Department of Open and Distance Learning

Punjabi University, Patiala

Class : B.A. 3 (Mathematics) **Semester : 6**
Paper : Opt.III (Discrete Mathematics-II) **Unit : I**
Medium : English

Lesson No.

Department website : www.pbidde.org

Department of Open and Distance Learning

Punjabi University, Patiala

Class : B.A. 3 (Mathematics) **Semester : 6**
Paper : Opt.III (Discrete Mathematics-II) **Unit : I**
Medium : English

Lesson No.

SECTION-A

Department website : www.pbidde.org

B.A. PART-III **MATHEMATICS OPT.-III**
SEMESTER-VI **DISCRETE MATHEMATICS-II**

LESSON NO. 1.1 **Author: Dr. Chanchal**

ANALYSIS OF ALGORITHMS

Structure:

1.1.0 Objectives

The prime goal of this unit is to enlighten the basic concepts of algorithm study, recurrence relations, discrete numeric functions and generating functions. During the study in this particular lesson, our main objective is to discuss problems that can be solved by using step-by-step methods, more formally known as algorithms. Further, we have discussed in detail about the

- Characteristics of algorithms.
- Efficiency of algorithms.
- Growth rates: the O notation.

1.1.1 Introduction to Algorithm

The word algorithm comes from the name of Persian author, Abu Jafar, who wrote a book on mathematics. It has several applications and the work regarding algorithm has gained significant importance. In computer science, the **analysis of algorithms** is the determination of the amount of resources (such as time and storage) necessary to execute them or we can say that algorithms are used to design a method that can be used by the computer to find out the solution of a particular problem. Most algorithms are designed to work with inputs of arbitrary length. Usually, the efficiency or running time of an algorithm is stated as a function relating the input length to the number of steps (time complexity) or storage locations (space complexity).

Algorithm analysis is an important part of a broader computational complexity theory, which provides theoretical estimates for the resources needed by any algorithm which solves a given computational problem. These estimates provide an insight into reasonable directions of search for efficient algorithms. So, an algorithm may be defined as follows :

- An algorithm is a set of rules for carrying out calculation either by hand or on a machine.
- It is a finite step-by-step list of well-defined instructions for solving a particular problem.
- An algorithm is a sequence of computational steps that transform the input into the output.

For example : The algorithm described below is designed to find out the minimum of three numbers a,b and c.

1. min= a
2. If b < min, then min= b .
3. If c < min, then min= c .

1.1.2 Various Characteristics of Algorithms

1. **Input :** The algorithm starts with an input or we can say that the algorithm receives input. The input involves the supply of one or more quantities.
2. **Output :** The algorithm ends with an output or we can say that the algorithm produces output. The result we obtain at the end is called output and at least one quantity is produced.
3. **Precision :** The steps involved in the algorithm are precisely stated. Each instruction mentioned in the algorithm should be clear and unambiguous.
4. **Determinism :** The intermediate results of each step of execution are unique and determined only by the inputs and the results of the preceding steps.
5. **Finiteness :** The number of steps in an algorithm should be finite. It means that if we trace out the instruction of an algorithm, then for all the cases, the algorithm must terminate after a finite number of steps.
6. **Correctness :** The output produced by an algorithm must be correct.
7. **Generality :** The algorithm must apply to a set of inputs.
8. **Effectiveness :** Every instruction stated in an algorithm should be very basic and clear so that it can be carried out very effectively.

1.1.3 Study of Algorithms

The study of algorithm involves several important and active areas of research out of which the most essential are discussed below:

1. **Creating an Algorithm :** The art of creating an algorithm can never be fully automated. By mastering these design strategies, it will become very easy to design new and useful algorithms.
2. **Algorithm Validation :** After the process of design of an algorithm, it is necessary to check that it computes the correct answer for all the possible legal inputs. This process is known as algorithm validation.
3. **Analysis of Algorithm or Performance Analysis :** As an algorithm is executed, it uses the computer's central processing unit (CPU) to perform operations and its memory to hold the program and data. Analysis of algorithms refers to the task of determining the computing time and storage that an algorithm requires and it should be done with great mathematical skills.
4. **Testing a Program :** It consists of two phases: debugging and profiling (or performance measurement). Debugging is the process of executing programs on sample data set to investigate whether faulty errors occur and, if so, correct them. Profiling is the process of executing a correct program on data sets and measuring the time and space it takes to compute the results.

1.1.3.1 Aspects of Algorithm Efficiency

The two important aspects of algorithm efficiency are:

I. The amount of time required to execute an algorithm and

II. The amount of memory space needed to run a program.

A computer requires a certain amount of time to carry out arithmetic operations. Moreover, different algorithms need different amount of space to hold numbers in memory for later use. An analysis of the time required to execute an algorithm of a particular size is referred to as the time complexity of the algorithm while an analysis of the computer memory required involves the space complexity of the algorithm.

Let M be an algorithm and n be the size of the input data. The time and space used by the algorithm are the two main features for the efficiency of M. The time is measured by counting the number of key operations. **For example :** In sorting and searching, one counts the number of comparisons but in arithmetic, one counts multiplications and neglects the additions.

These key operations are so defined that the time for the other operations is more than or at most proportional to the time for the key operations. The space is measured by counting the maximum of memory needed by an algorithm.

1.1.3.2 Some Important Functions

Functions play an important role in the study of algorithms and their analysis. Some of the important mathematical functions which are used very often in algorithms, are discussed below:

1. **Absolute Value Function :** Let x be any real number. Then, the absolute value of x, denoted by $|x|$ may be defined as

$$|x| = \begin{cases} x, x \geq 0 \\ -x, x < 0 \end{cases}$$

For example : $|-2| = 2, |9| = 9.$

2. **Characteristic Function :** Let A be any set and S be any subset of A. Then, characteristic function denoted by $c_S = \begin{cases} 1, x \in S \\ 0, x \notin S \end{cases}$

For example : If $A = \{a, b, c\}$ and $S = \{a, b\}$, then $c_S(a) = 1, c_S(b) = 1, c_s(c) = 0$ because $a, b \in S$ and $c \notin S$. So, we can write

$c_S = \{(a,1), (b,1), (c,0)\}$.

3. **Floor Function :** For any real number x, the floor function of x means the greatest integer which is less than or equal to x. It is denoted by $\lfloor x \rfloor$.

For example : $\lfloor 2.58 \rfloor = 2, \lfloor -4.4 \rfloor = -5, \lfloor 2 \rfloor = 2$.

4. **Ceiling Function :** For any real number x, the ceiling function of x means the least integer which is greater than or equal to x. It is denoted by $\lceil x \rceil$.

For example : $\lceil 2.58 \rceil = 3, \lceil -4.4 \rceil = -4, \lfloor 2 \rfloor = 2$.

5. **Integer Function :** For any real number x, the integer function of x converts x into an integer by deleting the fractional part of x. It is denoted by INT(x).

For example : INT(2.44)=2, INT(-4.44)=-4.

Note : (i) If x is an integer, then $\lfloor x \rfloor = \lceil x \rceil$. Otherwise $\lfloor x \rfloor + 1 = \lceil x \rceil$.

(ii) $\lfloor x \rfloor = n \Rightarrow n \leq x < n+1$ and $\lceil x \rceil = n \Rightarrow n-1 < x \leq n$.

(iii) INT(x)=$\lfloor x \rfloor$ if x is positive and INT(x)=$\lceil x \rceil$ if x is negative.

6. **Remainder Function :** Let M be a positive integer and k be any integer. Then, k (mod M) is called the remainder function and it denotes the integer remainder when k is divided by M. Also, k (mod M) is a unique integer such that $k = Mq + r$ where $0 \leq r < M$.

Note : (i) For positive numbers, we simply divide k by M to obtain remainder r but for negative numbers, we divibe $|k|$ by M to get remainder r' and $k\,(\text{mod } M) = M - r'$ if $r' \neq 0$.

For example : 26(mod4)=2 and -35(mod9)=9-8=1.

7. **Logarithm and Exponent Functions :** Let b be any positive integer. The logarithm of any positive number x to base b is written as $\log_b x$ and it represent exponent to which b must be raised to obtain x. Mathematically, we can write $y = \log_b x$ iff $b^y = x$.

   For example : $\log_3 216 = 6$

   Note : (i) For any base b, $\log_b 1 = 0$ and $\log_b b = 1$ because $b^0 = 1$ and $b^1 = b$.

   (ii) Logarithm of a negative number and logarithm of zero is not defined.

1.1.4 Recursive Algorithm

A recursive algorithm is an algorithm which is used with smaller or simpler input values and which obtains the result for the current input by applying simple operations to the returned value for the smaller or simpler input. In other words, if a problem can be solved utilizing solutions to smaller versions of the same problem, and the smaller versions reduce to easily solvable cases, then one can use a recursive algorithm to solve that problem. For example, the elements of a recursively defined ser or a recursively defined function can be obtained by a recursive algorithm.

If a set or a function is defined recursively, then a recursive algorithm to compute its members or values describes the definition. Initial steps of the recursive algorithm correspond to the basis clause of the recursive definition and they identify the basis elements. It is then followed by the steps corresponding to the inductive clause, which reduce the computation for an element of one generation to that of elements of the immediately preceding generation.

1.1.5 Complexity of Algorithms

For an algorithm M, the complexity may be described by the function $f(n)$ which gives the running tine and/or storage space requirement of the algorithm in terms of the size n of the input data. In most of the cases, the storage space required by an algorithm is simply a multiple of the data size. Accordingly, unless otherwise stated or implied, the term complexity shall refer to the running time of the algorithm. The complexity function $f(n)$, which we assume gives the running time of an algorithm, usually depends not only on the size n of the input data but also on the particular data. In the complexity theory, the following two cases are usually investigated:

1. Worst Case : The maximum value of $f(n)$ for any possible input.
2. Average Case : The expected value of $f(n)$.

The analysis of average case assumes a use of probability distribution for the input data and we assume that the possible permutations of a data set are equally likely. Also, the following result is used for an average case:

Suppose the numbers $n_1, n_2, ..., n_k$ occur with respective probabilities $p_1, p_2, ..., p_k$, then the expectation or average value E is given by

$E = n_1 p_1 + n_2 p_2 + ... + n_k p_k$.

1.1.5.1 Standard Functions Measuring Complexity of Algorithms

Algorithms are generally compared or analysed on the basis of their complexity which is further measured in terms of the size of input data n described by the mathematical function $f(n)$. As n grows, complexity of algorithm M also increases and our interest is to measure this rate of growth. For the purpose, we compare $f(n)$ with some standard functions with different rate growths such that $\log_2 n, n, n\log_2 n, n^2, n^3, 2^n$. Now, complexity of any algorithm is measured in terms of these standard functions and we use a special notation for this, called Big-O notation, as defined below:

Big- O **:** Let $f(x)$ and $g(x)$ are functions defined on the set (or subset) of real numbers. Then, $f(x)$ is called order of $g(x)$ or big- O of $g(x)$, written as $f(x) = \mathrm{O}(g(x))$, if there exist a real number m and a positive constant c such that for all $x \geq m$, we have $|f(x)| \leq c|g(x)|$.

To show that $f(x) = \mathrm{O}(g(x))$ we have to find the value of m and c. Further, big-O gives an upper bound on number of key operations or we can say that big-O gives information about maximum number of key operations. For getting lower bound, we define the function big-omega (Ω).

Big-omega : Let $f(x)$ and $g(x)$ are functions defined on the set (or subset) of real numbers. Then, $f(x) = \Omega(g(x))$ of there exist positive constants c and k such that $|f(x)| \geq c|g(x)|$ for all $x \geq k$. Further, $f(x)$ is called big-omega of $g(x)$.

Big-theta : Let $f(x)$ and $g(x)$ are functions defined on the set (or subset) of real numbers. Then, $f(x) = \Theta(g(x))$ of there exist positive constants c_1, c_2 and k such that $c_1|g(x)| \leq |f(x)| \leq c_2|g(x)|$ for all $x \geq k$. Further, $f(x)$ is called big-theta of $g(x)$ if $f(x)$ is both big-O and big-omega of $g(x)$.

1.1.6 Growth Rate Functions

The time efficiency of almost all the algorithms can be characterized by the following growth rate functions:

1. **O(l)-Constant Time :** This means that the algorithm requires the same fixed number of steps regardless of the size of the task.

   For Example (Assuming a reasonable implementation of the task) :

   i. Push and pop operations for a stack (containing n elements);

   ii. Insert and remove operations for a queue.

2. **O(n)-Linear Time :** This means that the algorithm requires a number of steps proportional to the size of the task.

   For Example (Assuming a reasonable implementation of the task) :

   i. Traversal of a tree with n nodes;

   ii. Calculating n-factorial or n^{th} Fibonacci number by using the method of iteration.

3. **O(n^2)-Quadratic Time :** This means that the algorithm requires a number of steps proportional to the square of size of the task.

   For Example :

   i. Comparing two dimensional array of size n by n;

   ii. Find duplicates in an unsorted list of n elements (implemented with two nested loops).

4. **O($\log n$)-Logarithmic Time :**

   For Example :

   i. Binary search in a sorted list of n elements;

   ii. Insert and find operations for a binary search tree with n nodes.

5. **O($n\log n$)-"$n\log n$" Time :**

   For Example :

   i. More advanced sorting algorithms - quicksort, mergesort.

6. **O(a^n)($a>1$) -Exponential Time :**

   For Example :

   i. Recursive Fibonacci Implementation;

   ii. Generating all permutations of n symbols.

Remarks : (i) The order of asymptotic behavior of the above described functions is

O(l)<O($\log n$)<O(n)<O($n\log n$)<O(n^2)-O(n^3)<O(a^n)

So, the best time is the constant time and the worst time is the exponential time and polynomial growth is considered manageable as compared to exponential growth.

(ii) If a function (which describes the order of growth of an algorithm) is a sum of several terms, its order of growth is determined by the **fastest growing term**. In particular, if we have a polynomial of the form

$p(n) = a_k n^k + a_{k-1}n^{k-1} + \dots\dots\dots\dots\dots\dots + a_1 n + a_0$, then its growth is of the order n^k i.e., $p(n) = \mathrm{O}(n^k)$.

1.1.7 Some Important Examples

Example 1.1 : Find $\lfloor \log_2 100 \rfloor$

Sol. $\because 2^6 = 64$ and $2^7 = 128$.

so $6 < \log_2 100 < 7$

$\Rightarrow \log_2 100 = 6.$

Example 1.2 : Show that $f(x) = x^2 + 2x + 1$ is $\mathrm{O}(x^2)$.

Sol. Let $x \geq 1$

which gives $1 \leq x \leq x^2$ ....(1)

Now, $|f(x)| = |x^2 + 2x + 1| \leq |x^2| + |2x| + |1|$ [since $|x+y| \leq |x| + |y|$]

$\Rightarrow |f(x)| = x^2 + 2x + 1 \leq x^2 + 2x^2 + x^2 = 4x^2$ [using (1)]

$\Rightarrow |f(x)| \leq 4|x^2| \forall x \geq 1$

which gives $f(x) = \mathrm{O}(x^2)$

Example 1.3 : Suppose the polynomial $P(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ is of degree n. Show that $P(x) = \mathrm{O}(x^n)$.

Sol. Let $x \geq 1$

so, $1 \leq x \leq x^2 \leq x^3 \leq .... \leq x^n$ ....(1)

Now, $|P(x)| = |a_0 + a_1 x + a_2 x^2 + ... + a_n x^n|$

$\leq |a_0| + |a_1 x| + |a_2 x^2| + ... + |a_n x^n|$ [since $|x+y| \leq |x| + |y|$]

$= |a_0| + |a_1| x + |a_2| x^2 + ... + |a_n| x^n$

$= |a_0| .1 + |a_1| x + |a_2| x^2 + ... + |a_n| x^n$

$\leq |a_0| x^n + |a_1| x^n + |a_2| x^n + ... + |a_n| x^n$ [using (1)]

$= [|a_0| + |a_1| + |a_2| + ... + |a_n|] x^n = cn^m$

where $c = |a_0| + |a_1| + |a_2| + ... + |a_n|$

so, $|P(x)| \leq c|x^n| \forall x \geq 1$

which gives $P(x) = \mathrm{O}(x^n)$.

Example 1.4 : Find Big-O notation for $\log \angle n$. Further give Big-O estimate for $f(n) = 3n\log\angle n + (n^2+3)\log n$

Sol. Let n be any natural number.

