DIRECTORATE OF DISTANCE EDUCATION
UNIVERSITY OF NORTH BENGAL

MASTER OF SCIENCES- MATHEMATICS

SEMESTER -III

DISCRETE MATHEMATICS

DEMATH3OLEC4

BLOCK-2

UNIVERSITY OF NORTH BENGAL

Postal Address:

The Registrar,

University of North Bengal,

Raja Rammohunpur,

P.O.-N.B.U., Dist-Darjeeling,

West Bengal, Pin-734013,

India.

Phone: (O) +91 0353-2776331/2699008

Fax: (0353) 2776313, 2699001

Email: regnbu@sancharnet.in ; regnbu@nbu.ac.in

Wesbsite: www.nbu.ac.in

First Published in 2019

This book is meant for educational and learning purpose. The authors of the book has/have taken all reasonable care to ensure that the contents of the book do not violate any existing copyright or other intellectual property rights of any person in any manner whatsoever. In the even the Authors has/ have been unable to track any source and if any copyright has been inadvertently infringed, please notify the publisher in writing for corrective action

FOREWORD

The Self Learning Material (SLM) is written with the aim of providing simple and organized study content to all the learners. The SLMs are prepared on the framework of being mutually cohesive, internally consistent and structured as per the university’s syllabi. It is a humble attempt to give glimpses of the various approaches and dimensions to the topic of study and to kindle the learner’s interest to the subject

We have tried to put together information from various sources into this book that has been written in an engaging style with interesting and relevant examples. It introduces you to the insights of subject concepts and theories and presents them in a way that is easy to understand and comprehend.

We always believe in continuous improvement and would periodically update the content in the very interest of the learners. It may be added that despite enormous efforts and coordination, there is every possibility for some omission or inadequacy in few areas or topics, which would definitely be rectified in future.

We hope you enjoy learning from this book and the experience truly enrich your learning and help you to advance in your career and future endeavours.

DISCRETE MATHEMATICS

BLOCK-1

BLOCK-2

BLOCK 2- DISCRETE MATHEMATICS

Important areas in applied mathematics include linear programming, coding theory, theory of computing. The mathematics in these applications is collectively called discrete mathematics. One of the first things you learn in mathematics is how to count.

Graphs are mathematical structures that have many applications to computer science, electrical engineering and more widely to engineering as a whole, but also to sciences such as biology, linguistics, and sociology, among others. For example, relations among objects can usually be encoded by graphs. Whenever a system has a notion of state and state transition function, graph methods may be applicable. Certain problems are naturally modeled by undirected graphs whereas others require directed graphs

UNIT 8: COMBINATROICS – I

STRUCTURE

8.0 OBJECTIVES

Understand the addition and product rule. How to apply it.

Understand the concept of permutation and combination

Enumerate the concept of solution of non-negative integers

8.1 INTRODUCTION

Combinatorics can be traced back more than 3000 years to India and China. For many centuries, it primarily comprised the solving of problems relating to the permutations and combinations of objects. The use of the word “combinatorial” can be traced back to Leibniz in his dissertation on the art of combinatorial in 1666. Over the centuries, combinatorics evolved in recreational pastimes.
These include the K¨onigsberg bridges problem, the four-colour map problem, the Tower of Hanoi, the birthday paradox and Fibonacci’s ‘rabbits’ problem.

8.2 ADDITION AND MULTIPLICATION RULES

Example: Let the cars in New Delhi have license plates containing 2 alphabets followed by two numbers. What is the total number of license plates possible?

Solution: Here, we observe that there are 26 choices for the first alphabet and another 26 choices for the second alphabet. After this, there are two choices for each of the two numbers in the license plate. Hence, we have a maximum of 26 × 26 × 10 × 10 = 67, 600 license plates.

Example: Let the cars in New Delhi have license plates containing 2 alphabets followed by two numbers with the added condition that “in the license plates that start with a vowel the sum of numbers should always be even”. What is the total number of license plates possible?

Solution: Here, we need to consider two cases.
Case 1**:** The license plate doesn’t start with a vowel. Then using the previous example, the number of license plates equals 21 × 26 × 10 × 10 = 54600.
Case 2**:** The license plate starts with a vowel. Then the number of license

plates equals

$5 \times 26 \times (5 \times 5 + 5 \times 5) = 6500.$

Hence, we have a maximum of 54600 + 6500 = 61100 license plates.

1. **[Multiplication/Product rule]** If a task consists of n *compulsory* parts and the i-th part can be completed in m_i ways, $i = 1, 2, . . . , n$, then the task can be completed in $m_1 m_2 \cdots m_n$ ways.

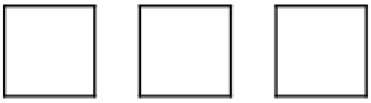
2. **[Addition rule]** If a task consists of n *alternative* parts, and the i-th part can be completed in m_i ways, $i = 1, . . . , n$, then the task can be completed in $m_1 + m_2 + \cdots + m_n$ ways.

Example: A] How many three digit natural numbers can be formed using digits $0, 1, \cdots , 9$?

Identify the number of parts in the task and the type of the parts (compulsory or alternative).

Which rule applies here?

Solution: The task of forming a three digit number can be viewed as filling three boxes kept in a horizontal row.



There are three compulsory parts.

Part 1: choose a digit for the leftmost place.

Part 2: choose a digit for the middle place.

Part 3: choose a digit for the rightmost place.

Multiplication rule applies i.e. $9 \times 10 \times 10$.

B] How many three digit natural numbers with distinct digits can be formed using digits 1, · · · , 9

such that each digit is odd or each digit is even? Identify the number of parts in the task and

the type of the parts (compulsory or alternative). Which rule applies here?

Solution : The task has two alternative parts.

Part 1: form a three digit number with distinct digits using digits from {1, 3, 5, 7, 9}. Using multiplication rule, that can be done in 5 × 4 × 3 ways

Part 2: form a three digit number with distinct digits using digits from {2, 4, 6, 8}. Observe that Part 1 is a task having three compulsory subparts. So, it can be done in 4 × 3 × 2 ways. Since our task has alternative parts, addition rule applies. **i.e. (**5 × 4 × 3**) +(**4 × 3 × 2**) = 84**

NOTE: There is another way to formulate the above rules. Let *Ai* be the set of all possible

ways in which the *i*-th part can be completed. In this setting, the multiplication rule can be re-written as: *if* $A_1, A_2, \ldots, A_n$ *are nonempty finite sets, then* $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$.

For the addition rule, note that, as the completion of one part does not result in the completion of any other part, $A_1, A_2, \ldots, A_n$ are disjoint. Thus, the addition rule can be re-written as: *if* $A_1, A_2, \ldots, A_n$ *are disjoint, nonempty finite sets, then* $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$

8.3 PERMUTATIONS AND COMBINATIONS

8.3.1 Counting Words Made With Elements Of A Set S

The first fundamental combinatorial object one commonly studies is a function $f : [k] \to S$. The set of all functions from A to B will be denoted by Map (A, B).

Discussion:

1. Let $k \in$ N and let $f \in$ Map ([k], S). Then, we may view f as the ordered k-tuple (f(1), . . . , f(k)). Thus f is an element of $S^k = S \times S \times \cdots \times S$, k times.

2. Consider an ordered k-tuple (x_1, x_2, . . . , x_k) of elements of X. If we remove the brackets and the commas, then what we get is $x_1x_2 \ldots x_k$, which is called a **word** of length k made with elements of X. Thus, the word corresponding to the tuple (a, a, b) is aab.

3. Consider a function f : [3] → {a, b, . . . , z}, defined by f(1) = a, f(2) = a and f(3) = b.

Technically, f = {(1, a), (2, a), 3, b)} and the ordered tuple it gives is (a, a, b) and the word related to it is aab. Because of this natural one-one correspondence, people use them interchangeably.

8.3.1 Theorem

Let n, r $\in$ N *be fixed. Then* |Map([n], [r])| = *rn.*

Proof. Forming such a function is a task with n compulsory parts, where each part can be done in r many ways. So, by the product rule, the number of such functions is rn.

Example: 1. How many functions are there from [9] to [12]?

Ans: $12^{9.}$ This task has 9 compulsory parts, where is each part can be done in 12 ways.

Discussion: [Use of complements] A simple technique which is used very frequently is counting the complement of a set, when we know the size of the whole set. For example, consider the following question.

Example: How many 5-letter words can be made using the letters *A*, *B*, *C*, *D* that do not contain the string "ADC"? For example, *ADCDD*, *BADCB* are not counted but *DACAD* is counted.

Solution: Let X be the set of all 5-letter words that can be made using A, B, C, D. Then $|X| = 45$.

Consider the sets $A = \{$words in X of the form $ADC * *\}$, $B = \{$words in X of the form $*ADC*\}$, and $C = \{$words in X of the form $* *ADC\}$. We see that $|A| = |B| = |C| = 4^2$. As the sets A, B, C are disjoint, we see that $|A \cup B \cup C| = 3 \times 4^2$.

Hence our answer to the original question is $4^5 - 3 \times 4^2$.

8.3.2 Counting Words With Distinct Letters Made With Elements Of A Set *S:*

We now discuss the next combinatorial object namely the one-one functions. For $n \in \mathrm{N}$, the term ***n*-set** is used for 'a set of size n'. Further, $n! = 1 \cdot 2 \cdot \cdots \cdot n$ and by convention, $0! = 1$.

Discussion. [Injections] Let $n, r \in \mathrm{N}$ and X be a non-empty set.

1. An injection $f : [r] \to X$ can be viewed as an ordered r-tuple of elements of X with distinct entries. It can also viewed as a word of length r with distinct letters made with elements of X.
The set of all injections from A to B will be denoted by $\mathrm{Inj}(A, B)$.

2. If $|X| = r$, then a bijection $f : X \to X$ is called a **permutation** of X. If $\mathrm{X} = \{\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{r}\}$, then $f(x_1), \ldots, f(x_r)$ is just a rearrangement of elements of X.

3. We define $\mathbf{P}(\mathbf{n}, \mathbf{r}) := |\mathrm{Inj}([r], [n])|$. As a convention, $P(n, 0) = 1$ for $n \geq 0$.

Example: How many one-one maps $f : [4] \rightarrow \{A, B, . . . , Z\}$ are there?

Solution: The task of forming such a one-one map has 4 compulsory parts: selecting $f(1)$, $f(2)$, $f(3)$ and $f(4)$.

Further, $f(2) \neq f(1)$, $f(3) \neq f(1)$, $f(2)$ and so on.

So, by the product rule, the number of one-one map equals $26 \cdot 25 \cdot 24 \cdot 23 = 26!\ 22!$

8.3.3 Theorem [Number of injections]

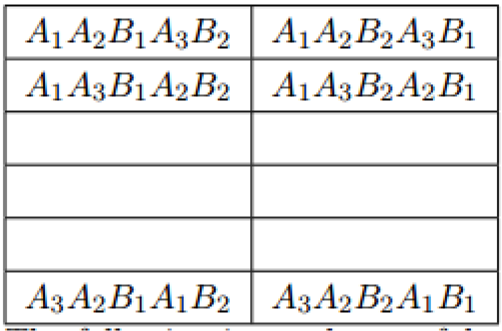
$f : [r] \rightarrow S$**]** *Let* $n, r \in \mathrm{N}$ *and* $|S| = n$. *Then the number* $P\ (n, r) = (n - n!r)!$.

Proof. The task is to from an r-tuple $(f(1), . . . , f(r))$ of distinct elements. It has r compulsory parts, namely selecting $f(1)$, $f(2)$, . . ., $f(r)$ with the condition that $f(k) \notin \{f(1), f(2), . . . , f(k - 1)\}$, for $2 \leq k \leq r$.

So, using the product rule, $P\ (n, r) = |\mathrm{Inj}\ ([r], [n])| = n(n - 1) \cdots (n - r + 1) = (n - n!r)!$.

8.3.4 Counting Words Where Letters May Repeat

Consider the word *AABAB*. We want to give subscripts 1, 2, 3 to the *A*'s and subscripts 1, 2 to the *B*'s so that we create words made with A_1, A_2, A_3, B_1, and B_2. For example, one such word is $A_2A_3B_2A_1B_1$. How many such words can we create? Fill the following table to get all such words. Notice that each of these words become *AABAB* when we erase the subscripts.



$A_1A_2B_1A_3B_2$	$A_1A_2B_2A_3B_1$
$A_1A_3B_1A_2B_2$	$A_1A_3B_2A_2B_1$
$A_3A_2B_1A_1B_2$	$A_3A_2B_2A_1B_1$

Proposition [Principle of disjoint pre-images of equal size] *Let A, B be nonempty finite sets*

and $f : A \to B$ be a function satisfying $|f^{-1}(i)| = k = |f^{-1}(j)|$, for each i, $j \in B$. Then, $|A| = k|B|$.

In particular, for $k = 1$ this principle is also called the principle of bijection.

Let $n_1, \ldots, n_k \in$ N. Suppose, we are given *ni* copies of the symbol *Ai*, for $i = 1, \ldots, k$. Then, by

an **arrangement** of these $n_1 + \cdot \cdot\cdot + n_k$ symbols, we mean a way of placing them in a row. It is a

word made with the symbols $A_1, \ldots, A_k$ containing the symbol *Ai* exactly *ni* times, $i = 1, \ldots, k$. For example, *ABBAA* is an arrangement of 3 copies of *A* and 2 copies of *B*.

Example: How many words of size 5 can be formed using three *A*'s and two *B*'s?

Solution: Let $A = \{$arrangements of $A_1, A_2, A_3, B_1, B_2\}$ and $B = \{$words of size 5 which use three

A's and two *B*'s$\}$. For each arrangement $a \in A$, define $Er(a)$ to be the word in *B* obtained by

erasing the subscripts. Then, the function $Er : A \to B$ satisfies:

'for each $b, c \in B, b \neq c$, we have $|Er-1(b)| = |Er-1(c)| = 3!2!$'.

Thus, by Proposition **[Principle of disjoint pre-images of equal size]**,

$|B| = \frac{|A|}{3!2!} = \frac{5!}{3!2!}$

Example: Determine the number of ways to place 4 couples in a row if each couple sits together.

Solution: Let *X* be the set of all arrangements of *A, B, C, D*. Let *Y* be the set of all arrangements

of *A, A, B, B, C, C, D, D* in which both the copies of each letter are together.

For example *AACCDDBB* $\in Y$ but *ABBCCDDA* $\notin Y$.

Let Z be the set of all arrangements of Ah, Aw, Bh, Bw, Ch, Cw, Dh, Dw in which Ah, Aw are together, Bh, Bw are together, Ch, Cw are together, and Dh, Dw are together.

In this setting, we need to find the size of Z.

So, define $Er : Z \rightarrow Y$ by $Er(z)$ equals the arrangement obtained by erasing the subscripts, namely h and w, that appear in z.

Note that each $y \in Y$ has 24 pre-images in Z.

Now, define $Mrg : Y \rightarrow X$ by $Mrg(y)$ equals the arrangement obtained by merging the two copies of the same letters into one single letter.

For example, $Mrg(BBAADDCC) = BADC$.

Note that each x in X has exactly one preimage in Y. By applying the principle of disjoint pre-images of equal size twice, we see that

$$|Z| = 2^4|Y| = 2^4|X| = 2^4 4!, \text{ as } |X| = 4!.$$

8.3.5 Theorem [Arrangements]

Let $n, n_1, n_2, \ldots, n_k \in$ N and suppose that we have ni copies of the symbol (object) Ai, for i = 1, . . . , *k and that n* = *n*1 + · · · + *nk. Then the number of arrangements of these n symbols is*

$$\frac{n!}{n_1!\, n_2! \ldots n_k!}$$

The formula remains valid even if we take some of the ni's to be 0.

Proof. Let S be set of all arrangements of the $n_1 + n_2 + \cdots + n_k$ symbols and let T be the set of

all arrangements of the symbols $A_{1,1}, \ldots, A_{1,n1}, A_{2,1}, \ldots, A_{2,n2}, \ldots, A_{k,1}, \ldots, A_{k\,,nk}$.

Define a function $E_r : T \rightarrow S$ by $Er(t)$ equals the arrangement obtained by erasing the second subscripts that appear in t. Notice that each $s \in S$ has $n_1!n_2! \cdots n_k!$ many pre-images. Hence, by the principle of disjoint pre-images of equal size, we have $|T| = n_1! \cdots n_k!|S|$. As $|T| = (n_1 + n_2 + \cdots + n_k)!$, we obtain the desired result.

Assume that some n_i's are 0 (all cannot be 0 as $n \in$ N). Then our arrangements do not involve the

corresponding *Ai*'s. Hence we can use the argument in the previous paragraph and get the number of arrangements. As 0! = 1, we can insert some 0! in the denominator.

Corollary

Let m, n $\in$ N. *Then the number of arrangements of m copies of A and n copies of B is*

$$\frac{(m+n)!}{m!\,n!}$$

8.3.4 Counting Subsets:

As an immediate application of Corollary **8.3.4**, we have the following result which counts the number of subsets of size *k* of a given set *S*.

Theorem

Let n $\in$ N *and k* $\in$ *{*0, 1, . . . , *n}. Then the number of subsets of* [*n*] *of size k is*

$\frac{n!}{k!(n-k)!.}$.

Proof. If $k = 0$ or n, then we know that there is only one subset of size k and the formula also gives us the same value.

So, let $1 \leq k \leq n - 1$ and let X be the set of all arrangements of k copies of T 's and $n - k$ copies of F 's.

For an arrangement $x = x_1x_2 \ldots x_n \in X$, define $f(x_1 \ldots x_n) = \{i \mid x_i = T\}$, *i.e.*, the set of positions where a *T* appears in *x*. Then, *f* is a bijection between *X* and the set of all *k*-subsets of [*n*]. Hence, the number of *k*-subsets of [*n*] = |*X*| = |*X*| = $\frac{n!}{k!(n-k)!.}$.by **Corollary**

<u>Discussion:</u>

1. For $n \in$ N and $r \in \{0, 1, \ldots, n\}$, the symbol $C(n, r)$ is used to denote the

number of *r*-subsets of [*n*]. The value of $C(0, 0)$ is taken to be 1. Many texts use the word

'*r*-combination' for an *r*-subset.

2. Using Theorem **8.4.1**, we see that for $n \in$ N0 and $r = 0, 1, \dots, n$, $C(n, r) = \frac{n!}{r!(n-r)!}$. Also it follows from the definition that $C(n, r) = 0$ if $n < r$, and $C(n, r) = 1$ if $n = r$.

3. Let $n \in \mathbb{N}$ and $n_1, n_2, \dots, n_k \in \mathbb{N}_0$ such that $n = n1 + \cdots + nk$. Then by $C(n; n_1, \dots, n_k)$ we

denote the number $n!$ $n_1!n_2!\cdots n_k!$. By Theorem **8.3.3**, it is the number of arrangements of n objects where ni are of type i, $i = 1, \dots, k$. By convention, $C(0; 0, \dots, 0) = 1$.

4. If $n \in$ N and $n_1, \dots, n_{k-1} \in \mathbb{N}_0$ with $n_1 + \cdots + n_{k-1} < n$, we also use $C(n; n_1, \dots, n_{k-1})$ to mean $C(n; n_1, \dots, n_{k-1}, n - n_1 - \cdots - n_{k-1})$.

8.3.5 Pascal's identity:

Theorem[Pascal] *Let n and r be non-negative integers. Then* $C(n, r) + C(n, r + 1) = C(n + 1, r + 1)$.

Proof. (This is not the combinatorial proof.) If $r > n$, then by definition all the three terms are zero. So, we have the identity. If $r = n$, then the first and the third terms are 1 and the second term is 0. So, again we have the identity. So, let us take $r < n$. Now we can use the formulas for $C(n, r)$, $C(n, r + 1)$ and $C(n + 1, r + 1)$ to verify the identity.

The combinatorial proof of Theorem 8.5.1:

Proof. If $r > n$, then by definition all the three terms are zero. So we have the identity. If $r = n$,

then the first and the third terms are 1 and the second term is 0. So, again we have the identity. So, assume that $r < n$.

Let $S = \{1, 2, \dots, n, n + 1\}$ and A bean $(r + 1)$-subset of S.

Then, by definition, there are

$C(n + 1, r + 1)$ such sets with either $n + 1 \in A$ or $n + 1 \notin A$.

Note that $n + 1 \in A$ if and only if $A \setminus \{n + 1\}$ is an r-subset of $\{1, 2, \dots, n\}$.

So, the number of $(r + 1)$-subsets of $\{1, 2, \dots, n, n + 1\}$ which contain the element $n + 1$ is, by definition, $C(n, r)$.

Also, $n + 1 \in / A$ if and only if A is an $(r + 1)$-subset of $\{1, 2, \dots, n\}$. So, a set *A* which does not contain *n* + 1 can be formed in *C*(*n*, *r* + 1) ways.

Therefore, using the above two cases, an (*r* + 1)-subset of *S* can be formed, by definition, in *C*(*n*, *r*) + *C*(*n*, *r* + 1) ways. Thus, the required result follows.

Counting in two ways:

Let *R* and *C* be two nonempty finite sets and take a function $f : R \times C \rightarrow$ R. View the function written as a matrix of real numbers with rows indexed by *R* and columns indexed by *C*. Then the total sum of the entries of that matrix can be obtained either 'by first taking the sum of entries in each row and then summing them' or 'by first taking the sum of the entries in each column and then summing them', *i.e.*,

$$\sum_{(x,y)\in R\times C} f(x,y) = \sum_{x\in R}(\sum_{y\in C} f(x,y) = \sum_{y\in C}(\sum_{x\in R} f(x,y)$$

This is known as 'counting in two ways' and it is a very useful tool to prove some combinatorial identities.

Example: [Newton's Identity] Let $n \geq r \geq k$ be natural numbers. Then $C(n, r)C(r, k) = C(n, k)C(n - k, r - k)$. In particular, for $k = 1$, the identity becomes $rC(n, r) = nC(n - 1, r - 1)$.

Solution: Let us use the method of 'counting in two ways'. So, we take two appropriate sets *R* = {all *r*-subsets of [*n*]} and *C* = {all *k*-subsets of [*n*]} and define *f* on *R* × *C* by $f(A, B) = 1$ if $B \subseteq A$, and $f(A, B) = 0$ if $B \not\subseteq A$.

Then given a set $A \in R$, it has *C*(*r*, *k*) many subsets of *A*. Thus,

$$\sum_{A\in R}\left(\sum_{B\in C} f(A,B)\right) = \sum_{A\in R} C(r,k) = C(n,r)C(r,k)$$

Similarly, given a set $B \in C$, there are $C(n - k, r - k)$ subsets of [*n*] that contains *B*. Hence,

$$\sum_{B\in C}\left(\sum_{A\in R} f(A,B)\right) = \sum_{B\in C} C(n-k, r-k) = C(n,k)C(n-k, r-k)$$

Hence, the identity is established.

