10,10,10,10,10,10,10,9,9,9,9\big).$$

Clearly, in both cases, G is not eulerian. However, we still have that G contains the cycle C_{11}, and hence G is a Hamiltonian graph. $\diamondsuit$

13 Trees and Rooted Trees

We start with the next definition.

Definition 13.1. *A **tree** is connected acyclic graph (without cycles).*

The next theorem is an important fact about trees.

Theorem 106. *If T is a tree with n vertices and e edges, then $e = n-1$.*

Proof. See your class notes. □

Q 107. *Show that every non-trivial tree T must contain at least two pendant vertices.*

Sol. Let a tree T has n vertices, say $v_1 \ldots, v_n$. Without Loss Of Generality (or simply WLOG), suppose $\deg(v_i) \geq 2$ for all $i \geq 3$. By Theorem 106, we know that T has $e = n-1$ edges. Also, by *handshaking theorem*, we have

$$\deg\big(v_1\big) + \deg\big(v_2\big) + \sum_{v \neq v_1, v_2} \deg\big(v\big) = 2\big(n-1\big).$$

It thus follows that

$$\deg\big(v_1\big) + \deg\big(v_2\big) = 2n - 2 - \sum_{v \neq v_1, v_2} \deg\big(v\big) \leq 2n - 2 - 2(n-2) = 2.$$

However, by connectedness property of T, we have $\deg\big(v_1\big), \deg\big(v_2\big) \geq 1$. Therefore, we conclude $\deg\big(v_1\big) = \deg\big(v_2\big) = 1$. Therefore, T has at least two pendant vertices. ♢

13.1 Rooted Tree

The next definition uses the fact that every tree has either one or two adjacent centers.

Definition 13.2. *A tree in which a particular vertex is designated as root is called a **rooted tree**.*

In view of part-(5) of Theorem 106, from the root of a *rooted tree*, any other vertex can be reached through a *unique path*. Therefore, a rooted tree is “naturally directed". The root is usually drawn at the top, and all edges are taken to be directed downwards from the root. A rooted tree, with the root R, is shown in Fig. 45.

For any fixed node v at level-i, every node at level higher than i that is reachable from v is called a **descendent** of v. In particular, a descendent at the level-$(i+1)$ is called the **children** of v. A node without any children is called a **leaf** (or a terminal or a pendant node). Each node of the rooted tree that is not a leaf is called an **internal node**. As such, all internal nodes and each leaf of a rooted tree is a descendent of the root.

Definition 13.3. *The length of the path from the root of a rooted tree to a vertex v is called the **level** (or **height** or **depth**) of the vertex v. The maximum level of any vertex is called the **height** (or the **depth**) of the rooted tree. The root itself is considered to be at level zero.*

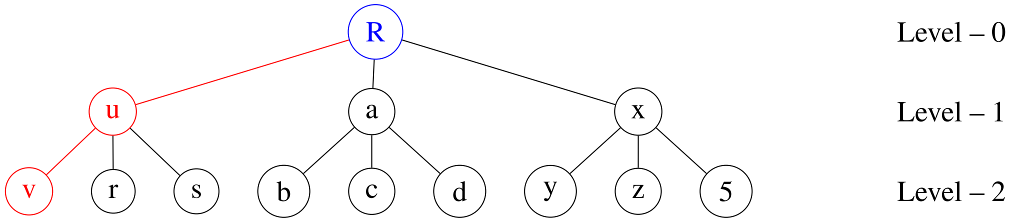


Figure 45: A three-level rooted tree with 10 nodes.

13.2 Binary Tree

For many applications, our main concern is to study a special type of rooted tree.

Definition 13.4. *A rooted tree is called a **binary tree** (a **full binary tree**) if every internal vertex has at most two (respectively, exactly two) children.*

Clearly, a *full binary tree* has exactly one vertex of degree 2 (root), and the rest all have degrees 3 or 1.

Q 108. *Show that a full binary tree T always has an odd number of vertices, and the number of leaves in T is equals $(n+1)/2$.*

Sol. The first assertion follows from the fact that there is only one vertex in T of degree 2, namely, the root. So, if T has n vertices, then the remaining $n-1$ vertices all have odd degrees. Therefore, $n-1$ must be even or, equivalently, n is odd (Theorem 95). For the second assertion, let T has p leaves so that the remaining $n-p-1$ vertices have degree 3. Also, we know that T has $n-1$ edges (Theorem 106). It thus follows from the *handshaking theorem* that

$$2\times 1+3\times\big(n-p-1\big)+1\times p=2\big(n-1\big),$$

which gives $p=(n+1)/2$. ♢

Q 109. *Let T be a binary tree of height h, with $h\geq 0$. Show that T has at most 2^{h+1} vertices.*

Sol. By definition, the maximum height that a vertex v of T may have is h. Suppose T has n vertices, and n_i vertices are at height i. It thus follows that

$$n=n_0+n_1+\cdots+n_h$$

Then, we have

$$n_0=1,\;\; n_1\leq 2^1,\;\; n_2\leq 2^2,\ldots,\;\; n_h\leq 2^h,$$

which implies

$$n=n_0+n_1+\cdots+n_h\leq 1+2^1+2^2+\cdots+2^h=2^{h+1}-1.$$

Hence, T has at most 2^{h+1} vertices. ♢

13.3 Binary Tree Traversal

One of the most common application involves *traversing* (walk along) a binary tree in a systematic manner so that each vertex is visited and processed exactly once. The three main traversal of a binary tree are known as the *pre-order traversal*, the *in-order traversal*, and the *post-order traversal*. More generally, if v is an internal node of a rooted tree T, then the subgraph consisting of v, its descendent and all the edges incident to these descendent, is called the **subtree** of T, with v as its root. In particular, for a binary tree, we can possibly have a **left-subtree** and a **right-subtree**.

Definition 13.5. *Consider a binary tree T, with root R, and $T_1, \ldots, T_n$ be its subtrees that we may visualise* from left to right.

1. *In **pre-order traversal**, we first visit R followed by traversing T_1 in* pre-order*, then T_2 in* pre-order*, and so on until T_n is traversed in* pre-order.

2. *In **in-order traversal**, we first traverse T_1 in* in-order*, followed by visiting R, and continuing traversing T_2 in* in-order*, and so on, until T_n is traversed in* in-order.

3. *In **post-order traversal**, we traverse T_1 in* post-order*, T_2 in* post-order*, so on, until T_n is traversed in* post-order*, and finally visit the root R.*

Therefore, for a binary tree, the *in-order traversal* is obtained by adopting the *left-root-right* scheme; the *pre-order traversal* is obtained by adopting the *root-left-right* scheme (as shown by dotted lines in Fig. 46); and, the *post-order traversal* is obtained by adopting the *left-right-root* scheme.

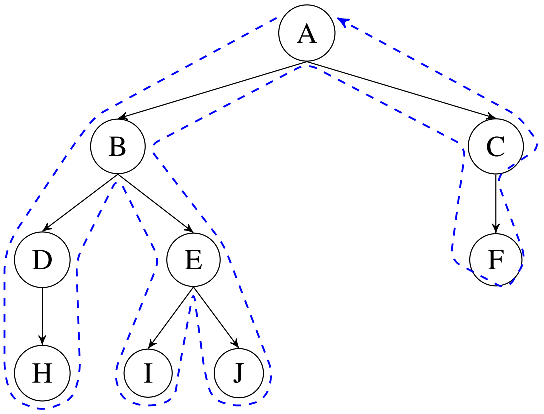


Figure 46: The binary tree for Example 13.1.

In the reverse process, we construct a binary tree T from a given combination of an *in-order traversal* with a *pre-order traversal* or a *post-order traversal*. In this case, the procedure we follow is as given below:

1. The root node of T at level-0 is obtained from *pre-order traversal* by scanning it **from the left**. The root node of T at level-0 is obtained from *post-order traversal* by scanning it **from the right**.

2. Consider the left and right segments of the given *in-order traversal*, with respect to the root node(s) obtained at level-$i\,(i \geq 0)$. Notice that the left segment represents the nodes of the *left subtree* and the right segment represents the nodes of the *right subtree*.

3. Use these segments to determine the roots of the left and right subtrees, while scanning the given *pre-order traversal* from the left or scanning the given *post-order traversal* from the right.

4. Repeat (2) and (3) to determine the roots of the left and right subtrees at level-$(i+1)$.

5. Stop when leaves of T are reached.

Example 13.1. *We use above procedure to construct binary tree T on 9 nodes, with two traversals given by*

$$Pre\text{-}order: \; ABDGEHIJCF \quad and \quad In\text{-}order: \; DGBEIHJACF$$

Scanning the given pre-order traversal from the left, it follows that A is the root node of T at level-0. With respect to node A, the two segments read from the given in-order traversal are DGBEIHJ and CF. We find the roots of the left and right subtrees of T by using these two segment. For, scanning the given pre-order traversal from the left side, it follows from the segment BDGEHIJCF that node B is the root of the left subtree, at level-1. Similarly, from the segment CF, it follows that C is the root node of the right subtrees, at level-1. Again, by using the segments DG and EIHJ of the given in-order traversal, the root nodes of the left subtrees at level-2 are respectively D and E, which we obtained by scanning the segment DGEHIJCF of the given pre-order from the left. Continuing in similar manner, the binary tree T is as shown in Fig. 46. It is easy to find the post-order traversal *of this binary tree.*

Q 110. *For each of the following, determine the binary tree, and also the missing traversal:*

(i) ***In-order*** : *ABDHIEJKCFG* *and* ***Post-order*** : *HDIBJEKAFCG.*

(ii) ***In-order*** : *BEHFACDGI* *and* ***Pre-order*** : *HFEABIGDC.*

(iii) ***In-order*** : *HFEABIGDC* *and* ***Post-order*** : *BEHFACDGI.*

Sol. For (i), to construct a binary tree T on 9 nodes, with two traversals given by

$$\text{In-order}: \; ABDHIEJKCFG \quad \text{and} \quad \text{Post-order}: \; HDIBJEKAFCG$$

we scanning the given *post-order traversal* from the right, so that node G is found to be the root of T at level-0. With respect to root G, we only have to consider the left segments ABDHIEJKCF of the given *in-order traversal*. Therefore, T has no right-subtree with respect to the root G. Now, we use the segment

ABDHIEJKCF to find the roots of the left subtree of T. For, we scan the given *post-order traversal* from the right, so that it is found from the segment ABDHIEJKCF that the node C is the root of the left subtree of T, at level-1. Next, with respect to root C, we need to consider the two segments ABDHIEJK and F, as read from the given *in-order traversal*. Therefore, the node F is the root of the right subtree at level-2. Also, it follows from the segment ABDHIEJK that the other root at this level is A, as obtained by scanning the given *post-order traversal* from the right. Futher, with respect to root A of the left subtree of T, we only have to consider the right segment BDHIEJK, as read from the given *in-order traversal*. Once again, by scanning the given *post-order traversal* from the right, it follows that the node K is the root at level-3 of the left subtree of T. Continuing in similar manner, the binary tree T is as shown in Fig. 47. It is easy to find the *pre-order traversal* of this binary tree. The binary trees for other two parts of the question can be obtained similarly. These are given by the figures shown below. ♢

Figure 47: Binary trees of Q. 110.