As we know $\angle n = 1.2.3............n$

Now, $1 < 2 < 3 < 4...................... \le n$

so, $|\angle n| = 1.2.3................n \le n.n.n...............n = n^n$

$\Rightarrow |\angle n| \le 1.n^n$ for all $n \ge 1$

so, $\angle n = O(n^n)$ with $c = 1, m = 1$

$\Rightarrow \log\angle n = O(\log n^n) = O(n\log n)$ ...(1)

For the second part, Let $n \ge 1$

so, $1 \le n \le n^2$ ...(2)

so, $|f(n)| = |3n\log\angle n + (n^2+3)\log n|$

$\le |3n\log\angle n| + |(n^2+3)\log n|$ [since $|x+y| \le |x| + |y|$]

$\le 3n.n\log n + (n^2 + 3.n^2)\log n$ [using (1) and (2)]

$= 3n^2\log n + 4n^2\log n$

$\Rightarrow |f(n)| \le 7.|n^2\log n|$ for all $n \ge 1$

so, f(n) is $O(n^2\log n)$ with $c = 7, m = 1$.

Example 1.5 : Prove that $f(x) = 8x^3 + 5x^2 + 7$ is $\Omega(g(x))$ where $g(x) = x^3$.

Sol. Let $x \ge 0$

then, $x^2 \ge 0$

Now, $|f(x)| = |8x^3 + 5x^2 + 7| \ge 8x^3$ $[\because 5x^2 + 7 \ge 0]$

$\Rightarrow |f(x)| \ge 8.|x^3|$ $\forall x \ge 0$

$\Rightarrow |f(x)| \ge 8.|g(x)|$ $\forall x \ge 0$

Hence $f(x)$ is $\Omega(g(x))$ where $c = 8, k = 0$.

1.1.8 Summary

In this lesson, we have studied about the algorithms. From our study, we can say that an algorithm is a sequence of instructions. Each individual instruction must be carried out, in its proper place, by the person or machine for whom the algorithm is intended. Consequently, an algorithm should always be considered in the context of certain assumptions. In more detail, we have discussed about the efficiency and complexity of algorithms, on the basis of which, we have learnt the procedure to compare the algorithms. Further, we have also given an idea of recursive algorithms that may be useful for understanding the recurrence relations which will be discussed in the next part of this unit.

1.1.9 Self Check Exercise

1) Show that $7x^2 - 9x + 4 = O(x^2)$.
2) Let $U = \{a, b, c, ..., x, y, z\}$ and $A = \{a, e, i, o, u\}$. Find the characteristic function of A.
3) Show that $g(n) = n^2(7n - 2)$ is $O(n^3)$.
4) Show that $x^4 + 9x^3 + 4x + 7$ is $O(x^4)$.
5) Find Big-O notation for $\angle n$.

1.1.10 Suggested Readings

1. Norman L. Biggs, *Discrete Mathematics*, Oxford University Press.
2. Harmohan Sharma, Ganesh Kumar Sethi, *Discrete Mathematics,* Sharma Publications, Jalandhar.
3. C.L. Liu, Elements of Discrete Mathematics (Second Edition), McGraw Hill, International Edition, Computer Science Series, 1986.

LESSON NO. 1.2 **Author: Dr. Chanchal**

DISCRETE NUMERIC FUNCTIONS AND GENERATING FUNCTIONS

Structure:

1.2.0 Objectives

The prime goal of this lesson is to enlighten the basic concepts of discrete numeric functions along with the detail elaboration of operations on numeric functions. Further, the knowledge about generating functions and several important results concerning them is also provided under this lesson.

1.2.1 Introduction

From our previous study, we are already familiar with the concept of function or mapping which may be defined as a rule $f: X \rightarrow Y$ that associates each element of X with a unique element of Y. Further, we recall the definition of sequence:

Def : Sequence

Let $\mathrm{N} = \{1,2,3,.....\}$ is the set of natural numbers and

$\mathrm{Z} = \{..........,-3,-2,-1,0,1,2,3,..........\}$ is the set of integers. A mapping $S: \mathrm{N} \rightarrow \mathrm{Z}$ is called the sequence of integers. The image of any natural number n is called the n^{th} term of S and denoted by $S(n)$ or S_n. Further, n is also called the index or argument.

So, we can write $S = \{a_1, a_2, a_3, ..., a_n, ...\}$.

Note: (i) Numeric functions, discrete functions etc. are also used for sequence.

(ii) The sequences can also be expressed in a compact form known as the **closed form expression**. For example, the closed form expression of $\sum_{i=1}^{n} i = 1+2+....+n$ is $\frac{n(n+1)}{2}$.

1.2.2 Discrete Numeric Function

A function whose domain is the set of natural numbers and range is the set of real numbers is known as discrete numeric function or simply numeric function. If $a : \mathrm{N} \to \Re$ is a discrete numeric function, then $a(0)$=value of a at 0 is denoted by a_0. Similarly, $a(1) = a_1$, $a(2) = a_2$,............., $a(r) = a_r$,.........so on. Here, a_r represents the general form of numeric function $a = \{a_0, a_1, a_2, ...a_r, ...\}$.

1.2.3 Operations on Numeric Functions

Let a and b be two numeric functions and α be any real number. Then, we may define the following operations on numeric functions:

I. **Sum:** The sum $a+b$ is a numeric function such that the value of $a+b$ at r is equal to the sum of the values of a and b at r.

II. **Product:** The product $a.b$ is a numeric function such that the value of $a.b$ at r is equal to the product of the values of a and b at r.

III. **Convolution:** The convolution of a and b denoted by $a * b$ is a numeric function c such that

$$c_r = a_o b_r + a_1 b_{r-1} + ... + a_r b_o = \sum_{i=0}^{r} a_i b_{r-i}$$

IV. **Modulus of Numeric Function:** The modulus of a numeric function a may be defined as : $|a| = a_r$ if a_r is non-negative and $|a| = -a_r$ if a_r is negative.

V. **Multiplication of Numeric Function by a Real Number:** The multiplication a numeric function a with real number α denoted by αa is also a numeric function whose value at r is equal to α times a_r.

VI. **Forward Difference of a Numeric Function:** The forward difference of a numeric function a is also a numeric function whose value at r is equal to $a_{r+1} - a_r$. It is denoted by Δa.

VII. **Backward Difference of a Numeric Function:** The forward difference of numeric function a is also a numeric function, denoted by ∇a, such that $\nabla a_r = a_r - a_{r-1}$ for $r \geq 1$ and $\nabla a_0 = 0$.

VIII. $S^i a$ **and** $S^{-i} a$ **Numeric Functions:** If we denote the numeric functions $S^i a$ and $S^{-i} a$ by b and c respectively, then these may be defined as follows:

$$b_r = \begin{cases} 0, 0 \le r \le i-1 \\ a_{r-i}, r \ge i \end{cases}$$

and $c_r = a_{r+i}$ for $r \ge 0$. Here, i is some positive integer.

1.2.4 Some Important Examples

Example 1: If $a_r = \begin{cases} 0, 0 \le r \le 2 \\ 2^{-r} + 5, r \ge 3 \end{cases}$ and $b_r = \begin{cases} 3 - 2^r, 0 \le r \le 1 \\ r + 2, r \ge 2 \end{cases}$

(i) Find c_r if $c_r = a_r + b_r$. (ii) Find d_r if $d_r = a_r b_r$.

Sol. By the definition of sum and product of two given numeric functions, we may express c_r and d_r as follows:

(i) $c_r = a_r + b_r = \begin{cases} 3 - 2^r, 0 \le r \le 1 \\ 4, r = 2 \\ 2^{-r} + r + 7, r \ge 3 \end{cases}$ and (ii) $d_r = a_r b_r = \begin{cases} 0, 0 \le r \le 2 \\ r.2^{-r} + 2^{-r+1} + 5r + 10, r \ge 3 \end{cases}$

Example 2: Evaluate $a * b$ for the following numeric functions:

$a_r = \begin{cases} 1, 0 \le r \le 2 \\ 0, r \ge 3 \end{cases}$ and $b_r = \begin{cases} r + 1, 0 \le r \le 2 \\ 0, r \ge 3 \end{cases}$

Sol. For the given a_r and b_r, the numeric functions a and b are given by

$a = \{1,1,1,0,0,0,......\}$ and $b = \{1,2,3,0,0,0,.......\}$.

The convolution of a and b is a numeric function $c = a * b$ such that

$$c_r = a_o b_r + a_1 b_{r-1} + ... + a_r b_o = \sum_{i=0}^{r} a_i b_{r-i}$$

So, we have

$$c_0 = a_0 b_0 = (1)(1) = 1$$
$$c_1 = a_0 b_1 + a_1 b_0 = (1)(2) + (1)(1) = 3$$
$$c_3 = a_0 b_2 + a_1 b_1 + a_2 b_0 = (1)(3) + (1)(2) + (1)(1) = 6$$

Similarly, $c_3 = 5, c_4 = 3$ and $c_r = 0$ for $r \ge 5$.

$\therefore$ Numeric function c is given by $c = \{1,3,6,5,3,0,0,0,..........\}$,

where $c_r = \begin{cases} 1, r = 0 \\ 3, r = 1 \\ 6, r = 2 \\ 5, r = 3 \\ 3, r = 4 \\ 0, r \ge 5 \end{cases}$

Example 3: If the numeric function a is defined as $a_r = \begin{cases} 2, 0 \le r \le 3 \\ 2^{-r} + 5, r \ge 4 \end{cases}$. Then, evaluate

(i) $S^2 a$ (ii) $S^{-2} a$ (iii) Δa (iv) ∇a.

Sol. (i) For the numeric function a, the numeric functions $S^i a$ is given by

$$S^i a_r = \begin{cases} 0, 0 \le r \le i-1 \\ a_{r-i}, r \ge i \end{cases}$$

For $i = 2$, $S^2 a_r = \begin{cases} 0, 0 \le r \le 1 \\ a_{r-2}, r \ge 2 \end{cases}$

For given a_r, we have $S^2 a_r = \begin{cases} 0, 0 \le r \le 1 \\ 2, 2 \le r \le 5 \\ 2^{-(r-2)} + 5, r \ge 6 \end{cases}$

(ii) The numeric functions $S^{-i} a$ is defined as $S^{-i} a_r = a_{r+i}$ for $r \ge 0$.

$\therefore$ $S^{-2} a_r = a_{r+2}$ for $r \ge 0$.

For given a_r, we have $S^{-2} a_r = \begin{cases} 2, 0 \le r \le 1 \\ 2^{-(r+2)} + 5, r \ge 2 \end{cases}$

(iii) The numeric function Δa is defined as

$\Delta a_r = a_{r+1} - a_r$ for $r \ge 0$.

For given a_r, we have $\Delta a_r = \begin{cases} 0, 0 \le r \le 2 \\ 2^{-4} + 3, r = 3 \\ 2^{-(r+1)} - 2^{-r}, r \ge 4 \end{cases}$

(iii) The numeric function ∇a is defined as

$\nabla a_r = a_r - a_{r-1}$ for $r \ge 1$ and $\nabla a_0 = 0$.

For given a_r, we have $\nabla a_r = \begin{cases} 2, r = 0 \\ 0, 1 \le r \le 3 \\ 2^{-4} + 5, r = 4 \\ 2^{-r} - 2^{-(r-1)}, r \ge 5 \end{cases}$

1.2.5 Generating Function

Let S be a sequence with terms $S_0, S_1, S_2, \ldots\ldots\ldots$ .so on. Then, we may define the generating function $G(S, z)$ of the sequence S by the following infinite series:

$$G(S,z) = \sum_{n=0}^{\infty} S_n z^n = S_0 + S_1 z + S_2 z^2 + S_3 z^3 + \ldots\ldots\ldots\ldots\ldots\infty.$$

For example : Let the sequence S is $1^2, 2^2, 3^2, \ldots\ldots\ldots\ldots\ldots\ldots$ so on.

Then, $G(S,z) = 1^2.z^0 + 2^2.z^1 + 3^2.z^2 + \ldots\ldots\ldots\ldots\ldots\infty = \sum_{n=0}^{\infty} (n+1)^2 z^n$

1.2.6 Generating Functions of Some Standard Sequences

I. $S_n = a\,,\ n \geq 0$

$$G(S,z) = \sum_{n=0}^{\infty} S_n z^n = \sum_{n=0}^{\infty} a z^n = a \sum_{n=0}^{\infty} z^n$$

$$\Rightarrow\ G(S,z) = a(1 + z + z^2 + z^3 + \ldots\ldots\ldots\ldots\infty)$$

$$\Rightarrow\ G(S,z) = \frac{a}{1-z} \qquad [\because S_\infty = \frac{a}{1-r}]$$

II. $S_n = b^n\,,\ n \geq 0$

$$G(S,z) = \sum_{n=0}^{\infty} S_n z^n = \sum_{n=0}^{\infty} b^n z^n = \sum_{n=0}^{\infty} (bz)^n$$

$$\Rightarrow\ G(S,z) = 1 + bz + (bz)^2 + (bz)^3 + \ldots\ldots\ldots\ldots\infty)$$

$$\Rightarrow\ G(S,z) = \frac{1}{1-bz}$$

III. $S_n = cb^n\,,\ n \geq 0$

On the similar lines as above, it can be proved that

$$G(S,z) = \frac{c}{1-bz}$$

IV. $S_n = n$

$$G(S,z) = \sum_{n=0}^{\infty} S_n z^n = \sum_{n=0}^{\infty} n z^n = 0 + z + 2z^2 + 3z^3 + \ldots\ldots\ldots\ldots\ldots\infty$$

$$\Rightarrow\ G(S,z) = z(1 + 2z + 3z^2 + \ldots\ldots\ldots\ldots\infty)$$

$$\Rightarrow\ G(S,z) = \frac{z}{(1-z)^2}$$

Result: Generating function of sum of two sequences is equal to the sum of their generating functions. or

If $S_n = a_n + b_n$, then $G(S,z) = G(a,z) + G(b,z)$.

Proof: We can prove this result very easily.

As we know that $G(S,z) = \sum_{n=0}^{\infty} S_n z^n$

which gives $G(S,z) = \sum_{n=0}^{\infty} (a_n + b_n) z^n = \sum_{n=0}^{\infty} a_n z^n + \sum_{n=0}^{\infty} b_n z^n$

Therefore, $G(S,z) = G(a,z) + G(b,z)$

1.2.7 Operations on Sequences

If s, t are two sequences of natural number n, then we may define the following operations:

1. $(s+t)(n) = s(n) + t(n)$

   $cs(n) = c(s(n))$, where c is constant.

   $st(n) = s(n)t(n)$

2. **Convolution Operation:**

   $$(s*t)(n) = \sum_{r=0}^{n} s(r)t(n-r)$$

3. **Pop Operation** $s\uparrow$ (read as s pop):

   $(s\uparrow)n = s(n+1)$

4. **Push Operation** $s\downarrow$ (read as s push):

   $$(s\downarrow)n = \begin{cases} s(n-1), n > 0 \\ 0, n = 0 \end{cases}$$

Def : If s is a sequence of numbers, we define

$s\uparrow n = (s\uparrow(n-1))\uparrow$ if $n > 1$ and $s\uparrow 1 = s\uparrow$

Also, $s\downarrow n = (s\downarrow(n-1))\downarrow$ and $s\downarrow 1 = s\downarrow$.

In general, $(s\uparrow n)m = s(n+m)$

and $(s\downarrow n)m = \begin{cases} 0, m < n \\ s(m-n), m \geq n \end{cases}$

On the basis of above operations on sequences, we may state the following **Important results**:

1. $G(s+t,z) = G(s,z) + G(t,z)$
2. $G(cs,z) = cG(s,z)$, where c is constant.
3. $G(s*t,z) = G(s,z)G(t,z)$
4. $G(s\uparrow,z) = \dfrac{G(s,z) - s(0)}{z}$
5. $G(s\downarrow,z) = zG(s,z)$
6. $G(s\uparrow n,z) = \dfrac{G(s,z) - \sum_{r=0}^{n-1} s(r)z^r}{z^n}$
7. $G(s\downarrow n,z) = z^n G(s,z)$

1.2.8 Some Important Examples

Example 11.4: Write the generating function of the sequence $s_n = 3.4^n + 2.(-1)^n + 7$.

Sol. For the given sequence s_n ,

$$G(s,z) = 3\left(\frac{1}{1-4z}\right) + 2\left(\frac{1}{1-(-1)z}\right) + 7.\frac{1}{1-z} = \frac{3}{1-4z} + \frac{2}{1+z} + \frac{7}{1-z}.$$

Example 2.5: Find the sequence whose generating function is $\dfrac{1}{1-z-z^2}$.