Example: Let *n, r* ∈N, *n* ≥ *r*. Then

C(1, *r*) + *C*(2, *r*) + · · · + *C*(*n*, *r*) = *C*(*n* + 1, *r* + 1). (5.1)

The RHS stands for the class *F* of all the subsets of [*n* + 1] of size *r* + 1.

Let *S* ∈*F*.

Note that *S* has a maximum element. A moments thought tells us that the maximum element of

such a set can vary from *r* + 1 to *n* + 1. If the maximum of *S* is *r* + 1, then the remaining

elements of *S* have to be chosen in *C*(*r*, *r*) ways. If the maximum of *S* is *r* + 2, then the

remaining elements of *S* has to be chosen in *C*(*r* + 1, *r*) ways and so on. If the maximum

of *S* is *n* + 1, then the remaining elements of *S* has to be chosen in *C*(*n*, *r*) ways. Thus,

C(*n* + 1, *r* + 1) = *C*(*r*, *r*) + *C*(*r* + 1, *r*) + · · · + *C*(*n* + 1, *r*) = *C*(1, *r*) + *C*(2, *r*) + · · · + *C*(*n*, *r*).

Observe that for *r* = 1, it gives us 1 + 2 + · · · + *n* = $\frac{n(n\ +1).}{2}$

Check Your Progress 1

1. State the Addition Rule

____

____

____

2. What do you understand by injection?

____

____

____

3. Discuss Arrangements

____

____

8. 4 SOLUTIONS IN NON-NEGATIVE INTEGERS

There are 3 types of ice-creams available in the market: *A*, *B*, *C*. We want to buy 5 ice-creams in total. In how many ways can we do that? For example, we can buy 5 of type *A* or we can buy 3 of *A* and 2 of *C*. In general, suppose we are buying n_1 of type *A*, n_2 of type *B* and n_3 of type *C*. Then, we must have $n_1 + n_2 + n_3 = 5$. So, we want to know the number of different possible tuples (n_1, n_2, n_3) satisfying certain condition(s). Recall that $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. A point $\mathbf{p} = (p1, . . . , pk) \in \mathbb{N}_0^k$ with $p_1 + \cdots + p_k = n$ is called a **solution of** $x_1 + \cdots + x_k = n$ **in non-negative integers** or a solution of $x_1 + \cdots + x_k = n$ in $\mathbb{N}_0$. Two solutions $(p_1, . . . , p_k)$ and $(q_1, . . . , q_k)$ are said to be the same if $pi = qi$, for each $i = 1, . . . , k$. Thus, (5, 0, 0, 5) and (0, 0, 5, 5) are two different solutions of $x + y + z + t = 10$ in $\mathbb{N}_0$.

8.4.1Theorem [Solutions in $\mathbb{N}_0$]

The number of solutions of $x1+\cdots+xr = n$ *in* $\mathbb{N}_0$ *is* $C(n+r-1, n)$.

Proof. Each solution $(x1, . . . , xr)$ may be viewed as an arrangement of n dots and $r - 1$ bars.

'Put $x1$ many dots; put a bar; put $x2$ many dots; put another bar; continue; and end by putting

x_r many dots.'

For example, (0, 2, 1, 0, 0) is associated to | • •| • || and vice-versa. As there are $C(n + r - 1, r - 1)$ arrangements of n dots and $r - 1$ bars, we see that the number of solutions of $x_1 + \cdots + x_r = n$ in $\mathbb{N}_0$ is $C(n + r - 1, n)$.

Example: Determine the number of words that can be made using all of 3 copies of *A* and 6

copies of *B*.

Solution: Note that this number equals the number of arrangements of 3 copies of *A* and 6 copies of *B*. Hence, this number is *C*(9, 3).

Alternate. First put the three *A*'s in row. Now put x_1 *B*'s to the left of the first *A*, x_2 *B*'s between

the first and the second *A*, x_3 *B*'s between the second and the third *A* and x_4 *B*'s after the third *A*.

Thus, we need to find number of solutions of $x_1 + x_2 + x_3 + x_4 = 6$ in $\mathbb{N}_0$. By Theorem 8.4.1, the

number is $C(6 + 4 - 1, 6) = C(9, 6)$.

Remark: The question of finding non-negative integers solutions can also be asked in some other styles.

1. In how many ways can we place 6 indistinguishable balls into 4 distinguishable boxes?

Taking *ni* as the number of balls to be put in the *i*-th box, it is asking us to find number of

solutions of $n_1 + n_2 + n_3 + n_4 = 6$ in $\mathbb{N}_0$.

2. A **multistep** is a generalization of a set where elements are allowed to repeat. For example,

{a, b, a} and *{a, a, b}* mean the same multisite (imagine carrying all of them in a bag). A set is

also a multistep. How many multisite of size 6 can be made using the symbols *a, b, c, d*?

Taking n_a as the number of *a*'s to be put in the multistep and so on, it is asking us to find

solutions of $n_a + n_b + n_c + n_d = 6$ in $\mathbb{N}_0$.

Example 1. Suppose there are 5 kinds of ice-creams available in our market complex. In

how many ways can we buy 15 of them for a party?

Solution: Suppose we buy *xi* ice-creams of the *i*-th type. Then, the problem reduces to finding the number of solutions of $x_1 + \cdots + x_5 = 15$ in non-negative integers.

Example: [Variables are bounded below by other numbers] How many solutions in $\mathbb{N}_0$ are there to $x + y + z = 60$ such that $x \geq 3, y \geq 4, z \geq 5$?

Solution: Note that (x, y, z) is such a solution if and only if $(x - 3, y - 4, z - 5)$ is a solution to

$x + y + z = 48$ in $\mathbb{N}_0$. So, the answer is C (50, 2).

Example: [Reducing a related problem] In how many ways can we pick integers $x_1 < x_2 < x_3 < x_4 < x_5$, from $\{1, 2, \ldots, 20\}$ so that $x_i - x_{i-1} \geq 3$, $i = 2, 3, 4, 5$? For example, one such choice is

(1, 5, 8, 11, 19).

Solution: For each choice of $(x1, x2, x3, x4, x5)$, note that

$$(x1 - 1) + (x2 - x1) + \cdots + (x5 - x4) + (20 - x5) = 19$$

i.e.

$$d_1 + d_2 + d_3 + d_4 + d_5 + d_6 = 19$$

where $d_1 \geq 0$, $d_2 \geq 3, \ldots, d_5 \geq 3$ and $d_6 \geq 0$. So, the problem reduces to finding the number of

solutions of $n_1 + n_2 + \cdots + n_6 = 7$ in $\mathbb{N}_0$.. Hence, the answer is C (12, 5).

Alternate. Take an arrangement of fifteen dots (•'s) and five bars (|'s) such that between two

consecutive bars, there are at least two dots. The position of the bars in each such arrangement

gives us one solution.

For example, • • | • • • | • • • | • •| • • • •|• → (3, 7, 11, 14, 19).

Conversely, each solution can be converted into such an arrangement by the following method:

let $n1$ be the number of dots present to the left of the first bar; $n2$ be the number of dots present

between the first bar and the second bar and so on. The problem now has been converted to

count integer solutions of $n_1 + n_2 + n_3 + n_4 + n_5 + n_6 = 15$, where $n_1, n_6 \geq 0, n_2, n_3, n_4, n_5 \geq 2$.

This is the same as the number of solutions of $n_1 + n_2 + n_3 + n_4 + n_5 + n_6 = = 7$ in $\mathbb{N}_0$.

Check Your Progress 2

1. Explain solutions in non-negative integers

____

____

____

2. Define Multistep.

____

____

____

8.5 SUMMARY

In the modern era, the subject has developed both in depth and variety and has cemented its position as an integral part of modern mathematics. Undoubtedly part of the reason for this importance has arisen from the growth of computer science and the increasing use of algorithmic methods for solving real-world practical problems. These have led to combinatorial applications in a wide range of subject areas, both within and outside mathematics, including network analysis, coding theory, and probability.

8.6 KEYWORDS

1. Non-negative Integer: A **non negative integer** is an **integer** that that is either positive or zero. It's the union of the natural numbers and the number zero

2. Solution: Any and all value(s) of the variable(s) that satisfies an equation, inequality, system of equations, or system of inequalities

3. Element: an **element**, or member, of a set is any one of the distinct objects that make up that set.

4. Identity: An equation that is true no matter what values are chosen.

8.7 QUESTIONS FOR REVIEW

1. Determine the number of arrangements of the letters of the word ABRACADABARAARCADA.
2. Determine the number of ways of selecting a committee of m people from a group consisting of n1 women and n2 men, with n1 + n2 ≥ m.
3. If n points are placed on the circumference of a circle and all the lines connecting them are joined, what is the largest number of points of intersection of these lines inside the circle that can be obtained?
4. Suppose there are 5 kinds of ice-creams available in our market complex. In how many ways can we buy 15 of them for a party?
5. Determine the number of solutions of $x + y + z = 7$ with $x, y, z \in \mathbb{N}$?

8.8 SUGGESTED READINGS

1. Kenneth H. Rosen - Discrete Mathematics and Its Applications, Tata Mc-Graw-Hill, 7th Edition, 2012.
2. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross-Discrete Mathematical Structures-Prentice Hall, 3rd Edition, 1996.
3. Grimaldi R-Discrete and Combinatorial Mathematics. 1-Pearson, Addison Wesley, 5th Edition, 2004.
4. C. L. Liu – Elements of Discrete Mathematics, McGraw-Hill, 1986.
5. F. Harary – Graph Theory, Addition Wesley Reading Mass, 1969.
6. N. Deo – Graph Theory With Applications to Engineering and Computer Science, Prentice Hall of India, 1987.
7. K. R. Parthasarathy – Basic Graph Theory, Tata McGraw-Hill, New Delhi, 1994.

8. G. Chartand and L. Lesniak – Graphs and Diagraphs, wadsworth and Brooks, 2nd Ed.,
9. Clark and D. A. Holton – A First Look at Graph Theory, Allied publishers.
10. D. B. West – Introduction to Graph Theory, Pearson Education Inc.,2001, 2nd Ed.,
11. J. A. Bondy and U. S. R. Murthy – Graph Theory with applications, Elsevier, 1976
12. J. P. Tremblay & R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co. 1997
13. S. Witala, Discrete Mathematics - A Unified Approach, McGraw Hill Book Co.

8.9 ANSWER TO CHECK YOUR PROGRESS

1. State the concept– 8.2 (2)
2. Explain the concept--- 8.3.2
3. Explain the Theorem with proof -- 8.3.3
4. Explain the concept--- 8.4
5. A **multistep** is a generalization of a set where elements are allowed to repeat. For example,

   {a, b, a} and *{a, a, b}* mean the same multisets (imagine carrying all of them in a bag). A set is

   also a multiset. How many multisets of size 6 can be made using the symbols *a, b, c, d*?

   Taking n_a as the number of *a*’s to be put in the multiset and so on, it is asking us to find

   solutions of $n_a + n_b + n_c + n_d = 6$ in $\mathbb{N}_0$.

UNIT 9: COMBINATROICS – II

STRUCTURE

9.0 OBJECTIVES

Understand the addition and product rule. How to apply it.

Understand the concept of permutation and combination

Enumerate the concept of solution of non-negative integers

9.1 BINOMIAL THEOREM

For all real numbers a and b and non-negative integers n,

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

$$(a+b)^0 = 1$$

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Proof. Let P(n) be the statement that for all real numbers a and b, $(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$

$$(a+b)^k = \sum_{r=0}^{k} \binom{k}{r} a^r b^{k-r} \qquad (1)$$

We want to prove that 'inductive conclusion' (the formula for n = k + 1, i.e., the statement P(k + 1))

$$(a+b)^{k+1} = \sum_{r=0}^{k} \binom{k}{r} a^r b^{k+1-r} \qquad (2)$$

After computing

$$(a+b)^{k+1} = (a+b)^k.(a+b) \qquad (3)$$

$$= \sum_{r=0}^{k} \binom{k}{r} a^r b^{k-r}.(a+b) \qquad \textit{by inductive hypothesis}$$

$$= \sum_{r=0}^{k} \binom{k}{r} a^{r+1} b^{k-r} + \sum_{r=0}^{k} \binom{k}{r} a^r b^{k+1-r} \quad \textit{by the distributive property}$$

indeed, when we multiply $a^r b^{k-r}$ in line 2 by a, the power of a increases by 1 to get $a^{r+1} b^{k-r}$ in the first term in line 3. Similarly, when we multiply $a^r b^{k-r}$ by a, we get $a^r b^{k+1-r}$ in the second term in line 3. Now $a^r b^{k+1-r}$ in line 3 of (3) matches the form of the right-hand side of (2). To make the term $a^{r+1} b^{k-r}$ in line 3 of (3) also match, we shift the variable r down by 1 as follows. Define s = r + 1. Then r = s − 1. Moreover, when r is summed from 0 to k, we then have that s is summed from 1 to k + 1. So the first term in line 3 of (3) may be rewritten a

$$\sum_{r=0}^{k} \binom{k}{r} a^{r+1} b^{k-r} = \sum_{s=1}^{k+1} \binom{k}{s-1} a^s b^{k+1-s}$$

(since k − (s − 1) = k + 1 − s). But s is just a name. So we can replace s by r to get

$$\sum_{r=0}^{k} \binom{k}{r} a^{r+1} b^{k-r} = \sum_{r=1}^{k+1} \binom{k}{r-1} a^r b^{k+1-r}.$$

Thus (3) implies

$$(a+b)^{k+1} = \sum_{r=1}^{k+1} \binom{k}{r-1} a^r b^{k+1-r} + \sum_{r=0}^{k} \binom{k}{r} a^r b^{k+1-r}.$$

combine the two sums on the right-hand side into one sum. But we have a slight mismatch in that the first sum is from 1 to k + 1 whereas the second sum is from 0 to k. So take out the r = k + 1 case from the first sum and we take out the r = 0 case from the first sum from the second

$$(a+b)^{k+1} = \binom{k}{(k+1)-1} a^{(k+1)} b^{k+1-(k+1)} + \sum_{r=1}^{k} \binom{k}{r-1} a^r b^{k+1-r} + \sum_{r=1}^{k} \binom{k}{r} a^r b^{k+1-r} + \binom{k}{0} a^0 b^{k+1-0}.$$

sum and combine things in the following way

Since

$$(a+b)^{k+1} = a^{k+1} + \sum_{r=1}^{k} \left(\binom{k}{r-1} + \binom{k}{r} \right) a^r b^{k+1-r} + b^{k+1}.$$

$\binom{k}{(k+1)-1} = \binom{k}{k} = 1$ and $\binom{k}{0} = 1$,

Since $1 \leq r \leq k$

$$\binom{k}{r-1} + \binom{k}{r} = \binom{k+1}{r}.$$

Hence

$$(a+b)^{k+1} = a^{k+1} + \sum_{r=1}^{k} \binom{k+1}{r} a^r b^{k+1-r} + b^{k+1}.$$

But noting $a^{k+1} = \binom{k+1}{k+1} a^{k+1} b^0$ that (is the r = k + 1 case in the sum)

$b^{k+1} = \binom{k+1}{0} a^0 b^{k+1}$ (is the r = 0 case in the sum)

This is the desired inductive conclusion (2). By mathematical induction, the proof of the Binomial Theorem is complete

$$(a+b)^{k+1} = \sum_{r=0}^{k+1} \binom{k+1}{r} a^r b^{k+1-r}.$$

Corollary: *Let* $n \in \mathrm{N}$. *Then the total number of subsets of* $[n]$ *is* 2^n

Proof. The number of subsets of size k is $C(n, k)$. Thus the total number of subsets is $C(n, 0) + C(n, 1) + \cdots + C(n, n)$ which is $(1 + 1)^n$ by the binomial theorem.

Example :1. Fix $m, n, k \in \mathrm{N}$. Then show that

$$C(m+n,k) = \sum_{i=0}^{k} C(m,i)\ C(n,k-i).$$

Solution: First, we give an argument using counting in two ways. We can form a committee of size k from a group consisting of m men and n women in $C(m + n, k)$ ways. On the other hand, such a committee can be formed by taking i many men and $n - i$ many women, where $0 \le i \le k$. In this way our answer is

$$\sum_{i=0}^{k} C(m,i)\ C(n,k-i).$$

Hence, they are the same.

Example: Let $n > m$ be natural numbers. Prove that

$$\sum_{k=m}^{n} C(k,m)C(n,k) = C(n,m)2^{n-m}.$$

As we know, $C(k, m)C(n, k) = C(n, m)C(n - m, k - m)$.

Hence,

$$\begin{aligned}\sum_{k=m}^{n} C(k,m)C(n,k) &= \sum_{k=m}^{n} C(n,m)C(n-m,k-m) = C(n,m)\sum_{k=m}^{n} C(n-m,k-m)\\ &= C(n,m)\sum_{s=0}^{n-m} C(n-m,s) = C(n,m)2^{n-m}.\end{aligned}$$

Alternate. Noticing a combinatorial proof is relatively harder. The RHS stands for (A, B)

where $A \subseteq [n]$ of size m and $B \subseteq [n] \setminus A$. For each fixed A, we have $2n-m$ choices of B, and this is why we have the RHS. On the other hand, we can first select a big set C of size $|C| \geq m$.

From this set C, we will take a subset A of size m and we will treat the remaining as B. The

LHS expresses the number of ways in which this task can be done.

Example: Determine the number of words of size 5 using letters from 'MATHEMATICIAN' (including multiplicity, *i.e.*, you may use *M* at most twice).

Solution: Note that to form such a word, suppose we have selected *xm* many *M*'s, *xa* many *A*'s,

and so on. Then, the problem reduces to finding the number of solutions in non-negative

numbers to $x_m + x_a + x_t + x_h + x_e + x_i + x_c + x_n = 5$, with $0 \leq x_m, x_t, x_i \leq 2$, $0 \leq x_a \leq 3$, $0 \leq x_h, x_c, x_n, x_e \leq 1$. In that case the number of words that can be formed from them is $C(5; x_m, x_t, x_i, x_a, x_h, x_c, x_n, x_e)$. Hence, the total number of such words.

$$\sum_{\substack{k_1+\cdots+k_8=5 \\ k_1\leq 2,k_2\leq 3,k_3\leq 2,k_4\leq 1,k_5\leq 1,k_6\leq 2,k_7\leq 1,k_8\leq 1}} C(5; k_1, \cdots, k_8).$$

9.2 CIRCULAR ARRANGEMENTS

Let *S* be a nonempty finite multistep. By a **circular arrangement** of elements of *S*, we mean an arrangement of the elements of *S* on a circle. Two circular arrangements are the same if each element has the same 'clockwise adjacent' element, *i.e.*, one can be obtained as a rotation of the other. By $[x_1, x_2, \ldots, x_n, x_1]$, we shall denote a circular arrangement, keeping the anticlockwise direction in a picture. We use the word **circular permutation** if elements of *S* are distinct. Thus, exactly two of the following pictures represent the same circular permutation.

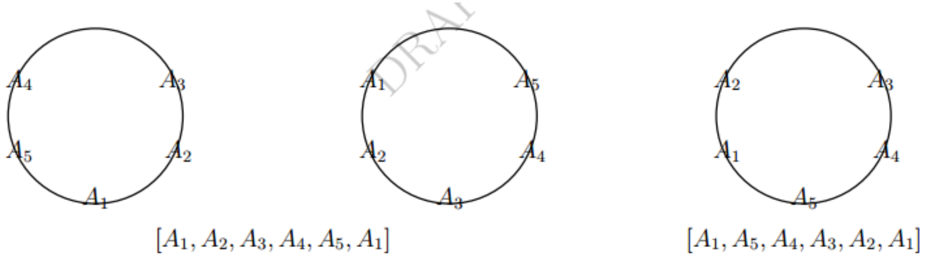


Fig 9.1 Circular permutation

Example: Determine the number of circular permutations of $X = \{A1, A2, A3, A4, A5\}$.

Ans: 4!. Let $B = \{$circular permutations of $X\}$ and $A = \{$permutations of $X\}$.

Now, define $f : A \to B$ as $f(a) = b$ if a is obtained by breaking the cycle b at some gap and then following in the anticlockwise direction.

For example, if we break the leftmost circular permutation in Figure 9.1 at the gap between $A1$ and A_2, we get $[A_2, A_3, A_4, A_5, A_1]$. Notice that $|f -1(b)| = 5$, for each $b \in B$.

Further if $b, c \in B$, then $f -1(b) \cap f -1(c) = \emptyset$ (why?1). Thus, by the principle of disjoint pre-images of equal size, the number of circular permutations is 5!/5.

Theorem :[Circular permutations] *The number of circular permutations of* $\{1, 2, . . . , n\}$ *is* $(n - 1)!$.

Proof.

Put $A = \{$circular permutations of $\{1, 2, . . . , n - 1, n\}$.

Put $B = \{$permutations of $\{1, 2, . . . , n -1\}$

Define $f : A \to B$ as $f([n, x1, x2, . . . , xn-1, n]) = [x1, x2, . . . , xn-1]$.

Define $g : B \to A$ as $g([x1, x2, . . . , xn-1]) = [n, x1, x2, . . . , xn-1, n]$.

Then, $g \circ f(a) = a$, for each $a \in A$ and $f \circ g(b) = b$, for each $b \in B$. Hence, by the bijection principle , f is a bijection.

Example : Find the number of circular arrangements of *{A, B, B, C, C, D, D, E, E}*.

Ans: There is only one *A*. Cutting *A* out from a circular arrangement we get a unique arrangement of *{B, B, C, C, D, D, E, E}*. So, the required answer is $\frac{8!}{2!^4}$

Definition: 1. Given an arrangement (not a circular arrangement) $[X_1, . . . , X_n]$ by a **rotation** $R_1([X_1, . . . , X_n])$, in short $R1(X_1, . . . , X_n)$, we mean the arrangement $[X_2, . . . , X_n, X_1]$ and

by $R_2(X_1, . . . , X_n)$ we mean the arrangement $[X_3, . . . , X_n, X_1, X_2]$.

On similar lines, we define R_i, $i \in \mathbb{N}$ and put $R_0 (X_1, . . . , X_n) = [X_1, . . . , X_n]$.

Thus, for each $k \in \mathbb{N}$,

$$R_0(X_1, . . . , X_n) = R_{kn}(X_1, . . . , X_n) = [X_1, . . . , X_n]$$

.

2. The **orbit size** of an arrangement $[X_1, . . . , X_n]$ is the smallest positive integer *i* which satisfies

$Ri(X_1, . . . , X_n) = [X_1, . . . , X_n]$. In that case, we call

$$\{R_0(X_1, . . . , X_n), R1(X_1, . . . , X_n), . . . , R_{i-1}(X_1, . . . , X_n)\}$$

the **orbit** of $[X_1, . . . , X_n]$.