14 Graph Colouring & Planar Graphs

We start with the next definition.

Definition 14.1. *By a **vertex coloring** (or an **edge coloring**) of a graph $G = (V,E)$ we mean assigning colors to vertices (or edges) in such a manner so that no two adjacent vertices (or adjacent edges) get the same color. The minimum number of different colors needed to* vertex color *(or* edge color*) a graph is called the **chromatic number** of the graph.*

The chromatic number of a graph G is usually denoted by $k = \chi(G)$. In this case, we also say that G is **k-colorable**. For example, the cycle C_n is 2-chromatic, when n is even; and, it is 3-chromatic, when n is odd. By definition, every bipartite graph is 2-chromatic. In particular, every tree with at least one edge is 2-chromatic. Clearly, for the complete graph K_n, we have $\chi(K_n) = n$; and, for the wheel W_n, we have $\chi(K_n) = n+1$.

Remark 14.1. *The self-loops and parallel edges have no influence on the chromatic number. Therefore, we may assume that our graph is a simple graph. Also the chromatic number of a disconnected graph is the largest of the chromatic numbers of the components.*

Definition 14.2. *The **line graph** of a graph $G = (V,E)$ is the graph $L(G)$ that has a vertex for each $e \in E$, and two vertices in $L(G)$ are* adjacent *if and only if the corresponding edges in the graph G share a vertex.*

Q 111. *Giving suitable example in each case, define (i)* vertex colouring*; (ii)* edge colouring*; and, (iii)* chromatic number *of a graph. How edge colouring is related to the concept of vertex colouring? Further, find the chromatic number of the graph shown in Fig. 48.*

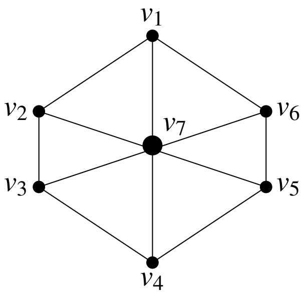


Figure 48: Graph G in Q.111.

Sol. A *vertex coloring* of a graph G is about assigning different colors to each vertex in such a manner so that no two "adjacent vertices" get the same color. For illustration, take any graph of order 6 or more.

An *edge coloring* of a graph G is about assigning different colors to each edge in such a manner so that no two "adjacent edges" get the same color. For illustration, take any graph of order 6 or more.

The minimum number of different colors needed to vertex color a graph is called the *chromatic number* of the graph. For illustration, take any specific class of graphs as mentioned above.

The edge chromatic number of G equals the vertex chromatic number of the line graph $L(G)$.

It is clear from the drawing shown in Fig. 48 that the color assigned to the vertex v_7 must be different from the colors assigned to the boundary vertices $v_1, \ldots, v_6$, which is C_6. Therefore, the chromatic number of the graph is 3. ♢

Definition 14.3. *A graph G is called a* plane graph *if it admits a plane drawing containing no* edges crossings. *Such a drawing is called a* plane representation *(or an* plane embedding*) of the graph.*

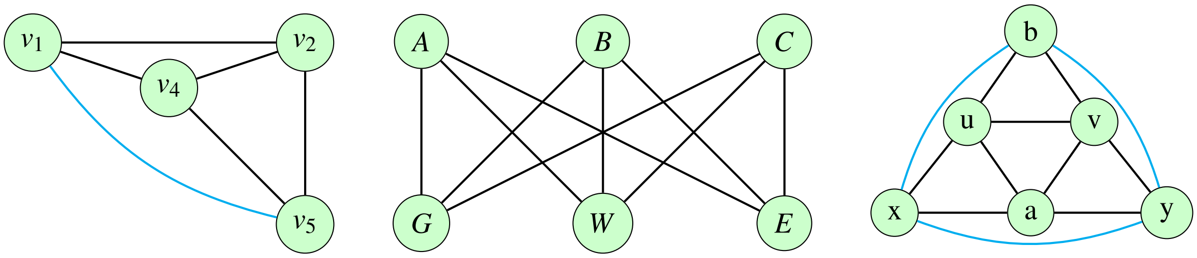


Figure 49: K_4 has planar representations, but not $K_{3,3}$.

The **utilities problem** is about how to supply to each of the three houses A, B, C the three services **G**as, **W**ater, and **E**lectricity such that no two supply lines cross each other in the layout. The related graph model in this case is the complete bipartite graph $K_{3,3}$, as shown by the middle drawing in Fig. 49, which is a typical example a graph that cannot be redrawn such that no two lines cross each other.

Definition 14.4. *A graph G is called a* ***planar graph*** *if it is isomorphic to a* plane graph. *Otherwise, we say G is a* non-planar graph.

Said differently, a graph is a *planar graph* if one of its drawing is a plane graph.

Example 14.1. *Clearly, every tree is a planar graph. Also, the complete graph K_4 is planar graph, with two plane representations as shown in Fig.* **??**. *The bipartite graph $K_{2,7}$ is a planar graph, with a plane representation as shown in Fig. 35. As shown later, the complete graph K_5 and the complete bipartite graph $K_{3,3}$ are non-planar graphs*[15].

Notice that each plane graph divides the plane into a number of *regions*, each bounded by three or more edges, except the one exterior (unbounded) region. The next theorem gives a fundamental formula for planar graphs that relates the number of vertices, the number of edges, and the number of regions. Since each component of a planar graph G is a connected planar graph, in all that follows, it is assumed that G is a connected.

[15] A celebrated theorem of Kuratowskii (Theorem **??**) proves that a graph is planar if and only if it doesn't contain any subgraph homeomorphic to K_5 or $K_{3,3}$.

Q 112. *Let $G = (V,E)$ be a connected planar graph, with $v = |V|$ and $e = |E|$. Show that we have*

$$v - e - r = 2, \tag{14.1}$$

where r denotes the number of regions formed by the edges of G.

Sol. Notice that formula (14.1) holds trivially when $e = 0,1$, or 2. Therefore, to complete the proof by induction on e, we assume that (14.1) holds for any planar graph with number of edges $< e$. We consider the following two cases.

Case-I When G is a tree. In this case, by Theorem 106, we have $e = v-1$. Also, $r = 1$. Therefore, (14.1) holds.

Case-II Suppose G is not a tree so that it contains a cycle, say C. Let f be an edge on C so that it cannot be a **bridge**. Therefore, the subgraph $G' = G - f$ is a connected planar graph with v vertices and $e-1$ edges. Further, the graph G' has $r-1$ regions because removal of an edge from a cycle reduces the number of regions by one. It thus follows from our induction hypotheses that formula (14.1) holds for the graph G'. That is, we have

$$2 = v - (e-1) + (r-1) = v - e + r.$$

This completes the proof. ♢

Q 113. *Let G be a connected planar graph with v vertices, $e \geq 3$ edges, and r regions. Show that $e \leq 3v-6$. Also, show that if G is triangle-free graph then $e \leq 2v-4$.*

Sol. While counting the number of edges over all regions, each edge that bounds two different regions is counted once for each region, and those that bound to a single region (such as in the case of a tree) will be counted twice. It thus follows that the number of edges counted in this manner is $2e$. Further, since every bound region has at least 3 boundary edges, we conclude that $2e \geq 3r$ or $e \geq 3r/2$. Substituting inequality $2e \geq 3r$ in the Euler's formula $v - e + r = 2$, we obtain

$$2e \geq 3e - 3v + 6 \qquad \Rightarrow \qquad e \leq 3v - 6.$$

Next, when G is a triangle-free graph, every bound region has four or more boundary edges. Therefore, we must have $2e \geq 4r$ or $e \geq 2r$. Hence, in this case, we have

$$e \geq 2e - 2n + 4 \qquad \Rightarrow \qquad e \leq 2v - 4.$$

This completes the solution. ♢

Q 114. *If G is a planar graph, with v vertices and $e \geq 3$ edges, show that it contains a vertex of degree ≤ 5.*

Sol. If $\deg(v) \geq 6$, for all vertices $v \in V(G)$, then by (11.3) we have

$$\delta(G) \geq 6 \qquad \Rightarrow \qquad \frac{2e}{v} \geq 6 \quad \text{i. e.,} \quad e \geq 3v.$$

As we also have $e \leq 3v - 6$, by Q. 113, the above inequality shows that at least one vertex of G must be of degree ≤ 5. ♢

The next theorem is very important fact about planar graphs.

Theorem 115. *The graphs K_5 and $K_{3,3}$ are non-planar.*

Proof. For K_5, we have $v = 5$ and $e = 10$, and every region is bounded by at least 3 edges. If K_5 were planar, then by Q, 113 we have

$$10 = e < 3n - 6 = 3 \times 5 - 6 = 9,$$

which is absurd. Therefore, K_5 is a non-planar graph. For $K_{3,3}$, we have $v = 6$ and $e = 9$, and every region is bounded by at least 4 edges. If $K_{3,3}$ were planar, then by the second part of Q. 113 we have $9 \leq 12 - 4 = 8$, which is again absurd. Therefore, $K_{3,3}$ is a non-planar graph. □

Q 116. *Let G be a connected planar $(6,12)$-graph. Show that every region in G is* triangular. *Further, find a planar connected graph G of order* 6 *such that* $\deg(v) \geq 3$*, for all* $v \in V(G)$.

Sol. It follows from *Euler formula* $v - e + r = 2$ that, in a plane representation of G, we have $r = 2 - v + e = 2 - 6 + 12 = 8$. Therefore, other than the unbounded region, G has 7 bounded regions, each having at least three edges as the boundary. Also, by *handshaking theorem*, we know that the *sum of degrees* of all 6 vertices is $2 \times 12 = 24$. It thus follows that each region is bounded by $24/8 = 3$ edges, i. e., every region in G is *triangular*. For the second part, see the right side drawing in Fig. 49 (notice that it is a 4-regular connected planar graph). ♢

Definition 14.5. *The **dual** of a planar graph $G = (V,E)$ is the graph G' that has a vertex for each region of G, and* adjacency *among vertices is defined in terms of common bounding edge of the correspond regions.*

For a planar graph, we may also consider coloring of the regions of a plane representation of the graph. The concept of *dual graph* allows us to turn "map coloring" of a planar graph into "vertex coloring" of its dual graph. In this way, the dual G' provides graph model for the *map coloring problem*. Further, it is an interesting fact that a connected planar graph is eulerian if and only if its dual graph is bipartite. Also, a Hamiltonian cycle in a planar graph G corresponds to a partition of the vertices of the dual graph into two subsets (the interior and exterior of the cycle) whose induced subgraphs are both trees.