Sol. Here, $G(s,z) = \dfrac{1}{1-z-z^2}$ (1)

The roots of the equation $1-z-z^2 = 0$ are given by

$1-z-z^2 = 0 \Rightarrow z^2 + z - 1 = 0$

which gives $z = \dfrac{\sqrt{5}-1}{2}, \dfrac{-(\sqrt{5}+1)}{2}$

Let $\alpha = \dfrac{\sqrt{5}-1}{2}, \beta = \dfrac{-\left(\sqrt{5}+1\right)}{2}$ (2)

$\therefore z^2 + z - 1 = (z-\alpha)(z-\beta)$ or $1-z-z^2 = -(z-\alpha)(z-\beta)$

$$\Rightarrow \frac{1}{1-z-z^2} = \frac{-1}{(z-\alpha)(z-\beta)} = \frac{-1}{(z-\alpha)(\alpha-\beta)} + \frac{-1}{(\beta-\alpha)(z-\beta)}$$

$$\Rightarrow \frac{1}{1-z-z^2} = \frac{1}{\alpha-\beta}\left[\frac{1}{z-\beta} - \frac{1}{z-\alpha}\right] = \frac{1}{\alpha-\beta}\left[\frac{1}{\alpha-z} - \frac{1}{\beta-z}\right]$$

$$\therefore G(s,z) = \frac{1}{\alpha-\beta}\left[\frac{1}{\alpha\left(1-\frac{z}{\alpha}\right)} - \frac{1}{\beta\left(1-\frac{z}{\beta}\right)}\right]$$

which gives $s_n = \dfrac{1}{\alpha-\beta}\left[\dfrac{1}{\alpha}\left(\dfrac{1}{\alpha}\right)^n - \dfrac{1}{\beta}\left(\dfrac{1}{\beta}\right)^n\right] = \dfrac{1}{\alpha-\beta}\left[\left(\dfrac{1}{\alpha}\right)^{n+1} - \left(\dfrac{1}{\beta}\right)^{n+1}\right]$

Using the values of α and β , from (2), we get the required solution as

$$s_n = \frac{1}{\sqrt{5}}\left[\left(\frac{2}{\sqrt{5}-1}\right)^{n+1} - \left(\frac{-2}{\sqrt{5}+1}\right)^{n+1}\right]$$

Example 6: If $s_n = n^2 + 1$ and $t_n = n + 4$. Find $(s * t)(n), (s \uparrow 3)(n)$ and $(t \downarrow 2)(n)$.

Sol. $(s*t)(n)=\sum_{r=0}^{n}s(r)t(n-r)$

which gives $(s*t)(n)=\sum_{r=0}^{n}(r^2+1)(n-r+4)=\sum_{r=0}^{n}(n+4)r^2-r^3-r+n+4$

or $(s*t)(n)=(n+4)\sum_{r=0}^{n}r^2-\sum_{r=0}^{n}r^3-\sum_{r=0}^{n}r+(n+4)\sum_{r=0}^{n}1$

or $(s*t)(n)=(n+4)\dfrac{n(n+1)(2n+1)}{6}-\dfrac{n^2(n+1)^2}{4}-\dfrac{n(n+1)}{2}+n(n+4)$

or $(s*t)(n)=\dfrac{1}{6}n(n+1)(n+4)(2n+1)-\dfrac{1}{4}n^2(n+1)^2-\dfrac{1}{2}n(n+1)+n(n+4)$

Now, $(s\uparrow 3)(n)=s(n+3)=(n+3)^2+1=n^2+6n+10$

and $(t\downarrow 2)(n)=t(n-2)=n-2+4=n+2$ for $n\geq 4$.

Example 7: If $a(n)=n, b(n)=n/2, c(n)=2^n$. Find $G(a\uparrow 2,z)$, $G(b*b,z)$ and $G(2c,z)$.

Sol. For $a(n)=n$, $(a\uparrow 2)(n)=n+2=s_1+s_2$ where $s_1=n, s_2=2$

$\therefore G(a\uparrow 2,z)=G(s_1,z)+G(s_2,z)=\dfrac{z}{(1-z)^2}+\dfrac{2}{1-z}$

Further, $b(n)=\dfrac{n}{2}\Rightarrow G(b,z)=\dfrac{1}{2}\dfrac{z}{(1-z)^2}$

$\therefore G(b*b,z)=G(b,z)G(b,z)=\dfrac{1}{4}\dfrac{z^2}{(1-z)^4}$

Now, $c(n)=2^n\Rightarrow G(2c,z)=2G(c,z)=\dfrac{2}{1-2z}$

1.2.9 Summary

In this lesson, we have studied in detail about the discrete numeric functions and learnt the various operations on these functions. These numeric functions will help us to understand the concept of recurrence relations which will be discussed in the next lesson. Further, we have also gained the knowledge about the generating functions of some standard sequences and their various operations. The concept is made more clear with the help of suitable examples.

1.2.10 Self Check Exercise

1. Determine $a*b$ for the following numeric functions:

   $a_r=\begin{cases}1, 0\leq r\leq 2\\ 0, r\geq 3\end{cases}$ and $b_r=\begin{cases}r+1, 0\leq r\leq 2\\ 0, r\geq 3\end{cases}$

2. Write the sequence whose generating function is

(i) $\dfrac{3-5z}{1-2z-3z^2}$ (ii) $\dfrac{2}{1+z}+\dfrac{z}{(1-z)^2}$

3. If $S_n = 2^n, T_n = 3^n$. Then, find the convolution $S*T$ and verify that $G(S*T,z) = G(S,z)G(T,z)$

1.2.11 Suggested Readings

1. Norman L. Biggs, *Discrete Mathematics*, Oxford University Press.
2. Harmohan Sharma, Ganesh Kumar Sethi, *Discrete Mathematics,* Sharma Publications, Jalandhar.
3. C.L. Liu, Elements of Discrete Mathematics (Second Edition), McGraw Hill, International Edition, Computer Science Series, 1986.

B.A. PART-III **OPT.-III**

SEMESTER-VI **DISCRETE MATHEMATICS-II**

LESSON NO. 1.3 **Author: Dr. Chanchal**

RECURRENCE RELATIONS

Structure:

3.0 Objectives

The prime goal of this lesson is to enlighten the basic concepts of recurrence relations and their solutions. During the study in this lesson, our main objectives are

- To study the basic concept of recursion.
- To understand the procedure of solving homogeneous and non-homogeneous recurrence relations.
- To understand the procedure of finding the generating function and sequence of a recurrence relation.

3.1 Introduction

The technique of defining a function, a set or an algorithm in terms of itself is known as **recursion**. An example is presented recursively, if every object is described in terms of two forms out of which one form is the **basis** for recursion which is written by a simple definition. The second form is written by a recursive description in which objects are described in terms of themselves i.e. the objects should be described in terms of simpler objects, where simpler means closer to the basis of recursion.

3.2 Some Recursive Definitions

I. The recursive definition of $\angle n$ is given by
$\angle 0 = 1$ and $\angle n = n(n-1)$.

Here n^{th} term is expressed as a function of previous term and $\angle 0 = 1$ is called basis.

II. The recursive definition of binomial coefficient $C(n,k)$ for $n \geq 0, k \geq 0, n \geq k$, is given by
$C(n,n) = 1, C(n,0) = 1$ and $C(n,k) = C(n-1,k) + C(n-1,k-1)$ if $n > k > 0$.

Here n^{th} term is expressed as a function of previous terms and $C(n,n) = 1, C(n,0) = 1$ are basis.

III. The recursive definition of a polynomial expression may be elaborated as:
Let S be the set of coefficients, then

(i) A zeroth degree polynomial is an element of S.

(ii) For $n \geq 1$, n^{th} degree polynomial expression is of the form $p(x)x + a$, where $p(x)$ is $(n-1)^{th}$ degree polynomial expression and $a \in S$.

IV. The recursive definition of **Fibonacci Sequence**, F is given by $F_0 = 1, F_1 = 1$ and $F_k = F_{k-2} + F_{k-1}$ for $k \geq 2$. Here, basis is the specification of first two numbers F_0 and F_1.

V. The recursive definition of positive integers can be given by the **Peano's Axioms**, as explained below:

Axiom 1: $1 \in \mathrm{N}$ i.e. 1 is a natural number.

Axiom 2: For each $n \in \mathrm{N}$, there exists a unique natural number n^*, called the successor of n given by $n^* = n + 1$.

Axiom 3: 1 is not the successor of any natural number.

Axiom 4: If $m, n \in \mathrm{N}$ and $m^* = n^*$, then $m = n$.

Axiom 5: If $A \subset \mathrm{N}$, such that (i) $1 \in A$ and (ii) $n \in A \Rightarrow n^* \in A$, then $A = \mathrm{N}$. This axiom is also called the **Principle of Mathematical Induction**.

In the above definition, number 1 is the basis element and recursion is that if n is a positive integer, then its successor is also a positive integer.

3.3 Some Important Examples

Example 3.1: Determine $C(3,2)$ by the recursive definition of binomial coefficient.

Sol. By recursive definition: $C(n,n) = 1, C(n,0) = 1$ and

$$C(n,k) = C(n-1,k) + C(n-1,k-1) \text{ if } n > k > 0. \quad (1)$$

Put $n=3, k=2$ in (1) and we get

$$C(3,2)=C(2,2)+C(2,1) \tag{2}$$

Now put $n=2, k=1$ in (1) and we get

$$C(2,1)=C(1,1)+C(1,0)=1+1=2$$

So, from (2), $C(3,2)=1+2=3$.

Example 3.2: Write $p(x)=4n^3+2n^2-8n+9$ in telescoping form.

Sol. Here, $p(x)=4n^3+2n^2-8n+9=(4n^2+2n-8)n+9=((4n+2)n-8)n+9$

$\Rightarrow p(x)=((((4)n)+2)n-8)n+9$ is the required telescoping form.

Example 3.3: If $B(0)=2$ and $B(k)=B(k-1)+3$ for $k\geq 1$. Evaluate $B(2)$ by the recursion formula and by the method of iteration.

Sol. By recursion formula:

$$B(2)=B(1)+3=(B(0)+3)+3=(2+3)+3=5+3=8$$

By iteration method:

$$B(1)=B(0)+3=2+3=5$$

$$B(2)=B(1)+3=5+3=8.$$

3.4 Recurrence Relation

For a numeric function $(a_0, a_1, a_2, ..., a_r, ...)$, an equation relating a_r, for any r, to one or more of the a_i's, $i<r$, is called a recurrence relation. It is also known as a **difference equation**. It is clear from the above definition that a step-by-step computation can be carried out to determine a_r from $a_{r-1}, a_{r-2}, ...$, and a_{r+1} from a_r, $a_{r-1}, ...$, and so on. It must be clear that the value of function at one or more points, known as the **boundary conditions**, must be given so that the computation procedure can be initiated. So, we may state here that the numeric function is also known as the solution of recurrence relation as it can be described by a recurrence relation together with an appropriate set of boundary conditions.

3.5 Linear Recurrence Relation with Constant Coefficients

A recurrence relation of the form

$$c_0 a_r + c_1 a_{r-1} + c_2 a_{r-2} + ... + c_k a_{r-k} = f(r) \tag{1}$$

is known as a linear recurrence relation with constant coefficients. Here, c_i's are constants and the above recurrence relation is of k^{th} order provided that the coefficients c_0 and c_k are non-zero.

Note: (i) Order of a recurrence relation is the difference between highest and lowest subscript. For example, $a_r + 8a_{r-2} = r^2 + 4$ is second order linear recurrence relation with constant coefficients.

(ii) The recurrence relation can also be determined from solution. For example, consider the closed form expression $S(k) = 9.2^k, k \geq 0.$

For $k \geq 1$, $S(k) = 9.(2.2^{k-1}) = 2.(9.2^{k-1}) = 2S(k-1)$

$\therefore S(k) - 2S(k-1) = 0$ and $S(0) = 9$ defines linear recurrence relation.

3.5.1 Homogeneous and Non-Homogeneous Recurrence Relation

A recurrence relation of the form

$$S(k) + C_1S(k-1) + C_2S(k-2) + \ldots\ldots\ldots\ldots\ldots\ldots + C_nS(k-n) = f(k)$$

is known as a (i) linear non-homogeneous relation if $f(k)$ is a function of k or a constant, (ii) homogeneous relation if $f(k) = 0$. Here $C_1, C_2, \ldots\ldots\ldots C_n$ are constants.

3.5.2 Characteristic Equation and Characteristic Roots

For n^{th} order linear recurrence relation of the form

$$S(k) + C_1S(k-1) + C_2S(k-2) + \ldots\ldots\ldots\ldots\ldots\ldots + C_nS(k-n) = f(k),$$

the characteristic equation is given by

$$a^n + C_1a^{n-1} + C_2a^{n-2} + \ldots\ldots\ldots\ldots\ldots + C_{n-1}a + C_n = 0.$$

Further, roots of the above characteristic equation are known as the characteristic roots and these roots may be real or imaginary.

3.6 How to Find Solutions of Recurrence Relation

Let the recurrence relation is of the form

$$S(k) + C_1S(k-1) + C_2S(k-2) + \ldots\ldots\ldots\ldots\ldots\ldots + C_nS(k-n) = f(k) \qquad (1)$$

Case I : For $f(k) = 0$, the above relation (1) is homogeneous relation for which the solution can be obtained as

Step I. Write down the characteristic equation given by

$$a^n + C_1a^{n-1} + C_2a^{n-2} + \ldots\ldots\ldots\ldots\ldots + C_{n-1}a + C_n = 0 \qquad (2)$$

Step II. Solve (2) and let the roots be $a_1, a_2, \ldots\ldots\ldots\ldots, a_n$.

Step III. If all the roots are different, then the general solution is given by

$$S(k) = b_1a_1^k + b_2a_2^k + \ldots\ldots\ldots\ldots\ldots b_na_n^k.$$

If two real roots a_1, a_2 are such that $a_1 = a_2$, then solution is given by

$S(k) = (b_1 + b_2k)a_1^k + b_3a_3^k + \ldots\ldots\ldots\ldots\ldots b_na_n^k$ and so on.

Case II : If $f(k)$ is a function of k , the above relation (1) is non-homogeneous relation whose solution consists of two parts out of which one is homogeneous solution and the other is particular solution and the general solution is given by $S(k)=S^{(h)}(k)+S^{(p)}(k)$. For the homogeneous solution $S^{(h)}(k)$, we put $f(k)=0$ and the solution is obtained as described under case I. The method for finding the particular solution $S^{(p)}(k)$ is explained below:

3.6.1 How to Find Particular Solution

Case I. When $f(k)$ is a constant

Let the particular solution is given by $S(k)=d$, then (1) becomes

$d+C_1d+C_2d+.....+C_nd=f(k)$ which gives $d=\dfrac{f(k)}{1+C_1+C_2+.......+C_n}$.

If $1+C_1+C_2+.....+C_n=0$, then it is a case of failure and we try for particular solution $S(k)=kd$. If for this too, the case fails, then the particular solution is taken as $S(k)=k^2d$ and so on.

Case II. When $f(k)$ is a linear function i.e., $f(k)=p_0+p_1k$

Let the particular solution is given by $S(k)=d_0+d_1k$, then (1) becomes

$$(d_0+d_1k)+C_1[d_0+d_1(k-1)]+C_2[d_0+d_1(k-2)]+.....+C_n[d_0+d_1(k-n)]=p_0+p_1k$$

On equating the coefficients of terms containing k and that of constant terms in the above expression, the values of d_0 and d_1 may be evaluated and then the particular solution $S(k)=d_0+d_1k$ is known.

Note: If $f(k)$ is an m^{th} degree polynomial of the form $f(k)=p_0+p_1k+p_2k^2+.....+p_mk^m$,

then the particular solution is given by $S(k)=d_0+d_1k+d_2k^2+.........+d_mk^m$.

It must be noted that if the particular solution contains any term similar to that of homogeneous solution, then the particular solution is multiplied by k.

Case III. When $f(k)$ is an exponential function i.e., $f(k)=pa^k$

Let the particular solution is given by $S(k)=da^k$, then (1) becomes

$da^k+C_1da^{k-1}+C_2da^{k-2}+.....+C_nda^{k-n}=pa^k$.

From the above equation, the value of d can be determined and then the particular solution is known. It must be noted that if the homogeneous solution contains a term containing a^k, then the particular solution is multiplied by k and given by $S(k)=dka^k$. Further, if the homogeneous solution contains a term containing ka^k, then the particular solution is given by $S(k)=dk^2a^k$ and so on.

3.7 How to Find Generating Function and Sequence of a Recurrence Relation

Let the recurrence relation is of the form

$S(n)+C_1S(n-1)+C_2S(n-2)+..................+C_rS(n-r)=0$ for $n \geq r.$

Step I. Multiply both sides by z^n and sum up terms from $n=r$ to ∞, we get

$$\sum_{n=r}^{\infty}S(n)z^n+C_1\sum_{n=r}^{\infty}S(n-1)z^n+C_2\sum_{n=r}^{\infty}S(n-2)z^n+.........+C_r\sum_{n=r}^{\infty}S(n-r)z^n=0.$$

Step II. If $G(S,z)=\sum_{n=0}^{\infty}S(n)z^n$ be the generating function, then write each term in terms of $G(S,z)$.

Step III. Solve the equation for $G(S,z)$ and then with the help of standard generating functions (as discussed in the previous lesson 11), the sequence $S(n)$ can be obtained.