Discussion. 1. We have *R*1(*ABCABCABC*) = [*BCABCABCA*],

*R*2(*ABCABCABC*) =

[*CABCABCAB*] and *R*3(*ABCABCABC*) = [*ABCABCABC*].

Thus, the orbit size of [*ABCABCABC*] is 3.

2. An arrangement of *S = {A, A, B, B, C, C}* with orbit size 6 is [*AABCBC*]. An arrangement of

S with orbit size 3 is [*ACBACB*].

3. There is no arrangement of *S = {A, A, B, B, C, C}* with orbit size 2. In fact, if there is an

arrangement with orbit size 2 then it's form, by definition, must be

[*X*1*X*2*X*1*X*2*X*1*X*2]. Thus
the element *X*1 repeats at least 3 times in *S*, which is not possible.

4. There is no arrangement of *{A, A, B, B, C, C}* with orbit size 1 or 2 or 4 or 5.

5. There are 3! arrangements of *{A, A, B, B, C, C}* with orbit size 3.

6. Take an arrangement of *{A, A, B, B, C, C}* with orbit size 3. Make a circular arrangement by
joining the ends. How many distinct arrangements can we generate by breaking the circular
arrangement at gaps?
Ans: 3. They are the elements of the same orbit.

7. Take an arrangement of *{A, A, B, B, C, C}* with orbit size 6. Make a circular arrangement by
joining the ends. How many distinct arrangements can we generate by breaking the circular
arrangement at gaps?
Ans: 6. They are the elements of the same orbit.

8. Take an arrangement of *n* elements with orbit size *k*. Make a circular arrangement by joining the ends. How many distinct arrangements can we generate by breaking the circular arrangement
at gaps?
Ans: *k*. They are the elements of the same orbit.

9. If we take the set of all arrangements of a finite multiset and group them into orbits (notice that
each orbit gives us exactly one circular arrangement), then the number of orbits is the number
of circular arrangements.

Proposition : *The orbit size of an arrangement of an n-multiset is a divisor of n.*

Proof. Suppose, the orbit size of $[X_1, . . . , X_n]$ is k and $n = kp + r$, for some r, $0 < r < k$. Then,

$$R_k(X_1, . . . , X_n) = R_{2k}(X_1, . . . , X_n) = \cdot \cdot \cdot = R_{kp}(X1, . . . , Xn) = R_{k-r}(X_1, . . . , X_n)$$

as $(p+1)k = pk+k = n-r+k \equiv k-r \pmod n$.

Thus, $Rk-r(X_1, . . . , X_n) = [X_1, . . . , X_n]$, contradicting the minimality of k.

Hence, $r = 0$. Equivalently, k divides n.

[Binary operations] : Another way to count the number of circular arrangements.

Let $[X_1, . . . , X_n]$ and $[Y_1, . . . , Y_n]$ be two arrangements of an n-multiset. Then, in the remainder of this section, we shall consider expressions like $[X_1, . . . , X_n] + [Y_1, . . . , Y_n]$.

By $[Ri+Rj](X_1, . . . , X_n)$, we mean the expression $Ri(X_1, . . . , X_n)+Rj(X_1, . . . , X_n)$. By $Ri([X_1, . . . , X_n]+ [Y_1, . . . , Y_n])$ we denote the expression $Ri(X_1, . . . , X_n) + Ri(Y_1, . . . , Y_n)$.

Example: Think of all arrangements $P_1, . . . , P_n$, of two A's, two B's and two C's, where

$n = \frac{6!}{2!2!2!}$. How many copies of $[ABCABC]$ are there in $[R_0 + \cdot \cdot \cdot + R_5](P_1 + \cdot \cdot \cdot + P_n)$?

Solution: Of course 6. $R0$, $R3$ take $[ABCABC]$ to itself; $R1$, $R4$ will take $[CABCAB]$ to $[ABCABC]$; $R2$, $R5$ will take $[BCABCA]$ to $[ABCABC]$; and no other arrangement

after rotation will give $[ABCABC]$.

Proposition : *Let $P_1, . . . , P_n$ be all the arrangements of an m-multiset. Then,*

$$[R_0 + \cdots + R_{m-1}](P_1 + \cdots + P_n) = m(P_1 + \cdots + P_n).$$

Proof. In fact, $[R_0 + \cdots + R_{m-1}](P_1 + \cdots + P_n)$ means, take all arrangements and apply all rotations $(R_0, \ldots , R_{m-1})$, and collect all resulting arrangements.

Note that, if we apply $R0$ on $(P_1 + \cdots +P_n)$, we get one copy of each arrangement. Similarly, if we apply Ri on $(P_1 +\cdots +P_n)$, we get one copy of each arrangement. So, $[R_0 +\cdots +R_{m-1}](P_1 +\cdots +P_n)$ will contain m copies of each arrangement.

Proposition: *Let P be an arrangement of an m-multiset which has orbit size k. Then the*

number of rotations Ri, $i = 0, 1, \ldots , m-1$ which **fix** *P (that is, satisfy $Ri(P) = P$) is $\frac{m}{k}$. Furthermore,*

$$[R_0 + R_1 + \cdots + R_{m-1}](P) = \frac{m}{k} \text{orbit}(P).$$

Proof. Ask is the orbit size of P , we already know that k divides m. Put $p = m/k$. Then

$R_0, R_k, \ldots , R_{(p-1)k}$ fix P . If there is any other s such that R_s fixes P , then noting that s is not a multiple of k, let $s = kj + r$, where $0 < r < k$. It now follows that $R_r(P) = P$.

This is a contradiction to the fact that k is the orbit size of P.

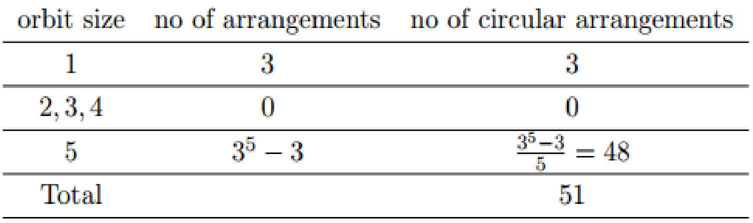
The next assertion follows from the fact that

$[R_0 + \cdots + R_{k-1}](P) = [R_k + \cdots + R_{2k-1}](P) = \cdots = [R_{(p-1)k} + \cdots + R_{pk-1}](P)$

is the orbit(P)

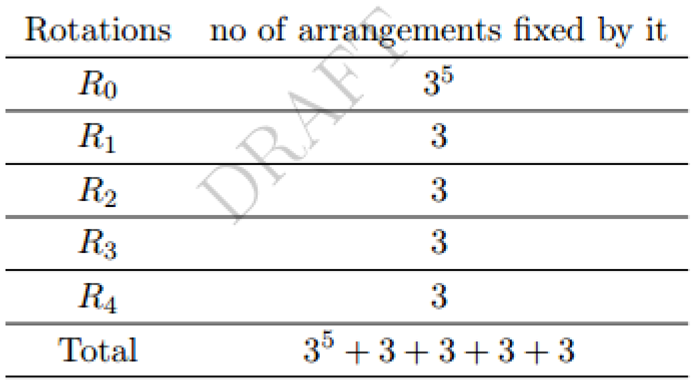
Example: Determine the number of circular arrangements of size 5 using the alphabets A, B and C.

Ans: First way:



orbit size	no of arrangements	no of circular arrangements
1	3	3
$2, 3, 4$	0	0
5	$3^5 - 3$	$\frac{3^5-3}{5} = 48$
Total		51

Second way:



Rotations	no of arrangements fixed by it
R_0	3^5
R_1	3
R_2	3
R_3	3
R_4	3
Total	$3^5+3+3+3+3$

Hence, the number of circular arrangements is $\frac{3^5+4.3}{5} = 51$

Check Your Progress 1

1. State Binomial Theorem

2. What is Circular Permutation?

9.3 SET PARTITIONS

Concept: Let *S* be a nonempty set and $k \in$N. A **partition of** *S* **into** *k* **subsets** means a collection of *k* pairwise disjoint nonempty subsets of *S* whose union is *S*. For brevity, a partition of *S* into *k* subsets is called a *k*-**partition of** *S*.

Example: (a) Each of the collections $\{1, 2\}, \{3\}, \{4, 5, 6\}$, $\{1, 3\}, \{2\}, \{4, 5, 6\}$ and

$\{1, 2, 3, 4\}, \{5\}, \{6\}$ is a 3-partition of [6], whereas the collection $\{\{1, 2,$

3}, {3, 4, 5, 6}} is not
a partition of any set.

Proposition : *Let n, r* $\in$N. *Then the number of partitions of n into at most r parts is equal to the number of partitions of n + r into r parts.*

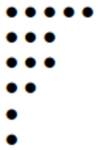
Proof. Given a partition of *n* into at most *r* parts, extend it to an *r*-tuple by adding some 0's at the right end. For example, if $n = 7$, $r = 4$, we change the partition (6, 1) which has at most four parts into (6, 1, 0, 0) which is a four tuple. This can be done uniquely. Next, add 1 to each component of the *r*-tuple. We get an *r*-partition of $n + r$. For example, our previous four tuple would now change to (7, 2, 1, 1) which is a partition of 11 into four parts.
Conversely, given an *r*-partition of $n+r$, subtract 1 from each component. Some of the components might become 0. Truncating them we get a partition of *n* into at most *r* parts.

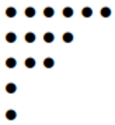
Remark [Recurrence for $\pi n(k)$**]** Another way of writing the previous result is
$\pi_{n}(k) = \pi_{n-k}(0) + \pi_{n-k}(1) + \cdots + \pi_{n-k}(k)$
and so
$\pi_n(k) = \pi_{n-1}(k - 1) + \pi_{n-k}(k)$.

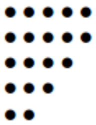
Definition : Let $n, k \in$N and $\lambda = (n_1, n_2, \cdots, n_k)$ be a *k*-partition of *n*.

1. Then, the **Ferrer's Diagram** of λ is a pictorial representation of the partition created in the
following way. The *i*-th part of the partition is represented by putting *ni* equally spaced dots in
a row. The first row is on the top. The leftmost dots of each row lies in the same column.
2. The (i, j)**-hook** of the partition consists of the (i, j)-dot along with the dots (of *i*-th row) to the right of it and the dots (of *j*-th column) below it. The **hook length** is the number of dots in that particular hook.

Example : Ferrer's diagram for the partitions $\lambda1 = (5, 3, 3, 2, 1, 1)$, $\lambda2 = (6, 4, 3, 1, 1)$ and $\lambda3 = (5, 5, 4, 3, 2)$ of 15, 15 and 19 are given below.


$(5, 3, 3, 2, 1, 1)$


$(6, 4, 3, 1, 1)$


$(5, 5, 4, 3, 2)$

Suppose that we have a Ferrer's diagram of some partition λ of n. Observe that the number of dots in the first column of the Ferrer's diagram is greater than or equal to the number of dots in the second column. In general, the number of dots in the i-th column is always greater than or equal to the number of dots in the $(i + 1)$-th column. Thus, if we interchange the rows and columns of the Ferrer's diagram (transposing), then the result is another Ferrer's diagram of some partition of n.

This new partition is called the **conjugate** of λ and is denoted by λ_0. A partition λ of n is called **self-conjugate** if $\lambda = \lambda_0$.

For instance, if $\lambda = (5, 3, 3, 2, 1, 1)$ is a partition of 15, then its conjugate is $\lambda_0 = (6, 4, 3, 1, 1)$. The partition $(5, 4, 3, 2, 1)$ is a self-conjugate partition of 15.

Remark: Let $\lambda = (n_1, . . . , n_k)$ be a partition (of some number). One can write the conjugate without drawing the Ferrer's diagram. It's conjugate $\lambda 0 = (p_1, . . . , p_{n1})$ has n_1 components and pi = the number of components in λ that are at least i. For example, the conjugate of $(5, 3, 1, 1)$ is a partition with 5 components $(p_1, . . . , p_5)$, where p_1 = the number of components in λ that are at least

1. So $p_1 = 4$. Now, p_2 = the number of components in λ that are at least 2. So $p_2 = 2$. Similarly,

$p_3 = 2$, $p_4 = 1$, and $p_5 = 1$. So $\lambda_0 = (4, 2, 2, 1, 1)$.

Proposition : Let n ∈ ℕ. Then the number of self-conjugate partitions of n is the same as the number of partitions of n whose parts are distinct odd numbers.

Proof. Let λ be a self-conjugate partition of n with k diagonal dots. For $1 \leq i \leq k$, define li = length of the (i, i)-th hook. Since λ is self-conjugate, each li is odd and $(l_1, \ldots, l_k)$ is a strictly decreasing sequence of positive integers with $l_1 + l_2 + \ldots + l_k = n$. Hence, from a self-conjugate partition λ of n we have got a partition of n whose parts are distinct and odd. Conversely, given any partition, say $l = (l_1, \ldots, l_k)$ where parts are distinct and odd, we can get a self-conjugate partition by putting $l1$ dots in the (1, 1)-th hook, l_2 dots in the (2, 2)-th hook and soon. Since each li is odd, the hook is symmetric and as the hook lengths decrease at least by 2, we see that the corresponding diagram of dots is indeed a Ferrer's diagram.

Proposition: Let $n \in \mathbb{N}$ *and* $f(n)$ *be the number of partitions of n in which no part is* 1.
Then $f(n) = \pi_n - \pi_{n-1}$.

Proof. For $n = 1$, both the sides of the equality are 0. So assume that $n > 1$.
We shall count the complement. Let $\lambda = (n_1, \ldots, n_k)$ be a partition of n with $n_k = 1$. (Since $n > 1$, there are at least two parts.) Then, λ gives rise to a partition of $n - 1$, namely $(n_1, \ldots, n_{k-1})$.
Conversely, if $\mu = (t_1, \ldots, t_k)$ is a partition of $n - 1$, then $(t_1, \ldots, t_k, 1)$ is a partition of n with last part 1. Hence, the number of partitions of n with last part 1 is $\pi_{n-1}(k - 1)$.
Thus, using Remark **[Recurrence for** $\pi_n(k)$], the number of partitions of n in which no part is 1 is $\pi_n - \pi_{n-1}$.

9.4 PIGEONHOLE PRINCIPLE

Theorem [Pigeonhole Principle, PHP] *Let A be a finite set and let* $f : A \to \{1, 2, \ldots, n\}$ *be a function. Let* $p_1, \ldots, p_n \in \mathbb{N}$*If* $|A| > p_1 + \cdots + p_n$, *then there exists* $i \in \{1, 2, \ldots, n\}$ *such that* $|f -1(i)| > pi$.
Proof. On the contrary, suppose that for each $i \in \{1, 2, \ldots, n\}$, $|f -1(i)| \leq pi$. As A is a disjoint union of the sets $f -1(i)$, we have $|A|$ = Pn i=1 $|f$

$-1(i)| \leq p_1 + \cdot \cdot\cdot + p_n < |A|$, a contradiction.

The elements of A are thought of as pigeons and the elements of B as pigeon holes; so that the principle is commonly formulated in the following forms, which come in handy in particular problems.

Discussion :[Pigeonhole principle (PHP)]

PHP1. If $n + 1$ pigeons stay in n holes then there is a hole with at least two pigeons.

PHP2. If k_{n+1} pigeons stay in n holes then there is a hole with at least $k + 1$ pigeons.

PHP3. If $p_1 + \cdot \cdot\cdot + p_{n+1}$ pigeons stay in n holes then there exists i, $1 \leq i \leq n$ such that the i-th hole contains at least p_{i+1} pigeons

Example: In a group of 6 people, prove that there are three mutual friends or three mutual strangers.

Solution: Let a be a person in the group. Let F be the set of friends of a and S the set of strangers to a. Clearly $|S| + |F| = 5$. By PHP either $|F| \geq 3$ or $|S| \geq 3$.

Case 1: $|F| \geq 3$. If any two in F are friends then those two along with a are three mutual friends. Else F is a set of mutual strangers of size at least 3.

Case 2: $|S| \geq 3$. If any pair in S are strangers then those two along with a are three mutual strangers. Else S becomes a set of mutual friends of size at least 3

Theorem : Let $r_1, r_2, \cdot \cdot \cdot , r_{mn+1}$ be a sequence of mn + 1 distinct real numbers. Then, prove that there is a subsequence of m + 1 numbers which is increasing or there is a subsequence of n + 1 numbers which is decreasing. Does the above statement hold for every collection of mn distinct numbers?

Proof: Define li to be the maximum length of an increasing subsequence starting at r_i. If some

$l_i \geq m + 1$ then we have nothing to prove. So, let $1 \leq l_i \leq m$. Since (l_i) is a sequence of mn + 1 integers, by PHP, there is one number which repeats at least n+1 times. Let $l_{i1} = l_{i2} = \cdot \cdot \cdot = l_{in+1} = s$,

where $i_1 < i_2 < \cdot \cdot \cdot < i_{n+1}$. Notice that $r_{i1} > r_{i2}$, because if $r_{i1} < r_{i2}$, then 'r_{i1} together with the increasing sequence of length s starting with r_{i2}' gives an increasing sequence of length s+1. Similarly, $r_{i2} > r_{i3} > \cdot \cdot \cdot > r_{in+1}$ and hence the required result holds.

Theorem: Corresponding to each irrational number a, there exist infinitely many rational numbers $\frac{p}{q}$ such that $\left|\frac{a-p}{q}\right| < \frac{1}{q^2}$.

Proof. It is enough to show that there are infinitely many (p, q) ∈ $\mathbb{Z}^2$ with $|qa - p| < 1/q$. As a is irrational, for every m ∈ ℕ, $0 < ia - \lfloor ia \rfloor < 1$, for i = 1, . . . , m + 1. Hence, by PHP there exist i, j with i < j such that

$$|(j-i)a - (\lfloor ja \rfloor - \lfloor ia \rfloor)| < \frac{1}{m} \leq \frac{1}{j-i}.$$

Then, the pair $(p_1, q_1) = (\lfloor ja \rfloor - \lfloor ia \rfloor, j - i)$ satisfies the required property. To generate another pair, find m_2 such that

$$\frac{1}{m_2} < |a - \frac{p_1}{q_1}|$$

and proceed as before to get (p_2, q_2) such that

$$|q_2 a - p_2| < \frac{1}{m_2} \leq \frac{1}{q_2}.$$

Since,

$$|a - \frac{p_2}{q_2}| < \frac{1}{m_2} < |a - \frac{p_1}{q_1}|,$$

we have $\frac{p_1}{q_1} \neq \frac{p_2}{q_2}$

Theorem:. Let α be a positive irrational number. Then prove that S = {m + nα : m, n ∈ Z} is dense in R.

Proof. Consider any open interval (a, b). By Archimedean property, there exists n ∈ ℕsuch that

$\frac{1}{n} < b - a$. Observe that $0 < r_k = k\alpha - \lfloor k\alpha \rfloor < 1$, k = 1, . . . , n + 1. By PHP, some two satisfy $0 < r_i - r_j < 1/n$. Then $x = r_i - r_j = (i - j)\alpha + \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor$ ∈ S. Let p be the smallest integer so

that px > a. If px ≥ b, then (a, b) ⊆ (p − 1)x, px and so $b - a \leq x < \frac{1}{n}$, which is not possible. So,

px ∈ (a, b) and px ∈ S as well. Thus, (a.b) ∩ S ≠ ∅.

Check Your Progress 2

1. What is k-partition?

2. Discuss Pigeonhole principle.

9.5 PRINCIPLE OF INCLUSION-EXCLUSION

Theorem: [Principle of Inclusion and Exclusion, PIE] Let A1, · · · , An be finite subsets of a set U. Then,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n}(-1)^{k+1}\left[\sum_{1\leq i_1<\cdots<i_k\leq n}\left|A_{i_1}\cap\cdots\cap A_{i_k}\right|\right].$$

(1) Or equivalently, the number of elements of U which are in none of A1, A2, . . . , An equals

$$\left|U \setminus \bigcup_{i=1}^{n} A_i\right| = |U| - \sum_{k=1}^{n} (-1)^k \left[\sum_{1 \leq i_1 < \cdots < i_k \leq n} \left|A_{i_1} \cap \cdots \cap A_{i_k}\right| \right].$$

Proof. Let x $\notin \bigcup_{i=1}^{n} A_i$ Then, we show that inclusion of x in some Ai contributes (increases the value) 1 to both sides of Equation (1). So, assume that x is included only in the sets $A_1, \cdots, A_r$. Then, the contribution of x to $|A_{i1} \cap \cdots \cap A_{ik}|$ is 1 if and only if $\{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, r\}$. Hence, the contribution of x to $\sum_{1 \leq i1 < \cdots < ik \leq n} |Ai1 \cap \cdots \cap Aik|$ is C(r, k). Thus, the contribution of x to the right hand side of Equation (6.1) is

$C(r, 1) - C(r, 2) + C(r, 3) - \cdots + (-1)^{r+1} C(r, r) = 1.$

The element x clearly contributes 1 to the left hand side of Equation (1) and hence the required result follows.

Example : How many integers between 1 and 10000 are divisible by none of 2, 3, 5, 7?

Ans: For $i \in \{2, 3, 5, 7\}$, let $Ai = \{n \in \mathrm{N} | n \leq 10000, i|n\}$. Therefore, the required answer is

$10000 - |A_2 \cup A_3 \cup A_5 \cup A_7| = 2285$

Definition [Euler Totient Function]

For a fixed $n \in \mathbb{N}$, the **Euler's totient function** is defined as $\phi(n) = |\{k \in \mathbb{N}: k \leq n, \gcd(k, n) = 1\}|$.

Thus, $\phi(n)$ is the number of natural numbers less than or equal to n and relatively prime ton.

For instance, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 3$, $\phi(12) = 4$, etc.

Definition [Derangement] A **derangement** of objects in a finite set S is a permutation/arrangement σ on S such that for each x, $\sigma(x) \neq x$. The number of derangements of $\{1, 2, \ldots, n\}$ is denoted by D_n with the convention that $D_0 = 1$.

For example, 2, 1, 4, 3 is a derangement of 1, 2, 3, 4, but 2, 3, 1, 4 is not a derangement of 1, 2, 3, 4. If a sequence (*xn*) converges to some limit `, we say that *xn* is approximately ` for large values of *n,* and write $xn \approx l$.

CHECK YOUR PROGRESS 3

1. State the Principle of Inclusion-Exclusion.

2. Define the following terms:

a. Euler Totient Function

b. Derangement

9.6 SUMMARY

The Pigeonhole Principle is an obvious but powerful tool in solving many combinatorial problems

9.7 KEYWORDS

1. Finite Subset: A **finite** set with n elements has 2^n distinct **subsets**. Any **subset** of a **finite** set is **finite**.
2. Principle: a fundamental truth or proposition that serves as the foundation for a system of belief or behaviour or for a chain of reasoning.
3. Irrational number: An **Irrational Number** is a real number that cannot be written as a simple fraction. Irrational **means** not Rational.
4. Open Interval : is an **interval** that does not include its end points.