15 Elementary Combinatorics

We discuss here methods of solving types of combinatorial problems dealing with "selections" and "arrangements" of objects, with or without repetitions. The problems related to former are about "combinations" and the problems related to latter are about "permutations". Recall that the symbol $\binom{n}{r}$ (or $C(n,r)$) denotes the number of combination of n distinct objects taken r at a time (without repetition), and $P(n,r)$ denotes the number of permutations of n distinct objects taken r at a time (without repetition).

Q 117. *How many triangles can be formed by joining* 10 *points such that* 5 *of these lie on the same line.*

Sol. We need three non-collinear points to make a triangle. Therefore, from 10 such points, we can make $\binom{10}{3} = 120$ number of triangles. However, when 5 of these 10 points are collinear, we can make only

$$\binom{10}{3} - \binom{5}{3} = 120 - 10 = 110$$

number of triangles. ♢

The two *counting principles* that one applies in more complex situations are as given below.

SUM RULE: The *sum rule* states that if n tasks $T_1, \ldots, T_n$ are such that T_i can be done in m_i-ways for $i = 1, \ldots, n$, then the task

$$T_1 \text{ or } T_2 \text{ or } \cdots \text{ or } T_n$$

can be sone in $m_1 + m_2 + \ldots + m_n$ ways.

Example 15.1. *A student pursuing an under-graduation engineering degree in computer science can choose a project topic from one of the three lists consisting of* 23, 15, *and* 19 *possible projects. From the first, there are* 23 *ways; from the second, there are* 15 *ways; and, from the third, there are* 19 *ways. Therefore, there are* $3 + 15 + 19 = 57$ *projects to choose from.*

We can also phrase the *sum rule* in terms of sets. For, let $A_1, \ldots, A_n$ be "disjoint sets", with a universal set U, such that $a_k = |A_k|$, for $k = 1, \ldots, n$. Then, the number of elements in their union is the sum of the sum of a_k's. That is,

$$\left|A_1 \cup \cdots \cup A_r\right| = a_1 + a_2 + \cdots + a_n. \tag{15.1}$$

To relate (15.1) to the previous description of the *sum rule*, let T_k be the task of choosing an element from the set A_k, for $k = 1, \ldots, n$. So, there are a_k ways to do T_k. By the *sum rule*, since no two task can be done at the same time, the number of ways to choose an element from one of these n sets is the same as the number of elements in their union.

Notice that, however, if the tasks T_i for certain pairs of values of i are not mutually independent, then the *sum rule* doesn't apply. In this case, we need to subtract from the sum the number of ways that are common to such tasks. For example, if T_1 is the task of choosing a prime < 15 and T_2 is the task of choosing an odd number < 10, then the task E_1 or E_2 can be done in $6+5-3=8$ ways, because the number of ways that are common to both tasks is 3. This is typical example wherein the *inclusion-exclusion principle* is used. This principle is also known as the *subtraction rule*, which we shall discuss in the next section.

PRODUCT RULE: The *product rule* states that if n tasks $T_1, \ldots, T_n$ are such that T_i can be performed in k_i-ways for $i = 1, \ldots, n$, in that order and independent of all previous tasks, then it takes $k_1 \times k_2 \times \ldots \times k_n$ ways to complete the task

$$T_1 \text{ and } T_2 \text{ and } \cdots \text{ and } T_n$$

Therefore, the product rule applies when a procedure is made up of several tasks.

Example 15.2. *Suppose a hotel have 7 AC-suits that the 3 checking-in persons want. In this case, the 1st person has 7 choices; the 2nd has 6 choices; and, the 3rd has 5 choices. Therefore, there are $7 \times 6 \times 5 = 210$ ways in total to make the suit allocations. Also, since each bit of a 7-bit string can be chosen in two ways, there are a total of $2^7 = 128$ different bit strings of length 7, by the product rule. By the same reasoning, it follows that the number of functions from a set of m elements to a set of n elements is $n \cdot n \cdots n(m \text{ terms}) = n^m$. Further, for $m \leq n$, the number of one-one functions from a set $A = \{a_1, \ldots, a_m\}$ elements to a set $B = b_1, \ldots, b_n$ is*

$$n\big(n-1\big)\big(n-2\big) \cdots \big(n-m+1\big),$$

because there are n ways to map the element $a_1 \in A$; $n-1$ ways to map the element $a_2 \in A; \ldots$; and, $n-m+1$ ways to map the element $a_m \in A$. Notice that the solution of Q. 2 also uses the same argument.

We can also phrase the *product rule* in terms of sets. For, let $A_1, \ldots, A_n$ be finite sets such that $a_k = \big|A_k\big|$, for $k = 1, \ldots, n$. Then, the number of elements in the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ is the product of a_k's. That is,

$$\big|A_1 \times A_2 \times \cdots \times A_n\big| = a_1 \cdot a_2 \cdots a_n. \tag{15.2}$$

To relate (15.2) to the above description of the *product rule*, notice that the task of choosing an element in the set $A_1 \times A_2 \times \cdots \times A_n$ is done by choosing an element in A_k, for $k = 1, \ldots, n$. Therefore, (15.2) holds, by the *product rule*. Further, a graphic way of counting $k_1 \times k_2 \times \ldots \times k_n$ ways of doing the task

$$T_1 \text{ and } T_2 \text{ and } \cdots \text{ and } T_n$$

is by using a **rooted tree** formed in the order $T_1 \to T_2 \to \cdots \to T_n$. A "branch" represents a possible choice, and "leaves" represent the possible outcomes. In a number of complex problems, we need to use both sum and product rules.

Q 118. *How many bit strings of length 8 start with a 1 bit or end with two bits 00?*

Sol. By product rule, since the first bit can be chosen in only one way and each of the remaining 7 bits can be chosen in two ways, the first task T_1 of constructing a bit string of length 8 beginning with a 1 bit can be done in $2^7 = 128$ ways. Also, since the first 6 bits can be chosen in two ways and each of the remaining 2 bits can be chosen in only one way, the second task T_2 of constructing a bit string of length 8 ending with two bits 00 can be done in $2^6 = 64$ ways. By the same reasoning, both tasks T_1 and T_2 of constructing a bit string of length 8 beginning with a 1 bit and ending with two bits 00 can be done in $2^5 = 32$ ways. Therefore, by *subtraction rule*, the number of bit strings of length 8 that starts with a 1 bit or end with two bits 00 is given by $128 + 64 - 32 = 160$. ♢

15.1 Inclusion-Exclusion Principle

The problems about "combinations" are much more complex when some of these n sets have elements in common. For, let $A_1, \ldots, A_r$ be sets with a universal set U. We write

$$a_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le r} \left| A_{i_1} \cap \cdots \cap A_{i_k} \right|, \qquad \text{for} \quad k = 1, \ldots, r. \tag{15.3}$$

Then, in general, we have

$$\left| A_1 \cup \cdots \cup A_r \right| = \sum_{k=1}^{r} \left(-1\right)^{k+1} a_k = a_1 - a_2 + \cdots + \left(-1\right)^{r+1} a_r; \tag{15.4a}$$

$$\left| A_1^c \cap \cdots \cap A_r^c \right| = \left| \left(A_1 \cup \cdots \cup A_r\right)^c \right| = \left| U \right| - \sum_{k=1}^{r} \left(-1\right)^{k+1} a_k, \tag{15.4b}$$

where the left side of the second equation in (15.4) is the number of elements which do not appear in any of the sets $A_1, \ldots, A_r$. This is known as the **inclusion–exclusion principle** (for r sets).

Q 119. *How many bit strings of length* 8 *start with a* 1 *bit or end with two bits* 00*?*

Sol. Let A_1 be the set of 8-bit strings that start with a 1 bit, and A_2 be the set of 8-bit strings that ends with two bits 00. Then, we have $A_1 \cup A_2$ contains 8-bit strings that starts with a 1 bit or end with two bits 00, and $A_1 \cap A_2$ is the set of 8-bit strings that begins with a 1 bit and ends with two bits 00. By the product rule, since the first bit can be chosen in only one way and each of the remaining 7 bits can be chosen in two ways, we have $|A_1| = 2^7 = 128$. Similarly, since the first 6 bits can be chosen in two ways and each of the remaining 2 bits can be chosen in only one way, we have $|A_2| = 2^6 = 64$. By the same reasoning, we have $|A_1 \cap A_2| = 2^5 = 32$. Therefore, by the case $r = 2$ of (15.4), we have

$$\left| A_1 \cup A_2 \right| = \left| A_1 \right| + \left| A_2 \right| - \left| A_1 \cap A_2 \right| = 128 + 64 - 32 = 160$$

This completes the solution. ♢

Q 120. *Find the numbers of* 10*-bit strings that begin with three* 0*'s or end with two* 1*'s.*

Sol. Let A_1 denote the set of 10-bit strings that begin with three 0's, and A_2 denote the set of 10-bit strings that end with two 1's. Then, we have $A_1 \cup A_2$ contains 10-bit strings that starts with 000 or end with two 11, and $A_1 \cap A_2$ is the set of 10-bit strings that begins with 000 bit and ends with 11. By the product rule, since the first three bits can be chosen in only one way and each of the remaining 7 bits can be chosen in two ways, we have $a_1 = |A_1| = 2^7 = 128$. Also, since the last two bits can be chosen in only one way and each of the remaining 8 bits can be chosen in two ways, we have $a_2 = |A_2| = 2^8 = 256$. By the same reasoning, we have $a_{12} = |A_1 \cap A_2| = 2^5 = 32$. Therefore, by $r = 2$ case of (15.4), the numbers of 10-bit strings that begin with 000 or ends with 11 is given by

$$\big|A_1 \cup A_2\big| = a_1 + a_2 - a_{12} = 128 + 256 - 32 = 352.$$

For more illustrations, suppose U be the set of positive integers not exceeding 1000, and S be the subset of integers that are not divisible by 3, 5, or 7. In this case, we may take A_1 as the set of integers which are divisible by $3, A_2$ the set of integers which are divisible by 5, and A_3 the set of integers which are divisible by 7. Then, the set $S = A_1^c \cap A_2^c \cap A_3^c$. By simple division, we have

$$\begin{gathered}\big|A_1\big| = \lfloor 1000/3 \rfloor = 333, \quad \big|A_2\big| = \lfloor 1000/5 \rfloor = 200, \quad \big|A_3\big| = \lfloor 1000/7 \rfloor = 142;\\ \big|A_1 \cap A_2\big| = \lfloor 1000/15 \rfloor = 66, \quad \big|A_1 \cap A_3\big| = \lfloor 1000/21 \rfloor = 47, \quad \big|A_2 \cap A_3\big| = \lfloor 1000/35 \rfloor = 28;\\ \big|A_1 \cap A_2 \cap A_3\big| = \lfloor 1000/105 \rfloor = 9.\end{gathered}$$

Therefore, by the case when $r = 3$ of *inclusion-exclusion principle*, we have

$$\big|S\big| = \big|U\big| - \sum_{k=1}^{3} \big(-1\big)^{k+1} a_k = 1000 - \big(333 + 200 + 142\big) + \big(66 + 47 + 28\big) - 9 = 457.$$

Q 121. *How many integers between* 1000 *and* 9999 *are divisible by* 7 *and* 11.