3.8 Some Important Examples

Example 9.4: Solve $S(k)-10S(k-1)+9S(k-2)=0, S(0)=3, S(1)=11.$

Sol. Put $S(k)=a^k$ in $S(k)-10S(k-1)+9S(k-2)=0$ and we obtain

$a^k-10a^{k-1}+9a^{k-2}=0 \Rightarrow a^{k-2}\left(a^2-10a+9\right)=0$

$\Rightarrow a^2-10a+9=0 \Rightarrow (a-1)(a-9)=0$

which gives $a=1, a=9$

$\therefore S(k)=C_1.1^k+C_2.9^k=C_1+C_2.9^k$ ...(1)

Put $k=0$ and $k=1$ in (1), we get

$S(0)=C_1+C_2.9^0 \Rightarrow 3=C_1+C_2$ ...(2)

and $S(1)=C_1+C_2.9^1 \Rightarrow 11=C_1+9C_2$ ...(3)

Now, subtracting (2) from (3), we have $8=8C_2 \Rightarrow C_2=1$

Put $C_2=1$ in (2), we obtain $C_1=2$.

So, $S(k)=2+9^k$ is the required solution.

Example 3.5: Solve the recurrence relation: $\sqrt{a_n}=\sqrt{a_{n-1}}+\sqrt{a_{n-2}}$

Sol. Let $\sqrt{a_n}=b_n \Rightarrow a_n={b_n}^2$

$\therefore$ the given equation becomes: $b_n=b_{n-1}+b_{n-2}$

Let $b_n=m^n$

$\therefore m^n=m^{n-1}+m^{n-2} \Rightarrow m^n-m^{n-1}-m^{n-2}=0 \Rightarrow m^{n-2}\left(m^2-m-1\right)=0$

$$\Rightarrow m^2 - m - 1 = 0 \Rightarrow m = \frac{-(-1) \pm \sqrt{(-1)^2 - 4.1.(-1)}}{2.1} = \frac{1 \pm \sqrt{5}}{2}$$

$$\Rightarrow m = \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}$$

which gives $b_n = C_1\left(\frac{1+\sqrt{5}}{2}\right)^n + C_2\left(\frac{1-\sqrt{5}}{2}\right)^n$ and the required solution is given by

$$a_n = b_n^{\ 2} = \left[C_1\left(\frac{1+\sqrt{5}}{2}\right)^n + C_2\left(\frac{1-\sqrt{5}}{2}\right)^n\right]^2$$

Example 3.6: Solve the recurrence relation: $s_n - 4s_{n-1} + 4s_{n-2} = 3n + 2^n$ with $s_0 = s_1 = 1$.

Sol. The solution of given non-homogeneous recurrence relation will consist of two parts i.e., homogeneous solution and particular solution.

Homogeneous Solution: The associated homogeneous relation is

$$s_n - 4s_{n-1} + 4s_{n-2} = 0$$

Its characteristic equation is $a^n - 4a^{n-1} + 4a^{n-2} = 0 \Rightarrow a^{n-2}\left(a^2 - 4a + 4\right) = 0$

$$\Rightarrow a^2 - 4a + 4 = 0 \Rightarrow (a-2)^2 = 0 \Rightarrow a = 2,2$$

$\therefore$ the homogeneous solution is $s_n^{(h)} = \left(c_1 + nc_2\right)2^n$

Particular Solution: Here $f(n) = 3n + 2^n$

Since base 2 in 2^n is a characteristic root repeated twice, therefore the particular solution is given by $s_n = cn + d + qn^2 2^n$

Using this value of s_n in the given equation, we obtain

$$cn + d + qn^2 2^n - 4\left(c(n-1) + d + q(n-1)^2 2^{n-1}\right) + 4\left(c(n-2) + d + q(n-2)^2 2^{n-2}\right) = 3n + 2^n$$

$$\Rightarrow cn + d + qn^2 2^n - 4cn - 4d + 4c - 2q\left(n^2 - 2n + 1\right)2^n + 4cn + 4d - 8c + q\left(n^2 - 4n + 4\right)2^2 = 3n + 2^n$$

$$\Rightarrow cn + d - 4c + 2q.2^n = 3n + 2^n$$

Equating the coefficients of like terms, we get

$$c = 3, d - 4c = 0, 2q = 1 \ \Rightarrow c = 3, d = 12, q = \frac{1}{2}$$

So, $s_n^{(p)} = 3n + 12 + \frac{1}{2}n^2 2^n = 3n + 12 + n^2 2^{n-1}$ is the required particular solution.

$\therefore$ general solution is

$$s_n = s_n^{(h)} + s_n^{(p)} = (c_1 + c_2 n)2^n + 3n + 12 + n^2 2^{n-1} \quad ...(1)$$

It is given that $s_0 = s_1 = 1$. So, put $n = 0$ and $n = 1$ in the general solution and we get

$$s_0 = (c_1 + 0)2^0 + 0 + 12 + 0 \Rightarrow 1 = c_1 + 12 \Rightarrow c_1 = -11$$

and $s_1 = (c_1 + c_2)2 + 3 + 12 + 1 \Rightarrow 1 = (-11 + c_2)2 + 16 = -22 + 2c_2 + 16 \Rightarrow c_2 = \dfrac{7}{2}$

Put in (1), $s_n = \left(-11 + \dfrac{7}{2}n\right)2^n + 3n + 12 + n^2 2^{n-1}$

Example 3.7: Find the particular solution of $s_r - 5s_{r-1} + 6s_{r-2} = 3r^2$

Sol. Let $s_r^{(p)} = a + br + cr^2$

Using this value of s_r in the given equation, we obtain

$$a + br + cr^2 - 5\left(a + b(r-1) + c(r-1)^2\right) + 6\left(a + b(r-2) + c(r-2)^2\right) = 3r^2$$

$$\Rightarrow a + br + cr^2 - 5a - 5br + 5b - 5cr^2 - 5c + 10cr + 6a + 6br - 12b + 6cr^2 + 24c - 24cr = 3r^2$$

$$\Rightarrow 2cr^2 + 2br - 14cr + 2a - 7b + 19c = 3r^2$$

Equating the coefficients of like terms, we get

r^2 : $2c = 3 \Rightarrow c = \dfrac{3}{2}$

r : $2b - 14c = 0 \Rightarrow 2b = 14 \times \dfrac{3}{2} = 21 \Rightarrow b = \dfrac{21}{2}$

constant : $2a - 7b + 19c = 0 \Rightarrow 2a - 7 \times \dfrac{21}{2} + 19 \times \dfrac{3}{2} = 0 \Rightarrow 2a = \dfrac{90}{2} \Rightarrow a = \dfrac{45}{2}$

$$\therefore a_r^{(p)} = \frac{45}{2} + \frac{21}{2}r + \frac{3}{2}r^2$$

Example 3.8: By finding the generating function of sequence $S(n)$, find the solution of recurrence relation $S(n+2) - 7S(n+1) + 12S(n) = 0$ for $n \geq 0$ with $S(0) = 2, S(1) = 5$

Sol. The given recurrence relation can also be written as

$$S(n) - 7S(n-1) + 12S(n-2) = 0$$

Multiplying both sides by z^n and summing up terms from $n = 2$ to ∞, we get

$$\sum_{n=2}^{\infty} S(n)z^n - 7\sum_{n=2}^{\infty} S(n-1)z^n + 12\sum_{n=2}^{\infty} S(n-2)z^n = 0$$

$$\Rightarrow G(S,z) - S(0) - S(1)z - 7z\sum_{n=2}^{\infty} S(n-1)z^{n-1} + 12\sum_{n=2}^{\infty} S(n-2)z^{n-2} = 0$$

$\Rightarrow G(S,z)-2-5z-7z[G(S,z)-S(0)]+12z^2G(S,z)=0$

$\Rightarrow G(S,z)-2-5z-7z[G(S,z)-2]+12z^2G(S,z)=0$

$\Rightarrow G(S,z)-2-5z-7zG(S,z)+14z+12z^2G(S,z)=0$

$\Rightarrow (1-7z+12z^2)G(S,z)=2-9z$

$$\Rightarrow G(S,z)=\frac{2-9z}{1-7z+12z^2}=\frac{2-9z}{(1-3z)(1-4z)}=\frac{2-3}{(1-3z)\left(1-\frac{4}{3}\right)}+\frac{2-\frac{9}{4}}{\left(1-\frac{3}{4}\right)(1-4z)}=\frac{3}{1-3z}-\frac{1}{1-4z}$$

which gives $S(n)=3.3^n-4^n=3^{n+1}-4^n$

3.9 Summary

In this lesson, we have tried to elaborate the concept of recursion with the help of recursive definitions. On the same ground, we have learnt about the recurrence relations and generating functions of recurrence relations. Further, this lesson teaches us the procedure to find out the general and particular solutions of recurrence relations. During the study, it is found that the numeric function is also known as the solution of recurrence relation. The concept is made more clear with the help of suitable examples.

3.10 Self Check Exercise

1) Write short note on recursion.
2) Solve $s_n+5s_{n-1}=9, s_0=6$.
3) Solve $s_n-4s_{n-1}+4s_{n-2}=(n+1)2^n$.
4) If the solution of recurrence relation $as_n+bs_{n-1}+cs_{n-2}=6$ is 3^n+4^n+2, then find a,b,c.
5) Define the Febonacci sequence and find its generating function.
6) By finding the generating function of sequence $S(n)$, find the solution of recurrence relation $S(n)+3S(n-1)-4S(n-2)=0$ for $n\geq 2$ with $S(0)=3, S(1)=-2$.

3.11 Suggested Readings

1. Norman L. Biggs, *Discrete Mathematics*, Oxford University Press.
2. Harmohan Sharma, Ganesh Kumar Sethi, *Discrete Mathematics,* Sharma Publications, Jalandhar.
3. C.L. Liu, Elements of Discrete Mathematics (Second Edition), McGraw Hill, International Edition, Computer Science Series, 1986.

B.A. Part-III **OPT-III**

Semester-VI **Discrete Mathematics-II**

Lesson No. 2.1 **Author : Dr. Chanchal**

Boolean Algebra-I

I An Introduction to Relations : As we are already familiar with the concept of sets. To further understand the theory of relations, we define following terms:

Ordered Pair : By an ordered pair, we mean a pair of the form (a, b) (written in particular order) where $a \in A$ and $b \in B$. Any two ordered pairs (a, b) and (c, d) are equal i.e. $(a, b) = (c, d)$ iff $a = c$ and $b = d$. Further, $(a, b) \neq (b, a)$ unless $a = b$.

Product Set : Consider two non-empty arbitrary sets A and B. The set of all ordered pairs (a, b) where $a \in A, b \in B$ is called the product or **Cartesian Product** of A and B, written as $A \times B$ read as A cross B, i.e. $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

NOTE : For $A \times A$, we write A^2.

For example : 1. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the set of ordered pairs of real numbers and $\mathbb{R}^2$ is known as the cartesian plane.

2. Let $A = \{1, 2\}$ and $B = \{a, b, c\}$, then $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$, $B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$. Note that $A \times B \neq B \times A$ and $n(A \times B) = n(A) \cdot n(B)$.

The idea of product of sets can be extended to any finite number of sets. For any non-empty sets $A_1, A_2, ..., A_n$, the set of all ordered n-tuples $(a_1, a_2, ..., a_n)$ where $a_i \in A_i\ \forall i = 1, 2, ..., n$, is called the product of the sets $A_1, A_2, ..., A_n$ denoted by $A_1 \times A_2 \times .... \times A_n = \prod_{i=1}^{n} A_i$.
Relation : Let A and B be non-empty arbitrary sets. A binary relation or simply a relation from A to B is a subset of $A \times B$. Suppose R is a relation from A to B. Then, R is the set of ordered pairs (a, b) where $a \in A$ and $b \in B$; and for each pair (a, b), exactly one of the following is true :

1. $(a, b) \in R$ i.e. a is related to b written as aRb.
2. $(a, b) \notin R$ i.e. a is not related to b written as $a\not{R}b$.

Remarks : 1. If R is a relation from a set A $(\neq \phi)$ to itself, i.e. R is a subset of $A^2 = A \times A$, then we say R is a relation on A.
2. The domain of a relation R is the set of all first elements of the ordered pairs which belong to R. Similarly, range R is the set of all second elements of ordered pairs that belong to R.
For example : Let $A = \{1, 2, 3\}$, $B = \{x, y, z\}$, $R = \{(1, y), (1, z), (3, y)\}$. Here $R \subset A \times B$,
$\therefore$ R is a relation from A to B with Domain$=\{1, 3\}$ and Range$=\{y, z\}$.
n-ary Relation : By the n-ary relation, we mean a set of ordered n-tuples. For any non-empty set S, a subset of the product set S^n is called an n-ary relation on S. In particular, a subset of S^3 is called a ternary relation on S.
Some Important Relations : Let A be any arbitrary non-empty set.

1. **Identity Relation** : An important relation on A is that of equality $\{(a, a) : a \in A\}$, usually denoted by '='. This relation is also called the identity or diagonal relation on A, denoted by $\triangle_A$ or $\triangle$ or I_A.
2. **Universal Relation** : The relation $A \times A$ is called Universal relation on A.
3. **Empty Relation** : The relation $\phi \subset A \times A$ is known as empty or void or null relation on A.

Inverse Relation : Let R be any relation from a set A to set B. The inverse of R, denoted by R^{-1} is a relation from B to A such that $R^{-1} = \{(b, a) : (a, b) \in R\}$.
For example : Let $R = \{(1, y), (1, z), (3, y)\}$ be a relation from $A = \{1, 2, 4\}$ to $B = \{x, y, z\}$, then $R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$. Note that domain of R becomes range of R^{-1} and vice versa.
Remarks : 1. $(R^{-1})^{-1} = R$.

2. If R is a relation on A $(\neq \phi)$, then R^{-1} is also a relation on the set A.

Types of Relations: Consider any arbitrary set A $(\neq \phi)$.

1. **Reflexive Relation** : A relation R on set A is reflexive if $(a, a) \in R$ or aRa $\forall a \in A$.

   For example : (i) Let $A = \{1, 2, 3\}$, then the relation $R = \{(1, 1), (1, 2), (2, 2), (1, 3), (3, 3)\}$ is reflexive on A as $\forall a \in A$, $(a, a) \in R$ but $R_1 = \{(1, 1), (1, 2), (2, 2), (2, 3)\}$ is not reflexive since $3 \in A$ but $(3, 3) \notin R$.

   (ii) The relation of 'less than equal to' i.e. $\leq$ on $\mathbb{Z}$ (the set of integers) is a reflexive relation since every number is less than equal to itself.

   (iii) The relation of inclusion i.e. $\subseteq$ on $P(A)$ (where $A \neq \phi$) is a reflexive relation since every set is a subset of itself.

   NOTE : An identity relation on A $(\neq \phi)$ denoted by 'I_A' is always a reflexive relation on A but the converse is not true.

2. **Symmetric Relation** : A relation R on set A is said to be symmetric if whenever $(a, b) \in R$, then $(b, a) \in R$ or if aRb then bRa for $a, b \in A$.

   For example : (i) Let $A = \{1, 2, 3\}$, then the relation $R = \{(1, 1), (1, 2), (2, 1), (3, 3)\}$ is symmetric on A but $R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3)\}$ is not symmetric since $(2, 3) \in R$ but $(3, 2) \notin R$.

   (ii) The relation of 'less than equal to' i.e. $\leq$ on $\mathbb{Z}$ (the set of integers) is not a symmetric relation because if $a \leq b$ (i.e. aRb), then $b \not\leq a$ (i.e. $b \not R a$), where $a, b \in \mathbb{Z}$.

   (iii) The relation of parallelism on the set L of lines in a plane is symmetric because if $l_1, l_2 \in L$ such that $l_1 R l_2$ i.e. l_1 is parallel to l_2, then l_2 is also parallel to l_1 i.e. $l_2 R l_1$.

3. **Anti-Symmetric Relation** : It is just the opposite of symmetric relation. A relation R on set A is said to be anti-symmetric if whenever $(a, b) \in R$ and $(b, a) \in R$ or if aRb and bRa, then $a = b$, where $a, b \in A$.

   For example : (i) Let $A = \{1, 2, 3\}$, then the relation $R = \{(1, 1), (1, 2), (3, 3)\}$ is anti-symmetric on A but $R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3)\}$ is not anti-symmetric because $(1, 2), (2, 1) \in R$ but $1 \neq 2$.

   (ii) The relation of 'less than equal to' i.e. $\leq$ on $\mathbb{Z}$ (the set of integers) is an anti- symmetric relation since if $a \leq b$, then $b \not\leq a$, where $a, b \in \mathbb{Z}$.

(iii) The relation of inclusion i.e. $\subseteq$ on $P(A)$ (where $A \neq \phi$) is an anti-symmetric relation because if $R \subseteq S$, then $S \not\subseteq R$, where $R, S \subseteq A$.

4. **Transitive Relation** : A relation R on set A is said to be transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ or if aRb and bRc, then aRc, where $a, b, c \in A$.