9.8 QUESTIONS FOR REVIEW

1.Let n > m be natural numbers. Prove that

$$\sum_{k=m}^{n} C(k, m)C(n, k) = C(n, m)2^{n-m}.$$

2. Let us assume that any two garlands are same if one can be obtained from the other by rotation. Then, determine the number of distinct garlands that can be formed using 6 flowers, in the following cases.

(a) The flowers can have colors ‘red’ or ‘blue’.

(b) The flowers can have the colors ‘red’, ‘blue’ or ‘green’.

3. Prove that there exist two powers of 3 whose difference is divisible by 2021

4. Suppose that f(x) is a polynomial with integer coefficients. If f(x) = 5 for three distinct integers,

then for no integer x, f(x) can be equal to 4.

5. Suppose that f(x) is a polynomial with integer coefficients. If (a) f(x) = 14 for three distinct integers, then for no integer x, f(x) can be equal to 15.

(b) f(x) = 11 for five distinct integers, then for no integer x, f(x) can be equal to 9.

9.9 SUGGESTED READINGS

1. Kenneth H. Rosen - Discrete Mathematics and Its Applications, Tata Mc-Graw-Hill, 7th Edition, 2012.
2. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross-Discrete Mathematical Structures-Prentice Hall, 3rd Edition, 1996.
3. Grimaldi R-Discrete and Combinatorial Mathematics. 1-Pearson, Addison Wesley, 5th Edition, 2004.
4. C. L. Liu – Elements of Discrete Mathematics, McGraw-Hill, 1986.
5. F. Harary – Graph Theory, Addition Wesley Reading Mass, 1969.

6. N. Deo – Graph Theory With Applications to Engineering and Computer Science, Prentice Hall of India, 1987.
7. K. R. Parthasarathy – Basic Graph Theory, Tata McGraw-Hill, New Delhi, 1994.
8. G. Chartand and L. Lesniak – Graphs and Diagraphs, wadsworth and Brooks, 2nd Ed.,
9. Clark and D. A. Holton – A First Look at Graph Theory, Allied publishers.
10. D. B. West – Introduction to Graph Theory, Pearson Education Inc.,2001, 2nd Ed.,
11. J. A. Bondy and U. S. R. Murthy – Graph Theory with applications, Elsevier, 1976
12. J. P. Tremblay & R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co. 1997
13. S. Witala, Discrete Mathematics - A Unified Approach, McGraw Hill Book Co.

9.10 ANSWER TO CHECK YOUR PROGRESS

1. Explain the concept – 9.1
2. Explain the concept with examples--- 9.2
3. State the concept -- 9.3.1
4. Explain the Theorem, discussion and example--- 9.4
5. State the theorem and proof --9.5
6. Provide the definition (a) –9.5.1 & (B) – 9.5.2

UNIT 10: NUMBER THEORY

STRUCTURE

10.0 OBJECTIVES

Study the division algorithm

Understand the concept of greatest common divisor

Understand the meaning of prime numbers

10.1 THE DIVISION ALGORITHM

Theorem 10.1.1 *If a and b are integers and b* 6= 0*, then there is a unique pair of integers q and r, such that* $a = qb + r$ *and* $0 \leq r < |b|$.

Proof. We need to prove two things: that there is some such pair q, r (existence) and that this pair is unique (uniqueness).

Let's begin with existence. First we show that there is a pair $q, r \in \mathbb{Z}$ that satisfies $a = qb + r$ for some $r \geq 0$.

Take $q = -|ab|/b$ and $r = a + |ab|$. Since $|b| \geq 1$, it holds that $r \geq 0$. Now we need to show that such $q, r \in \mathbb{Z}$ exist with r in addition being smaller than $|b|$.

For this, consider the set S of all $r \in \mathbb{N}$ that satisfy $a = qb + r$ for some $q \in Z$. We've just shown that S is nonempty, so it must have a smallest element, call it $r0$. We have $a = q0b + r0$. If $r_0 < |b|$ we're done.

Otherwise, we have $a = (q0b + |b|) + (r0 - |b|)$, which means that $r0 - |b|$ is a smaller element of S than $r0$, leading to a contradiction. This completes the existence proof.
To prove uniqueness, suppose that $a = qb + r = sb + t$, with $0 \leq r, t < |b|$.

Thus $(q - s)b + (r - t) = 0$. Since $0 \leq r, t < |b|$, we have $|r - t| < |b|$, hence $|(q - s)b| < |b|$ and $|q - s| < 1$. Since q and s are integers, this implies $q = s$. From this we have $r = t$ and the uniqueness proof is complete

The Well-Ordering Principle. In proving the division algorithm, we considered a certain set $S \subseteq N$ and argued that since it is nonempty, it must have a smallest element. Why is this true? As with induction, we accept this proposition as an axiom. In general, the "well-ordering principle" states that *any nonempty set of natural numbers must have a smallest element.*

Remainders

A more algorithmic view of Theorem 10.1.1 is as follows: If we divide the equation
$a = qb + r$ by b we get

$$\frac{a}{b} = q + \frac{r}{b}$$

Since $0 \leq r < |b|$, we get that if $b > 0$, then $0 \leq \frac{r}{b} < 1$*and thus* $q = \left\lfloor \frac{a}{b} \right\rfloor$ the greatest integer less than or equal to a/b. If $b < 0$, then $0 \geq r\ b > -1$ and thus $q = \ a\ b$, the least integer greater or equal to a/bThis can be used to calculate q, from which we can derive r.

In Theorem 10.1.1, we call *q* the *quotient* and *r* the *remainder*. We use the notation *r* = *a* rem *b* to denote that *r* is the remainder when *a* is divided by *b*. There is no need for a special notation for quotient, since we can just $\left\lfloor \frac{a}{b} \right\rfloor$ and $\left\lceil \frac{a}{b} \right\rceil$ depending on the sign of *b*.

Definition: If *a* and *b* are such that *a* rem *b* = 0 we say that *a* is a *multiple* of *b*, or that *b divides a* (or is a *divisor* of *a*). Note that this holds when there exists some integer *q*, such that *a* = *qb*. In particular, every integer divides 0, and every integer is a multiple of 1. When *b* divides *a* we write $b|a$, and when *b* does not divide *a* we write $b \nmid a$.

Definition: An integer *u* is called a *linear combination* of a set of integers $a_1, a_2, \ldots, a_n$
if and only if there exist integer coefficients $c_1, c_2, \ldots, c_n$ that satisfy

$$u = \sum_{i=1}^{n} c_i a_i$$

Theorem 10.1.2. *Properties of divisibility:*
(a) If b|a and c|b then c|a.
(b) If b|a and a $\neq 0$ *then* $|b| \le |a|$.
*(c) If b divides each of a*1*, a*2*, . . . , an, then b divides all linear combinations of* $a_1, a_2, \ldots, a_n$.
(d) a|b and b|a if and only if a = ±*b.*

Proof. We prove the properties in turn:
(a) Since *b*|*a*, there exists an integer *q*, such that *a* = *qb*. Similarly, there exists an integer *r*, such that *b* = *rc*. Thus *a* = *qb* = *qrc*. Since *qr* is an integer, it holds that *c*|*a*.
(b) Since *b*|*a*, there exists an integer *q*, such that *a* = *qb*. This implies |*a*| = |*q*| · |*b*|. Assume for the sake of contradiction that *a* 6= 0 but |*b*| > |*a*|. Then |*q*|·|*b*| < |*b*|. Since |*b*| > |*a*| > 0, we can divide by |*b*| to get |*q*| < 1, implying *q* = 0. Thus *a* = *qb* = 0, which is a contradiction.
(c) Consider a linear combination $u = \sum_{i=1}^{n} c_i a_i$ Since *b*|*ai*, there exists an integer *qi*, such that *ai* = *qib*, for all 1 ≤ *i* ≤ *n*. Thus

$$u = \sum_{i=1}^{n} c_i a_i = \sum_{i=1}^{n} c_i q_i b = b \cdot \sum_{i=1}^{n} c_i q_i.$$

Since $\sum_{i=1}^{n} c_i q_i$ is an integer, we have $b|u$.

(d) For the "if" statement, note that if $a = \pm b$ then $b = qa$ and $a = qb$, for $q = \pm 1$, so $a|b$ and $b|a$. To prove the "only if" statement, assume that $a|b$ and $b|a$. This implies the existence of integers q and r, such that $b = qa$ and $a = rb$. Thus $b = qrb$. If $b = 0$ then $a = 0$ and the claim that $a = \pm b$ holds. Otherwise we can divide by b to get $qr = 1$. Note that in this case $q, r \neq 0$. Part (b) of the

theorem implies that $|q| \leq 1$ and $|r| \leq 1$. Thus $q, r = \pm 1$ and the claim that $a = \pm b$ follows

10.2 GREATEST COMMON DIVISORS

If $d|a$ and $d|b$ then d is a *common divisor* of a and b. For example, 1 is a common divisor of any pair a, b. If a and b are not both 0 then, by Theorem 10.1.2 (b), anycommon divisor of a and b is not greater than $\max(|a|, |b|)$. Thus the set of common divisors of a and b has a largest element, called the *greatest common divisor* of a and b, or gcd(a, b). This is the integer d that satisfies the following two criteria:

- $d|a$ and $d|b$.
- If $c|a$ and $c|b$ then $c \leq d$.

OR

Let a and b be two nonzero integers. Then the set S of their common positive divisors is nonempty and finite. Thus, S contains its greatest element. This element is called the **greatest common divisor** of a and b and is denoted by gcd(a, b). The gcd is also called the **highest common factor**

Note that when $a = b = 0$, there is no greatest common divisor, since any integer divides 0. When a and b are not both 0, we often want to compute gcd(a, b) efficiently.

Note that the set of divisors of a and $-a$ is the same, and similarly for b and $-b$. Furthermore, if $a = 0$ then gcd(a, b) = b, and if $a = b$ then gcd(a, b) = $a = b$. Thus it suffices to concentrate on the case $a > b > 0$, without loss of generality.

Since $1 \leq \gcd(a, b) \leq b$, we can just test all integers between 1 and b and choose the largest one that divides both a and b. However, there is a much more efficient way to find greatest common divisors, called Euclid's algorithm. This algorithm, one of the earliest in recorded history, is based on the following lemma.

Lemma *If* $a = qb + r$ *then* $\gcd(a, b) = \gcd(b, r)$.

Proof. By Theorem 10.1.2 (c), all common divisors of b and r also divide a, since a is a linear combination of b and r. Thus a common divisor of b and r is also a common divisor of a and b. Similarly, since $r = a - qb$, a common divisor of a and b also divides r, so it is a common divisor of b and r. Thus a, b and b, r have the same set of common divisors, and in particular the same greatest common divisor.

With this lemma in our toolbelt, Euclid's algorithm is easy to describe. To find $\gcd(a, b)$, use the division algorithm (Theorem 4.1.1) to represent $a = qb + r$, where $0 \leq r < b$. (Remember that we are assuming that $a > b > 0$.) If $r = 0$ then $b|a$ and $\gcd(a, b) = b$. Otherwise $\gcd(a, b) = \gcd(b, r)$ and $b > r > 0$. We can thus repeat the above procedure recursively with the pair b, r. Every recursive call strictly reduces both numbers in the pair, so after at most b steps the algorithm will terminate with a valid greatest common divisor of a and b.

Greatest common divisors and linear combinations

10.2.1 Theorem

For two integers a and b that are not both 0, $\gcd(a, b)$ *is a linear combination of a and b.*

Proof. As above, we can concentrate on the case $a > b > 0$. The proof proceeds bystrong induction on the value of a. In the base case, $a = 2$, $b = 1$, and $\gcd(a, b) =1 = 0 \cdot a + 1 \cdot b$. Assume that the theorem holds for all pairs a, b with $0 < b < a \leq k$.

Consider a pair a', b' with $0 < b' < a' = k + 1$. If $b'|a'$then $\gcd(a', b') = b_0$ and the theorem trivially holds. Otherwise use the division algorithm to express $a' = qb' + r$, where $0 < r < b_0$. By the induction hypothesis, there exist coefficients u and v, such that $\gcd(b_0, r) = ub0 + vr$.

Lemma 10.2.1shows that $\gcd(a', b') = \gcd(b', r)$, therefore
$\gcd(a', b') = ub' + vr = ub' + v(a' – qb') = va' + (u − vq)b'$. This shows that $\gcd(a', b')$
is a linear combination of $a0$ and $b0$ and completes the proof by induction.\

Corollary: *An integer z is a linear combination of a and b if and only if it is a multiple of* $\gcd(a, b)$. *In particular,* $\gcd(a, b)$ *is the least positive linear combination of a and b.*
Proof. By 10.1.2 (c), since $\gcd(a, b)$ divides both a and b, it divides any linear combination z of a and b, and thus z is a multiple of $\gcd(a, b)$. On the other hand, we know by Bezout's identity that there are coefficients u and v, such that $\gcd(a, b) = ua + vb$, so if $z = c \cdot \gcd(a, b)$, then $z = c(ua + vb) = (cu)a + (cu)v$.

10.2.2 Theorem [Bezout's identity]

´ Let a and b be two nonzero integers and let d = $\gcd(a, b)$. *Then there exist integers* x_0, y_0 *such that* $d = ax_0 + by_0$.

Proof. Consider the set $S = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Then, either $a \in S$ or $-a \in S$. Thus, S is a
nonempty subset of N. By the well ordering principle, S contains its least element, say d. As $d \in S$, we have $d = ax_0 + by_0$, for some $x_0, y_0 \in \mathbb{Z}$. We show that $d = \gcd(a, b)$.
By the division algorithm, there exist integers q and r such that $a = dq + r$, with $0 \le r < d$. If
$r > 0$, then
$r = a - dq = a - q(ax0 + by0) = a(1 - qx0) + b(-qy0) \in \{ax + by : x, y \in \mathbb{Z}\}$.

In this case, r is a positive integer in S which is strictly less than d. This contradicts the choice of d as the least element of S.

Thus, $r = 0$. Consequently, $d|a$. Similarly, $d|b$. Hence $d \leq \gcd(a, b)$.

Now, $\gcd(a, b)|a$ and $\gcd(a, b)|b$. Since $d = ax0 + by0$ for some $x0, y0 \in$ Z, we have $\gcd(a, b)|d$.

That is, $d = k \times \gcd(a, b)$ for some integer k. However, both $\gcd(a, b)$ and d are positive. Thus k is a positive integer. Hence $d \geq \gcd(a, b)$.

Therefore, $d = \gcd(a, b)$.

We prove three useful corollaries to B´ *e*zout's identity.

Corollary. Let a, b ∈ Z and let d ∈ N. Then, d = gcd(a, b) if and only if d|a, d|b, and each common divisor of a and b divides d.

Proof. Suppose $d = \gcd(a, b)$. Then $d|a$ and $d|b$. By B´ *e*zout's identity, $d = ak + bm$ for some $k, m \in$ Z.

Thus, any common divisor of a and b divides $d = \gcd(a, b)$.

Conversely, suppose $d|a$, $d|b$ and each common divisor of a and b divides d. Since d is a common divisor of a and b, by what we have just proved, $d|\gcd(a, b)$. Further, $\gcd(a, b)$ is a common divisor of a and b; so, by assumption $\gcd(a, b)|d$. So, $d = \gcd(a, b)$.

Corollary. *Let a, b be nonzero integers. Then* $\gcd(a, b) = 1$ *if and only if there exist integers*

x_0 *and* y_0 *such that* $ax_0 + by_0 = 1$.

Proof. If $\gcd(a, b) = 1$, then by B´ *e*zout's identity, there exist integers $x0$ and $y0$ such that $ax_0+by_0 = 1$.

Conversely, suppose there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$. If $\gcd(a, b) = k$, then k is a positive integer such that $k|1$. It follows that $k \leq 1$; consequently, $k = 1$.

Corollary. *Let* $n_1, \ldots, n_k$ *be positive integers which are pairwise coprimes. If* $a \in$ Z *is such that* $n_1|a, \ldots, n_k|a$, *then* $n_1 \cdots n_k|a$.

Proof. The positive integers $n1, \ldots, nk$ are pair wise coprimes means that if i 6= j, then gcd(ni, nj) = 1.

Let $a \in \mathbb{Z}$ be such that $n_1|a, \ldots, n_k|a$. We show by induction that $n_1 \cdots n_k|a$. For $k = 2$, it is given that $n_1|a$, $n_2|a$ and gcd(n_1, n_2) = 1. By B´ ezout's identity, there exist $x, y \in \mathbb{Z}$ such that $n_1x+n_2y = 1$.

Multiplying by a, we have $a = an_1x + an_2y = n_1n_2\left(x\left(\frac{a}{n_2}\right)+y\left(\frac{a}{n_1}\right)\right)$.

Since n$_2$|a and n$_1$|a, we see that $\frac{a}{n_2}, \frac{a}{n_1} \in$ Z so that $\left(x\left(\frac{a}{n_2}\right)+y\left(\frac{a}{n_1}\right)\right) \in$ Z.

Hence n$_1$n$_2$|a. Assume the induction hypothesis that the statement is true for k = m. Let each of n$_1$, . . . , n$_{m+1}$ divide a and that they are pairwise coprimes. Let n$_1$ · · · n$_m$ = `. Then gcd(l, n$_{m+1}$) = 1. By the induction hypothesis, l |a. By the basis case, (k = 2 as proved), we conclude that l, n$_{m+1}$|a. That is, n$_1$ · · · n$_{m+1}$|a. $\left(x\left(\frac{a}{n_2}\right)+y\left(\frac{a}{n_1}\right)\right)$.

Since $n_2|a$ and $n_1|a$, we see that $\frac{a}{n_2}, \frac{a}{n_1} \in$ Z so that $\left(x\left(\frac{a}{n_2}\right)+y\left(\frac{a}{n_1}\right)\right)$. $\in$ Z. Hence $n_1n_2|a$.

Assume the induction hypothesis that the statement is true for $k = m$. Let each of n1, . . . , nm+1
divide a and that they are pairwise coprimes. Let $n_1 \cdots n_m = l$. Then gcd(l, n_{m+1}) = 1.
By the induction hypothesis, l |a. By the basis case, (k = 2 as proved), we conclude that ` $n_{m+1}|a$. That is, $n_1 \cdots n_{m+1}|a$.

The division algorithm helps to algorithmically compute the greatest common divisor of two nonzero integers, commonly known as the Euclid's algorithm.

Let a, and b be nonzero integers. By the division algorithm, there exists integers q and r with $0 \leq r < |b|$ such that $a = |b|q + r$. We apply our observation that a common divisor of two integers divides their gcd.
Now, gcd($|b|$, r) divides both $|b|$ and r; hence it divides a. Again, gcd($|b|$, r) divides both a and $|b|$. Hence gcd($|b|$, r)| gcd(a, $|b|$).
Similarly, with $r = a - |b|q$, we see that gcd(a, $|b|$) divides both a and $|b|$; hence gcd(a, $|b|$)|r.

Consequently, gcd(a, $|b|$)| gcd($|b|$, r).

Further, the gcd of any two integers is positive. Thus,

$$\gcd(a, b) = \gcd(a, |b|).$$

So, we obtain

$$\gcd(a, b) = \gcd(a, |b|) = \gcd(|b|, r).$$

Euclid's algorithm applies this idea repeatedly to find the greatest common divisor of two given nonzero integers, which we now present.

Euclid's algorithm

Input: Two nonzero integers a and b; Output: gcd(a, b).

$$\begin{array}{rcll}
a & = & b\,q_0 + r_0 & \text{with} \quad 0 \le r_0 < b \\
b & = & r_0\,q_1 + r_1 & \text{with} \quad 0 \le r_1 < r_0 \\
r_0 & = & r_1\,q_2 + r_2 & \text{with} \quad 0 \le r_2 < r_1 \\
r_1 & = & r_2\,q_3 + r_3 & \text{with} \quad 0 \le r_3 < r_2 \\
 & & \vdots & \\
r_{l-1} & = & r_l\,q_{l+1} + r_{l+1} & \text{with} \quad 0 \le r_{l+1} < r_l \\
r_l & = & r_{l+1}\,q_{l+2} & \\
\gcd(a, b) & = & r_{l+1} &
\end{array}$$

The process will take at most $b - 1$ steps as $0 \le r_0 < b$. Also, note that r_{l+1}can be expressed in the form $r_{l+1} = a\,x_0 + b\,y_0$ for integers x_0, y_0 using backtracking.

That is,

$$r_{l+1} = r_{l-1} - r_l\,q_{l+1} = r_{l-1} - q_{l+1}\,(r_{l-2} - r_{l-1}\,q_l) = r_{l-1}\,(1 + q_{l+1}\,q_l`) - q_{l+1}\,r_{l-2} = \cdots$$

Example

We apply Euclid's algorithm for computing gcd(155, −275) as follows.

−275 = (−2) · 155 + 35 (so, gcd(−275, 155) = gcd(155, 35))

155 = 4 · 35 + 15 (so, gcd(155, 35) = gcd(35, 15))

35 = 2 · 15 + 5 (so, gcd(35, 15) = gcd(15, 5))

15 = 3 · 5 (so, gcd(15, 5) = 5).

To write 5 = gcd(155, −275) in the form $155x_0 + (-275)y_0$, notice that

5 = 35− 2· 15 = 35− 2(155− 4· 35) = 9· 35− 2· 155 = 9(−275 + 2· 155)−

$2 \cdot 155 = 9 \cdot (-275) + 16 \cdot 155$.

Also, note that $275 = 5 \cdot 55$ and $155 = 5 \cdot 31$ and thus, $5 = (9 + 31x) \cdot (-275) + (16 + 55x) \cdot 155$, for all $x \in$ Z. Therefore, we see that there are infinite number of choices for the pair $(x, y) \in \mathbb{Z}^2$, for which $d = ax + by$

Check Your Progress1

1. Explain the Well-ordering Principle

2. Explain the concept of Greatest Common Divisor

10.3 LEAST COMMON MULTIPLE

Definition. The **least common multiple** of integers *a* and *b*, denoted as lcm(*a, b*), is the smallest positive integer that is a multiple of both *a* and *b*.

Lemma 10.3.1 . *Let a, b* ∈ Z *and let* ` ∈ N. *Then,* ` = lcm(*a, b*) *if and only if a*|`, *b*|` *and* ` *divides each common multiple of a and b.*

Proof. Let ` = lcm(*a, b*). Clearly, *a*|` and *b*|`. Let *x* be a common multiple of both *a* and *b*. If ` - *x*, then by the division algorithm, *x* = ` · *q* + *r* for some integer *q* and some *r* with 0 < *r* < `. Notice that *a*|*x* and *a*|`. So, *a*|*r*. Similarly, *b*|*r*. That is, *r* is a positive common multiple of both *a* and *b* which is less than lcm(*a, b*). This is a contradiction. Hence, ` = lcm(*a, b*) divides each common multiple of *a* and *b*.