Sol. Suppose U is the set of integers between 1000 and 9999, and S be the subset of integers that are not divisible by 7 or 11. Let A and B be respectively the set of integers between 1000 and 9999 (both inclusive) that are divisible by 7 and 11. We thus we have

$$\begin{aligned}\big|A\big| &= \left\lfloor \frac{9999}{7} \right\rfloor - \left\lfloor \frac{1000}{7} \right\rfloor = 1428 - 142 = 1286;\\ \big|B\big| &= \left\lfloor \frac{9999}{11} \right\rfloor - \left\lfloor \frac{1000}{11} \right\rfloor = 909 - 90 = 919.\end{aligned}$$

Similarly, since 7 and 11 are relatively prime, we have

$$\mathbb{A} \cap B = \left\lfloor \frac{9999}{77} \right\rfloor - \left\lfloor \frac{1000}{77} \right\rfloor = 129 - 12 = 117.$$

It thus follows from the *inclusion-exclusion principle* that the number of integers between 1000 and 9999 divisible by 7 or 11 is given by

$$\big|S\big| = \big|A\big| + \big|B\big| - \big|A \cap B\big| = 1286 + 919 - 117 = 2205 - 117 = 2088.$$

Therefore, the number of integers between 1000 and 9999 that are divisible by 7 and 11 is given by $9000 - 2088 = 6912$. ♢

Q 122. *How many integers between* 1 *and* 500 *are* not divisible by 2, 3, 5*, or* 7.

Sol. Suppose U be the set of positive integers not exceeding 500, and S be the subset of integers that are not divisible by 2, 3, 5, or 7. In this case, let A, B, C, D be respectively the set of integers between 1 and 500 that are divisible by 2, 3, 5, and 7. We thus we have

$$\begin{aligned} |A| &= \left\lfloor \frac{500}{2} \right\rfloor = 250; & |B| &= \left\lfloor \frac{500}{3} \right\rfloor = 166; \\ |C| &= \left\lfloor \frac{500}{5} \right\rfloor = 100; & |D| &= \left\lfloor \frac{500}{7} \right\rfloor = 71. \end{aligned}$$

Similarly, since 2, 3, 5, 7 are relatively prime, we have

$$\begin{aligned} |A \cap B| &= \left\lceil \frac{500}{6} \right\rceil =; & |A \cap C| &= \left\lceil \frac{500}{10} \right\rceil =; \\ |A \cap D| &= \left\lceil \frac{500}{14} \right\rceil =; & |B \cap C| &= \left\lceil \frac{500}{15} \right\rceil =; \\ |B \cap D| &= \left\lceil \frac{500}{21} \right\rceil =; & |C \cap D| &= \left\lceil \frac{500}{35} \right\rceil = . \end{aligned}$$

It thus follows from the *inclusion-exclusion principle* that ♢

Q 123 (2019)**.** *In a class C of* 2092 *students,* 1232 *are pursuing a course in Spanish;* 879 *in French; and,* 114 *in Russian. Further,* 103 *are pursuing courses in both Spanish and French;* 23 *in both Spanish and Russian; and,* 14 *in both French and Russian. Assuming that each student is pursuing at least one of three language courses, find how many of them are pursuing a course in all the three languages.*

Sol. Let S, F, and R respectively denote the set of students who are pursuing a course in Spanish, French, and Russian (see the left side Venn diagram in Fig. 50). According to the given data, we have

$$\begin{gathered} |S| = 1232, \quad |F| = 879, \quad |R| = 114, \quad |S \cap F| = 103, \\ |S \cap R| = 23, \quad |F \cap R| = 14, \quad |S \cup F \cup R| = 23. \end{gathered}$$

It thus follows from the *inclusion-exclusion principle* (for three sets) that

$$\begin{aligned} & |S \cup F \cup R| = |S| + |F| + |R| - |S \cap F| - |S \cap R| - |F \cap R| + |S \cap F \cap R|, \\ \Rightarrow \qquad & 2092 = 1232 + 879 + 114 - 103 - 23 - 14 + |S \cap F \cap R|. \end{aligned}$$

Solving the last equation for $|S \cap F \cap R|$, our answer is 7. ♢

Q 124 (2020)**.** *How many integers between* 100 *and* 1000 *are divisible by* 3, 5*, or* 7.

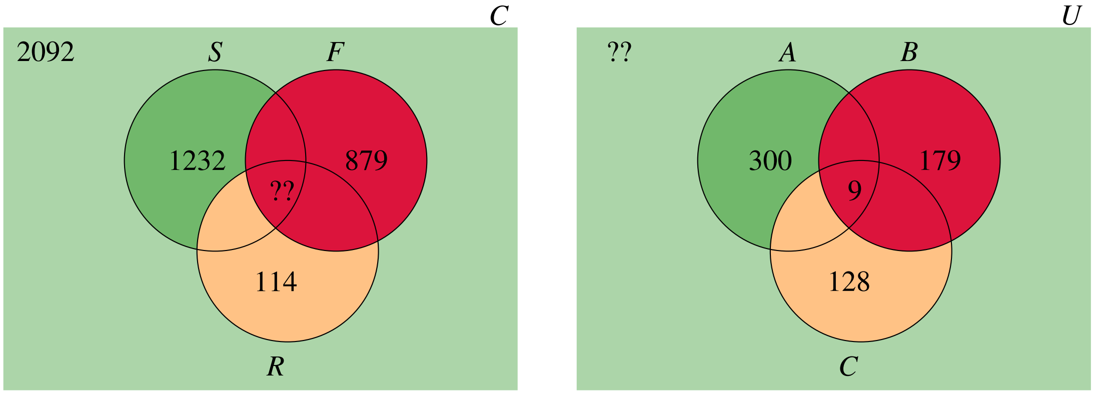


Figure 50: Illustration of inclusion-exclusion principle for three sets.

Sol. Let A, B, and C respectively denote the set of integers between 100 and 1000 that are divisible by 3, 5, and 7 (see the right side Venn diagram in Fig. 50). We thus have

$$\begin{aligned} |A| &= \left\lfloor \frac{1000}{3} \right\rfloor - \left\lfloor \frac{100}{3} \right\rfloor = 300; \\ |B| &= \left\lfloor \frac{1000}{5} \right\rfloor - \left\lfloor \frac{100}{5} \right\rfloor = 179; \\ |C| &= \left\lfloor \frac{1000}{7} \right\rfloor - \left\lfloor \frac{100}{7} \right\rfloor = 128. \end{aligned}$$

Also, since $3, 5$, and 7 are relatively prime integers, we have

$$\begin{aligned} |A \cap B| &= \left\lceil \frac{1000}{15} \right\rceil - \left\lceil \frac{100}{15} \right\rceil = 60; \\ |A \cap C| &= \left\lceil \frac{1000}{21} \right\rceil - \left\lceil \frac{100}{21} \right\rceil = 40; \\ |B \cap C| &= \left\lceil \frac{1000}{35} \right\rceil - \left\lceil \frac{100}{35} \right\rceil = 26; \\ |A \cap B \cap C| &= \left\lceil \frac{1000}{105} \right\rceil - \left\lceil \frac{100}{105} \right\rceil = 9. \end{aligned}$$

It thus follows from the *inclusion-exclusion principle* (for three sets) that

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|, \\ &= 300 + 179 + 128 - 60 - 40 - 26 + 9 = 490. \end{aligned}$$

Hence, our answer is 490. ♢

Finally, we discuss an application of the fact that, from a set of n indistinguishable objects, the number of combinations (or selections) of r objects with repetitions allowed is given by the formula

$$C\big(n+r-1, r\big) = C\big(n+r-1, n-1\big).$$

Suppose we have to find the number of *integer solutions* of the equation

$$x_1+x_2+x_3+x_4=32, \qquad \text{subject to that} \quad x_i \geq 0 \ \text{ for all } \ 1 \leq i \leq 4.$$

The above problem is about selection of $r=4$ objects from $n=32$ indistinguishable objects, with repetition allowed. Therefore, the number of *integer solutions* of the equation is given by

$$C\big(n+r-1,r\big)=C\big(4+32-1,32\big)=C\big(35,32\big)=6545.$$

The other variations of the above problem can be dealt with the same argument, by making suitable *change of variables*.

Q 125. *Find the number of integer solutions of the equation* $x_1+x_2+x_3+x_4+x_5=30$*, subject to constraints*

$$x_1 \geq 2, \quad x_2 \geq 3, \quad x_3 \geq 4, \quad x_4 \geq 2, \quad \textit{and} \quad x_5 \geq 0.$$

Sol. Taking $u_1=x_1-2$, $u_2=x_2-3, u_3=x_3-4$, $u_4=x_4-2$, and $u_5=x_5$, so that we have $u_1+2=x_1$, $u_2+3=x_2, u_3+4=x_3$, $u_4+2=x_4$, and $u_5=x_5$. Therefore, the given problem asks to find the number of *integer solutions* of the equation

$$u_1+u_2+u_3+u_4+u_5=19, \qquad \text{subject to that} \quad u_i \geq 0 \ \text{ for all } \ 1 \leq i \leq 5.$$

Hence, the number is given by

$$C\big(n+r-1,r\big)=C\big(5+19-1,19\big)=C\big(23,19\big)=??.$$

This completes the solution. ♢

15.2 Pigeon-Hole Principle

The following statement was first formulated by the German mathematician *Gustav Dirichlet* (1805 - 1859).

Pigeonhole Principle: *If* $k+1$ *or more pigeons are to be accommodated in k pigeonholes, then at least one pigeonhole must contain at least two pigeons.*

Of course, if none of the pigeonhole contains more than one pigeon, then the total number of pigeons would be at most k, which is not the case. Notice that the above principle applies to other objects besides pigeons and pigeonholes. We thus reformulate the *pigeonhole principle* as follows: *If n objects are to be placed in m boxes, with n* $>$ *m, then at least one box must contain two or more objects*.