   For example : (i) Let $A = \{1, 2, 3\}$, then the relation $R = \{(1, 1), (1, 2), (3, 3)\}$ is transitive relation on A but $R_1 = \{(1, 1), (1, 2), (2, 3), (2, 2)\}$ is not transitive since $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$.

   (ii) The relation of 'less than equal to' i.e. $\leq$ on $\mathbb{Z}$ (the set of integers) is a transitive relation, $\because$ if $a \leq b$ and $b \leq c$, then $a \leq c$, where $a, b, c \in \mathbb{Z}$.

   (iii) The relation of inclusion i.e. $\subseteq$ on $P(A)$ (where $A \neq \phi$) is a transitive relation, $\because$ if $R \subseteq S$ and $S \subseteq T$, then $R \subseteq T$, where $R, S, T \in P(A)$.

5. **Equivalence Relation** : A relation R on set A is said to be an equivalence relation if it is reflexive, symmetric and transitive.

   For example : (i) Let $A = \{1, 2, 3\}$, then the relation

   $R = \{(1, 1), (2, 2), (1, 2), (2, 1), (3, 3), (2, 3), (3, 2), (3, 1), (1, 3)\}$ is an equivalence relation on A since it is reflexive, symmetric and transitive.

   (ii) The relation of parallelism on the set L of lines in a plane is an equivalence relation.

   Reflexivity : Since every line is parallel to itself, $\therefore l_1 R l_1 \ \forall \ l_1 \in L$.

   Symmetry : Let $l_1, l_2 \in L$ be such that l_1 is parallel to l_2, then l_2 is also parallel to l_1 i.e. if $l_1 R l_2$, then $l_2 R l_1$.

   Transitivity : Let $l_1, l_2, l_3 \in L$ be such that l_1 is parallel to l_2 and l_2 is parallel to l_3, then l_1 is also parallel to l_3 i.e. if $l_1 R l_2$ and $l_2 R l_3$, then $l_1 R l_3$.

6. **Partial Order Relation** : A relation R on set A is said to be an partial order relation if it is reflexive, anti-symmetric and transitive.

   For example : (i) Let $A = \{1, 2, 3\}$, then the relation

   $R = \{(1, 1), (2, 2), (1, 2), (3, 3), (2, 3), (1, 3)\}$ is a partial order relation on A since it is reflexive, anti-symmetric and transitive.

   (ii) Let A be any arbitrary set and $P(A)$ denotes the power set of A. Then, the relation of inclusion '$\subseteq$' on $P(A)$ is a partial order relation.

Reflexivity : Since every set is a subset of itself, $\therefore$ LRL $\forall L \in P(A)$.

Anti-Symmetry : Let $L, M \in P(A)$ be such that $L \subseteq M$ and $M \subseteq L$, then $L = M$.

Transitivity : Let $L, M, N \in P(A)$ be such that $L \subseteq M$ and $M \subseteq N$, then $L \subseteq N$.

II POSET : A non-empty set P together with a partial order relation R on P, is called a partially ordered set or POSET. It is represented as (P, R) or $(P, \leq)$. Here '$\leq$' denotes the partial order relation on the set P.

For example : 1. $(\mathbb{N}, \leq)$ (here $\leq$ stands for 'divisibility') is a POSET.

2. Let $X \neq \phi$, then $(P(X), \leq)$ (here $\leq$ stands for '$\subseteq$') is a POSET.

3. $(\mathbb{N}, \leq)$ (here $\leq$ stands for 'less than equal to $\leq$') is a POSET.

II(a) Comparable and Non-Comparable Elements : Let $(P, \leq)$ be a POSET, then $a, b \in P$ are said to be comparable if $a \leq b$ or $b \leq a$. Otherwise a and b are said to be non-comparable.

For example : In POSET $(\mathbb{N}, \leq)$ (where $\leq$ stands for 'less than equal to $\leq$'), $2 \leq 3$ $\therefore$ 2 and 3 are comparable. Moreover in this POSET, any two elements are comparable.

TOSET : A partially ordered set $(P, \leq)$ in which every two elements are comparable is called a totally ordered set (TOSET) or linearly ordered set. In other words, if $(P, \leq)$ is a TOSET as if $a, b \in P$, then either $a \leq b$ or $b \leq a$. In this case, $\leq$' is called a total ordering relation.

For example : $(\mathbb{N}, \leq)$ (here $\leq$ stands for 'less than equal to $\leq$') is a TOSET.

II(b) Hasse Diagram : It is the pictorial representation of a POSET $(P, \leq)$. It is a directed graph whose vertices are the elements of P and there is a directed edge from a to b whenever $a << b$ in P (which means a is immediate predecessor of b or b is immediate successor of a or b is a cover of a). Instead of drawing an arrow from a to b, we place b higher than a and draw a line between them. Also, there is a directed path from vertex x to vertex y if $x < y$ (i.e. either $x << y$ or $\exists a_1, a_2, ..., a_m$ such that $x << a_1 << a_2 << \ldots\ldots\ldots << a_m << y$).

Remarks : 1. If $a \leq b$, then a lies below b and if $b \leq a$, then b lies below a.

2. No horizontal line is drawn in Hasse diagram.

3. There can be no cycles in a Hasse diagram since the relation is anti-symmetric.

For example : Firstly we define the set D_m : Set of positive divisors of m $(m \in \mathbb{Z}^+)$ under the relation of divisibility. Clearly $(D_m, \leq)$ is a POSET.

1. $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$, $(D_{36}, \leq)$ is a POSET.

2. $D_{12} = \{1, 2, 3, 4, 6, 12\}$, $(D_{12}, \leq)$ is a POSET.

The Hasse diagrams of D_{36} and D_{12} are shown in the following diagrams.

[a] [b]

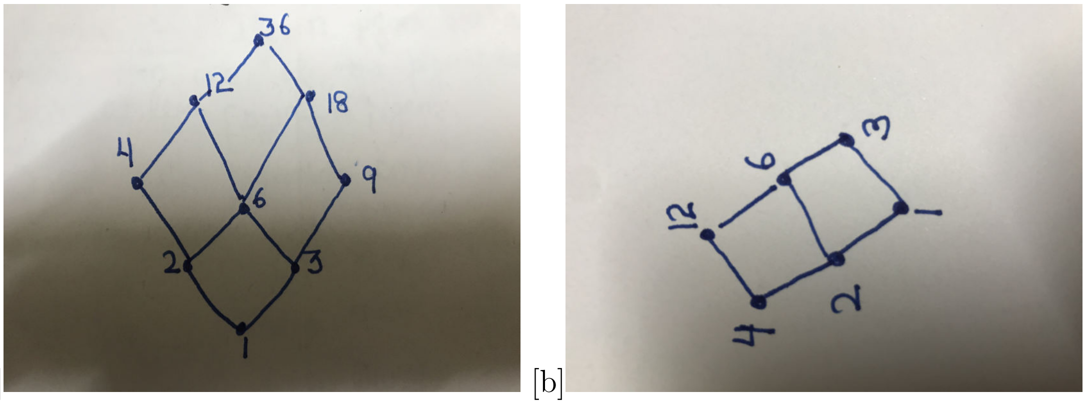


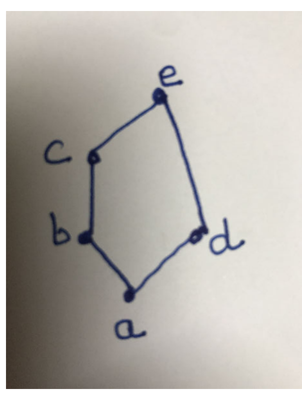
Figure 1:

II(c) Chain and Anti-Chain : Let $(P, \leq)$ be a POSET. A subset of P is called a chain if every two elements in the subset are related. Moreover, number of elements in a chain refers to the length of chain. Now, a subset of P is called an anti-chain if no two distinct elements in the subset are related to each other.

For example : Consider a relation

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

on the set $A = \{a,b,c,d,e\}$. Clearly R is a partial order relation on A and Hasse diagram is given by



Clearly, $\{a,b,c,e\},\{a,b,c\},\{a,d,e\}$ are chains and $\{b,d\},\{c,d\}$ are anti-chains.

Remark : If the POSET $(P, \leq)$ is a TOSET, then it is also called a chain.

II(d) Maximal and Minimal Elements : Let $(P, \leq)$ be a POSET.

Maximal Element : An element $a \in P$ is called maximal element of P if there is no element c in P such that $a \leq c$.

Minimal Element : An element $b \in P$ is called minimal element of P if there is no element c in P such that $c \leq b$.

Remarks : 1. b is called minimal element if no edge enters b (from below) and a is called maximal element if no edge leaves a (in upward direction) in the Hasse diagram.

2. If P is infinite set, then P may have no maximal and no minimal element.

For example : $(\mathbb{Z}, \leq)$

3. If P is finite set, then P must have atleast one maximal element and atleast one minimal element.

II(e) Greatest and Least Elements

Let $(P, \leq)$ be a POSET. If $\exists$ an element $a \in P$ such that $x \leq a \; \forall x \in P$, then a is called greatest or last or unity element of P. It is denoted by '1'. Similarly, If $\exists$ an element $b \in P$ such that $b \leq x \; \forall x \in P$, then b is called least or first or zero element of P. It is denoted by '0'.

Remarks : 1. Greatest and least elements are related to every element of the POSET.

2. If a POSET has both least and greatest element, it is called a bounded POSET.

3. P can have atmost one first element, which must be a minimal element and P can have atmost one last element which must be a maximal element. P may have neither a first element nor a last element even when P is finite.

For example : Let $X = \{1, 2, 3\}$, $(P(X), \leq)$ ($\leq$ stands for $\subseteq$) is POSET.

Let $A = \{\phi, \{1, 2\}, \{2, 3\}\}$, then $(A, \leq)$ is POSET with ϕ as least element but no greatest element.

Similarly, $B = \{\{1, 2\}, \{2\}, \{3\}, \{1, 2, 3\}\}$, then $(B, \leq)$ is POSET with no least element but $\{1, 2, 3\}$ greatest element.

$C = \{\phi, \{1, 2\}, \{1\}, \{2\}\}$, then $(C, \leq)$ is POSET with both least element and greatest element.

$D = \{\{1\}, \{2\}, \{1, 3\}\}$, then $(D, \leq)$ is POSET with neither least element nor greatest element.

II(f) l.u.b and g.l.b : Let $(P, \leq)$ be a POSET. Let S be a non-empty subset of P. An element $a \in P$ is called an upper bound of S if $x \leq a \; \forall x \in S$. Further, if a is an upper bound of S such that $a \leq b$ for all other upper bounds b of S, then a is called l.u.b or supremum of S.

Similarly, An element $c \in P$ is called a lower bound of S if $c \leq y \; \forall y \in S$. Further, if c is a lower bound of S such that $d \leq c$ for all other lower bounds d of S, then c is called g.l.b or infimum of S.

Remark : Greatest and least element belong to the set whereas l.u.b and g.l.b may or may not belong to the set.

For example : 1. $(\mathbb{Z}, \leq)$ ($\leq$ stands for 'less than equal to') is a POSET.

Let $S = \{.......... -2, -1, 0, 1, 2\}$, then Sup S=l.u.b. S =2 but it has no infimum.

2. Consider $D_{105} = \{1, 3, 5, 7, 15, 21, 35, 105\}$, then $(D_{105}, \leq)$ is a POSET.

l.u.b of 3 and 7 is 21 (upper bounds are 21 and 105).

l.u.b of 3 and 5 is 15 (upper bounds are 15 and 105).

g.l.b of 15 and 35 is 5 (lower bounds are 5 and 1).

Moreover, least element of the POSET is 1 and the greatest element is 105. These evaluations are very easy to understand from the Hasse diagram of D_{105}.

[a] [b]

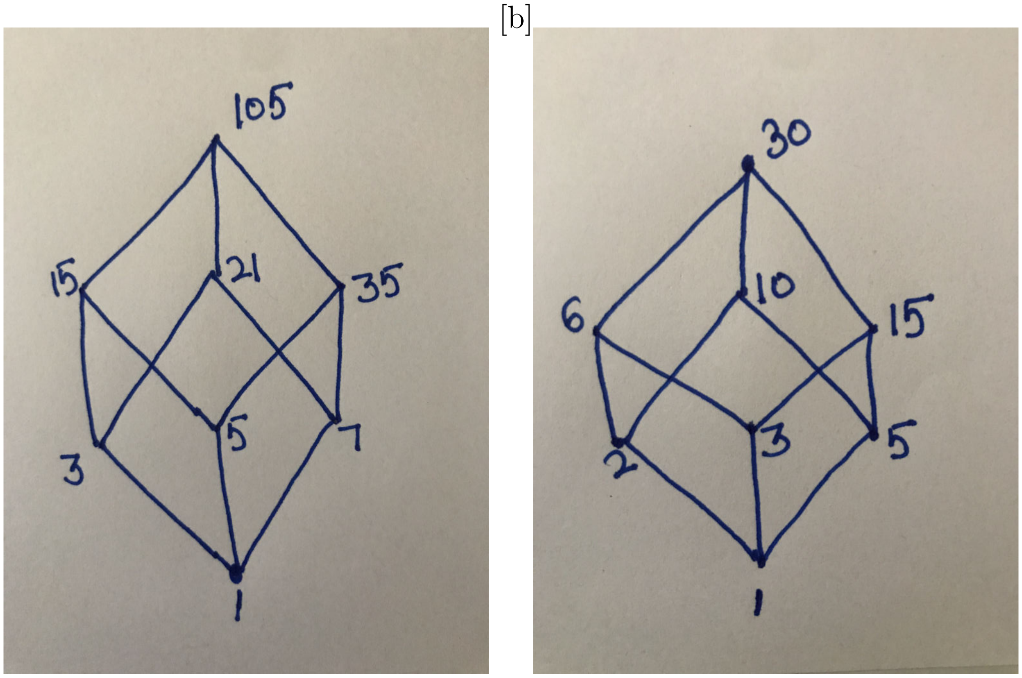


Figure 2:

3. Consider the Hasse diagram of $(D_{30}, \leq)$ (shown in the above figure).

Clearly, l.u.b and g.l.b of 10 and 15 are 30 and 5 respectively.

Remark : 1) If the relation is of set inclusion $(\subseteq)$, then the l.u.b and g.l.b of two sets are the union and intersection of two sets respectively.

2) If the relation is of divisibility $(/)$, then the l.u.b and g.l.b of two numbers are the l.c.m and g.c.d of two numbers respectively.

3) If the relation is of less than equal to $(\leq)$, then the l.u.b and g.l.b of two numbers are the greater and smaller of two numbers respectively.

The brief concept of l.u.b and g.l.b for the most common relations is summarised below:

III Product of Two POSETs : Let (A, R) and (B, R') be two POSETs. Then, prove that $(A \times B, R'')$ is a POSET with partial order relation R'' defined by $(a, b)R''(a', b')$ if aRa' in A and $bR'b'$ in B.

Proof : **Reflexivity** : Let $(a, b) \in A \times B$ be any arbitrary element.

Relation	l.u.b	g.l.b
$\subseteq$	union	intersection
$/$	l.c.m	g.c.d
$\leq$	greater element	smaller element

Then $a \in A$ and $b \in B$. $\therefore$ aRa in A and bR'b in B.

$\implies$ $(a,b)R''(a',b')$ (by def^n), showing that R'' is reflexive relation on $A \times B$.

Anti-Symmetry : Let $(a,b),(c,d) \in A \times B$ be such that $(a,b)R''(c,d)$ and $(c,d)R''(a,b)$.

$\implies$ aRc in A, $bR'd$ in B and cRa in A, $dR'c$ in B.

$\implies$ aRc, cRa in A and $bR'd$, $dR'b$ in B, which gives $a = c$ in A and $b = d$ in B ($\because$ R and R' are anti-symmetric relations on A and B respectively.)

$\therefore$ $(a,b) = (c,d)$ in $A \times B$ $\implies$ R'' is anti-symmetric relation on $A \times B$.

Transtivity : Let $(a,b),(c,d),(e,f) \in A \times B$ be such that $(a,b)R''(c,d)$ and $(c,d)R''(e,f)$.

$\implies$ aRc in A, $bR'd$ in B and cRe in A, $dR'f$ in B.

$\implies$ aRc, cRe in A and $bR'd$, $dR'f$ in B, which gives aRe in A and $bR'f$ in B (since R and R' are transitive relations on A and B respectively).

$\therefore$ $(a,b)R''(e,f)$ in $A \times B$ (by def^n) which shows that R'' is transitive relation on $A \times B$.

Hence $(A \times B, R'')$ is a POSET.

IV Lattice : A POSET $(P, \leq)$ is said to be a lattice if every pair of elements have g.l.b and l.u.b that belongs to P i.e. $\forall a, b \in P$, $a \wedge b \in P$ and $a \vee b \in P$,

where $a \vee b$ = l.u.b$\{a,b\}$=Sup.$\{a,b\}$ and $a \wedge b$ =g.l.b$\{a,b\}$=inf.$\{a,b\}$.