Conversely, suppose *a*|*l*, *b*|*l* and ` divides each common multiple of *a* and *b*. By what we have just proved, lcm(*a, b*)|`. Further, lcm(*a, b*) is a common multiple of *a* and *b*. Thus *l*| lcm(*a, b*). We conclude that *l* = lcm(*a, b*).

10.3.1 Theorem

Let a, b ∈N. Then gcd(a, b) · lcm(a, b) = ab*. In particular,* lcm(a, b) = ab *if and only if* gcd(a, b) = 1.

Proof. Let d = gcd(a, b). Then $a = a_1d$ and $b = b_1d$ for some a_1, b_1 ∈N. Further,

$$ab = a_1d\, b_1d = (a_1b_1d) \cdot \gcd(a, b).$$

Thus, it is enough to show that lcm(a, b) = a_1b_1d.

Towards this, notice that $a1b1d$ = $ab1$ = $a1b$, that is, $a|a1b1d$ and $b|a1b1d$. Let c ∈N be any common multiple of a and b. Then $\frac{c}{a}, \frac{c}{b} \in \mathbb{Z}$. Further, by B´ ezout's identity, $d = as + bt$ for some s, t ∈Z. So

$$\frac{c}{a_1b_1d} = \frac{cd}{(a_1d)\cdot(b_1d)} = \frac{c(as+bt)}{ab} = \frac{c}{b}s + \frac{c}{a}t \in \mathbb{Z}.$$

Hence $a1b1d|c$. That is, $a1b1d$ divides each common multiple of a and b. By Lemma 10.3.1 , $a1b1d$ = lcm(a, b).

10.4 PRIME NUMBERS

Definition: An integer $p > 1$ is said to be *prime* if its only positive divisors are 1 and p itself. All other integers greater than 1 are called composite. A composite number n can be written as a product $n = ab$ of two strictly smaller numbers $1 < a, b < n$. Note that, by convention, 1 is neither prime nor composite.

Here are all primes below 100:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Given a prime p and another integer a, either a is a multiple of p or gcd(p, a) = 1. Indeed, gcd(p, a) divides p, so it must be either 1 or p, and since gcd(p, a) also divides a then either gcd(p, a) = 1 or a is a multiple of p. This can be used to prove a very important property of primes:

Theorem 10.4.1. *Let p be a prime.*

(a) Given two integers a and b, if $p|ab$ then either $p|a$ or $p|b$.

(b) Given k integers $a1, a2, \ldots, ak$, if $p|\prod_{i=1}^{k} a_i$then $p|ai$ for some $1 \le i \le k$.

Proof.

(a) If $p|a$ we are done. Otherwise gcd(p, a) = 1 and by Bezout's identity there exist linear coefficients u and v for which $1 = ua + vp$. Multiplying both sides by b we get $b = uab + vpb$. Since p divides ab, p divides the whole sum $uab + vpb$.

Therefore $p|b$.

(b) The proof proceeds by induction. The case $k = 1$ is trivial and $k = 2$ is handled in part (a). So we assume that the claim holds for some $k > 1$ and prove that it also holds for $k + 1$. Given that $p|\prod_{i=1}^{k+1} a_i$ we put $b = \prod_{i=1}^{k} a_i$ Since, $p|ba_{k+1}$ part (a) implies that either $p|a_{k+1}$ or $p|b$. In both cases the claim holds, in the latter case by the induction hypothesis. This completes the proof by induction.

10.4.1 Theorem (Fundamental Theorem of Arithmetic).

Every positive integer can

be represented in a unique way as a product of primes, $n = p_1p_2 \cdots p_k$

($p_1 \le p_2 \le \ldots \le p_k$).

Proof. We first prove existence and then uniqueness. Actually, we already proved existence in one of the previous lectures as an illustration of strong induction, but give the prove here again for completeness. So, to prove that every integer can be represented as a product of primes we use strong induction. The base case $n = 1$ holds because the *empty product,* as we previously discussed, is defined to equal 1.

The induction hypothesis assumes that for some $n > 1$, all positive integers $k < n$ can be represented as a product of primes. If n is prime, then it is trivially a product of primes.

Otherwise it can be written as $n = ab$, for $1 < a, b < n$. By the induction hypothesis, both a and b are products of primes, so their product n is also a product of primes. This proves existence.

The proof that the above representation is unique proceeds by contradiction. Assume then that there exists some positive integer that can be represented as a product of primes in (at least) two ways. By the well-ordering principle, there is a smallest such integer n. It holds that $n = p_1p_2 \cdot\cdot\cdot p_k = q_1q_2 \cdot\cdot\cdot q_l$, where $p_1 \leq p_2 \leq . . . \leq p_k$, $q_1 \leq q_2 \leq . . . \leq q_l$, and $pi \neq qi$ for some i. By Theorem 10.3.1(b), since $p_i|q_1q_2 \cdot\cdot\cdot q_l$, there must exist some qj for which $p_{i|}q_j$. Since q_j is prime and $p_i > 1$, this can only occur when $p_i = q_j$. Thus we can eliminate p_i and q_j from the equation $p_1p_2 \cdot\cdot\cdot p_k = q_1q_2 \cdot\cdot\cdot q_l$ and get two distinct representations of the positive integer number n/pi as a product of primes. This contradicts the assumption that n is the smallest positive integer with this property, and concludes the proof of uniqueness.

The infinity of primes

Here is another fundamental result with a proof from Euclid's *Elements*:

10.4.3 Theorem There Are Infinitely Many Primes.

Proof. Assume for the sake of contradiction that there is only a finite set of primes,

$p_1, p_2, . . . , p_n$. Consider the number $p = p_1p_2 . . . p_{n+1}$.

By Theorem 10.3.2, p has a prime divisor, which has to be pi, for some $1 \leq i \leq n$. Since p_i divides both p and $p_1p_2 . . . p_n$, it also divides $p - p_1p_2 . . . p_n = 1$. However, this is impossible since $p_i > 1$. This contradiction proves the theorem.

Let's get some more mileage out of Euclid's proof. The results below show that not only do the primes never stop, but the number of primes $p \leq x$ is at least a certain natural function of x, namely at least log log x. (Here the base of the logarithm is 2.)

10.4.2 Theorem

The n-th prime pn satisfies pn $\leq 2^{2^{n-1}}$ *for all n* ≥ 1.

Proof. We proceed using strong induction. For the base case, the first prime is $2 = 2^{2^0}$. Assume that the claim holds for all primes *p*1 through p_k. Consider $p = p_1p_2 \ldots p_{k+1}$. As in the above proof, *p* has a prime factor that is not one of the first *k* primes. This prime factor is thus at least as large as p_{k+1}, which implies

$$\begin{aligned} p_{k+1} \leq p = p_1p_2 \ldots p_k + 1 &\leq 2^{2^0}2^{2^1} \cdots 2^{2^{k-1}} + 1 \\ &= 2^{1+2+4+\ldots+2^{k-1}} + 1 \\ &= 2^{2^k-1} + 1 \\ &= \frac{1}{2}2^{2^k} + 1 \\ &\leq 2^{2^k}. \end{aligned}$$

This is precisely the induction step we needed, and concludes the proof by strong induction. Denote by $\pi(x)$ the number of primes $p \leq x$.

Corollary: *For* $x \geq 2$, $\pi(x) \geq \lfloor \log \log x \rfloor + 1$.

Proof. Plugging *n* = *b*log log *xc* + 1 into Theorem 10.3.4 implies that the *n*-th prime is at most *x*. Thus there are at least *n* primes below *x*. For general education, you should know that this is by far not the best possible estimate. A celebrated achievement in number theory is the Prime Number Theorem due to Hadamard and de la Vall´ee Poussin, which states that *x/* ln *x* (here we use the natural logarithm) is the “right” bound, in the sense that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} \to 1.$$

Check Your Progress1

1. What is Least common multiple?

____

____

____

2. Explain the concept of the infinity of primes

10.5 SUMMARY

Number theory has wide application in mathematics, computer science and almost every science related topics.

10.6 KEYWORDS

1. Divisor: a number by which another number is to be divided.

2. Multiple: a number that may be divided by another a certain number of times without a remainder.

3. Algorithm: a process or set of rules to be followed in calculations or other problem-solving operations

4. Mathematical Induction is a mathematical technique which is used to prove a statement, a formula or a theorem is true for every natural number

10.7 QUESTIONS FOR REVIEW

1. Prove The n-th prime pn satisfies pn ≤ $2^{2^{n-1}}$for all n ≥ 1.

2. Explain for two integers a and b that are not both 0, gcd(a, b) is a linear combination of a and b.

3.State the properties of divisibility and prove them

4. Explain the concept of remainder

10.8 SUGGESTED READINGS

1. Kenneth H. Rosen - Discrete Mathematics and Its Applications, Tata Mc-Graw-Hill, 7th Edition, 2012.
2. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross-Discrete Mathematical Structures-Prentice Hall, 3rd Edition, 1996.
3. Grimaldi R-Discrete and Combinatorial Mathematics. 1-Pearson, Addison Wesley, 5th Edition, 2004.
4. C. L. Liu – Elements of Discrete Mathematics, McGraw-Hill, 1986.
5. F. Harary – Graph Theory, Addition Wesley Reading Mass, 1969.
6. N. Deo – Graph Theory With Applications to Engineering and Computer Science, Prentice Hall of India, 1987.
7. K. R. Parthasarathy – Basic Graph Theory, Tata McGraw-Hill, New Delhi, 1994.
8. G. Chartand and L. Lesniak – Graphs and Diagraphs, wadsworth and Brooks, 2nd Ed.,
9. Clark and D. A. Holton – A First Look at Graph Theory, Allied publishers.
10. D. B. West – Introduction to Graph Theory, Pearson Education Inc.,2001, 2nd Ed.,
11. J. A. Bondy and U. S. R. Murthy – Graph Theory with applications, Elsevier, 1976
12. J. P. Tremblay & R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co. 1997
13. S. Witala, Discrete Mathematics - A Unified Approach, McGraw Hill Book Co.

10.9 ANSWER TO CHECK YOUR PROGRESS

1. In general, the “well-ordering principle” states that *any nonempty set of natural numbers must have a smallest element*
2. Explain the concept --10.2
3. Provide the definition -- 10.3
4. Explain the Theorem with proof --- 10.4.3

UNIT 11: NUMBER THEORY – II

STRUCTURE

11.0 OBJECTIVE

Comprehend the concept of congruence, modular division.

Understand the number theory in cryptography

11.1 INTRODUCTION

We usually associate arithmetic with the infinite set of integer numbers. However, *modular arithmetic* on finite sets is commonly used in our daily life. As an example, if it is now 1 am and we let 1000 hours pass, what time will it be? We can use the division algorithm to see that 1000 = 41 × 24 + 16 and conclude that adding 1000 hours is like adding 16 hours, since the clock returns to the same position every 24 hours. So after 1000 hours it will be 5 pm (17 hours after midnight). There are many examples in which it is natural and useful to limit our number system to a finite range of integers, such as 0 through $n-1$, for some n. This number system is denoted by $\mathbb{Z}n$. Days of the week, hours of the day, minutes in an hour are all familiar examples of finite number systems, as are numbers in microprocessor registers, commonly limited to 32 binary digits.

Modular arithmetic allows us to add, subtract, multiply, and sometimes divide numbers while staying within the finite set $\mathbb{Z}n$. The number n is called the *modulus.* A central notion in modular arithmetic is *congruence*. We say that two integers are congruent modulo n if they leave the same remainder when divided by n.

11.2 CONGRUENCE

Definition: Two integers $a, b \in \mathbb{Z}$ are said to be *congruent modulo n*, written as $a \equiv_n b$ or $a \equiv b$ (mod n), if and only if they leave the same remainder when divided by n, that is, a rem n = b rem n.

Lemma *$a \equiv n\ b$ if and only if $n|(a - b)$.*

Proof: If $a \equiv n\ b$ then a rem n = b rem n. Put r = a rem n = b rem n. Then there exist two integers $q1$ and $q2$, such that $a = q_1n + r$ and $b = q_2n + r$. Subtracting the second equation from the first, we get $a - b = (q_1 - q_2)n$ and $n|(a - b)$.

On the other hand, if $n|(a-b)$ then there exists an integer d, such that $a-b = nd$. By the division algorithm, there exist integers $q_1, q_2 \in$ Z, and $0 \leq r_1, r_2 < n$, such that $a = q_1n + r_1$ and $b = q_2n + r_2$. Thus $(q_1 - q_2)n + (r_1 - r_2) = nd$, and $r_1 - r_2 = (q_2 - q_1 + d)n$. Thus $n|(r_1 - r_2)$. However, $|r_1 - r_2| < n$, so necessarily $r_1 - r_2 = 0$, which implies that a rem n = b rem n, and $a \equiv n\ b$.

You should use the definition to verify that for any $a, b, c \in \mathbb{Z}$,

- $a \equiv n\ a$. (Reflexivity.)
- If $a \equiv n\ b$ then $b \equiv n\ a$. (Symmetry.)
- If $a \equiv n\ b$ and $b \equiv n\ c$ then $a \equiv n\ c$. (Transitivity.)

The operations of addition, subtraction, and multiplication on $\mathbb{Z}n$ are defined by first doing the corresponding operation in Z and then taking the remainder modulo

n. That is, if we denote these respective operations by $+n$, $-n$, and $\cdot n$, then

$a +_n b = (a + b)$ rem n

$a -_n b = (a - b)$ rem n

$a \cdot_n b = (ab)$ rem n

Exponentiation is defined through repeated multiplication.

Lemma *Properties of congruence:*

(a) (a rem n) rem n = a rem n

(b) (a rem n) $\equiv_n a$

(c) (ab) rem n = (a rem n)(b rem n) rem n

(d) (a rem n)(b rem n) $\equiv_n ab$

(e) $\prod_{i=1}^{k}(a_i \text{ rem } n)$ $i \equiv_n \prod_{i=1}^{k} a_i$

(f) If $a_1 \equiv_n a_2$ *and* $b_1 \equiv_n b_2$ *then*

$$a_1 + b_1 \equiv_n a_2 + b_2$$

$$a1 - b_1 \equiv_n a_2 - b_2$$

$$a_1 b_1 \equiv_n a_2 b_2$$

Proof. (b) is just a restatement of (a). To prove these we need to show that $n|(a - (a$ rem $n))$.

Put $r = a$ rem n. By the division algorithm, there exists $q \in$ Z, such that $a = qn + r$. Thus $a - r = qn$, which implies that $n|a - r$ and concludes the proof.

(d) is a restatement of (c), and (e) can be proved from (d) by induction.

To prove (c) we need to show that $n|(ab - (a$ rem $n)(b$ rem $n))$.

Use the division algorithm to represent $a = q_1 n + r_1$ and $b = q_2 n + r_2$. Then

$ab - (a$ rem $n)(b$ rem $n) = (q_1 n + r_1)(q_2 n + r_2) - r_1 r_2 = (q_1 q_2 n + r_1 q_2 + q_1 r_2)n$,

which implies the claim.

We now prove (f). We know that $n|(a_1 - a_2)$ and $n|(b_1 - b_2)$. That is, there exist integers q and s, such that $a1-a2 = qn$ and $b1-b_2 = s_n$.

Adding these equations gives $(a_1 + b_1) - (a_2 + b_2) = (q + s)n$, which yields the first part of the claim.

Subtracting similarly gives the second part.

Writing $a_1 = a_2+qn$ and $b_1 = b_2+sn$ and multiplying the equations gives

$$a_1b_1 = a_2b_2 + b_2qn + a_2sn + qsn^2$$
$$a_1b_1 - a_2b_2 = (b_2q + a_2s + qsn)n,$$

Which yields the third part.

11.3 MODULAR DIVISION

The division operation is not defined for the integers in general: There is no integer that corresponds to 5 divided by 4, for instance. (In other words, there is no $x \in \mathbb{Z}$, such that $4x = 5$.) This distinguishes $\mathbb{Z}$ from sets like $\mathbb{Q}$ or $\mathbb{R}$ that are *closed under division*.

Division in $\mathbb{Z}_n$ appears even more unruly. For example, in $\mathbb{Z}_6$, the equation $2x = 4$ is satisfied by both $x = 2$ and $x = 5$, while the equation $2x = 3$ has no solutions. So the notion of "*b* divided by *a*" can be undefined or even ambiguous in $\mathbb{Z}_n$. In particular, we cannot generally cancel a multiplier from both sides of a congruence, that is, if $ab \equiv_n ac$ we cannot reason that $b \equiv^n c$. To take the above illustration,

$2 \cdot 2 \equiv_6 2 \cdot 5$, but $2 \not\equiv_6 5$.

Quite remarkably, however, the division operation is well-defined when *n* is a prime *p*. Thus Z*p* is in a sense as well-behaved as the real numbers, despite being a finite set! After a small digression that explores what "well-behaved" actually means here, we will state an even more general result on modular division.

Digression (notions from abstract algebra): There is a way to precisely state what we mean by "well-behaved" above. Jumping the gun, I'll say that $\mathbb{Z}_p$ is a *field*, not just a *ring*. Now let me tell you what this means. The notion of a ring in algebra is meant to abstract our intuition concerning the essential properties of the integers.

Given a set S equipped with two operations, + (addition) and · (multiplication), we say that S is a ring if the following all hold for any a, $b, c \in S$:

- $a + b \in S$ and $a \cdot b \in S$.
- $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- $a + b = b + a$ and $a \cdot b = b \cdot a$.
- $a \cdot (b + c) = a \cdot b + a \cdot c$.
- There exists an *additive identity* element $0 \in S$ that satisfies $a + 0 = a$ and a *multiplicative identity* element $1 \in S$ that satisfies $a \cdot 1 = a$ for all $a \in S$. For every $a \in S$ there exists an *additive inverse* $-a \in S$ for which $a+(-a) = 0$.

All the number systems we have encountered so far are rings, including Z, Q, R, and Z$_n$. However, some of them possess additional structure that allows the division operation. Namely, a ring is said to be a *field* if, in addition to the above, the following holds

- For every $a \in S$, such that a 6= 0, there exists a *multiplicative inverse* $a-1 \in S$ for which $a \cdot a-1 = 1$.

The number systems R and Q, as well as Zp when p is prime, are fields. In fields the division operation is well-defined, and $b/a = b{\cdot}a-1$, as can be verified by plugging $x = b \cdot a-1$ into the equation $ax = b$. A field with a finite number of elements is called a *Galois field*, after the French mathematician Everest Galois. (A feisty young man who died in a duel at the age of 20, *after* making significant enough contributions to mathematics to have a whole field (sic) named in his honor!) Anyway, now that we know what fields are, let's see why $\mathbb{Z}_p$ is one. In fact, we prove something more general:

11.3.1 Theorem

If a and n are coprime then there exists exactly one $x \in \mathbb{Z}_n$ *for which* $ax \equiv_n b$, *for any* $b \in$ Z.

Proof. We need to prove existence and uniqueness of x as described in the theorem. $ax \equiv_n b$ if and only if there exists $q \in Z$, such that $ax - b = nq$, or $ax - nq = b$. Now, since $\gcd(a, n) = 1$, any integer, including b, is a linear combination of a and n. This proves existence.

To prove uniqueness, assume that for $x, y \in \mathbb{Z}_n$ it holds that $ax \equiv_n b$ and $ay \equiv_n b$. Thus $ax-ay \equiv n\ 0$, or $n|a(x-y)$. As you proved in one of the homework assignments, since n and a are coprime, this implies that $n|(x - y)$, and therefore that $x - y \equiv_n 0$.

Thus $x \equiv_n y$, which proves uniqueness.

Corollary *For a prime p and any a, b* $\in Z$, *such that* $a \not\equiv_p 0$, *there exists exactly one* $x \in \mathbb{Z}_p$ *for which* $ax \equiv_p b$. The fact that division is well-defined in $\mathbb{Z}_p$ when p is prime also means that cancelations become valid. Thus if $a \not\equiv_p 0$ and $ab \equiv p\ ac$ we can safely conclude that $b \equiv_p c$.
We now know that b/a is well-defined in $\mathbb{Z}_p$, but how do we find it? That is, how do we find $x \in \mathbb{Z}_p$, for which $ax \equiv_p b$. This question is particularly important when p is large and it takes too long to simply enumerate all the elements of $\mathbb{Z}_p$, Fortunately, the following result, known as *Fermat's Little Theorem*, can help us:

11.3.3 Theorem

For a prime p and any $a \not\equiv_p 0$, $a^{p-1} \equiv_p 1$.
Proof. Consider the set S, defined as $1 \cdot a, 2 \cdot a, \ldots, (p - 1) \cdot a$. None of these $p - 1$ integers are congruent modulo p, since we have seen that if $ia \equiv_p ja$ then $i \equiv_p j$. However, each element of S is congruent to some element of c. Since there are $p - 1$ elements in S and $p - 1$ nonzero elements in $\mathbb{Z}_p$ the elements of S must be congruent to each of $1, 2, \ldots, (p - 1)$ in some order. Therefore,
$1 \cdot 2 \cdot \cdots \cdot (p - 1) \equiv_p 1a \cdot 2a \cdot \cdots \cdot (p - 1)a$,
or $1 \cdot 2 \cdot \cdots \cdot (p - 1) \equiv_p 1 \cdot 2 \cdot \cdots \cdot (p - 1) \cdot a^{p-1}$.
We can cancel each of $1, 2, \ldots, (p - 1)$ from both sides of the congruence, obtaining

$a^{p-1} \equiv_p 1$.

Fermat’s Little Theorem allows us to quickly perform division in Zp. The element

$x \in \mathbb{Z}_p$ for which $ax \equiv p\ b$ is simply ($a^{p-2}\ b$ rem p).

Example: Solve for x : 5x ≡ 1 mod 12.

Solution: One method is as follows. We know that gcd(5, 12) = 1, so some linear combination of 5 and 12 is equal to 1. In Section 1 we had a general method for doing this, and we also had a spreadsheet approach. However, we can simply note by observation that

$1=5 \cdot 5+(-2) \cdot 12$

So both sides of this equality are congruent to each other mod 12. Hence

$1 \equiv 5 \cdot 5+(-2) \cdot 12 \equiv 5 \cdot 5 \bmod 12$.