Example 15.3. *Since there are only* 366 *days in a non-leap year, among* 367 *people, at least two must share their birthday. Since there are only* 26 *English alphabets, among* 27 *English words, at least two must have the same first letter.*

We can be more specific as in the following statement of *generalised pigeonhole principle*:

Generalised Pigeonhole Principle: *If n objects are to be placed in m boxes, with n > m, then one box must contain at least*

$$\left\lfloor \frac{n-1}{m} \right\rfloor + 1$$

objects, where $\lfloor \ \rfloor$ *denotes the* greatest integer function.

Said differently, if $nk+1$ objects are placed into n boxes, then at least one box contains more than k objects.

`Proof.` [of generalised pigeonhole principle] Suppose each box contains at most $k = \lfloor (n-1)/m \rfloor$ objects, then the maximum number of objects accommodated in m boxes is given by

$$mk = m \left\lfloor \frac{n-1}{m} \right\rfloor \leq m \cdot \frac{n-1}{m} = n-1,$$

which is not the case. Alternatively, by *division algorithm*, we can find positive integers q, r such that

$$m = qn + r, \qquad \text{with} \quad 0 \leq r < n.$$

Suppose no box contains $\lceil m/n \rceil$ objects, and let us consider the following two cases:

1. When $r = 0$ so that $\lceil m/n \rceil = m/n = q$, we have that every box contains less than q objects and hence there are less than $nq = m$ objects in total in the n boxes, which is a contradiction.

2. When $1 \leq r < n$ so that $\lceil m/n \rceil = q+1$, every box contains at most q objects, and hence $nq = m - r < m$ objects in total, which again give a contradiction.

Example 15.4. *Since there are only* 12 *months in an year, among* 25 *students in a class, at least*

$$\left\lfloor \frac{25-1}{12} \right\rfloor + 1 = 3$$

were born in the same month. In this case, we have m = 12 *and n* = 25*. Also, among* 25 *students in a class, at least*

$$\left\lfloor \frac{25-1}{7} \right\rfloor + 1 = 4$$

were born on the same day of a week. In this case, we have m = 7 *and n* = 25*.*

We can also ask: *What must be the minimum number of students in a class so that at least* 5 *were born in the same month ?* In such cases, in general, we need to use the following equivalently version of the *generalized pigeonhole principle*: *If m boxes contains km* + 1 *or more objects for some positive integer k, then at least one box must contain k* + 1 *or more objects*. For example, to answer the above question, we have $m = 12$ (months of an year) and $k+1 = 5$, i. e., $k = 4$. Therefore, the minimum numbers of students in the class is given by $km + 1 = 4 \times 12 + 1 = 49$.

Q 126. *Suppose* 45 *time slots are available to prepare a time-tables for* 500 *classes. How many classrooms are needed to do so.*

Sol. We have to prepare a time-tables for $n = 500$ classes to be conducted in $m = 45$ time slots. Therefore, by the generalized pigeonhole principle, we have

$$\left\lfloor \frac{n-1}{m} \right\rfloor + 1 = \left\lfloor \frac{500-1}{45} \right\rfloor + 1 = 12.$$

Hence, the least number of classrooms needed is 12. ♢

Q 127. *Show that, among six people, at least three are mutual friends or at least three are complete strangers.*

Sol. Suppose "Aman" is one of the six people. We consider two disjoint sets consisting of "friends of Aman" and "stranger to Aman". We do have names of these remaining five people. By the *generalized pigeonhole principle*, there are at least $\lfloor \frac{5-1}{2} \rfloor + 1 = 3$ names in one of the two sets. ♢

16 Recurrence Relations

Definition 16.1. *A **linear recurrence relation** for a sequence* $\big(a_n\big)$ *is an equation of the form*

$$c_0\,a_n + c_1\,a_{n-1} + c_2\,a_{n-2}, \ldots, c_k\,a_{n-k} = g\big(n\big), \qquad \textit{with} \quad c_k \not\equiv 0, \tag{16.1}$$

where the coefficients $c_0, c_1, \ldots, c_k$ *in general may be functions of n, and g is a simple function. In this case, since* $c_k \not\equiv 0$*, we say* (16.1) *is a recurrence relation of **order**[16] k.*

When all the coefficients c_i are constants, we say (16.1) is a linear recurrence relation with *constant coefficients*. Further, when $g \equiv 0$, (16.1) is called a **homogeneous** linear recurrence relation. Otherwise, it is said to be **non-homogeneous**.

16.1 Method of Characteristics

In general, the **general solution** of a non-homogeneous recurrence relation of the form (16.1) is given by

$$a_n = a_n^{(h)} + a_n^{(p)}, \qquad \text{for} \quad n \geq 0, \tag{16.2}$$

where $a_n^{(h)}$ is the solution of the *associated homogeneous equation* given by

$$c_0 a_n + c_1\,a_{n-1} + c_2\,a_{n-2}, \ldots, c_k\,a_{n-k} = 0, \qquad \text{with} \quad c_k \not\equiv 0, \tag{16.3}$$

as obtained by the method described below, and $a_n^{(p)}$ s a *particular solution* of the non-homogeneous recurrence relation that one may obtain by applying the scheme as described in the second part of the section. However, for notational convenience, we may write $a_n^{(h)}$ or $a_n^{(p)}$ simply as a_n.

Let $a_n = r^n \ (r \neq 0)$ be a solution of the *homogeneous recurrence relation* of the form (16.3). Then, we have

$$c_0\,r^n + c_1\,r^{n-1} + \cdots + c_{n-k}\,r^{n-k} = 0.$$

Dividing the above equation throughout by r^{n-k}, we obtain

$$c_0\,r^k + c_1\,r^{k-1} + \ \ldots \ + c_{n-k} = 0,$$

which is a polynomial equation of the degree k. It is called the **characteristic equation** of the linear recurrence relation (16.1). Let we write the k roots as $r_1, \ldots, r_k$. The part $a_n^{(h)}$ of the general solution of the form (16.2) is determined by the nature of these k roots. In particular, for a second order recurrence relation of the form

$$c_0\,a_n + c_1\,a_{n-1} + c_2\,a_{n-2} = 0, \qquad \text{for} \quad n \geq 2, \tag{16.4}$$

[16] In some texts, terminology **degree** is used in place of order.

if r_1 and r_2 are the two roots of its *characteristic equation* given by

$$c_0 r^2 + c_1 r + c_2 = 0, \tag{16.5}$$

then the solution $a_n^{(h)}$ of (16.4) is given by the next theorem.

Theorem 128. *With notations as above, we have*

1. *When $r_1 \neq r_2$, there are constants A, B such that $a_n = A\,r_1^n + B\,r_2^n$;*
2. *When $r_1 == r$ (say), there are constants A, B such that $a_n = A\,r^n + B\,n\,r^n$.*
3. *When r_1, r_2 are complex numbers $a \pm ib$, there are constants A, B such that*

$$a_n = \alpha^n \big[A \cos n\theta + B \sin n\theta\big], \tag{16.6}$$

where $\alpha = |a+ib|$ and $\theta = \arg(a+ib)$. The type of general solution given by (16.6) *is also known as the* modulus-argument form.

We find here the solution of some homogeneous recurrence relations.

Q 129. *Solve the recurrence $a_n - 2\,a_{n-1} - 3\,a_{n-2} = 0$, where $a_0 = 3$ and $a_1 = 1$.*

Sol. The characteristic equation $r^2 - 2r - 3 = 0$ has two roots given by $r_1 = -1$ and $r_2 = 3$. Therefore, the general solution is given by

$$a_n = A\big(-1\big)^n + B\,3^n, \qquad \text{for} \quad n \geq 0.$$

Next, using the initial conditions $a_0 = 3$ and $a_1 = 1$, it follows that constants A and B satisfy the equations

$$A + B = 3 \qquad \text{and} \qquad -A + 3B = 1.$$

Therefore, we obtain $A = 2$ and $B = 1$. Hence, the complete solution of the given recurrence relation is obtained as

$$a_n = 2\big(-1\big)^n + 3^n, \qquad \text{for} \quad n \geq 0.$$

This completes the solution. ♢

Q 130. *Solve the recurrence $a_n = 6\,a_{n-1} - 11\,a_{n-2} + 6a_{n-3}$, where $a_0 = 2$, $a_1 = 5$, and $a_3 = 15$.*

Sol. Clearly, the characteristic equation $r^3 - 6r^2 + 11r - 6 = 0$ has $r = 1$ as one root. Therefore, the other two roots are given by the quadratic equation $r^2 - 5r + 6 = 0$, which are $r_2 = 2$ and $r_3 = 3$. It thus follows that the general solution of the recurrence relation is given by

$$a_n = A\,1^n + B\,2^n + C\,3^n == A + B\,2^n + C\,3^n, \qquad \text{for} \quad n \geq 0.$$

Next, using the initial conditions $a_0 = 2$, $a_1 = 5$ and $a_2 = 15$, it follows that constants A, B, and C are given by the linear equations given by

$$A+B+C=2, \quad A+2B+2C=5, \quad \text{and} \quad A+4B+9C=15.$$

By solving the above three equations, we obtain $A=-1, B=11/5$, and $C=4/5$. Hence, the complete solution of the given recurrence relation is obtained as

$$a_n = \frac{1}{5}\Big[-5+11\,2^n+4\,3^n\Big], \qquad \text{for} \quad n \geq 0.$$

This completes the solution. ♢

Q 131. *Solve the recurrence $a_n - 7\,a_{n-1} + 10\,a_{n-2} = 0$, where $a_0 = 0$ and $a_1 = 3$.*

Sol. See the previous year "compact notes", as shared earlier. ♢

Q 132. *Solve the recurrence $a_n + a_{n-1} - 20\,a_{n-2} = 0$, where $a_0 = -3$ and $a_1 = -10$.*

Sol. The characteristic equation $r^2+r-20=0$ has two roots given by $r_1=-5$ and $r_2=4$. Therefore, the general solution is given by

$$a_n = A\big(-5\big)^n + B\,4^n, \qquad \text{for} \quad n \geq 0.$$

Next, using the initial conditions $a_0 = -3$ and $a_1 = -10$, it follows that constants A and B satisfy the linear equations

$$A+B=-3 \qquad \text{and} \qquad -5A+4B=-10.$$

Therefore, we obtain $A=-52/9$ and $B=25/9$. Hence, the complete solution of the given recurrence relation is obtained as

$$a_n = \frac{1}{9}\Big[-52(-5)^n+25\,4^n\Big], \qquad \text{for} \quad n \geq 0.$$

This completes the solution. ♢

16.2 Particular Solution

To find a **particular solution** $a_n^{(p)}$ of a recurrence relation of the form (16.1), depending upon the form of the function $g(n)$ in any particular problem, we shall use as a trial solution the functions given in the second column of Table 17. In particular, when $g(n)=r^n$ or $(a+bn)r^n$ with r being a non-repeating root, we take

$$a_n^{(p)} = \alpha\,n\,r^n \qquad \text{or} \qquad a_n^{(p)} = \gamma n(\alpha+\beta\,n)\,r^n, \quad \text{respectively.} \tag{16.7}$$

On the other hand, when r is a double root of the characteristic equation, we take

$$a_n^{(p)} = \alpha\,n^2\,r^n \qquad \text{or} \qquad a_n^{(p)} = \gamma n(\alpha+\beta\,n)\,r^n,\ \ldots, \quad \text{and so on.} \tag{16.8}$$

Table 17: Scheme for choosing a trial particular solution.