Here $a \vee b$ is read as 'a join b' and $a \wedge b$ is read as 'a meet b'. $(P, \vee, \wedge)$ is the algebraic structure defined by lattice $(P, \leq)$.

For example : 1. The POSET $(D_{12}, \leq)$ (where $\leq$ stands for divisibility) is lattice. We can show it with the help of following operation tables :

Clearly, $\forall a, b \in D_{12}$, $a \vee b \in D_{12}$ and $a \wedge b \in D_{12}$, $\therefore$ $(D_{12}, \leq)$ is a lattice.

2. $(D_{30}, \leq)$ ($\leq$ stands for $/$) is a lattice.

3. $(P(X), \leq)$ ($\leq$ stands for $\subseteq$) is a lattice.

4. $(\mathbb{N}, \leq)$ (where $\leq$ is $\leq$ or $/$) are lattices.

Remark : For any a, b in lattice $(P, \leq)$, a (or b) $\leq a \vee b$ and $a \wedge b \leq a$ (or b).

Result 1 : Every chain is a lattice.

$\vee$	1	2	3	4	6	12
1	1	2	3	4	6	12
2	2	2	6	4	6	12
3	3	6	3	12	6	12
4	4	4	12	4	12	12
6	6	6	6	12	6	12
12	12	12	12	12	12	12

$\wedge$	1	2	3	4	6	12
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
6	1	2	3	2	6	6
12	1	2	3	4	6	12

Proof : In a chain $(P, \leq)$, every two elements are comparable i.e. either $a \leq b$ or $b \leq a$ $\forall a, b \in P$. If $a \leq b$, then sup$\{a, b\}$=$b \in P$ and inf $\{a, b\}$=$a \in P$, similarly for $b \leq a$. Hence every pair of elements have l.u.b and g.l.b belonging to the set P, therefore $(P, \leq)$ is a lattice.

Result 2 : Show that a lattice with three of fewer elements is a chain (try yourself).

Result 3 : Let $(L, \leq)$ be a lattice. For any elements $a, b \in L$, prove that $a \wedge b = a$ iff $a \vee b = b$.

Proof : Let $a, b \in L$ and $a \wedge b = a$, $\implies$ $a =$glb$\{a, b\}$ which gives $a \leq b$.

$\therefore$ $a \vee b =$lub $\{a, b\} = b$.

Result 4 : Let $(L, \leq)$ be a lattice. For any elements $a, b \in L$, prove that

If a and b have lub (or glb), then this lub (or glb) is unique.

Proof : If possible, let l_1 and l_2 be two distinct lub's (or glb's) of a and b.

Let l_1 be lub (or glb) and $l_2 \in P$, then $l_2 \leq l_1$ (or $l_1 \leq l_2$).

Let l_2 be lub (or glb) and $l_1 \in P$, then $l_1 \leq l_2$ (or $l_2 \leq l_1$).

$\therefore$ By the anti-symmetry property, $l_1 = l_2$.

Lesson No. 2.2 **Author : Dr. Chanchal**

Boolean Algebra-II

I Product of Two Lattices

II Properties of Lattice

III Principle of Duality

IV Complete Lattice

V Sublattice

VI Bounded Lattice

VII Isomorphic Lattices

VIII Distributive Lattice

IX Complemented Lattice

X Boolean Algebra

XI Laws of Boolean Algebra

XII Boolean Functions and Expressions

I Product of Two Lattices : Let $(A, \leq)$ and $(B, \leq)$ be two lattices. Then $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$ is a POSET under $\leq$ defined by $(a_1, b_1) \leq (a_2, b_2)$ iff $a_1 \leq a_2$ in A and $b_1 \leq b_2$ in B. Here, $(A \times B, \leq)$ is called product of lattices.

Theorem 1 : Prove that product of two lattices is a lattice.

Proof : Let (a_1, b_1), $(a_2, b_2) \in A \times B$, $\implies a_1, a_2 \in A$ and $b_1, b_2 \in B$.

$\implies a_1 \wedge a_2 \in A$ and $b_1 \wedge b_2 \in B$ ($\because (A, \leq)$ and $(B, \leq)$ are lattices).

$\therefore a_1 \wedge a_2 \leq a_1$ and $b_1 \wedge b_2 \leq b_1$.

Also, $a_1 \wedge a_2 \leq a_2$ and $b_1 \wedge b_2 \leq b_2$.

$\implies (a_1 \wedge a_2, b_1 \wedge b_2) \leq (a_1, b_1)$ and $(a_1 \wedge a_1, b_1 \wedge b_2) \leq (a_2, b_2)$,

$\therefore (a_1 \wedge a_2, b_1 \wedge b_2)$ is lower bound of $\{(a_1, b_1), (a_2, b_2)\}$.

Suppose (a, b) is any other lower bound of $\{(a_1, b_1), (a_2, b_2)\}$.

So, $(a, b) \leq (a_1, b_1)$ and $(a, b) \leq (a_2, b_2)$, $\implies a \leq a_1,\ a \leq a_2,\ b \leq b_1,\ b \leq b_2$.

$\implies a$ is lower bound of $\{a_1, a_2\}$ in A and b is lower bound of $\{b_1, b_2\}$ in B.

$\implies a \leq a_1 \wedge a_2$, ($\because a_1 \wedge a_2$ is g.l.b)

Similarly, $b \leq b_1 \wedge b_2$, ($\because b_1 \wedge b_2$ is g.l.b)

$\implies (a, b) \leq (a_1 \wedge a_2, b_1 \wedge b_2)$.

$\therefore (a_1 \wedge a_2, b_1 \wedge b_2)$ is g.l.b of $\{(a_1, b_1), (a_2, b_2)\}$.

Similarly, we can prove that $(a_1 \vee a_2, b_1 \vee b_2)$ is l.u.b of $\{(a_1, b_1), (a_2, b_2)\}$.

So, both g.l.b and l.u.b of (a_1, b_1), (a_2, b_2) exist and belong to $A \times B$.

$\implies A \times B$ is a lattice.

II Properties of Lattice

Let $(P, \vee, \wedge)$ be the algebraic system defined by the lattice $(P, \leq)$.

- **Idempotency Law** : $a \wedge a = a$, $a \vee a = a\ \forall a \in P$ ($a \wedge a = \text{Inf}\{a, a\} = a$, $a \vee a = \sup\{a, a\} = a$).

- **commutative Law** : $a \wedge b = b \wedge a$, $a \vee b = b \vee a\ \forall a, b \in P$.

- **Associative Law** : (i) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$, (ii) $a \vee (b \vee c) = (a \vee b) \vee c\ \forall a, b, c \in P$

  Proof of (ii) : Let $a \vee (b \vee c) = g$ and $(a \vee b) \vee c = h$

  T.P. $h = g$ (so, we prove $h \leq g$ and $g \leq h$).

  Since g is the join of a and $b \vee c$, $\therefore a \leq g$ and $b \vee c \leq g$.

  Further $b \vee c \leq g \implies b \leq g$ and $c \leq g$.

  Now, $a \leq g$, $b \leq g \implies g$ is an u.b. of $\{a, b\}$.

  $\implies a \vee b \leq g$ ($\because a \vee b$ is the l.u.b of $\{a, b\}$).

  Now $c \leq g$ and $a \vee b \leq g$, $\implies g$ is an u.b. of $\{a \vee b, c\}$

  $\implies (a \vee b) \vee c \leq g$ or $h \leq g$ ($\because (a \vee b) \vee c$ is the l.u.b of $\{a \vee b, c\}$).

  Similarly, we can prove that $g \leq h$. Combining the two, we get $g = h$.

- **Absorption Law** : $a \wedge (a \vee b) = a,\ a \vee (a \wedge b) = a\ \forall a, b \in P$.

  Proof : Since $a \leq a \vee b$, therefore $a \wedge (a \vee b) = a$.

- **Consistency Law** : $a \leq b$ iff $a \wedge b = a$ iff $a \vee b = b$.

  Proof : $a \leq b$ (given). Also $a \leq a$, $\therefore a$ is the lower bound of $\{a, b\}$.

  $\implies a \leq a \wedge b$ ....(1) ($\because a \wedge b$ is the g.l.b of $\{a, b\}$).

  Again $a \wedge b$=g.l.b $\{a, b\}$ and g.l.b $\{a, b\} \leq a$ i.e. $a \wedge b \leq a$.........(2)

  Combining (1) and (2), we get $a \wedge b = a$

  $\therefore a \leq b \implies a \wedge b = a$.

  Further, $a = a \wedge b \implies a \leq b$

  Hence $a \leq b$ iff $a \wedge b = a$.

  Similarly, we can prove that $a \leq b$ iff $a \vee b = b$.

  On similar lines, we can prove part (i).

III Product of Two Lattices : Let $(A, \leq)$ be a POSET. Define a binary relation $\leq_R$ on A such that $a \leq_R b$ iff $b \leq a$ (or $a \geq b$) for $a, b \in A$. Moreover, $(A, \leq_R)$ is also a POSET. Further if $(A, \leq)$ is a lattice, then $(A, \leq_R)$ is also a lattice.

For writing the dual of a statement : interchange $\vee$ with $\wedge$, $\wedge$ with $\vee$ and $\leq$ (i.e. $a \leq b$) with $\leq_R$ or $\geq$ (i.e. $a \leq_R b$ or $a \geq b$).

Problem : For any a, b, c, d in a lattice $(A, \leq)$: if $a \leq b$ and $c \leq d$, then $a \vee c \leq b \vee d$ and $a \wedge c \leq b \wedge d$.

Proof : Since $b \leq b \vee d$ and $d \leq b \vee d$.

Now $a \leq b$ and $b \leq b \vee d \implies a \leq b \vee d$.

Similarly $c \leq d$ and $d \leq b \vee d \implies c \leq b \vee d$.

$\implies b \vee d$ is the u.b. of $\{a, c\}$.

$\implies a \vee c \leq b \vee d$

Similarly, the other part can be proved.

IV Complete Lattice : A lattice $(P, \leq)$ is said to be complete iff every non empty subset of P has supremum and infimum in P.

For example : 1. Every finite lattice is complete lattice.

2. $(\mathbb{Z}, \leq)$ is a lattice but it is not complete since $\{x \in \mathbb{Z} : x > 0\} \subseteq \mathbb{Z}$ has no supremum in $\mathbb{Z}$.

V Sublattice : Let $(P, \leq)$ be a lattice. A non-empty subset S of P is called a sublattice of P if for all $a, b \in S$, $a \vee b, a \wedge b \in S$.

For example : 1. Every lattice is sublattice of itself.

2. If $(P, \leq)$ be any lattice and $a \in P$, then $(\{a\}, \leq)$ is a sublattice of $(P, \leq)$.

VI Bounded Lattice : Let $(P, \leq)$ be any lattice. Then '0' is called universal lower bound of P if for any $x \in P, 0 \leq x$. Also, P has universal upper bound '1' if for any $x \in P, x \leq 1$. If a lattice has both universal lower bound and universal upper bound, then it is called a bounded lattice.

For example : 1. Let $A \neq \phi$, then $(P(A), \leq)$ (where $\leq$ stands for $\subseteq$) is a bounded lattice with ϕ as universal lower bound and A as universal upper bound.

2. $(\mathbb{N}, \leq)$ (where the relation is $\leq$) is a lattice but it is not bounded as '1' is the universal lower bound but there is no such upper bound.

Remark : The universal lower bound and upper bound (if exist) are always unique (prove it).

Result 1 : $(i) a \vee 1 = 1, (ii) a \wedge 1 = a, (iii) a \vee 0 = a, (iv) a \wedge 0 = 0 \forall a \in P$.

Proof (i) : $1 \leq a \vee 1$...........(1)

Moreover, 1 is the universal upper bound, $\therefore a \vee 1 \leq 1$...........(2)

Combining (1) and (2), $a \vee 1 = 1$

(ii) : $a \wedge 1 \leq a$............(3)

Further, $a \leq a$ and $a \leq 1$,

$\implies a \wedge a \leq a \wedge 1$ ($\because a \leq b$ and $c \leq d$ gives $a \wedge b \leq c \wedge d$)

which gives, $a \leq a \wedge 1$............(4)

Combining (3) and (4), $a = a \wedge 1$.

Similarly, we can prove the other two parts.

VII Isomorphic Lattices : A lattice $(P_1, \leq)$ is said to be isomorphic to lattice $(P_2, \leq)$ if there exists a bijection f from P_1 onto P_2 such that

$f(a \wedge b) = f(a) \wedge f(b)$ and $f(a \vee b) = f(a) \vee f(b)$ $\forall a, b \in P_1$.

VIII Distributive Lattice : A lattice $(P, \leq)$ is said to be distributive lattice iff distributive laws hold, i.e.

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ $\forall a, b, c \in P$.

Otherwise, it is called non-distributive lattice.

For example : $(P(X), \leq)$ $(X \neq \phi$ and $\leq$ stands for $\subseteq)$ is a distributive lattice since

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $\forall A, B, C \in P(X)$

Article 1 : In any lattice $(P, \leq)$, prove the following distributive inequalities :

(i) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$,

(ii) $a \vee (b \wedge c) \geq (a \vee b) \wedge (a \vee c)$ $\forall a, b, c \in P$.

Proof : (i) $a \wedge b = \text{Inf } \{a, b\} \leq a$ and $a \wedge b \leq b$.

Also, $b \leq \text{Sup } \{b, c\} = b \vee c$,

$\therefore a \wedge b \leq b \vee c$ (since $a \wedge b \leq b$ and $b \leq b \vee c$),

$\implies a \wedge b$ is the lower bound of $\{a, b \vee c\}$,

$\implies a \wedge b \leq a \wedge (b \vee c)$............(1)

Similarly, $a \wedge c \leq c \leq b \vee c$, $\implies a \wedge c \leq b \vee c$

Also, $a \wedge c \leq a$,

$\implies a \wedge c \leq a \wedge (b \vee c)$............(2)

From (1) and (2), $a \wedge (b \vee c)$ is the upper bound of $\{a \wedge b, a \wedge c\}$,

which gives $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.

On similar lines, we can prove the (ii) part.

Article 2 : Prove that direct product of two distributive lattices is distributive.

Proof : Let $(L, \leq)$ and $(M, \leq)$ be two distributive lattices.

T.P. $L \times M = \{(a, b) : a \in L, b \in M\}$ is distributive lattice.

Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in L \times M$.

$\implies a_1, a_2, a_3 \in L$ and $b_1, b_2, b_3 \in M$

Now, $(a_1, b_1) \wedge [(a_2, b_2) \vee (a_3, b_3)] = (a_1, b_1) \wedge (a_2 \vee a_3, b_2 \vee b_3)$

$= (a_1 \wedge (a_2 \vee a_3), b_1 \wedge (b_2 \vee b_3))$

$= ((a_1 \wedge a_2) \vee (a_1 \wedge a_3), (b_1 \wedge b_2) \vee (b_1 \wedge b_3))$ ($\because L$ and M are distributive lattices.)

$= (a_1 \wedge a_2, b_1 \wedge b_2) \vee (a_1 \wedge a_3, b_1 \wedge b_3)$

$= [(a_1, b_1) \wedge (a_2, b_2)] \vee [(a_1, b_1) \wedge (a_3, b_3)]$

Similarly, we can prove the other part of distributive law and hence $L \times M$ is also distributive lattice.

Article 3 : Prove that every sub-lattice of distributive lattice is distributive.

Proof : Let $(S, \leq)$ be a sub-lattice of distributive lattice $(P, \leq)$.

Let $a, b, c \in S \implies a, b, c \in P$

$\implies a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ in P

Since S is closed under $\vee$ and $\wedge$.

$\therefore a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ in S

Hence $(S, \leq)$ is distributive lattice.

Article 4 : Prove that dual of distributive lattice is also distributive.

Proof : Try yourself.

IX Complemented Lattice : To define complemented lattice, we firstly introduce the concept of complement of an element.

Complement : An element x of a bounded lattice $(P, \vee, \wedge, 0, 1)$, where 0 is the universal lower bound and 1 is the universal upper bound, is called a complement of an element $a \in P$ if $a \vee x = 1$ and $a \wedge x = 0$. Due to commutative property, we can also say that a is the complement of x.

Remarks : 1. An element of a lattice may or may not have the complement.

2. An element of a lattice may have more than one complement in the lattice.

3. $0 \vee 1 = 1$ and $0 \wedge 1 = 0$ i.e. 0 and 1 are complements of each other.

Theorem 2 (Uniqueness Theorem) : Let $(P, \leq)$ be a bounded distributive lattice. Prove that complement of any element (if it exists) is unique.

Proof : Let $a \in P$. Suppose that a_1 and a_2 are two complements of a in P.

By definition of complement, $a \vee a_1 = 1 = a \vee a_2$, $a \wedge a_1 = 0 = a \wedge a_2$.