So one solution is x = 5. More generally, if

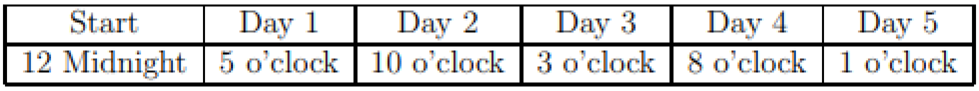
$x \equiv 5 \bmod 12$ then $5x \equiv 25 \equiv 1 \bmod 12$

Here is another approach: Start with the equation 5x ≡ 1 mod 12. If this were an equality, we would simply divide by 5 to get x = 1/5. But we are in the realm of integers so this won’t work. Instead we multiply by 5 to get

$25x \equiv 5 \bmod 12$ or $x \equiv 5 \bmod 12$.

Note that we multiplied by 5 to get a coefficient of 1: $5 \cdot 5 \equiv 1 \bmod 12$.

Example: Imagine you are a mouse and that each day you travel clockwise around a clock, passing through 25 minutes on the clock. You start at 12 o’clock. Here is what you journey will look like:



Start	Day 1	Day 2	Day 3	Day 4	Day 5
12 Midnight	5 o’clock	10 o’clock	3 o’clock	8 o’clock	1 o’clock

Note that the transition from 10 o'clock was not to 15 o'clock, but (working mod 12) to 15 mod 12 or 3 o'clock. In terms of clocks, we asked when the mouse would land at the 1 o'clock spot on the clock. We can quickly find when the mouse will land at 4 o'clock. The equation is $5x \equiv 4 \bmod 12$ Multiply by 5 to get $25x \equiv 20 \bmod 12$ or simply $x \equiv 8 \bmod 12$. It take 8 days.

Example: Find $7^{222} \bmod 11$.

Solution: By Fermat's little theorem, we know that

$7^{10} \equiv 1 \bmod 11$, and so $(7^{10})^{k} \equiv 1(\bmod 11)$ for every positive integer k.

Therefore, $7^{222} = 7^{22\cdot10+2} = (7^{10})^{22}7^{2} \equiv 1^{22} \cdot 49 \equiv 5(\bmod 11)$.

Hence, $7^{222} \bmod 11 = 5$.

Check Your Progress 1

1. Define Congruence and state its properties

____

____

____

2. What do you understand by Digression?

____

____

____

11.4 CRYPTOGRAPHY

11.4.1 Classical Cryptography:

Ever since writing was invented, people have been interested not only in using it to communicate with their partners, but also in trying to conceal the content of their messagefrom their adversaries. This leads to cryptography (or cryptology), the science of secret communication.

The basic situation is that one party, say King Arthur, wants to send a message to King Bela. There is, however, a danger that the evil Caesar

Caligula intercepts the message and learns things that he is not supposed to know about. The message, understandable even for Caligula, is called the plain text. To protect its content, King Arthur encrypts his message. When King Bela receives it, he must decrypt it in order to be able to read it. For the Kings to be able to encrypt and decrypt the message, they must know something that that the Caesar does not know: this information is the key.

Many cryptosystems have been used in history; most of them, in fact, turn out to be insecure, especially if the adversary can use powerful computing tools to break it. Perhaps the simplest method is substitution code: we replace each letter of the alphabet by another letter. The key is the table that contains for each letter the letter to be substituted for it. While a message encrypted this way looks totally scrambled, substitution codes are in fact easy to break. Solving exercise 16.3 will make it clear how the length and positions of the words can be used to figure out the original meaning of letters, if the breaking into words is preserved (i.e., ”Space” is not replaced by another character). But even if the splitting into words is hidden, an analysis of the frequency of various letter gives enough information to break the substitution code.

11.4.2 One-Time Pads

There is another simple, frequently used method, which is much more secure: the use of “one-time pads”. This method is very safe; it was used e.g. during World War II for communication between the American President and the British Prime Minister. Its disadvantage is that it requires a very long key, which can only be used once. A one-time pad is a randomly generated string of 0’s and 1’s. Say, here is one:

1100011100001000011001010010010010110011001010110000111011
0000010

Both Kings Arthur and Bela has this sequence (it was sent well in advance by a messenger).

Now King Arthur wants to send the following message to King Bela:

ATTACK MONDAY

First, he has to convert it to 0’s and 1’s. It is not clear that medieval kings had the
knowledge to do so, but the reader should be able to think of various ways: using ASCII codes, or Unicodes of the letters, for example. But we want to keep things simple, so we just number the letters from 1 to 26, and then write down the binary representation of the numbers, putting 0’s in front so that we get a string of length 5 for each letter. Thus we have “00001” for A, “00010” for B, etc. We use “00000” for “Space”. The above message
becomes:

0000110010100100000100011010110000001101011110111000100000
0111001

This might look cryptic enough, but Caligula (or rather one the excellent Greek scientist he keeps in his court) could easily figure out what it stands for. To encode it, Arthur adds the one-time pad to the message bit-by-bit. To the first bit of the message (which is 0) he adds the first bit of the pad (1) and writes down the first bit of the encoded message: 0+1 = 1. He computes the second, third, etc. bits similarly: 0+1 = 1, 0+0 = 0, 0+0 = 0, 1 + 0 = 1, 1 + 1 = 0,... (What is this 1 + 1 = 0? Isn’t 1 + 1 = 2? Or, if we want to use the binary number system, 1 + 1 = 10? Well, all that happens is that we ignore the “carry”, and just write down the last bit. We could also say that the computation is done modulo
2). Another way of saying what King Arthur does is the following: if the k-th bit of the pad is 1, he flips the k-th bit of the text; else, he leaves it as it was.
So Arthur computes the encoded message:

1100101110101100011101001000100010111110010100001000011011
0111011

He sends this to King Bela, who looking at the one-time pad, can easily flip back the appropriate bits, and recover the original message. But

Caligula (and even his excellent scientists) does not know the one-time pad, so he does not know which bits were flipped, and so he is helpless. The message is safe. It can be expensive to make sure that Sender and Receiver both have such a common key; but note that the key can be sent at a safer time and by a completely different method than the message; moreover, it may be possible to agree on a key even without actually passing it.

11.4.3 How To Save The Last Move In Chess?

Modern cryptography started in the late 1970's with the idea that it is not only lack of information that can protect our message against an unauthorized eavesdropper, but also the computational complexity of processing it. The idea can is illustrated by the following simple example.

Alice and Bob are playing chess over the phone. They want to interrupt the game for the night; how can they do it so that the person to move should not get the improper advantage of being able to think about his move whole night? At a tournament, the last move is not made on the board, only written down, put in an envelope, and deposited with the referee. But now the two players have no referee, no envelope, no contact other than the telephone line. The player making the last move (say, Alice) has to send Bob some message. The next morning (or whenever they continue the game) she has to give some additional information, some "key", which allows Bob to reconstruct the move. Bob should not be able to reconstruct Alice's move without the key; Alice should not be able to change her mind overnight and modify her move.

Surely this seems to be impossible! If she gives enough information the first time to uniquely determine her move, Bob will know the move too soon; if the information given the first time allows several moves, then she can think about it overnight, figure out the best among these, and give the remaining information, the "key" accordingly.

If we measure information in the sense of classical information theory, then there is no way out of this dilemma. But complexity comes to our help: it is not enough to communicate information, it must also be processed.

So here is a solution to the problem, using elementary number theory! (Many other schemes can be designed.) Alice and Bob agree to encode every move as a 4-digit number (say, ‘11’ means ‘K’, ‘6’ means ‘f’, and ‘3’ means itself, so ‘1163’ means ‘Kf3’). So far, this is just notation.

Next, Alice extends the four digits describing her move to a prime number p = 1163... with 200 digits. She also generates another prime q with 201 digits and computes the product N = pq (this would take rather long on paper, but is trivial using a personal computer). The result is a number with 400 or 401 digits; she sends this number to Bob. Next morning, she sends both prime factors p and q to Bob. He reconstructs Alice’s move from the first four digits of the smaller prime. To make sure that Alice was not cheating, he should check that p and q are primes and that their product is N. Let us argue that this protocol does the job.

First, Alice cannot change her mind overnight. This is because the number N contains all the information about her move: this is encoded as the first four digits of the smaller prime factor of N. So Alice commits herself to the move when sending N. But exactly because the number N contains all the information about Alice’s move,Bob seems to have the advantage, and he indeed would have if he had unlimited time or unbelievably powerful computers. What he has to do is to find the prime factors of the number N. But since N has 400 digits (or more), this is a hopelessly difficult task with current technology.

Can Alice cheat by sending a different pair (p′, q′) of primes the next morning? No, because Bob can easily compute the product p′q′, and check that this is indeed the number N that was sent the previous night.

All the information about Alice’s move is encoded in the first 4 digits of the smaller prime factor p. We could say that the rest of p and the other prime factor q serve as a “deposit box”: they hide this information from Bob, and can be opened only if the appropriate key (the factorization of N) is available. The crucial ingredient of this scheme is complexity: the computational difficulty to find the factorization of an integer. With the spread of electronic communication in business, many solutions of traditional correspondence and trade must be replaced by electronic versions. We have seen an electronic “deposit box” above. Other schemes (similar or more involved) can be found for electronic passwords, authorization, authentication, signatures, watermarking, etc. These schemes are extremely important in computer security, cryptography, automatic teller machines, and many other fields. The protocols are often based on simple number theory; in the next section we discuss (a very simplified version of) one of them.

114.4 How To Verify A Password—Without Learning It?

In a bank, a cash machine works by name and password. This system is safe as long as the password is kept in secret. But there is one week point in security: the computer of the bank must store the password, and the administrator of this computer may learn it and later misuse it.

Complexity theory provides a scheme where the bank can verify that the customer does indeed know the password—without storing the password itself! At the first glance this looks impossible—just as the problem with filing the last chess move was. And the solution (at least the one we discuss here) uses the same kind of construction as our telephone chess example.

Suppose that the password is a 100-digit prime number p (this is, of course, too long for everyday use, but it illustrates the idea best). When the customer chooses the password, he chooses another prime q with 101 digits, forms the product N = pq of the two primes, and tells the bank the number N. When the teller is used, the customer tells his name and the password p. The computer of the bank checks whether or not p is a divisor of N; if so, it accepts p as a proper password. The division of a 200 digit number by a 100 digit number is a trivial task for a computer.

Let us assume that the system administrator learns the number N stored along with the files of our customer. To use this in order to impersonate the customer, he has to find a 100-digit number that is a divisor of N; but this is essentially the same problem as finding the prime factorization of N, and this is hopelessly difficult. So—even though all the necessary information is contained in the number N—the computational complexity of the factoring problem protects the password of the customer!

11.4.5 How To Find These Primes?

In our two simple examples of “modern cryptography”, as well as in almost all the others, one needs large prime numbers. We know that there are arbitrarily large primes , but are there any with 200 digits, starting with 1163 (or any other 4 given digits)? Maple found (in a few seconds on a laptop!) the smallest such prime number:

1163000000000000000000000000000000000000000000000000000000
000000000
0000000000000000000000000000000000000000000000000000000000
000000000
0000000000000000000000000000000000000000000000000000000000
00000371

The smallest 200 digit integer starting with 1163 is 1163 · 10196. This is of course not a prime, but above we found a prime very close by. There must be zillions of such primes! In fact, a computation very similar to what we did in section 8.4 shows that the number of primes Alice can choose from is about 1.95 ·10193.

This is a lot of possibilities, but how to find one? It would not be good to use the prime above (the smallest eligible): Bob could guess this and thereby find out Alice’s move. What Alice can do is to fill in the missing 196 digits randomly, and then test whether the number she obtains is a prime. If not, she can throw it away and try again. As we computed in section 8.4, one in every 460 200-digit numbers is a prime, so on the average in about 460 trials she gets a prime. This looks like a lot of trials, but of course she uses a computer; here is one we computed for you with this method (in a few seconds again):

1163146712876555763279909704559660690828365476006668873814
489354662
4743604198911046804111038868958805745715572480009569639174
033385458
4185935354886223237823175775598647396527011271770972783894
65414589

So we see that in the “envelope” scheme above, both computational facts mentioned in section 8.7 play a crucial role: it is easy to test whether a number is a prime (and thereby it is easy to compute the encryption), but it is difficult to find the prime factors of a composite number (and so it is difficult to break the cryptosystem).

1 For the following message, the Kings used substitution code. Caligula intercepted the message and quite easily broke it. Can you do it too?

U GXUAY LS ZXMEKW AMG TGGTIY HMD TAMGXSD LSSY, FEG
GXSA LUGX HEKK HMDIS. FSKT.

2 At one time, Arthur made the mistake of using the one-time pad shifted: the first
bit of the plain text he encoded using the second bit of the pad, the second bit of the plain text he encoded using the third bit of the pad etc. He noticed his error after he sent the message off. Being afraid that Bela will not understand his message, he encoded it again (now correctly) using the same one-time pad, and sent it to Bela by another courier, explaining what happened.

Caligula intercepted both messages, and was able to recover the plain text. How?

3 The Kings were running low on one-time pads, and so Bela had to use the same
pad to encode his reply as they used for Arthur’s message. Caligula intercepted both messages, and was able to reconstruct the plain texts. Can you explain how?

4 Motivated by the one-time pad method, Alice suggests the following protocol
for saving the last move in their chess game: in the evening, she encrypts her move
(perhaps with other text added, to make it reasonably long) using a

randomly generated 0-1 sequence as the key (just like in the one-time pad method). The next morning she sends the key to Bob, so that he can decrypt the message. Should Bob accept this suggestion?

5 Alice modifies her suggestion as follows: instead of the random 0-1 sequence,
she offers to use a random, but meaningful text as the key. For whom would this be advantageous?

11.4.6 Public Key Cryptography

Cryptographic systems used in real life are more complex than those described in the previous section—but they are based on similar principles. In this section we sketch the
math behind the most commonly used system, the RSA code (named after its inventors,
Rivest, Shamir and Adleman). the protocol. Let Alice generate two 100-digit prime numbers, p and q and computes their product m = pq. Then she generates two 200-digit numbers d and e such that (p−1)(q−1) is a divisor ed –

1. The numbers m and e she publishes on her web site, or in the phone book, but the prime factors p and q and the number d remain her closely guarded secrets. The number d is called her private key, and the number e, her public key (the number p and q she may even forget—they will not be needed to operate the system, just to set it up.Suppose first that Bob wants to send a message to Alice. He writes the message as a number x (we have seen before how to do so). This number x must be a non-negative integer less than m (if the message is longer, he can just break it up into smaller chunks).
The next step is the trickiest: Bob computes the remainder of xe modulo m. Since both x and e are huge integers (200 digits), the number xd has more that 10200 digits – we could not even write it down, let alone compute it! Luckily, we don't have to compute this number, only its remainder when dividing with m. This is still a large number - but at least it can be written down in 2-3 lines. We'll return to computing it in the exercises.

So let r be this remainder; this is sent to Alice. When she receives it, she can decrypt it using her private key d by doing essentially the same procedure as Bob did: she computes the remainder of rd modulo m. And—a black magic of number theory, until you see the explanations—this remainder is just the plain text x.

What if Alice wants to send a message to Bob? He also needs to go through the trouble of generating his private and public keys. He has to pick two primes p' and q', compute their product m', select two positive integers d' and e' so that $(p' - 1)(q' - 1)$ s a divisor or $e'd' - 1$, and finally publish m' and e'. Then Alice can send him a secure message.

The black math magic behind the protocol. The key fact from mathematics we use

is Fermat's Theorem 8.6. Recall that x is the plain text (written as an integer) and the encrypted message r is the remainder of xe modulo m. So we can write

$$r = xe - km$$

with an appropriate integer k (the value of k is irrelevant for us). To decrypt, Alice raises this to the d-th power, to get

$$rd = (xe - km)d = xed + k'm,$$

where k' is again some integer. To be more precise, she computes the remainder of this modulo m, which is the same as the remainder of xed modulo m. We want to show that this is just x. Since $0 \leq x < m$, it suffices to argue that $x^{ed} - x$ is divisible by m. Since $m = pq$ is the product of two distinct primes, it suffices to prove that $x^{ed} - x$ is divisible by each of p and q.

Let us consider divisibility by p, for example. The main property of e and d is that

$ed - 1$ is divisible by $(p - 1)(q - 1)$, and hence also by p. This means that we can write $ed = (p - 1)\, l + 1$, where l is a positive integer. we have

$$x^{ed} - x = x(x^{(p-1)l} - 1bigr).$$

Here $x^{(p-1)\,l} - 1$ is divisible by $x^{p-1} - 1$ and so $x(x^{(p-1)\,l} - 1 \text{ bigr})$ is divisible by $x^p - x$, which in turn is divisible by p by Fermat's "Little" Theorem.

How to do all this computation? We already discussed how to find primes, and Alice can follow the the method described in section 8.7.

The next issue is the computation of the two keys e and d. One of them, say e, Alice can choose at random, from the range 1..(p−1)(q −1)−1. She has to check that it is relatively prime to (p−1)(q−1); this can be done efficiently with the help of the Euclidean Algorithm discussed in section 8.6. If the number she chose is not relatively prime to (p − 1)(q − 1), she just throws it out, and tries another one. This is similar to the method we used for finding a prime, and it is not hard to see that she'll find a good number on more trials than she can find a prime.

But if the euclidean algorithm finally succeeds, it also gives two integers m and n so that

$$em + (p - 1)(q - 1)n = 1.$$

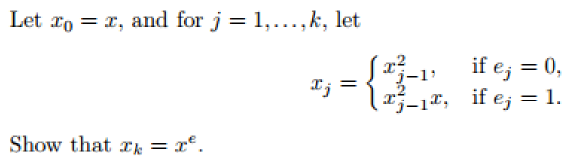
So em−1 is divisible by (p−1)(q−1). Let d denote the remainder of m modulo (p−1)(q−1),

then ed − 1 is also divisible by (p − 1)(q − 1), and so we have found a suitable key d.

Finally, we have to address the question: how to compute the remainder of x^e modulo m, when just to write down x^e would fill the universe? The answer is easy: after each operation, we can replace the number we get by its remainder modulo m. This way we never get numbers with more than 400 digits, which is manageable.

But there is another problem: x^e denotes x multiplied by itself e ≈ 10200 times; even if we carry out 1 billion multiplications every second, we will not finish before the end of the universe! The first hint that something can be done comes if we think of the special case when $e = 2^k$ is a power of 2. In this case, we don't have to multiply with x $2^k - 1$ times; instead, we can repeatedly square x just k times: we get x^2, $(x^2)^2 = x^4$, $(x^4)^2 = x^8$ etc.

If e is not a power of 2, but say the sum of two powers of 2: $e = 2^k + 2^l$, then we can separately



Let $x_0 = x$, and for $j = 1, \ldots, k$, let

$$x_j = \begin{cases} x_{j-1}^2, & \text{if } e_j = 0, \\ x_{j-1}^2 x, & \text{if } e_j = 1. \end{cases}$$

Show that $x_k = x^e$.

compute x^{2^k} and $x^{2^l}$by this repeated squaring, and then multiply these 2 numbers (not forgetting that after each squaring and multiplication, we replace the number by its remainder modulo m). This works similarly if m is the sum of a small number of powers of 2.

But every number is the sum of a small number of powers of 2: just think of its

representation in binary. The binary representation 1011001012 actually means that the

number is $2^8 + 2^6 + 2^5 + 2^2 + 2^0$. A 200 digit number is the sum of at most 665 powers of

2. We can easily compute (with a computer, of course) x^{2^k} for every k ≤ 664 by repeated

squaring, and then the product of these numbers.

6 Let e = e0e1 ...ek be the expression of e in binary (e_i = 0 or 1, e_0 is always 1).

Signatures, etc. There are many other nice things this system can do. For example, suppose that Alice gets a message from Bob as described above. How can she know that it indeed came from Bob? Just because it is signed “Bob”, it could have come from anybody. But Bob can do the following. First, he encrypts the message with his private key, then adds “Bob”, and encrypts it again with Alice’s public key. When Alice receives it, she can decrypt it with her private key. She’ll see a still encrypted message, signed “Bob”. She can cut away the signature, look up Bob’s public key in the phonebook, and use it to decrypt the message.

One can use similar tricks to implement many other electronic gadgets, using RSA.

Security. The security of the RSA protocol is a difficult issue, and since its inception in 1977, thousands of researchers have investigated it. The fact that no attack has been generally successful is a good sign; but unfortunately no exact proof of it security has been found (and it appears that current mathematics lacks the tools to provide such a proof in the foreseeable future.

We can give, however, at least some arguments that support its security. Suppose that you intercept the message of Bob, and want to decipher it. You know the remainder r (this is the intercepted message). You also know Alice's public key e, and the number m. One could think of two lines of attack: either you can figure out her private key d and then decrypt the message just as she does, or you could somehow more directly find the integer x, knowing the remainder of xe modulo m.

Unfortunately there is no theorem stating that either of this is impossible in less than astronomical time. But one can justify the security of the system with the following fact: if one can break the RSA system, then one can use the same algorithm to find the prime factors of m (see exercise ??). Since the factorization problem has been studied by so many and no efficient method has been found, this makes the security of RSA quite probable.

7 Suppose that Bob develops an algorithm that can break RSA in the first, more
direct way described above: knowing Alice's public key m and e, he can find her private key d.

(a) Show that he can use this to find the number $(p - 1)(q - 1)$;

(b) from this, he can find the prime factorization $m = pq$.

The real word. How practical could such a complicated system be? It seems that only a few mathematicians could ever use it. But in fact you have probably used it yourself hundreds of times! RSA is used in SSL (Secure Socket Layer), which in turn is used in https (secure http). Any time you visit a "secure site" of the internet, your computer generates a public and private key for you, and uses them to make sure that your credit card number and other personal data remain secret. It does not have to involve you in this at all—all you notice is that the connection is a bit slower.

In practice, the two 100 digit primes are not considered sufficiently secure. Commercial applications use more than twice this length, military applications, more than 4 times. While the hairy computations of raising the plain text x to an exponent which itself has hundreds of digits are surprisingly efficient, it would still be too slow to encrypt and decrypt each message this way. A way out is to send, as a first message, the key to a simpler system (think of a one-time pad, although one uses a more efficient system in practice, like DES, the Digital Encryption Standard). This key is then used for a few minutes to encode the messages going back and force, then thrown away. The idea is that in a short session, the number of encoded messages is not enough for an eavesdropper to break the system

Check Your Progress 2

1. What is Public cryptography?

___

___

___

2. Explain Security key.

___

___

___

11.5 SUMMARY

Number theory has a great application in daily life as well as in modern algebra. It has got wide application in different academic fields and practical application. Cryptography is used widely for transmitting information in digital format over internet or 4G.

11.6 KEYWORDS

1. Key - In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm.

2. Ring - A ring is a set R equipped with two binary operations + and · satisfying the following three sets of axioms, called the ring axioms

3. Linear Combination. A sum of the elements from some set with constant coefficients placed in front of each

4. Congruent: identical in form; coinciding exactly when superimposed

11.7 QUESTIONS FOR REVIEW

1. What is the value of 5^{-1} mod 7?
2. Solve the congruence 8x ≡ 13 mod 29.
3. If a ≡ b mod 2 show that both a and b are both odd, or they are both even.
4. Explain in detail the concept of cryptography with example.