WHEN $\mathbf{g(n)} =$	**USE** $\mathbf{a_n^{(p)}} =$
a constant	a constant, say α;
$P_k(n)$, a polynomial of degree k	$\alpha_0 + \alpha_1 n + \cdots + \alpha_k n^k$;
r^n	αr^n; when r is not a root of Ch. Eqn.
	$\alpha n^m r^n$; when r is a root of Ch. Eqn. of order m;
$r^n P_k(n)$	$r^n \left(\alpha_0 + \alpha_1 n + \cdots + \alpha_k n^k\right)$,
	when r is not a root of Ch. Eqn.;
$r^n P_k(n)$	$n^m r^n \left(\alpha_0 + \alpha_1 n + \cdots + \alpha_k n^k\right)$,
	when r is a root of Ch. Eqn. of order m;
$\sin(\alpha n)$ or $\cos(\alpha n)$	$A \sin(\alpha n) + B \cos(\alpha n)$;
$r^n \sin(\alpha n)$ or $r^n \cos(\alpha n)$	$r^n \left(A \sin(\alpha n) + B \cos(\alpha n)\right)$

Finally, when $g(n)$ is a linear combination of some functions of the form as in Table 17, we may use a similar type of linear combination of functions for $a_n^{(p)}$. More specifically, if the involved functions are $g_1(n), \ldots, g_s(n)$, then we choose $a_{n1}^{(p)}, \ldots, a_{ns}^{(p)}$ as trial particular solution according to the scheme given in Table 17. Subsequently, the particular solution of the recurrence relation (16.1) is given by

$$a_n^{(p)} = a_{n1}^{(p)} + a_{n2}^{(p)} + \cdots + a_{ns}^{(p)}.$$

Finally, the general solution is written as

$$a_n = a_n^{(h)} + a_n^{(p)}.$$

The **complete solution** is obtained from a general solution by substituting initial values “at this stage” to find the constants appearing in the expression for a_n^h.

Before solving the assigned problems, we give below some simple examples to illustrate how to find the particular solution of (non-homogeneous) recurrence relation.

Example 16.1. *Consider the first order non-homogeneous recurrence relation given by*

$$a_n - 2a_{n-1} = 3^n, \qquad \textit{for} \quad n \geq 1, \quad \textit{with} \;\; a_1 = 5.$$

The characteristic equation of the associated homogeneous recurrence relation has the root given by $r = 2$. *Therefore, we have* $a_n^{(h)} = c\,2^n$. *Next, we have* $g(n) = 3^n$ *and, in this case,* 3 *is* not a root *of the characteristic* *equation. Hence, by the scheme given in Table 17, we may take* $a_n^p = A\,3^n$ *as a trial particular solution. Substituting this into the given equation, we obtain*

$$A3^n - 2A3^{n-1} = 3^n \qquad or \qquad A = 3.$$

Therefore, the general solution of given recurrence relation is given by

$$a_n = c\,2^n + 3^{n+1}, \qquad for \quad n \geq 1.$$

Finally, using the initial condition $a_1 = 5$, *we get* $c = -2$. *Hence, the solution is obtained as*

$$a_n = 3^{n+1} - 2^{n+1}, \qquad for \quad n \geq 1.$$

Notice that, however, for the non-homogeneous recurrence relation given by

$$a_n - 2a_{n-1} = 2^n, \qquad with \quad a_0 = 2,$$

we need to take $a_n^p = A\,n\,2^n$ *as a trial particular solution, because* $g(n) = 2^n$ *and* 2 *is* a root *of the characteristic equation. Substituting this into the given equation, we obtain*

$$An2^n - 2A(n-1)2^{n-1} = 2^n \qquad or \qquad A = 1.$$

Therefore, the general solution of given recurrence relation is given by

$$a_n = \big(c + n\big)\,2^n, \qquad for \quad n \geq 0.$$

Finally, by using $a_0 = 2$, *we get* $c = 2$. *In this case, the* complete solution *is obtained as*

$$a_n = \big(n + 2\big)\,2^n, \qquad for \quad n \geq 1.$$

Example 16.2. *Consider the first order non-homogeneous recurrence relation given by*

$$a_{n+1} - a_n = 3\,n^2 - n, \qquad for \quad n \geq 0, \quad with \;\; a_0 = 3.$$

The characteristic equation of the associated homogeneous recurrence relation has the root given by $r = 1$. *Therefore, we have* $a_n^{(h)} = c\,1^n = c$. *Next, we have*

$$g\big(n\big) = 3\,n^2 - n = \big(3\,n^2 - n\big)\cdot 1^n$$

Since 1 *is* a root *of the characteristic equation, by the scheme given in Table 17, we need to take*

$$a_n^p = \big(A_0 n^2 + A_1 n + A_2\big)\,n = \big(A_0\,n^3 + A_1\,n^2 + A_2\,n\big)$$

as a trial particular solution. Substituting this into the given equation, we obtain

$$\big\{A_0\big(n+1\big)^3 + A_1\big(n+1\big)^2 + A_2\big(n+1\big)\big\} - \big\{A_0\,n^3 + A_1 n^2 + A_2\,n\big\} = 3n^2 - n,$$

which on simplification yields

$$A_0\big(3n^2+3n+1\big)+A_1\big(2n+1\big)+A_2=3n^2-n,$$

Comparing coefficients of the same powers of n, we obtain

$$3A_0=3, \qquad 3A_0+2A_1=-1, \quad \textit{and} \quad A_0+A_1+A_2=0.$$

By solving above equations, we get $A_0=1, A_1=-2$, and $A_2=1$. Therefore, the general solution of given recurrence relation is given by

$$a_n=c+n\big(n+1\big)^2, \qquad \textit{for} \quad n\geq 0.$$

Finally, using the initial condition $a_0=3$, we get $c=3$. Hence, the solution is obtained as

$$a_n=3+n\big(n+1\big)^2, \qquad \textit{for} \quad n\geq 0.$$

This is the complete solution.

Q 133. *Solve the recurrence $a_n-6\,a_{n-1}+8\,a_{n-2}=n4^n$, where $a_0=8$ and $a_1=1$.*

Sol. The characteristic equation of the associated homogeneous recurrence relation is $r^2-6r+8=0$, which has the two root given by $r_1=2$ and $r_2=4$. Therefore, we have $a_n^h=A\,2^n+B\,4^n$. Further, since $g(n)=n\,4^n$ and $r=4$ is root of the characteristic equation, by the scheme given in Table 17, we may take trial particular solution as

$$a_n^p=\big(A_0n+A_1\big)\,n\,4^n=\big(A_0\,n^2+A_1\,n\big)4^n.$$

Substituting this into the given equation, we obtain

$$\big(A_0\,n^2+A_1\,n\big)4^n-6\big(A_0(n-1)^2+A_1(n-1)\big)4^{n-1}+8\big(A_0(n-2)^2+A_1(n-2)\big)4^{n-2}=n\,4^n.$$

That is,

$$16\big(A_0\,n^2+A_1\,n\big)-24\big(A_0(n-1)^2+A_1(n-1)\big)+8\big(A_0(n-2)^2+A_1(n-2)\big)=16n,$$

which on simplification yields

$$A_0\big(16n+8\big)+8A_1=16n,$$

Comparing coefficients of the same powers of n, we obtain

$$16A_0=16, \qquad \text{and} \qquad A_0+A_1=0.$$

By solving above equations, we get $A_0=1$ and $A_1=-1$. Therefore, the general solution of given recurrence relation is given by

$$a_n=A\,2^n+B\,4^n+\big(n^2-n\big)4^n, \qquad \text{for} \quad n\geq 0.$$

Finally, using the initial conditions $a_0 = 8$ and $a_1 = 1$, we find constants A and B satisfy the equations $A + B = 8$ and $2A + 4B = 1$, which give $A = 1/2$ and $B = 15/2$. Hence, the complete solution is obtained as

$$a_n = 2^{n-1} + \frac{1}{2}\Big[15 + 2\big(n^2 - n\big)\Big]4^n, \qquad \text{for} \quad n \geq 0.$$

This completes the solution. ♢

Q 134. *Solve the recurrence $a_n - 4a_{n-1} + 4a_{n-2} = 3n + 2^n$, where $a_0 = a_1 = 1$.*

Sol. The characteristic equation of the recurrence relation is $r^2 - 4r + 4 = 0$, which has repeated roots $r_1 = 2$ and $r_2 = 2$. Therefore, we have

$$a_n^{(h)} = \big(a + bn\big)2^n, \qquad \text{for some constants} \quad a, b.$$

Next, since $g(n) = 3n + 2^n$ and the characteristic equation has $r = 2$ as repeated root **of order 2**, we take

$$a_n^{(p)} = \big(An + B\big) + Cn^2\, 2^n,$$

as a trial particular solution. Substituting this into the given equation, we obtain

$$\big(An + B\big) + Cn^2 2^n - 4\big(A\,(n-1) + B\big) - 4C\,(n-1)^2\, 2^{n-1} + 4\big(A\,(n-2) + B\big) + 4C\,(n-2)^2\, 2^{n-2} = 3n + 2^n$$

That is, on simplification, we have

$$An - \big(4A - B\big) + 2C\,2^n = 3n + 2^n$$

Comparing coefficients of the same powers of n and 2^n, we obtain $A = 3$, $B = 12$, and $C = 1/2$. Therefore, the general solution of the recurrence relation is given by

$$a_n = \big(a + bn\big)2^n + \big(3n + 12\big) + n^2\, 2^{n-1}, \qquad \text{for} \quad n \geq 0.$$

Finally, using $a_0 = a_1 = 1$, we find that the constants A and B are given by $a = -11$ and $b = 7/2$. Hence, we obtain

$$a_n = \big(n^2 + 7n - 22\big)2^{n-1} + 3n + 12, \qquad \text{for} \quad n \geq 0,$$

which is the complete solution of the given recurrence relation. ♢

Q 135. *Solve the recurrence $a_n + 4a_{n-1} + 4a_{n-2} = n^2$, taking $a_0 = a$ and $a_1 = b$.*

Sol. The characteristic equation of the recurrence relation is $r^2 + 4r + 4 = 0$, which has repeated roots $r_1 = -2$ and $r_2 = -2$. Therefore, we have

$$a_n^{(h)} = \big(c + dn\big)\big(-2\big)^n, \qquad \text{for some constants} \quad c, d.$$