Now, $a_1 = a_1 \vee 0 = a_1 \vee (a \wedge a_2) = (a_1 \vee a) \wedge (a_1 \vee a_2) = 1 \wedge (a_1 \vee a_2) = a_1 \vee a_2$

$\therefore a_1 = a_1 \vee a_2$...............(1)

Similarly, $a_2 = a_2 \vee 0 = a_2 \vee (a \wedge a_1) = (a_2 \vee a) \wedge (a_2 \vee a_1) = 1 \wedge (a_2 \vee a_1) = a_2 \vee a_1$

i.e. $a_2 = a_1 \vee a_2$..................(2)

From (1) and (2), $a_1 = a_2$ i.e. complement of every element is unique.

Complemented Lattice : A lattice $(P, \leq)$ is said to be complemented if it is bounded and every element in P has a complement.

For example : 1. $(D_6, \leq)$ is a complemented lattice, as it is bounded lattice with 1 as universal lower bound and 6 as universal upper bound. Moreover, $\bar{1} = 6$, $\bar{2} = 3$, $\bar{3} = 2$, $\bar{6} = 1$.

2. Let $X \neq \phi$, then $(P(X), \cup, \cap, \phi, X)$ is a complemented lattice since $\forall A \in P(X)$, $X - A(A^c)$ is the complement of A. Moreover, it is a bounded distributive lattice, therefore complement of every element is unique.

3. $(D_{12}, \leq)$ is not a distributive lattice. It is bounded with 1 as universal lower bound and 12

as universal upper bound. Moreover, $\bar{1} = 12$, $\bar{12} = 1$, $\bar{3} = 4$, $\bar{4} = 3$ but complement of 2 and 6 does not exist.

X Boolean Algebra : A complemented and distributive lattice is called a **Boolean Lattice**. An algebraic system $(B, \vee, \wedge, ')$ or $(B, +, \cdot, ')$ defined by the boolean lattice $(B, \leq)$ is known as a boolean algebra.

For example : 1. Let $X \neq \phi$, then $(P(X), \cup, \cap, ')$ is a boolean algebra.

2. $(D_{70}, \leq)$ is a boolean algebra.

Remarks : 1. A finite boolean algebra has exactly 2^n elements for some $n > 0$.

2. $a + b, a \cdot b \in B\ \forall a, b \in B$.

3. $a + b = b + a$ and $a \cdot b = b \cdot a\ \forall a, b \in B$.

4. $\exists 0, 1 \in B$ such that $a + 0 = 0$ and $a.1 = a\ \forall a, b \in B$.

5. $\forall a \in B\ \exists a' \in B$ such that $a + a' = 1$ and $a \cdot a' = 0$.

6. $\forall a, b, c \in B$, $a + (b \cdot c) = (a + b) \cdot (a + c)$ and $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

XI Laws of Boolean Algebra

Let $(B, +, \cdot, ')$ be a boolean algebra.

- **Idempotent Laws** : $a + a = a$ and $a \cdot a = a$, $\forall a \in B$.

  Proof : $a + a = (a + a) \cdot 1 = (a + a) \cdot (a + a') = a + (a \cdot a') = a + 0 = a$.

  Now, $a \cdot a = a \cdot a + 0 = a \cdot a + a \cdot \bar{a} = a \cdot (a + a') = a \cdot 1 = a$.

- **Absorption Laws** : $a + a \cdot b = a$, $a \cdot (a + b) = a\ \forall a, b \in B$.

  Proof : $a + a \cdot b = a \cdot 1 + a \cdot b = a \cdot (1 + b) = a \cdot 1 = a$.

  Now, $a \cdot (a + b) = a \cdot a + a \cdot b = a + a \cdot b$

- **Involution Law** : $(a')' = a$, $\forall a \in B$.

  Proof : Since $a' + a = 1$ and $a' \cdot a = 0$, $\therefore a$ is the complement of a'.

  Moreover, being a bounded distributive lattice, this complement is unique.

  Hence, $(a')' = a$.

- **De-Morgans's Laws** : $(a + b)' = a' \cdot b'$ and $(a \cdot b)' = a' + b'$, $\forall a, b \in B$.

Proof : To prove the first part, we prove that the complement of $a+b$ is $a' \cdot b'$ i.e. $(a+b)+(a' \cdot b') = 1$ and $(a+b) \cdot (a' \cdot b') = 0$.

Now, $(a+b)+(a' \cdot b') = (a+b+a') \cdot (a+b+a')$ $(\because (a+b \cdot c) = (a+b) \cdot (a+c))$,

$= (a+a'+b) \cdot (a+1) = (1+b) \cdot (a+1) = 1 \cdot 1 = 1$.

Now, $(a+b) \cdot (a' \cdot b') = a \cdot (a' \cdot b') + b \cdot (a' \cdot b')$, $(\because, (a+b) \cdot c = a \cdot c + b \cdot c)$,

$= (a \cdot a') \cdot b' + (b \cdot b') \cdot a' = 0 \cdot b' + 0 \cdot a' = 0 + 0 = 0$

$\therefore (a+b)' = a' \cdot b'$.

Similarly, we can prove the other part.

Problem : Reduce the following using boolean algebra :
(i) $((A \cdot B' + A \cdot B \cdot C)' + A \cdot (B + A \cdot B'))'$, (ii) $A \cdot B + A \cdot C' + A' \cdot B' \cdot C \cdot (A \cdot B + C)$
Solution : (i) $A \cdot (B + A \cdot B') = A \cdot (B+A) \cdot (B+B') = A \cdot ((B+A) \cdot 1)$
$= A \cdot (B+A) = A \cdot B + A \cdot A = A \cdot B + A \cdot 1 = A \cdot (B+1) = A \cdot 1 = A$,
i.e. $A \cdot (B + A \cdot B') = A$............(1)
Now, $A \cdot B' + A \cdot B \cdot C = A \cdot B' + A \cdot (B \cdot C) = A \cdot (B' + (B \cdot C)) = A \cdot (B'+B) \cdot (B'+C)$
$= (A \cdot 1) \cdot (B'+C) = A \cdot B' + A \cdot C$,
$\implies (A \cdot B' + A \cdot B \cdot C)' = (A \cdot B' + A \cdot C)' = (A \cdot B')' \cdot (A \cdot C)' = (A' + (B')') \cdot (A' + C')$
$= (A'+B) \cdot (A'+C') = A' + (B \cdot C')$,
i.e. $(A \cdot B' + A \cdot B \cdot C)' = A' + (B \cdot C')$.............(2)
Adding (1) and (2), we get
$A \cdot (B + A \cdot B') + (A \cdot B' + A \cdot B \cdot C)' = A + A' + (B \cdot C') = 1 + B \cdot C' = B + B' + B \cdot C'$
$= B' + B + B \cdot C' = B' + B \cdot (1 + C') = B' + B \cdot 1 = B' + B = 1$,
Hence, $(A \cdot (B + A \cdot B') + (A \cdot B' + A \cdot B \cdot C)')' = 1' = 0$
Try yourself for part (ii).

XII Boolean Expressions and Functions

Let $(B, \vee, \wedge, ')$ be a boolean algebra. Then, a boolean expression over $(B, \vee, \wedge, ')$ is defined as follows :

(i) Any element of B is a boolean expression.

(ii) Any variable name is a boolean expression.

(iii) If e_1 and e_2 are boolean expressions, then e_1', $e_1 \vee e_2$, $e_1 \wedge e_2$ etc. are also boolean expressions.

For example : $0 \vee x$, $((2 \wedge 3)' \vee (x_1 \vee x_2') \wedge (x_1 \wedge x_3)')$ are boolean expressions over the boolean algebra $(\{0, 1, 2, 3\}, \vee, \wedge, ')$.

Remark : A boolean expression that contains n distinct variables is known as boolean expression of n variables.

Assignment of Values : Let $E(x_1, x_2, ..., x_n)$ be a boolean expression of n variables over a boolean algebra $(B, \vee, \wedge, ')$. By an assignment of values to the variables $x_1, x_2, ..., x_n$, we mean an assignment of elements of B to the values of the variables.

For example : Consider the boolean expression $E(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (x_1' \vee x_2') \wedge (x_2 \vee x_3)'$ over boolean algebra $(\{0, 1\}, \vee, \wedge, ')$, then the assignment of values $x_1 = 0, x_2 = 1, x_3 = 0$ yields $E(0, 1, 0) = (0 \vee 1) \wedge (0' \vee 1') \wedge (1 \vee 0)' = 1 \wedge 1 \wedge 0 = 0$.

Equivalent Boolean Expressions : Two boolean expressions $E_1(x_1, x_2, ...x_n)$ and $E_2(x_1, x_2, ..., x_n)$ of n variables are said to be equivalent if they assume the same value for every assignment of values to the n variables. We write it as $E_1(x_1, x_2, ...x_n) = E_2(x_1, x_2, ..., x_n)$

For example : 1. $(x_1 \wedge x_2) \vee (x_1 \wedge x_3')$ and $x_1 \wedge (x_2 \vee x_3')$ are equivalent .

2. $f_1 = x_1 \vee (x_2 \vee x_3)$ and $f_2 = (x_1 \vee x_2) \vee x_3$ are equivalent over the boolean algebra $(\{0, 1\}, \vee, \wedge, ')$, as shown in the following table

x_1	x_2	x_3	$x_1 \vee x_2$	$x_2 \vee x_3$	f_1	f_2
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	1	0	1	1
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

Boolean Function : A boolean function from B^n to B is specified by a boolean expression $E(x_1, x_2, x_3, ..., x_n)$ (or we can say that boolean expression is closed form expression for specifying a boolean function). Let each assignment of values to the variables $x_1, x_2, x_3, ..., x_n$ be an ordered n-tuple in the domain B^n and let the corresponding value of $E(x_1, x_2, x_3, ..., x_n)$ be the corresponding image in the range B.

For example : Boolean expression $(x_1' \wedge x_2 \wedge x_3') \vee (x_1 \wedge x_2') \vee (x_1 \wedge x_3)$ over the boolean algebra $(\{0,1\}, \vee, \wedge, ')$ defines the following function f:

3-tuple	f
(0,0,0)	0
(0,0,1)	0
(0,1,0)	1
(0,1,1)	0
(1,0,0)	1
(1,0,1)	1
(1,1,0)	0
(1,1,1)	1

Note : 1. Every function from B^n to B is not specified with the help of boolean expression over $(B, \vee, \wedge, ')$.

For example : There is no boolean expression over the boolean algebra of four elements that defines the following boolean function :

2-tuple	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
f	1	0	0	3	1	1	0	3
2-tuple	(2,0)	(2,1)	(2,2)	(2,3)	(3,0)	(3,1)	(3,2)	(3,3)
f	2	0	1	1	3	0	0	2

2. A function from B^n to B is called a boolean function if it can be specified by a boolean expression of n-variables.

Min Term and Max Term Normal Forms : We explain the concept of disjunctive normal form (or min term normal form) and conjunctive normal form (or max term normal form) with the help of following example :

Consider the following expression of three variables : $f(x,y,z) = (\bar{x} \wedge z) \vee (y \wedge z) \vee (y \wedge \bar{z})$ over the boolean algebra $(\{0,1\}, \vee, \wedge, ')$, here 'bar' denotes the complement.

It can be simplified as : $f(x,y,z) = (\bar{x} \wedge z) \vee (y \wedge z) \vee (y \wedge \bar{z}) = (\bar{x} \wedge z) \vee [y \wedge (z \vee \bar{z})] = (\bar{x} \wedge z) \vee (y \wedge 1) = (\bar{x} \wedge z) \vee y$.

The simplified expression takes the following values for possible assignment of values to variables x, y, z:

x	y	z	$\bar{x}$	$\bar{x} \wedge z$	f
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	0	0	0
1	0	1	0	0	0
1	1	0	0	0	1
1	1	1	0	0	1

Now, $f = 1$ and $f = 0$ corresponds to min-terms and max-terms respectively. So min terms are $\bar{x} \wedge \bar{y} \wedge z$, $\bar{x} \wedge y \wedge \bar{z}$, $\bar{x} \wedge y \wedge z$, $x \wedge y \wedge \bar{z}$ and $x \wedge y \wedge z$. Now, max terms are $x \vee y \vee z$, $\bar{x} \vee y \vee z$ and $\bar{x} \vee y \vee \bar{z}$.

For writing the disjunctive normal form, we take the join of all the min-terms as :

$(\bar{x} \wedge \bar{y} \wedge z) \vee (\bar{x} \wedge y \wedge \bar{z}) \vee (\bar{x} \wedge y \wedge z) \vee (x \wedge y \wedge \bar{z}) \vee (x \wedge y \wedge z)$.

For writing the conjunctive normal form, we take the meet of all the max-terms as :

$(x \vee y \vee z) \wedge (\bar{x} \vee y \vee z) \wedge (\bar{x} \vee y \vee \bar{z})$.

Atom and Anti-atom : An element a is called an atom if it is an immediate successor of '0', i.e. $a \neq 0$ is an atom if $0 \leq b \leq a$, then either $b = 0$ or $b = a$. Similarly, an element a is called an anti-atom if it is an immediate predecessor of '1', i.e. $a \neq 1$ is an anti-atom if $a \leq b \leq 1$, then either $b = 1$ or $b = 1$.

For example : In $(D_{110}, \vee, \wedge, ')$ where $D_{110} = \{1, 2, 5, 10, 11, 22, 55, 110\}$, the atoms are 2,5,11 and anti-atoms are 10,22,55.

Sub-Algebra : Let $(B, +, \cdot, ')$ be a boolean algebra and $A \subseteq B$. Then $(A, +, \cdot, ')$ is called a sub-algebra of B if A itself is a boolean algebra.

For example : For the boolean algebra $(D_{70}, \vee, \wedge, ')$, the two sub -algebras are given by $A = \{1, 7, 10, 70\}$ and $B = \{1, 2, 35, 70\}$.

Isomophic Boolean Algebras : Two boolean algebras $(B, +, \cdot, ')$ and $(B', +, \cdot, ')$ are said to be isomorphic if there is one-one correspondence between them, i.e., there exists a bijective map $f : B \to B'$ such that $f(a + b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$ and $f(a') = (f(a))'$.

B.A. Part-III **OPT-III**

Semester-VI **Discrete Mathematics-II**

Lesson No. 2.3 **Author : Dr. Chanchal**

Propositional Calculus

I Proposition

II Compound Proposition

III Basic Logical Operations

IV Another Definition of Proposition

V Logical Equivalence

VI Laws of the Algebra of Propositions

VII Conditional and Bi-conditional Statements

VIII Principle of Duality

IX Argument

X Logical Implication

XI Propositional Function

XII Universal Quantifier

XIII Existential Quantifier

XIV Negation of Quantified Statements

I Proposition : A proposition (or statement) is a declarative sentence [1] which is either true or false but not both.

For example : It rains today (T or F but not both), I will go to college tomorrow (T or F but not both), Taj Mahal is in Delhi (F), 2+3=6 (F) are propositions whereas the sentences like

[1] It is a sensible combination of words

What time is it?, Please submit your report as soon as possible, May god bless you! are not the propositions as these are not declarative in nature.

Remarks:

1. A proposition is denoted with the help of letters (small or capital) like p, q, P, Q etc.

2. A proposition that is true under all circumstances is referred to as a **Tautology** but a proposition which is false under all circumstances is referred to as a **Contradiction**.

3. The area of logic which deals with propositions is known as **Propositional Calculus**.

II Compound Proposition: A proposition whose nature (T or F) does not explicitly depend upon another propositions is called a simple proposition. But many propositions are composite in nature i.e. these are composed of sub-propositions and various connectives and such propositions are called compound propositions. The simple propositions which are used to make compound propositions are called **components**.The phrases or words which connect two simple propositions are called logical connectives or simply connectives. Some of the connectives are : and, or, not, if then, if and only if. Now, to show the truth values of a compound statement, we draw a table known as **truth table** consisting of rows and columns. The number of columns depend upon the number of simple propositions and how their relationships are involved while the number of rows depend only upon the number of simple propositions. If there are n simple propositions, then the no. of rows is 2^n.

III Basic Logical Operations : Firstly, we discuss three basic logical operations viz. Conjunction ($\wedge$), Disjunction ($\vee$) and Negation ($\sim$).

Conjunction : Any two propositions p and q can be combined by the word 'and' to form a compound proposition called the conjunction of the original propositions. Symbolically, $p \wedge q$ read as 'p and q' denotes conjunction of p and q. If p and q are true, then $p \wedge q$ is true otherwise it is false. The truth table is as shown below:

For example : 1. Let $p : 3 + 5 = 8$ and $q = 3$ is an even number, then $p \wedge q : 3 + 5 = 8$and 3 is an even number. Now p is true but q is false, so $p \wedge q$ is false.