11. 8 SUGGESTED READINGS

1. Kenneth H. Rosen - Discrete Mathematics and Its Applications, Tata Mc-Graw-Hill, 7th Edition, 2012.
2. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross-Discrete Mathematical Structures-Prentice Hall, 3rd Edition, 1996.
3. Grimaldi R-Discrete and Combinatorial Mathematics. 1-Pearson, Addison Wesley, 5th Edition, 2004.
4. C. L. Liu – Elements of Discrete Mathematics, McGraw-Hill, 1986.
5. F. Harary – Graph Theory, Addition Wesley Reading Mass, 1969.
6. N. Deo – Graph Theory With Applications to Engineering and Computer Science, Prentice Hall of India, 1987.
7. K. R. Parthasarathy – Basic Graph Theory, Tata McGraw-Hill, New Delhi, 1994.
8. G. Chartand and L. Lesniak – Graphs and Diagraphs, wadsworth and Brooks, 2nd Ed.,
9. Clark and D. A. Holton – A First Look at Graph Theory, Allied publishers.
10. D. B. West – Introduction to Graph Theory, Pearson Education Inc.,2001, 2nd Ed.,

11. J. A. Bondy and U. S. R. Murthy – Graph Theory with applications, Elsevier, 1976

12. J. P. Tremblay & R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co. 1997

13. S. Witala, Discrete Mathematics - A Unified Approach, McGraw Hill Book Co

11.9 ANSWER TO CHECK YOUR PROGRESS

1. State the concept – 11.2 & state the properties 11.2.1
2. Explain the concept –11.3.1
3. Explain the concept -- 11.4.6
4. Explain the security key concept from --- 11.4.6

UNIT 12: GROUP AND CODING THEORY

STRUCTURE

12.0 OBJECTIVES

To understand the concepts of : Group, semi group, products & quotients of semi groups. Hornomorphism, Isornorphism& auto orphism of semi groups & Groups. To know about group code. To know about parity check matrix and decode words using maximum likelihood technique.

12.1 BINARY OPERATION

A binary operation on a set A is an everywhere defined function $f : A \times A \to$ A. Generally operation is defined by ∗ *If* ∗ is binary operation on A then $a * b \in A \forall a,b \in A.$

Properties of binary operation : - Let ∗ be a binary operation on a set A,

Then ∗ satisfies the following properties for any a, b and c in A

1. $a =$ a * a	Identity property
2. $a * b = b * a$	Commutative property
3. $a * (b*c) = (a * b) * c$	Associative property

12.1.1 Types of Binary Operations

Commutative

A binary operation * on a set A is commutative if a * b = b * a, for all (a, b) ∈ A (non-empty set). Let addition be the operating binary operation for a = 8 and b = 9, a + b = 17 = b + a.

Associative

The associative property of binary operations hold if, for a non-empty set A, we can write (a * b) *c = a*(b * c). Suppose **N** be the set of natural numbers and multiplication be the binary operation. Let a = 4, b = 5 c = 6. We can write (a × b) × c = 120 = a × (b × c).

Distributive

Let * and o be two binary operations defined on a non-empty set A. The binary operations are distributive if a*(b o c) = (a * b) o (a * c) or (b o c)*a = (b * a) o (c * a). Consider * to be multiplication and o be subtraction. And a = 2, b = 5, c = 4. Then, a*(b o c) = a × (b − c) = 2 × (5 − 4) = 2. And (a * b) o (a * c) = (a × b) − (a × c) = (2 × 5) − (2 × 4) = 10 − 6 = 2.

Identity

If A be the non-empty set and * be the binary operation on A. An element e is the identity element of a ∈ A, if a * e = a = e * a. If the binary operation is addition(+), e = 0 and for * is multiplication(×), e = 1.

Inverse

If a binary operation * on a set A which satisfies a * b = b * a = e, for all a, b ∈ A. a^{-1} is invertible if for a * b = b * a= e, a^{-1} = b. 1 is invertible when * is multiplication.

Example: Show that division is not a binary operation in **N** nor subtraction in **N**.

Solution: Let a, b ∈ **N**

Case 1: Binary operation * = division(÷)

–: **N** × **N**→**N** given by (a, b) → (a/b) ∉ **N** (as 5/3 ∉ **N**)

Case 2: Binary operation * = Subtraction(−)

–: **N** × **N**→**N** given by (a, b)→ a − b ∉ **N** (as 3 − 2 = 1 ∈ **N** but 2−3 = −1 ∉ **N**).

Example: Show that $*$ defined as $x* y = x$ is a binary operation on the set of positive integers. Show that $*$ is not commutative but is associative.

Solution : Consider two positive integers x and y. By definition $x* y = x$ is a binary operation which is a positive integer. Hence $\cdot$ is a binary operation.

For commutativity : $x * y = x$ and $y * x = x$. Hence $x * y \neq y * x$ in general

$\therefore$ $*$ is not commutative.

But $x * (y * z) = x * y = x$ and$(x * y) * z = x * z = x$. Hence

$x * (y * z) = (x * y) *$

$\therefore$ $*$ is associative

12.2 SEMI GROUP

A non-empty set S together with a binary operation $*$ is called as a semi group if –

i) binary operation $*$ is closed

ii) binary operation $*$ is associative

we denote the semi group by (S, $*$)

Commutative Semigroup :- A semi group (S, $*$) is said to be commutative if $*$ is commutative i.e. $a* b =b* a \ \ \forall a \in S$

Examples : 1) (z, +) is a commutative semi group

2) The set P(S), where S is a set, together with operation of union is a commutative semi group.

3) (Z, –) is not a semi group. The operation subtraction is not associative

12.3 IDENTITY ELEMENT

An element e of a semigroup (S, $*$) is called an identity element if $e * a = a *e \ a*a \quad \forall a \in S$

Monoid: A non-empty set M together with a binary operation *defined on it, is called as a monoid if –

i) binary operation $*$ is closed
ii) binary operation $*$ is associative and
iii) (M, $*$) has an identity.
i.e. A monoid is a semi group that has an identity

Check Your Progress 1

1.What is Binary operations?

2. Define Semi group & identity element.

12. 4 GROUP

A a non-empty set G together with a binary operation $*$ defined on it is called a group if

(i) binary operation ∗ is close,

(ii) binary operation ∗ is associative,

(iii) (G, ∗) has an identity,

(iv) every element in G has inverse in G,

We denote the group by (G, ∗)

Commutative (Abelian Group : A group (G, ∗) is said to be commutative if ∗ is commutative. i.e. $a * b = b * a \ \forall \ a, \ b \in G$

Cyclic Group : If every element of a group can be expressed as some powers of an element of the group, then that group is called as cyclic group. The element is called as generator of the group. If G is a group and a is its generator then we write *G = <a>*. For example consider *G = {1, -1, i, -I }*. G is a group under the binary operation of multiplication. Note that *G= <i>*. Because $a = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$.

12.5 SUB-SEMI GROUP :

Let (S, ∗) be a semi group and let T be a subset of S. If T is closed under operation ∗, then (T, ∗) is called a subsemigroup of (S, ∗).

Submonoid : Let (S, ∗) be a monoid with identity e, and let T be a nonempty subset of S. If T is closed under the operation ∗ T, then (T,∈and e ∗) is called a submonoid of (S, ∗).

Subgroup : Let (G, ∗) be a group. A subset H of G is called as subgroup of G if (H, ∗) itself is a group.

Necessary and Sufficient Condition for subgroup : Let (G; ∗) be a group. A subset H of G is a subgroup of G if and only if $a * b^{-1} \in H * 1$

$$\forall a \ b \in H$$

12.6 PRODUCTS AND QUOTIENTS

12.6.1 GROUPS

Definition: The direct product of groups A and B consists of the set A × B, and the group operation is done component-wise: if (a, b), (c, d) ∈ A × B, then (a, b) ∗ (c, d) = (ac, bd).

A and B are the factors of the direct product.

The direct product of two groups joins them so they act independently of each other

12.6.1.1 Cayley Diagrams Of Direct Products:

Let e_A be the identity of A and e_B the identity of B.

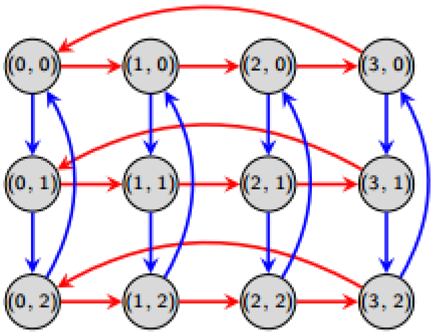
Given a Cayley diagram of A with generators $a_1, \ldots, a_k$, and a Cayley diagram of B with generators $b_1, \ldots, b_l$, we can create a Cayley diagram for $A \times B$ as follows:

Vertex set: $\{(a, b) \mid a \in A, b \in B\}$.

Generators: $(a_1, e_b), \ldots, (a_k, e_b)$ and $(e_a, b_1), \ldots, (e_k, b_l)$.

Frequently it is helpful to arrange the vertices in a rectangular grid.

For example, here is a Cayley diagram for the group $\mathbb{Z}_4 \times \mathbb{Z}_3$



What are the subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_3$? There are six (did you find them all?), they are:

$\mathbb{Z}_4 \times \mathbb{Z}_3$, $\{0\} \times \{0\}$, $\{0\} \times \mathbb{Z}_3$, $\mathbb{Z}_4 \times \{0\}$, $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \{0\}$.

Subgroups of direct products

Note: If $H \leq A$, and $K \leq B$, then $H \times K$ is a subgroup of $A \times B$.

For example, consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, which is really just V_4. Since $\mathbb{Z}_2$

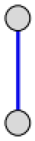
has two subgroups, the following four sets are subgroups of $\mathbb{Z}_2\times \mathbb{Z}_2$:

$\mathbb{Z}_2\times \mathbb{Z}_2$, $\{0\} \times \{0\}$, $\mathbb{Z}_2 \times \{0\} = \langle(1,0)\rangle$, $\{0\} \times \mathbb{Z}_2 = \langle(1,0)\rangle$,

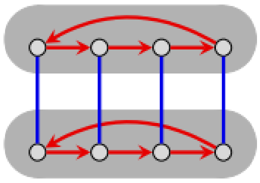
However, one subgroup of $\mathbb{Z}_2\times \mathbb{Z}_2$ is missing from this list: $h(1, 1)i = \{(0, 0), (1, 1)\}$.

To make a Cayley diagram of $A \times B$ from the Cayley diagrams of A and B:

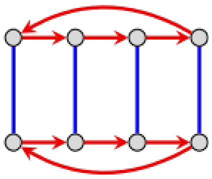
1. Begin with the Cayley diagram for A.
2. Inflate each node, and place in it a copy of the Cayley diagram for B. (Use different colors for the two Cayley diagrams.)
3. Remove the (inflated) nodes of A while using the arrows of A to connect corresponding nodes from each copy of B. That is, remove the A diagram but treat its arrows as a blueprint for how to connect corresponding nodes in the copies of B.



Cyclic group $\mathbb{Z}_2$



each node contains a copy of $\mathbb{Z}_4$



direct product group $\mathbb{Z}_4 \times \mathbb{Z}_2$

12.6.1.2 Quotients:

To divide a group G by one of its subgroups H, follow these steps:

1. Organize a Cayley diagram of G by H (so that we can "see" the subgroup H in the diagram for G).
2. Collapse each left coset of H into one large node. Unite those arrows that now have the same start and end nodes. This forms a new diagram with fewer nodes and arrows.
3. IF (and *only* if) the resulting diagram is a Cayley diagram of a group, you have obtained the quotient group of G by H, denoted G/H (say: "G mod H".) If not, then G cannot be divided by H.

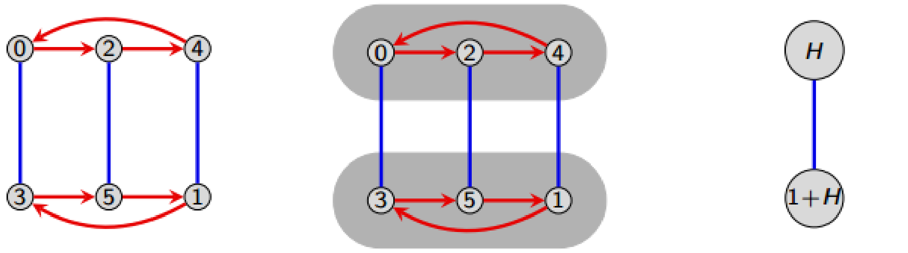
Example: $\mathbb{Z}_3 < \mathbb{Z}_6$

Consider the group $G = \mathbb{Z}_6$ and its normal subgroup $H = \langle 2\rangle = \{0, 2, 4\}$.

Notes

There are two (left) cosets: $H = \{0, 2, 4\}$ and $1 + H = \{1, 3, 5\}$.

The following diagram shows how to take a quotient of $\mathbb{Z}_6$ by H



$\mathbb{Z}_6$ organized by the subgroup $H = \langle 2 \rangle$

Left cosets of H are near each other

Collapse cosets into single nodes

In this example, the resulting diagram *is* a Cayley diagram. So, we *can* divide $\mathbb{Z}_6$ by

$h2i$, and we see that $\mathbb{Z}_6/H$ is isomorphic to $\mathbb{Z}_2$.

We write this as $\mathbb{Z}_6/H \cong \mathbb{Z}_2$

Theorem: When $H \lhd G$, the set of cosets G/H forms a group.

Proof: There is a well-defined binary operation on the set of left (equivalently, right) cosets:

$aH \cdot bH = abH$. We need to verify the three remaining properties of a group:

Identity. The coset $H = eH$ is the identity because for any coset $aH \in G/H$, $aH \cdot H = aeH = aH = eaH = H \cdot aH$.

Inverses. Given a coset aH, its inverse is $a-1H$, because $aH \cdot a^{-1}H = eH = a^{-1}H \cdot aH$.

Closure. This is immediate, because $aH \cdot bH = abH$ is another coset in G/H.

12.6.2 SEMIGROUPS

12.6.1 Product:

Theorem: If (S, *) and (T, *') are semigroups, then (S ×T, *”) is a semigroup, where ∗” is defined by (s_1,t_1) ∗”$(s_2,t_2) = (s_1 * s_2 , t_1 * 't_2)$

Theorem: If S and T are monoids with identities $e_S \times e_T$, respectively, then, S ×T
is a monoid with identity (e_S, e_T)

12.6.2.2 Quotient

Theorem:

Let R be congruence relation on the semigroup (S, ∗). Consider the relation from S/R × S/R to S/R in which the ordered pair ([a], [b]) is, for a and b in S, related to [a ∗ b].

a) ⊗ is a function from S/R× S/R to S/R, and as usual we denote ⊗ ([a],[b]) by [a] ∗ [b]. Thus [a] ⊗ [b] =.[a ∗b]

(b) (S/R, ⊗) is a semigroup.

Proof : Suppose that ([a],[b]) = ([a’],[b’]). Then aRa’ and bRb’, so we must have a ∗bRa’ ∗b’, since R is a congruence relation. Thus [a ∗b]=[a’ ∗ b’] that is, ⊗ is a function. This means that ⊗ ; is a binary operation on S/R.

Next, we must verify that ⊗ is an associative operation. . We have [(a⊗[b]⊗[c])=[a]⊗ [a ∗(b*c)] = [(a*b) ∗c] by associative property of ∗ in S

= [a ∗ b] ⊗ [c]

= ([a] ⊗[b]) ⊗ [c],

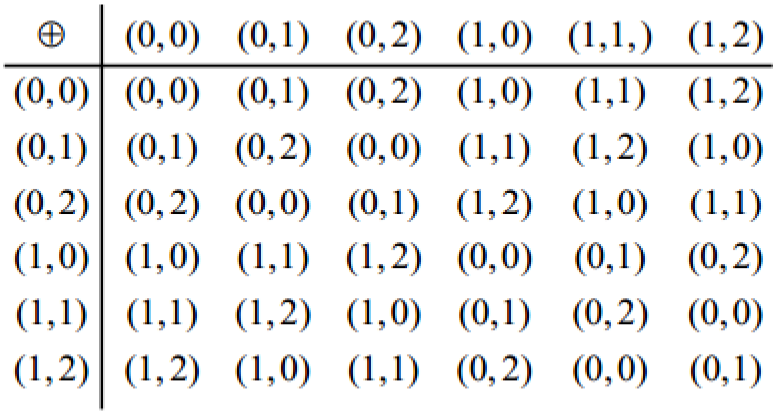
Hence S/R is a semigroup. We call S/R the ***quotient semigroup*** or ***factor semigroup.*** Observe that ⊗ is a type of “quotient binary relation” on S/R that is constructed from the original binary relation ∗ on S by the congruence relation R.

Example: Let Z be the set of integers, and Zm, be the set of eduivalences classes generated by the equivalence relation “congruence modulo m” for any positive integer m.

Z_m is a group with operation ⊕ where [a] ⊕ [b] = [a+b]

For Z_2 and Z_3 defined according to the above definition, write the multiplication table for the group $Z_2 \times Z_3$

Solution : The multiplication table for the group $Z_2 \times Z_3$



$\oplus$	(0,0)	(0,1)	(0,2)	(1,0)	(1,1,)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

12.7 HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM

SEMI GROUP : Homomorphism : Let $(S, *)$ And $(T, *')$ Be Two semi groups. An everywhere defined function f: S → T is called a homomorphism from $(S, *)$ to $(T, *')$ if $f(a*b) = f(a) *' f(b)$ $\forall a, b \in S$

Isomorphism : Let $(S, *)$ and $(T, *')$ be two semi groups. A function T is called a isomorphism from $(S, \rightarrow f : S \ \ *)$ to $(T, *')$ if

(i) it is one-to-one correspondence from S to T

(ii) $f(a*b) = f(a) * f(b)'$ $\forall$ a, b $\in$ S

$(S, *)$ and $(T, *')$ are isomorphic' is denoted by $S \cong T$

Auto orphism: An isomorphism from a semi group to itself is called an is called auto orphism of the semigoup. An isonorptism f:s→ s auto orphism.

GROUP:

Homomorphism: Let $(G, *)$ and $(G', *')$ be two groups. An everywhere defined function f: G→ G' is called a homomorphism from $(G, *)$ to $(G', *')$ if

$f(a * b) = f(a) * G'$ $\forall a,b \in G$ x

Isomorphism : Let (G, $*$) and (G’, $*$’) be two groups. A function G’ is called a isomorphism from (G,$\rightarrow$f : G $*$) to (G’, $*$’) if

(i) it is one-to-one correspondence from G to G’ (ii) f is onto.

(iii) f(a $*$ b) = f (a) $*$’f (b) $\forall$a, b$\in$ G

‘(G, $*$) and (G’, $*$ G’.$\cong$’) are isomorphic’ is denoted by G

Auto orphism: An isomorphism from a group to itself is called an is calledautomorphism of the group. An isomorphism f :G $\rightarrow$G is called Auto orphism.

Theorem 6.6 : Let f be a homomorphism from a semi group (S, $*$) to a semi group (T, $*$’). If S’ is a subsemigroup of (S, $*$), then

F(S’) = {t $\in$ T| t = f (s) for some s $\in$ S}

The image of S’ under f, is subsemigroup of (T, $*$’).

Proof : If t_1, and t_2 are any elements of F(S’), then there exist s_1 and s_2 in S’ with t_1= f(s_1) and t_2 = f(s_2).

Therefore,

$t_1 * t_2 = f(s_1)* f(s_2)= f(s_1 * s_2) = f(s_2 * s_1)=t_2*t_1.$

Hence (T, $*$') is also commutative.

Example: Let G be a group. Show that the function f : G $\rightarrow$ G defined by f(a) = a^2 is a homomorphism iff G is abelian.

Solution :

Step-1 : Assume G is abelian. Prove that f : G $\rightarrow$G defined by f(a) = a^2 a^2 is a homomorphism.

G$\in$Let a,b $\therefore$ f(a) = a^2, f(b) = b^2 and f(ab) = $(ab)^2$ by definition of f.

f(ab) = $(ab)^2$

= (ab)(ab).

= a(ba)b associativity

= a(ab)b G is abelian

= (aa)(bb) associativity

= a^2b^2

= f(a)f(b) definition of f

$\therefore$ f is a homomorphism.

Step 2 : $\forall$ y = a^2 $\in$ G $\exists$ a $\in$ Gst

f(a) = y = a^2

$\therefore$ f is onto.

Step-3 : Assume, f : G$\rightarrow$ G defined by f(a) = a^2 s a homomorphism. Prove that G is abelian.

Let a,b $\in$ G.

f(a) = a^2, f(b) = b^2 and f(ab) = $(ab)^2$ by definition of f.

f(ab) = f(a)f(b) f is homomorphism

$\therefore$ $(ab)^2 = a^2b^2$ definition of f

$\therefore$ (ab)(ab) = (aa)(bb)

$\therefore$ a(ba)b = a(ab)b associativity

$\therefore$ba = ab left and right cancellation laws

$\therefore$G is abelian.

CHECK YOUR PROGRESS 2

1. Explain Groups?

2. Explain the Quotient of Group.

3. What do you understand by homomorphism of groups

Example: Let G be a group and let a be a fixed element of G. Show that the function $f_a : G \rightarrow G$ defined by $f_a(x) = axa^{-1}$ for $x \in G$ is an isomorphism.

Solution :

Step-1: Show that f is 1-1.

$f_a(x) = axa^{-1}$

$f_a(x) = f_a(y)$ for x, y ∈ G

$axa^{-1} = aya^{-1}$ definition of f

x = y left and right cancellation laws

f is 1- 1

Step 2 : $\forall\ y = axa^{-1} \in G \ \exists\ x\ G$ s.t

$f_a(x) = axa^{-1}$

∴ f is onto

Step-3 : Show that f is homomorphism.

For x, y ∈ G

$f(x) = a * x * a^{-1}$ $f(y) = a * y * a^{-1}$ and $f(x*y) = a * (x*y)*a^{-1}$

Consider $f(x*y) = a * (x*y)*a^{-1}$

$f(x*y) = a * (x*e* y)*a^{-1}$ e ∈G is identity

$= a * (x* a^{-1}* a* y)*a^{-1}$ $a^{-1}*a = e$

$= (a * x* a^{-1}) * (a * y* a^{-1})$ associativity

$f(x*y) = f(x)*f(y)$

∴ f is homomorphism.

∴ Since f is 1-1 and homomorphism, it is isomorphism.