Next, since $g(n) = n^2$ and 1 <u>is not a root</u> of the characteristic equation, we take

$$a_n^{(p)} = An^2 + Bn + C,$$

as a trial particular solution. Substituting this into the given equation, we obtain

$$\big(An^2 + Bn + C\big) + 4\big(A(n-1)^2 + B(n-1) + C\big) + 4\big(A(n-2)^2 + B(n-2) + C\big) = n^2,$$

which on simplification gives

$$9An^2 + 9Bn - 24An + 9C + 4A - 12B = n^2.$$

Comparing coefficients of the same powers of n, we obtain $A = 1/9$, $B = 8/27$, and $C = 28/9$. Therefore, the general solution of the recurrence relation is given by

$$a_n = \big(c + dn\big)\big(-2\big)^n + \frac{1}{27}\big[3n^2 + 8n + 84\big], \qquad \text{for} \quad n \geq 0.$$

Finally, using any specific values for a and b, we can find the constants c and d, and hence the complete solution of the recurrence relation. ♢

Q 136. *Solve the recurrence $f(k) - 7f(k-1) + 10f(n-2) = 8k + 6$, taking $a_0 = a$ and $a_1 = b$.*

Sol. For brevity, we may take $a_k = f(k)$, for $k \geq 0$, so that the given recurrence relation may be written as $a_k - 7a_{k-1} + 10a_{k-2} = 8k + 6$. The characteristic equation of the recurrence relation is $r^2 - 7r + 10 = 0$, which has distinct roots $r_1 = 2$ and $r_2 = 5$. Therefore, we have

$$a_k^{(h)} = c\,2^k + d\,5^k, \qquad \text{for some constants} \quad c, d.$$

Next, since $g(k) = 8k + 6$ and 1 <u>is not a root</u> of the characteristic equation, we take

$$a_k^{(p)} = Ak + B,$$

as a trial particular solution. Substituting this into the given equation, we obtain

$$\big(Ak + B\big) - 7\big(A(k-1) + B\big) + 10\big(A(k-2) + B\big) = 8k + 6$$

which on simplification gives

$$4Ak - 13A + 4B = 8k + 6$$

Comparing coefficients of the same powers of n, we obtain $A = 2$ and $B = 8$. Therefore, the general solution of the recurrence relation is given by

$$a_k = c\,2^k + d\,5^k + 2k + 8.$$

The rest of the details are simple to work out. You may use any suitable values for a and b. ♢

17 Generating Functions

We begin with the next definition.

Definition 17.1. *The **generation function** of a sequence $\big(a_n\big)$ is a formal power series of the form*

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots , \tag{17.1}$$

which we write as $G\big((a_n);x\big)$ (or simply as $G\big(x\big)$).

Example 17.1. *We first consider the sequence $1, 1, 1, \ldots$. In this case, the sequence $\big(a_n\big)$ is given by $a_n = 1$, for all $n \geq 0$. Therefore, by (17.1), the generation function $G(x)$ of the sequence $\big(a_n\big)$ is given by*

$$1 + x + x^2 + \cdots = \big(1-x\big)^{-1} = \frac{1}{1-x}. \tag{17.2}$$

Recall that, in analytical terms, the above equality is valid only when $\big|x\big| < 1$, but here we don't have to worry about that. More generally, for the sequence $1, a, a^2, \ldots$ given by

$$a_n = a^n, \quad \textit{with} \quad n \geq 0, \quad \textit{and a number} \quad a \neq 0,$$

the generating function $G(x)$ is given by

$$1 + ax + a^2x^2 + \cdots = \frac{1}{1-ax}. \tag{17.3}$$

Notice that the above may also be obtained from the relation (17.2) by taking ax in place of the "symbol" x. As said above, in analytical terms, the above equality is valid for $\big|x\big| < 1/a$. However, we also use the generating function $G(x)$ for the sequence $1, -1, 1, -1, \ldots$ given by $a_n = \big(-1\big)^n$, for $n \geq 0$. It is given by

$$1 - x + x^2 - x^3 + \cdots = \big(1+x\big)^{-1} = \frac{1}{1+x}. \tag{17.4}$$

Once again, the above may also be obtained from the relation (17.2) by taking $-x$ in place of x. Also, for the sequence $1, 0, 1, 0, \ldots$ given by

$$a_n = 1 + \big(-1\big)^n, \qquad \textit{for} \quad n \geq 1, \quad \textit{and taking} \quad a_0 = 1,$$

the generating function $G(x)$ is given by

$$\sum_{n=0}^{\infty} a_n x^{2n} = 1 + x^2 + x^4 - x^6 + \cdots = \frac{1}{1-x^2}. \tag{17.5}$$

Finally, we consider the sequence $\big(a_n\big)$ given by

$$a_n = \frac{1}{n!}, \quad \textit{for} \quad n \geq 0.$$

In this specific case, the generating function $E(x)$ is given by

$$\sum_{n=0}^{\infty} a_n x^n = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = e^x, \tag{17.6}$$

which is a special case of the exponential generating series.

17.1 Important Properties

We start with the next theorem.

Theorem 137. *Consider two generating functions $G(x)$ and $H(x)$ respectively for the sequences $\big(a_n\big)$ and $\big(b_n\big)$. That is, we have*

$$\begin{aligned} G(x) &= \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \ \dots\ ; \\ H(x) &= \sum_{n=0}^{\infty} b_n x^n = b_0 + b_1 x + b_2 x^2 + \ \dots\ . \end{aligned} \tag{17.7}$$

*Then the **sum, difference**, and the **product** of $G(x)$ and $H(x)$ are respectively given by the sequences $\big(c_n\big)$, $\big(d_n\big)$ and $\big(e_n\big)$, where*

$$c_n = a_n + b_n, \quad d_n = a_n - b_n, \quad \textit{and} \quad e_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0, \tag{17.8}$$

for $n \geq 0$. More generally, if α, β are constants, then the generating function $\alpha G(x) + \beta H(x)$ is given by the sequence $\big(\alpha a_n + \beta b_n\big)$. That is, we have

$$\alpha G(x) + \beta H(x) = \sum_{n=0}^{\infty} \big(\alpha a_n + \beta b_n\big) x^n = \big(\alpha a_0 + \beta b_0\big) + \big(\alpha a_1 + \beta b_1\big) x + \ \dots\ . \tag{17.9}$$

*Further, if $b_0 \neq 0$, then the **quotient** $G(x)/H(x)$ is given by the sequences $\big(f_n\big)$ such that*

$$a_n = b_0 f_n + b_1 f_{n-1} + \cdots + b_n f_0, \qquad \textit{for} \quad n \geq 0. \tag{17.10}$$

Notice that , it follows from (17.10) that we can construct the whole sequence $\big(f_n\big)$, starting with the assumption $b_0 \neq 0$. For, we have

$$\begin{aligned} a_0 &= b_0 f_0 \quad \Rightarrow \qquad f_0 = a_0/b_0; \\ a_1 &= b_0 f_1 + b_1 f_0 \quad \Rightarrow \qquad f_1 = \frac{a_1 b_0 - a_0 b_1}{b_0^2}; \\ &\vdots \end{aligned}$$

In the next example, we use the above operations to find generating functions of some other sequences.

Example 17.2. *By* (17.3)*, the generating function of the sequence* $1, 3, 9, 27, \dots$ *is given by*

$$1 + 3x + 9x^2 + 27x^3 + \cdots \ = \frac{1}{1 - 3x}.$$

It thus follows from (17.8) *that the generating function of the* sum *of two sequences* $1, , 1, 1, \dots$ *and* $1, 3, 9, 27, \dots$ *is given by*

$$2 + 4x + 10x^2 + 28x^3 + \cdots \ = \frac{1}{1 - x} + \frac{1}{1 - 3x} = \frac{2(1 - 2x)}{(1 - x)(1 - 3x)}.$$

Further, differentiating (17.2) *with respect x, we obtain*

$$1+2x+3x^2+\cdots=\frac{1}{(1-x)^2}.$$

It thus follows that the generating function of the sequence $1,2,3,4,\ldots$ *is given by*

$$\sum_{n=0}^{\infty}\big(n+1\big)x^n=1+2x+3x^2+4x^3+\cdots=\frac{1}{(1-x)^2}. \tag{17.11}$$

Similarly, it follows that the generating function of triangular numbers $1,3,6,10,15,\ldots$ *is given by*

$$\sum_{n=0}^{\infty}\binom{n+2}{2}x^n=1+3x+6x^2+10x^3+\cdots=\frac{1}{(1-x)^3}. \tag{17.12}$$

Also, the generating function of square numbers $1,4,9,16,25,\ldots$ *is given by*

$$\begin{aligned}\sum_{n=0}^{\infty}n^2x^n&=\sum_{n=0}^{\infty}n(n-1)x^n+\sum_{n=0}^{\infty}nx^n\\&=x^2\frac{d}{dx}\left[\frac{1}{(1-x)^2}\right]+x\frac{d}{dx}\left[\frac{1}{1-x}\right]\\&=\frac{2x^2}{(1-x)^3}+\frac{x}{(1-x)^2}\\&=\frac{x(x+1)}{(1-x)^3}.\end{aligned} \tag{17.13}$$

Q 138. *Consider the sequence* $\big(a_n\big)$ *given by*

$$a_n=\frac{n+1}{3^n}, \qquad \textit{for} \quad n\geq 0.$$

Obtain the generating function *of* $\big(a_n\big)$.

Sol. By definition, the generating function of the sequence $\big(a_n\big)$ is given by

$$\begin{aligned}\sum_{n=0}^{\infty}a_nx^n&=\sum_{n=0}^{\infty}\frac{n+1}{3^n}x^n\\&=\sum_{n=0}^{\infty}\big(n+1\big)\frac{x^n}{3^n}\\&=\sum_{n=0}^{\infty}\big(n+1\big)\big(x/3\big)^n\\&=\frac{1}{\big(1-(x/3)\big)^2}=\frac{9}{(x-3)^2},\end{aligned}$$

by using (17.11). ♢

17.2 Generating Function Method

We illustrate here how to apply generation functions to solve linear recurrence relations. According to *generation function method*, we first multiply the equation by x^n, and subsequently sum all equations for $n \geq k$, where k is the *order* of the given recurrence relation. Let us start with the next example.