2. Let p : Every even number is divisible by 2 and q : 5 is a prime number, then $p \wedge q$: Every even number is divisible by 2 and 5 is a prime number. Here, p and q both are true, so $p \wedge q$ is also true.

Disjunction : Any two propositions p and q can be combined by the word 'or' to form a compound proposition called the disjunction of the original propositions. Symbolically, $p \vee q$

Table 1: $p \wedge q$

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

read as 'p or q' denotes disjunction of p or q. If p and q both are false, only then $p \vee q$ is false otherwise it is true. The truth table is as shown below:

Table 2: $p \vee q$

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

For example : 1. Let $p : 3 + 5 = 8$ and $q = 3$ is an even number, then $p \vee q : 3 + 5 = 8$ or 3 is an even number. Now p is true but q is false, so $p \vee q$ is true.
2. Let p : Every even number is divisible by 3 and q : 4 is a prime number, then $p \vee q$: Every even number is divisible by 3 or 4 is a prime number. Here, p and q both are false, so $p \vee q$ is also false.

Negation : Given any proposition p, another proposition called the negation of p, can be formed by writing 'It is not the case that' or 'It is false that' before p or, if possible by inserting in p the word 'not'. Symbolically, $\sim p$ read 'not p' denotes negation of p. If p is true, $\sim p$ is false and vice versa, as shown in the table below:
For example : 1. Let p : He is a good student. Then $\sim p$: It is not the case that he is a good student or It if false that he is a good student or He is not a good student.

IV Another Definition of Proposition : Let $P(p, q, ...)$ denote an expression constructed from logical variables $p, q, ...$ which take on the value true (T) or false (F), and the logical

Table 3: $\sim p$

p	$\sim p$
T	F
F	T

connectives $\wedge, \vee$ and $\sim$. Such an expression $P(p.q, ...)$ will be called a proposition. Moreover, its truth value depends exclusively upon the truth values of its variables. For example : If P is $p \wedge q$, then its truth value depends upon the truth values of p and q.

Tautology : Some propositions $P(p, q, ...)$ contain only T in the last column of their truth table i.e. they are true for any truth values of their variables. Such propositions are called tautologies. Similarly, the propositions $P(p, q, ...)$ which are false for any truth values of their variables i.e. contain only F in the last column of their truth table, are called contradictions. For example : $p \vee \sim p$ is a tautology and $p \wedge \sim p$ is a contradiction, as shown below:

Table 4: $p \vee \sim p$, $p \wedge \sim p$

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
T	F	T	F
F	T	T	F

V Logical Equivalence : Two propositions $P(p, q, ...)$ and $Q(p, q, ...)$ are said to be logically equivalent or simply equivalent or equal, denoted by $P(p, q, ...) \equiv Q(p, q, ...)$, if they have identical truth tables.

For example : $\sim (p \wedge q) \equiv \sim p \vee \sim q$ as shown in the table below :

Let p : Roses are red, q : Violets are blue, then $\sim p \wedge \sim q$: Roses are not red and violets are not blue and $\sim (p \vee q)$: It is not the case that roses are red or violets are blue.

VI Laws of the Algebra of Propositions

1. **Idempotent Laws** : $p \vee p \equiv p$ and $p \wedge p \equiv p$

2. **Associative Laws** : $p \vee (q \vee r) \equiv (p \vee q) \vee r$ and $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

3. **Commutative Laws** : $p \vee q \equiv q \vee p$ and $p \wedge q \equiv q \wedge p$

Table 5: $\sim(p \wedge q) \equiv \sim p \vee \sim q$

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$	$\sim p \vee \sim q$
T	T	F	F	T	F	F
T	F	F	T	F	T	T
F	T	T	F	F	T	T
F	F	T	T	F	T	T

4. **Distributive Laws** : $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ and $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

5. **Identity Laws** : $p \vee F \equiv p$ and $p \wedge T \equiv p$

6. **Negation Laws** : $p \vee \sim p \equiv T$ and $p \wedge \sim p \equiv F$, $\sim T \equiv F$ and $\sim F \equiv T$

7. **Involution Law** : $\sim(\sim p) \equiv p$

8. **De-Morgan's Laws** : $\sim(p \wedge q) \equiv \sim p \vee \sim q$ and $\sim(p \vee q) \equiv \sim p \wedge \sim q$

Here T (or 0) refers to tautology and F (or 1) refers to contradiction. All the above mentioned laws can be proved very easily with the help of truth tables. For reference, see the proof of negation laws in table 4 and the proof of De-Morgan's laws in table 5.

VII Conditional and Bi-conditional Statements : Let p and q be the propositions. Then the compound statement symbolically written as '$p \to q$' read as 'If p then q' or 'p implies q' or 'p only if q', is known as the conditional statement. Here p is called the hypothesis and q is called the conclusion. Moreover, $p \to q$ is true if p is false or q is true or both and it is false if the hypothesis i.e. p is true but the conclusion q is false. If $p \to q$ is the conditional statement, then $q \to p$ is called its converse, $\sim p \to \sim q$ is called its inverse and $\sim q \to \sim p$ is called its contrapositive.

Now, the compound statement symbolically written as '$p \leftrightarrow q$' read as 'p if and only if q' stated as 'p is a NASC for q', is known as the biconditional statement. This biconditional statement is true if either p and q both true or false, and is false otherwise. The truth tables are as shown below:

It is clear from the above table that $p \to q$ and $\sim q \to \sim p$ are logically equivalent. Similarly, $q \to p$ and $\sim p \to \sim q$ are logically equivalent.

Table 6: Conditional and Bi-conditional Statements

p	q	$\sim p$	$\sim q$	$p \to q$	$q \to p$	$\sim p \to \sim q$	$\sim q \to \sim p$	$p \leftrightarrow q$
T	T	F	F	T	T	T	T	T
T	F	F	T	F	T	T	F	F
F	T	T	F	T	F	F	T	F
F	F	T	T	T	T	T	T	T

For example : 1. Let $p : 3+5=8$ and $q = 3$ is an even number, then $p \to q : If 3+5=8$ then 3 is an even number and $p \leftrightarrow q$: 3+5=8 iff 3 is an even number. Now p is true but q is false, so $p \to q$ is false and $p \leftrightarrow q$ is also false.
2. Let p : Every even number is divisible by 2 and q : 3 is a prime number, then $p \to q$: If every even number is divisible by 3 then 3 is a prime number and $p \leftrightarrow q$: Every even number is divisible by 3 iff 3 is a prime number . Here, p and q both are true, so $p \to q$ and $p \leftrightarrow q$ are also true.
NOTE: Any two propositions P(p,q,...) and Q(p,q,.....) are equivalent if $P \leftrightarrow Q$ is a tautology.

VIII Principle of Duality : Let S be a statement which is a tautology, then the statement formed by interchanging $\wedge$ with $\vee$, $\vee$ with $\wedge$, 0 with 1, 1 with 0, called dual of S denoted by S^* is also a tautology.
For example : 1. Dual of $p \vee 0 = p$ is $p \wedge 1 = p$ and both are tautologies.
2. Dual of $\sim (p \wedge q) \equiv \sim p \vee \sim q$ is $\sim (p \vee q) \equiv \sim p \wedge \sim q$ and both are true i.e. tautologies.

IX Argument : An argument is an assertion that a given set of propositions $P_1, P_2, ..., P_n$, called premises yield another proposition Q (called the conclusion). Such an argument is denoted by $P_1, P_2, ...P_n \vdash Q$. An argument $P_1, P_2, ...P_n \vdash Q$ is said to be valid or logical or true, if Q is true whenever all the premises the true otherwise the argument is not valid and it is called a fallacy.
For example : The argument (i) $p, p \to q \vdash q$ (known as the law of detachment) is a valid argument whereas the argument (ii) $p \to q, q \vdash p$ is a fallacy. See the following truth table :
The premises p and $p \to q$ are true only in the first row and the conclusion q is also true. So, argument (i) is valid. For argument (ii), the premises $p \to q$ and q are true in first row and

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

third row, but the conclusion p is not true for both. So, argument (ii) is a fallacy.

Remark : The propositions $P_1, P_2, ..., P_n$ are true simultaneously iff the proposition $P_1 \wedge P_2 \wedge P_3 .... \wedge P_n$ is true. Therefore, the argument $P_1, P_2, ...P_n \vdash Q$ is valid iff Q is true whenever $P_1 \wedge P_2 \wedge P_3 .... \wedge P_n$ is true or iff $(P_1 \wedge P_2 \wedge P_3 ..... \wedge P_n) \to Q$ is a tautology.

For example : Let us prove the validity of the argument : If p implies q and q implies r, then p implies r i.e. $p \to q, q \to r \vdash p \to r$. To prove the validity, it is sufficient to show that $[(p \to q) \wedge (q \to r)] \to (p \to r)$ is a tautology. The following table 7 proves for the same.

Table 7: Validity of $p \to q, q \to r \vdash p \to r$

p	q	. r	$p \to q$	$q \to r$	(i) $p \to r$	(ii) $(p \to q) \wedge (q \to r)$	(ii) $\to$ (i)
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

On similar lines, we can prove the argument :

P_1 : If a man is bachelor, he is unhappy.

P_2 : If a man is unhappy, he dies young.

Q : Bachelors die young.

Let p : He is bachelor, q : He is unhappy, r : He dies young.

So, the argument is $p \to q, q \to r \vdash p \to r$ and the above table proves the same.

X Logical Implication: A proposition $P(p, q, ...)$ is said to logically imply a proposition $Q(p, q, ...)$ written as $P(p, q, ...) \implies Q(p, q.......)$ if $Q(p, q, ...)$ is true whenever $P(p, q, ...)$ is true, or in other words $P(p, q, ...) \to Q(p, q.......)$ is a tautology.

For example : p logically implies $p \vee q$ as $p \vee q$ is true whenever p is true (see table 2).

Remark : $Q(p, q, ...)$ is true whenever $P(p, q, ...)$ is true, so the argument $P(p, q, ...) \vdash Q(p, q, ...)$ is valid and conversely. Or we can say that $P \vdash Q$ is valid iff the conditional statement $P \to Q$ is always true i.e. a tautology. The following result holds :

For any propositions $P(p, q, ...)$ and $Q(p, q, ...)$, the following statements are equivalent:

(a) $P(p, q, ...)$ logicallly implies $Q(p, q, ...)$.

(b) The argument $P(p, q, ...) \vdash Q(p, q, ...)$ is valid.

(c) The conditional statement $P(p, q, ...) \to Q(p, q, ...)$ is a tautology.

XI Propositional Function : Let A be the given non-empty set. A propositional function defined on A is an expression $p(x)$, which has the property that $p(a)$ is true or false for $a \in A$ i.e. it becomes a statement whenever $x \in A$. The set A is called domain of $p(x)$ and the set T_p of all those elements of A for which $p(a)$ is true is called truth set of $p(x)$. Mathematically, $T_p = \{x : x \in A \text{ and } p(x) \text{ is true}\}$.

For example : Let the domain set A be $\mathbb{N}$.

(i) Let $p(x)$ be '$x + 2 > 7$', then $T_p = \{x : x \in \mathbb{N} \text{ and } x + 2 > 7\} = \{6, 7, 8, ...\}$.

(ii) Let $p(x)$ be '$x + 5 < 3$', then $T_p = \{x : x \in \mathbb{N} \text{ and } x + 5 < 3\} = \phi$.

(iii) Let $p(x)$ be '$x + 5 > 1$', then $T_p = \{x : x \in \mathbb{N} \text{ and } x + 5 > 1\} = \mathbb{N}$.

Remarks : If $p(x)$ is a propositional function defined on the set A, then

(i) $p(x)$ can be true for all $x \in A$ ($T_p = A$), for some $x \in A$ ($T_p \subset A$) or for no $x \in A$ ($T_p = \phi$).

(ii) $\sim p(x)$ is true iff $p(x)$ is false (i.e. $a \in T_p^c$ iff $a \notin T_p$).

(iii) $p(x) \wedge q(x)$ is true whenever $p(x)$ is true and $q(x)$ is true (i.e. $a \in T_p \cap T_q$ iff $a \in T_p$ and $a \in T_q$).

(iv) $p(x) \vee q(x)$ is true whenever either $p(x)$ is true or $q(x)$ is true (i.e. $a \in T_p \cup T_q$ iff $a \in T_p$ or $a \in T_q$).

(v) De-Morgan's Laws for Propositional Functions : $\sim (p(x) \wedge q(x)) \equiv (\sim p(x)) \vee (\sim q(x))$, $\sim (p(x) \vee q(x)) \equiv (\sim p(x)) \wedge (\sim q(x))$ (i.e.$(T_p \cap T_q)^c = T_p^c \cup T_q^c$, $(T_p \cup T_q)^c = T_p^c \cap T_q^c$).

XII Universal Quantifier : Let $p(x)$ be a propositional function defined on the set A. Consider the expression $(\forall x \in A)p(x)$ or $\forall x, p(x)$, which reads 'For every x in A, $p(x)$ is a true statement'. The symbol $\forall$ which reads 'for all' is known as the universal quantifier.

It is equivalent to $T_p = \{x : x \in A, p(x) \text{ is true }\} = A$.

For example : (i) The proposition $(\forall n \text{ in } \mathbb{N})(n+4 > 3)$ is true,$\because T_p = \{n : n \in \mathbb{N}, n+4 > 3\} = \mathbb{N}$.

(ii) The proposition $(\forall n \text{ in } \mathbb{N})(n+2 > 8)$ is false, $\because T_p = \{n : n \in \mathbb{N}, n+2 > 3\} = \{7, 8, ...\} \neq \mathbb{N}$.

XIII Existential Quantifier : Let $p(x)$ be a propositional function defined on the set A. Consider the expression $(\exists x \in A)p(x)$ or $\exists x, p(x)$, which reads 'There exists an x in A such that $p(x)$ is a true statement'. The symbol $\exists$ which reads 'there exists' of 'for some' or 'for atleast one' is known as the existential quantifier.

It is equivalent to $T_p = \{x : x \in A, p(x) \text{ is true }\} \neq \phi$.

For example : (i) The proposition $(\exists n \text{ in } \mathbb{N})(n + 4 < 7)$ is true,$\because T_p = \{n : n \in \mathbb{N}, n + 4 > 7\} = \{1, 2\} \neq \phi$.

(ii) The proposition $(\exists n \text{ in } \mathbb{N})(n + 6 < 4)$ is false, $\because T_p = \{n : n \in \mathbb{N}, n + 6 < 4\} = \phi$.

XIV Negation of Quantified Statements : We understand this concept with the help of examples.

(i) Let the statement be 'All math majors are males'. Its negation is 'It is not the case that all math majors are males' or 'There exists atleast one math major who is not a male.' Now, we write it in the form of quantifiers:

Let M be the set of math majors.

$\therefore \sim (\forall x \in M)$ (x is male) $\equiv (\exists x \in M)$ (x is not male).

or $\sim (\forall x \in M)\ p(x) \equiv (\exists x \in M)\ (\sim p(x))$, where $p(x) : x$ is male.

Similarly, $\sim (\exists x \in M)\ p(x) \equiv (\forall x \in M)\ (\sim p(x))$

NOTE : The above statements are known as De-Morgan's laws.

(ii) Let the statement be 'For all positive integers n, we have $n + 2 > 8$. Its negation is 'There exists a positive integer n such that $n + 2 \not> 8$.

Exercise Set

1. Prove that : (i) $p \to q \equiv (\sim p) \vee q$, (ii) $\sim (p \to q) \equiv p \wedge (\sim q)$.

2. Write the following statements in symbolic form and give their negations :

   (i) If you work hard, you will get the first devision.

   (ii) If it rains, he will not go to school.

3. Prove that $p \to (q \wedge r) \equiv (p \to q) \wedge (p \to r)$.

4. Prove that $p \leftrightarrow q \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$.

5. Prove that $\{[(p \to q) \vee p] \wedge q\} \to q$ is a tautology.

6. State the converse, inverse and contrapositive of the following implications :

   (i) If $4x - 2 = 10$, then $x = 3$.

   (ii) If it snows tonight, then I will stay at home.

7. Test the validity of following arguments :

   (i) It it rains, then crop will be good. It did not rain. Therefore, the crop will not be good.

   (ii) If I work, I cannot study. Either I work or pass Mathematics. I passed Mathematics. Therefore, I studies.

8. Over the Universe of positive integers :

   $p(n)$: n is prime and $n < 32$.

   $q(n)$: n is a power of 3.

   $r(n)$: n is a divisor of 27.

   (a) What are the truth sets of these propositions?

   (b) Which of the three propositions implies one of the others?

9. Use quantifier to say that $\sqrt{5}$ is not a rational number.

10. Let $C(x)$ be 'x is cold blooded. Let $F(x)$ be 'x is a fish and let $S(x)$ be 'x lives in the sea'.

    Translate into a formula : Every fish is cold blooded.

    Translate into English : $(\exists x)(S(x) \wedge \sim F(x))$ and $(\forall x)(F(x) \to S(x))$.