Example 17.3. *We use generation functions to solve the linear recurrence relation given by*

$$a_n = 3a_{n-1} + 1, \ \textit{for} \ \ n \geq 1, \quad \textit{with} \ \ a_0 = 1. \tag{17.14}$$

We may write $G(x) = \sum_{n=0}^{\infty} a_n x^n$ *so that we have*

$$\sum_{n=1}^{\infty} a_n x^n = G(x) - a_0 = G(x) - 1, \tag{17.15}$$

using $a_0 = 1$. *Notice that, in this case, the recurrence relation* (17.14) *is of order* 1. *Therefore, multiplying it by* x^n*, and taking sum of all equations for* $n \geq 1$*, it follows that we have*

$$\begin{aligned}
&\sum_{n=1}^{\infty} a_n x^n = 3\sum_{n=1}^{\infty} a_{n-1} x^n + \sum_{n=1}^{\infty} x^n = 3x\sum_{n=1}^{\infty} a_{n-1} x^{n-1} + \sum_{n=1}^{\infty} x^n \\
\Rightarrow \quad &\Big(\sum_{n=0}^{\infty} a_n x^n - a_0\Big) = 3x\sum_{n=0}^{\infty} a_n x^n + \Big(\sum_{n=0}^{\infty} x^n - 1\Big) \\
\Rightarrow \quad &G(x) = 3xG(x) + \frac{1}{1-x} \qquad (\textit{by } (17.15) \textit{ and } (17.2))
\end{aligned}$$

Therefore, by the method of partial fractions, *we obtain*

$$\begin{aligned}
G(x) &= \frac{x}{(1-8x)(1-10x)} + \frac{9}{8(1-8x)} = -\frac{1}{2(1-x)} + \frac{3}{2(1-3x)}, \\
&= -\frac{1}{2}\big[1 + x + x^2 + \dots\big] + \frac{3}{2}\big[1 + 3x + 9x^2 + \dots\big] \\
&= -\frac{1}{2}\sum_{n=0}^{\infty} x^n + \frac{3}{2}\sum_{n=0}^{\infty} (3x)^n
\end{aligned}$$

Hence, by comparing the coefficients of powers of x on the both sides of the last equation, it follows that

$$a_n = \frac{1}{2}\Big[3^{n+1} - 1\Big], \qquad \textit{for} \quad n \geq 1,$$

which is the solution of the linear recurrence relation (17.14).

Q 139 (2019)**.** *Let* a_n *denotes the number of* valid codewords *in decimal notation of length n. It is known that* a_n *satisfies the recurrence relation*

$$a_n = 8a_{n-1} + 10^{n-1}, \ \textit{for} \ \ n \geq 2, \quad \textit{with} \ \ a_1 = 9.$$

Use generating function method to find an explicit formula for a_n*.*

Sol. Equivalently, by taking $a_0 = 1$, we solve the recurrence relation

$$a_{n+1} = 8a_n + 10^n, \text{ for } n \geq 0, \quad \text{with } a_0 = 1. \tag{17.16}$$

We may write $G(x) = \sum_{n=0}^{\infty} a_n x^n$ so that we have

$$\sum_{n=1}^{\infty} a_n x^n = G(x) - a_0 = G(x) - 1. \tag{17.17}$$

Notice that, in this case, the recurrence relation (17.16) is of order 1. Therefore, multiplying it by x^n, and taking sum of all equations for $n \geq 1$, it follows that we have

$$\begin{aligned}
& \big(1/x\big) \sum_{n=1}^{\infty} a_{n+1} x^{n+1} = 8 \sum_{n=1}^{\infty} a_n x^n + \sum_{n=1}^{\infty} 10^n x^n = 8\Big(\sum_{n=0}^{\infty} a_n x^n - a_0\Big) + \Big(\sum_{n=0}^{\infty} \big(10x\big)^n - 1\Big) \\
\Rightarrow \quad & \sum_{n=0}^{\infty} a_n x^n - a_0 - a_1 x = 8x\Big(\sum_{n=0}^{\infty} a_n x^n - 1\Big) + x\Big(\sum_{n=0}^{\infty} \big(10x\big)^n - 1\Big) \\
\Rightarrow \quad & G(x) - 1 - 9x = 8x\,G(x) - 8x + \frac{x}{1 - 10x} - x \quad \text{(by (17.15) and (17.2))}
\end{aligned}$$

Therefore, by the method of *partial fractions*, we obtain

$$\begin{aligned}
G(x) &= \frac{1 - 9x}{(1 - 10x)(1 - 8x)} = \frac{1}{2}\Big[+\frac{1}{1 - 8x} + \frac{1}{1 - 10x}\Big] \\
&= \frac{1}{2}\Big[1 + 8x + 64x^2 + \ldots\Big] + \frac{1}{2}\Big[1 + 10x + 100x^2 + \ldots\Big] \\
&= \frac{1}{2} \sum_{n=0}^{\infty} \big(8x\big)^n + \frac{1}{2} \sum_{n=0}^{\infty} \big(10x\big)^n
\end{aligned}$$

Hence, by comparing the coefficients of powers of x on the both sides of the last equation, it follows that

$$a_n = \frac{1}{2}\Big[8^n + 10^n\Big], \qquad \text{for} \quad n \geq 1,$$

which is the solution of the linear recurrence relation (17.16). ♢

Example 17.4. *We use generation functions to solve the linear recurrence relation given by*

$$a_n = 4a_{n-1} - 4a_{n-2} + 4^n, \ \textit{for} \ n \geq 2, \quad \textit{with} \ a_0 = 2 \textit{ and } a_1 = 8. \tag{17.18}$$

We may write $G(x) = \sum_{n=0}^{\infty} a_n x^n$ *so that we have*

$$\sum_{n=1}^{\infty} a_n x^n = G(x) - a_0 = G(x) - 2; \tag{17.19a}$$

$$\sum_{n=2}^{\infty} a_n x^n = G(x) - a_0 - a_1 x = G(x) - 2 - 8x, \tag{17.19b}$$

using $a_0 = 2$ *and* $a_1 = 8$*. Notice that, in this case, the recurrence relation* (17.18) *is of order* 2*. Therefore, multiplying it by* x^n*, and taking sum of all equations for* $n \geq 2$*, it follows that we have*

$$\begin{aligned}
&\sum_{n=2}^{\infty} a_n x^n = 4\sum_{n=2}^{\infty} a_{n-1} x^n - 4\sum_{n=2}^{\infty} a_{n-2} x^n + \sum_{n=2}^{\infty} 4^n x^n \\
\Rightarrow \quad &\sum_{n=0}^{\infty} a_n x^n - a_0 - a_1 x = 4x\sum_{n=2}^{\infty} a_{n-1} x^{n-1} - 4x^2\sum_{n=2}^{\infty} a_{n-2} x^{n-2} + \Big(\sum_{n=0}^{\infty} 4^n x^n - 1 - 4x\Big) \\
\Rightarrow \quad &G(x) - 2 - 8x = 4x\Big(\sum_{n=0}^{\infty} a_n x^n - 2\Big) - 4x^2\sum_{n=0}^{\infty} a_n x^n + \Big(\sum_{n=0}^{\infty} (4x)^n - 1 - 4x\Big) \\
&\qquad = 4xG(x) - 8x - 4x^2 G(x) + \sum_{n=0}^{\infty} 4^n x^n - 1 - 4x \quad \textit{(using equations (17.19))}
\end{aligned}$$

which implies by using (17.3) *that*

$$\big(4x^2 - 4x + 1\big)\, G(x) = \frac{1}{1-4x} - 4x + 1.$$

Therefore, by the method of partial fractions*, we obtain*

$$\begin{aligned}
G(x) &= \frac{1}{(1-4x)(1-2x)^2} - \frac{4x}{(1-2x)^2} + \frac{1}{(1-2x)^2} \\
&=,
\end{aligned}$$

Hence, by comparing the coefficients of powers of x on the both sides of the last equation, it follows that

$$a_n = 4^{n+1} - \big(n+1\big)2^{n+1}, \qquad \textit{for} \quad n \geq 1,$$

which is the solution of the linear recurrence relation (17.18).

Q 140. *Use* generating function method *to solve the recurrence relation*

$$a_n - 2a_{n-1} + a_{n-2} = 2^n, \quad \textit{with} \quad a_0 = 2 \textit{ and } a_1 = 1. \tag{17.20}$$

Sol. We may write $G(x) = \sum_{n=0}^{\infty} a_n x^n$ so that we have

$$\sum_{n=1}^{\infty} a_n x^n = G(x) - a_0 = G(x) - 2; \tag{17.21a}$$

$$\sum_{n=2}^{\infty} a_n x^n = G(x) - a_0 - a_1 x = G(x) - 2 - x, \tag{17.21b}$$

using $a_0 = 2$ and $a_1 = 1$. In this case, the recurrence relation (17.20) is of order 2. Therefore, multiplying it by x^n, and taking sum of all equations for $n \geq 2$, it follows that we have

$$\begin{aligned}
& \sum_{n=2}^{\infty} a_n x^n = 2 \sum_{n=2}^{\infty} a_{n-1} x^n - \sum_{n=2}^{\infty} a_{n-2} x^n + \sum_{n=2}^{\infty} 2^n x^n \\
\Rightarrow \qquad & G(x) - 2 - x = 2x \sum_{n=2}^{\infty} a_{n-1} x^{n-1} - x^2 \sum_{n=2}^{\infty} a_{n-2} x^{n-2} + \Big(\sum_{n=0}^{\infty} 2^n x^n - 1 - 2x \Big) \quad \text{(using equations (17.21))} \\
& \qquad = 2x \Big(G(x) - 2 \Big) - x^2 G(x) + \Big(\sum_{n=0}^{\infty} \big(2x\big)^n - 1 - 2x \Big) \\
& \qquad = 2x G(x) - 4x - x^2 G(x) + \sum_{n=0}^{\infty} 2^n x^n - 1 - 2x
\end{aligned}$$

which implies by using (17.3) that

$$\big(x^2 - 2x + 1\big) G(x) = \frac{1}{1-2x} - 5x - 1 = \frac{10x^2 + 3x - 1}{1-2x}.$$

Therefore, using *partial fractions*, we obtain

$$\begin{aligned}
G(x) &= \frac{10x^2 + 3x - 1}{(1-2x)(1-x)^2} \\
&=,
\end{aligned}$$

Hence, by comparing the coefficients of powers of x on both sides of the last equation, it follows that

$$a_n = 4^{n+1} - \big(n+1\big) 2^{n+1}, \qquad \text{for} \quad n \geq 1,$$

which is the complete solution of the recurrence relation (17.20). ♢

Q 141. *Use generating function method to solve the recurrence relation*

$$a_{n+2} - 7\, a_{n+1} + 10\, a_n = 2,$$

where $a_0 = a_1 = 3$.

References

[1] Lipschutz, S., Lipson, M. L. and Patil, Varsha H., *Discrete Mathematics* (3/e), Tata McGraw- Hill, 2007.

[2] Rosen, K., *Discrete Mathematics and Its Applications with Combinatorics and Graph Theory* (4/e), McGraw Hill, 2017.

[3] Sarkar, S. K., *Textbook of Discrete Mathematics* (9/e), S Chand & Co Ltd, 2016.

Index