12.8 SOLVED EXAMPLES

Example: Determine whether the following set together with the binary peration is a semigroup, a monoid or neither. If it is a monoid, specify the identity. If it is a semigroup or a monoid determine whether it is commutative.

i) A = set of all positive integers. $a * b = \max\{\, a, b \,\}$ i.e. bigger of a and b

ii) Set S = {1, 2, 3, 6, 12} where $a * b = \; G\,C\,D\,(a, b)$

Solution :

i) A = set of all positive integers. $a * b = \max\{\, a, b \,\}$ i.e. bigger of a and b.

Closure Property: $\therefore$ Since Max {a, b} is either a orb $\therefore a * b \in A$.

Hence closure property is verified.

Associative Property :

Since $a * (b{*}c) \; = \max\{\{\, a ,b \,\}, c\} = \max\,\{\, a, b, c \,\}$

$= \text{Max}\{a,\{b, c\}\,\} = (a.b).c$

$\therefore\; *$ is associative.

$\therefore$ (A, $*$) is a semigroup.

Existence of identity : $1 \in$ A is the identity because

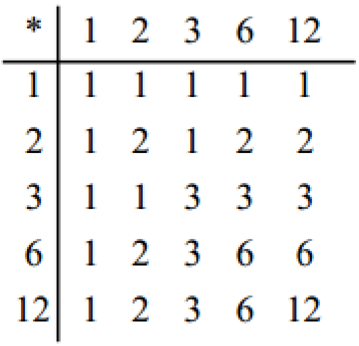
1.a = Max{ 1,a}= a $\qquad$ $a \forall \in$ A

(A,$\therefore\; *$) is a monoid.

Commutative property : Since Max{a, b) = max{b, a) we have $a * b = b * a$ Hence $*$ is commutative.

Therefore A is commutative monoid.

ii) Set S = { 1,2,3,6,12} where $a * b = G\,C\,D$ (a,b).



*	1	2	3	6	12
1	1	1	1	1	1
2	1	2	1	2	2
3	1	1	3	3	3
6	1	2	3	6	6
12	1	2	3	6	12

Closure Property : Since all the elements of the table ∈ S, closure property is satisfied.

Associative Property : Since

$a * (b * c) = a * (b * c) = a * GCD\{b, c\}\ GCD\{a, b, c\} = \ = \ = * (\ )\ (\ )$

$\{\ ,\ \}\ \{\ ,\ ,\ \}\ *$

And $(a * b) * c = GCD\{ a, b \} * c = GCD\{ a, b, c \}$

$\therefore a * (b * c) = (a * b) * c$

$\therefore$ $*$ is associative.

(S,$\therefore$ $*$) is a semigroup.

Existence of identity: From the table we observe that 12 ∈ S is the identity

$\therefore$ (S, $*$) is a monoid.

Commutative property : Since GCD{a,b}= GCD{b,a) we have

$a\ b\ b\ a * = *$. Hence $*$ is commutative.

Therefore A is commutative monoid

Example: State and prove right or left cancellation property for a group.

Solution : Let (G, $*$) be a group.

(i) To prove the right cancellation law i.e. $a*b = c * b \Rightarrow a = c$

Let a, b, c ∈ G. Since G is a group, every element has inverse in G

$\therefore b^{-1} \in G$

Consider $a * b = c * b$

Multiply both sides by from the right.

:. $(a * b) * b^{-1} = (c * b) * b^{-1}$

$\therefore a * (b * b^{-1}) = c * (b * b^{-1})$ Associative property

$\therefore e * a = e * c$ $b * b^{-1} = e \in G$

$\therefore a = c$ e ∈ G is the identity

(ii) To prove the left cancellation law i.e. $a * b = c * b \Rightarrow a = c$

G: Since G is a group, every element has inverse in G.∈Let a, b, c

$\therefore\ a^{-1} \in G$

Consider $a * b = a * c$

Multiply both sides by a^{-1} from the left

$\therefore\ a^{-1} * (a * b) = a^{-1} * (a * c)$

$\therefore\ (a^{-1} * a) * b = (a^{-1} * a) * c$ Associative property

$\therefore\ e * b = e * c$ $a^{-1} * a = e \in G$

$\therefore\ b = c$ $e \in G$ is the identity

Example: Show that if every element in a group is its own inverse, then the group must be abelian.

Solution : Let G be a group.

$\therefore$ For $a \in G$, $a^{-1} \in G$

$\therefore$ Consider $(ab)^{-1}$

$\therefore\ (ab)^{-1} = b^{-1}a^{-1}$ reversal law of inverse.

$\therefore$ ab = ba every element is its own inverse

$\therefore$ G is abelian.

Example: Consider the group G = {1,2,3,4,5,6} under multiplication modulo 7.

(i) Find the multiplication table of G

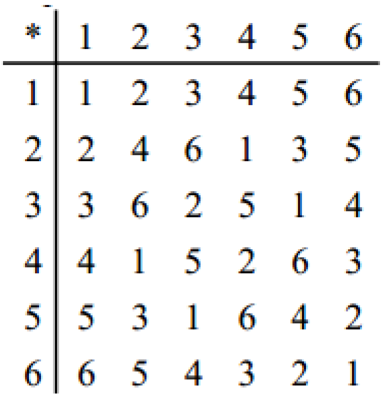
(ii) Find 2–1, 3–1, 6–1.

(iii) Find the order of the subgroups generated by 2 and 3.

(iv) Is G cyclic?

Solution : (i) Multiplication table of G

Binary operation $*$ is multiplication modulo 7.



*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

From the table we observe that $1 \in G$ is identity.

(ii) To find 2^{-1}, 3^{-1}, 6^{-1}.

From the table we get $2^{-1}= 4$, $3^{-1}= 5$, $6^{-1} = 6$

To find the order of the subgroups generated by 2.

Consider $2° = 1$ = Identity, $2^1 = 2$; $2^2 = 4$, $2^3 = 1$ = Identity

$< 2 > = \{2^1, 2^2, 2^3\}$

$\therefore$ Order of the subgroup generated by 2 =3

To find the order of the subgroups generated by 3.

Consider $3° = 1$ = identity, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$ = Identity

$< 3 > = \{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\}$

$\therefore$ Order of the subgroup generated by 3 = 6

(iv) G is cyclic because G = < 3 >.

12.9 CODING OF BINARY INFORMATION AND ERROR DETECTION

Important Terminology:

Let us choose an integer n > m and one-to-one function $e: B^m \rightarrow B^n$.

1) Encoding Function :

The function e is called an (m, n) encoding function. It means that every word in B^m as a word in B^n.

2) Code word : If $b \in B^m$ then e(b) is called the code word

3) Weight : For $x \in B^n$ the number of 1's in x is called the weight of x and is denoted by |x| .

Example: e.g. i) x 10011 $\in B^5$ $\therefore$ w(x) = 3

4) $x \oplus y \rightarrow$ Let $x,y \in B^n$ is a sequence of length n that has 1's in those positions x & y differ and has O's in those positions are the same. x & y

The operation + is defined as then i.e. 0 + 0 = 0 0 + 1 = 1 1 + 1= 0 1 + 0 = 1

Example: If x,y ∊ B^5

x = 00101, y = 10110

x ⊕ y = 10011

w (x ⊕ y) = 3

5) Hamming Distance :

Let x, y ∈Bm.The Hamming Distance δ(x,y) between x and y isthe weight of x ⊕ y. It is denoted by |x ⊕ y |. . e.g. Hamming distance between x & y can be calculated as follows :

if x = 110110, y = 000101

x ⊕ y = 110011 & |x ⊕ y | = 4

6) Minimum distance :

Let x, y∈ B^n then minimum distance = min {d (x,y) / x,y∈ B ^{n}). Let x_1, x_2 ---x_n are the code words, let any x_i i=1,---n is a transmitted word and y be the corresponding received word. Then y x $_k$ if d (x_k ,y) is the minimum distane for k = 1, 2, --- n. This criteria is known as minimum distance criteria.

7) Detection of errors :

Let e : $B^m \rightarrow B^n$ (m < n) is an encoding function then if minimum distane of e is (k + 1) then it can detect k or fewer errors.

8) Correction of errors :

Let e : $B^m \rightarrow B^n$ (m < n) is an encoding function then if minimum distance of e is (2k + 1) then it can correct k or fewer errors.

Weight of a code word : It is the number of 1's present in the given code word.

Hamming distance between two code words : Let $x{=}x_1, x_2,...x_m$ and $y{=}y_1, y_2,...y_m$ be two code words. The Hamming distance betweenthem δ($x\, y$,) , is the number of occurrences such that $x_i \neq y_i$.= for i = 1, m .

Example: Define weight of a codeword. Find the weights of the following.

a. $x = 010000$ b. $x = 11100$

Solution: a. $|x| = |010000| = 1$

b. $|x| = |11100| = 3$

Example: Find the Hamming distance between the codes.

$x = 010000$, y = 000101

Solution : Hamming distance :

$\delta(x,y) = |x \oplus y| = |010000 \oplus 000101| = |010101| = 3$

Example: The following encoding function $f: B^m \to B^{m+1}$ is called the parity $(m, m+1)$ check code. If $b= b_1 b_2 \ldots b_m \in B^m$ define $e(b) = b_1 b_2 \ldots b_m b_{m+1}$ where

b_{m+1} = 0 if |b| is even.

= 1 if |b| is odd.

Find e(b) if (a) b = 01010 (b) b = 01110

Solution: (a) e(b) = 01010 (b) e(b) = 011101

Example 7.6 : Let $e: B^2 \to B^6$ *is an* (2,6) encoding function defined as→

e(00) = 000000, e(01) = 011101

e(10) = 001110, e(11) = 111111

a) Find minimum distance.

b) How many errors can e detect?

c) How many errors can e correts?

Solution: Let x0, x1, x2, x3 ∊ B^6 where x_0 = 000000, x_1 = 011101, x_2= 001110, x_3= 111111 2 3.

$w(x_0 \oplus x_1) = w(011101) = 4$

$w(x_0 \oplus x_2) = w\ (001110) = 3$

$w(x_0 \oplus x_3) = w(111111) = 6$

$w(x_1 \oplus x_2) = w(010011) = 3$

$w(x_1 \oplus x_3) = w\ (100010) = 2$

$w(x_2 \oplus x_3) = w(110001) = 3$

Minimum distance = e = 2

d) Minimum distance = 2

An encoding function e can detect k or fewer errors if the minimum

$= \therefore\ = +k\ 1\ 2\ k\ 1\ \therefore$ distance is k + 1.

The function can detect 1 or fewer (i.e. 0) error.

e) e can correct k or fewer error if minimum distance is 2k + 1.

2k + 1 = 2

k = 1/2

$\therefore$ e can correct1/2 or less than ½ i.e. 0 errors.

Group Code: An (m, n) encoding function $e: B^m \rightarrow B^n$ is called a group code if range of e is a subgroup of B^n) i.e. (Ran (e), ⊕) is a group. Since Ran (e) CB^n and if (Ran (e), ⊕) is a group then Ran(e) is a subgroup of B^n. If an encoding function $e: B^m \rightarrow B^n$ (n < n) is a group code, then the minimum distance of e is the minimum weight of a nonzero codeword.

12.10 DECODING AND ERROR CORRECTION:

Consider an (m, n) encoding function $e: B^m \rightarrow B^n$, we require an (n,m) decoding function associate with e as $d : B^n \rightarrow B^m$. The method to determine a decoding function d is called maximum likelihood technique.

Since $|B^m| = 2^m$ m.

Let xk ∊ B^m be a codeword, k = 1, 2, ---m and the received word is y then.

Min $1 \leq k \leq 2^m \{d\ (x_k, y)\} = d(x_i, y)$ for same i then x_i is a codeword which is closest to y. If minimum distance is not unique then select on priority

MAXIMUM LIKELIHOOD TECHNIQUE:

Given an (m, n) encoding function $e: B^m \rightarrow B^n$ we often need to determine an (n, m) decoding function $d: B^n \rightarrow B^m$. associated with e. We now discuss a method, called the maximum likelihood techniques, for

determining a decoding function d for a given e. Since Bm has 2^m elements, there are 2^m code words in B^n . We first list the code words in a fixed order.

$$x^{(1)}, x^{(2)}, \ldots, x^{\left(2^m\right)}$$

If the received word is $x1$, we compute δ ($x^{(i)}$, x_1) for $1 \leq i \leq 2^m$ and choose the first code word, say it is $x^{(s)}$, such that

$$\min_{1 \leq i \leq 2^m} \left\{\delta\left(x^{(i)}, x_1\right)\right\} = \delta\left(x^{(s)}, x_1\right)$$

That is, $x^{(s)}$ is a code word that is closest to $x1$, and the first in the list. If *x e b* (*s*) =) (, we define the maximum likelihood decoding function d associated with e by

$$d(x_t) = b$$

Example: Define group code. Show that (2, 5) encoding function e: $B^2 \rightarrow B^5$ defined by e (00) = 0000, e(10) = 10101, e (11)= 11011 is a group code.

⊕	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

Solution : Group Code

Since closure property is satisfied, it is a group code.

12.11 SUMMARY

Coding theory has developed techniques to detect and correct errors. In today’s modern world of communication, data items are constantly being transmitted from point to point and coding theory has huge application in transmitting data.

12.12 KEYWORDS

1. Positive Integers: The **positive integers** are the numbers 1, 2, 3, ... (OEIS A000027), sometimes called the counting numbers or natural numbers.

2. Binary numbers:In **mathematics** and digital electronics, a **binary** number is a number expressed in the base-2 numeral system or **binary** numeral system, which uses only two symbols: typically "0" (zero) and "1" (one).

3. Coding and **decoding**: In the **mathematical** literature an encoding (coding) is a mapping of an arbitrary set into the set of finite sequences (words) over some alphabet , while the inverse mapping is called a **decoding.**

4. Error : in applied **mathematics**, the difference between a true value and an estimate, or approximation, of that value.

12.13 QUESTIONS FOR REVIEW

1. Let G be a group. Show that the function f: G → G defined by f(a) = a^{-1} is an isomorphism if and only if G is abelian.
2. Let G be a group of real numbers under addition, and let G’ be the group of positive numbers under multiplication.Let f: G → G be defined by f(x) = e^x. Show that f is an isomorphism from G to G’
3. Define Hamming distance. Find the Hamming distance between the codes x = 001100, y = 010110.

4. Let d be the (4, 3) decoding function defined by d : $B^4 \rightarrow B^3$

   If y = $y_1y_2\ldots y_{m+1}$, d(y) = $y_1y_2\ldots y_m$. Determine d(y) for the word y is B^4

   a) d(y)= 0110 b) d(y) 1011

5. Consider the (2, 4) encoding function e as follows. How many errors will e detect?

   e (00) = 0000, e (01) = 0110, e (10) = 1011, e (11) = 1100

12.14 SUGGESTED READINGS

1. Kenneth H. Rosen - Discrete Mathematics and Its Applications, Tata Mc-Graw-Hill, 7th Edition, 2012.
2. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross-Discrete Mathematical Structures-Prentice Hall, 3rd Edition, 1996.
3. Grimaldi R-Discrete and Combinatorial Mathematics. 1-Pearson, Addison Wesley, 5th Edition, 2004.
4. C. L. Liu – Elements of Discrete Mathematics, McGraw-Hill, 1986.
5. F. Harary – Graph Theory, Addition Wesley Reading Mass, 1969.
6. N. Deo – Graph Theory With Applications to Engineering and Computer Science, Prentice Hall of India, 1987.
7. K. R. Parthasarathy – Basic Graph Theory, Tata McGraw-Hill, New Delhi, 1994.
8. G. Chartand and L. Lesniak – Graphs and Diagraphs, wadsworth and Brooks, 2nd Ed.,
9. Clark and D. A. Holton – A First Look at Graph Theory, Allied publishers.
10. D. B. West – Introduction to Graph Theory, Pearson Education Inc.,2001, 2nd Ed.,
11. J. A. Bondy and U. S. R. Murthy – Graph Theory with applications, Elsevier, 1976
12. J. P. Tremblay & R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co. 1997
13. S. Witala, Discrete Mathematics - A Unified Approach, McGraw Hill Book Co

12.14 ANSWER TO CHECK YOUR PROGRESS

1. Explain the concept-- 12.1
2. Explain the concept –12.2 & 12.3
3. Explain the concept -- 12.6.1
4. Explain the concept --- 12.6.1.2
5. Explain the concept of Homomorphism of group –12.7

UNIT 13: GRAPH THEORY I

STRUCTURE

13.0 OBJECTIVE

- What is Graph and its different types?
- Concept of Graph Isomorphism
- Concept of Reachability & connectedness.
- What is Euler & Hamiltonian Path?

13.1 CONCEPT:

A graph **G** is a pair of sets (V, E) where **V** is a set of vertices and **E** is set of edges. If **G** is a directed graph, the elements of **E** are ordered pairs of vertices. In this case an edge $(v, v')$is said to be from *v* to *v'* and to join *v* to *v'*. If G is non-directed graph the elements of E are unordered pairs (sets) of vertices. In this case an edge {*v, v'*} is said to join *v* and *v'* or to be between v and v'.

An edge that is between the vertex and itself is called a **self-loop (loop for short).**

A graph with no loops is said to be **simple or loop-free**.

If G is a graph, V(G) and E(G) denotes its sets of vertices and edges, respectively. Ordinarily, V(G) is assumed to be a finite set, in which case E(G) must also be finite and so G is finite.If G is finite, |V(G)| denotes the number of vertices in G, and is called the order of G.

In similar way, if G is finite , |E(G)|denotes the number of edges in G, and is called the size of G. If more than one edge join a pair of vertices, the result is called as a multigraph.

Example 1:

- ✓ In the below figure 7.1(a) and (b), they both demonstrate two nondirected graphs. The graph **G** shown in (a) is not simple as there is a loop incident on vertex *c*. By contrast, the graph **G***'* shown in (b) is simple.
- ✓ On the other hand in (c) graph **G***"* represents a multigraph since there are three edges between the vertices b and c.
- ✓ From the figure, it is clear that V(G) = {a, b, c, d} and E(G) = {{a, b}, {a, c},{b, c}, {c, c},{a, d},{c, d}}. Also, V(G) = V(G*'*) and E(G') = E(G) – {{c, c}}.
- ✓ To list the edges of **G***"* it is required to indicate the multiplicity of edges between b and c.

  For example, we can list E(**G***"*) = {{a, b}, {a, c},3{b, c},{a, d},{c, d}}, where 3{b, c} implies that there are three edges between b and c.

  The graph G has order 4 and size 6 while G' has order 4 and size 5 and multigraph G" has order 4 and size 7 respectively.

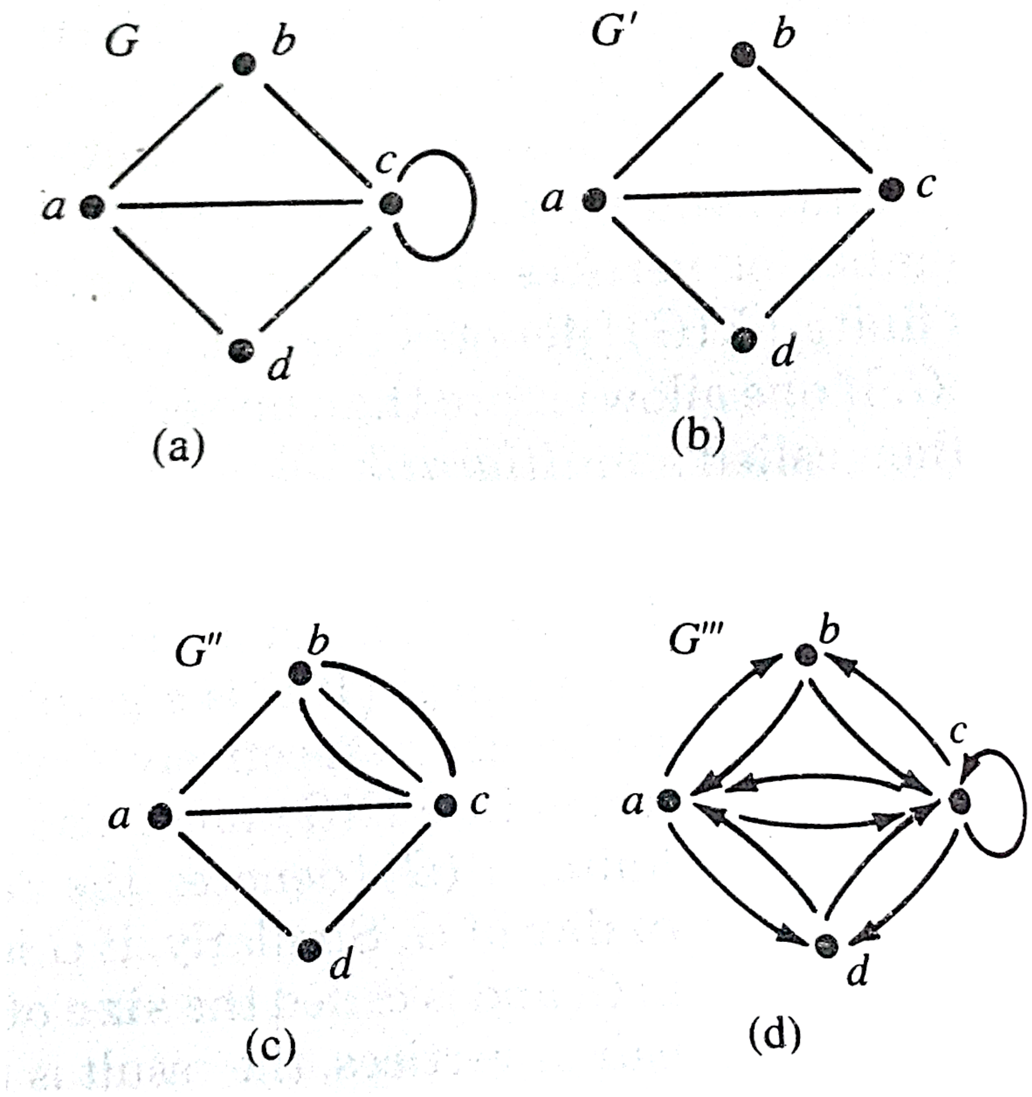


Figure 13.1: a) A non-simple graph, b) A simple graph, c) A multigraph d) A symmetric directed graph

<u>**CONCEPTS**</u>:

- ✓ In a directed graph (*v, v'*) is said to be **incident from** *v*, and to be **incident to***v'*. In a particular graph, the number of edges incident to a vertex is called the **in-degree** of the vertex and it is denoted by $degree_G{}^+(v)$ and the number of edges incident from it is called its **out-degree** and it is denoted by $degree_G{}^-(v)$. Th degree of vertex is determined by counting each loop incident on it twice and each other edge once. The degree of a vertex *v* in a graph **G** may be denoted by $degree_G(v)$ or $deg_G(v)$ and if it is clear from context, the subscript g can be omitted.

[Note: In the case of a nondirected graph an unordered pair {v, v'} is an edge incident on v and v'.]

- ✓ A vertex of degree zero is called an **isolated vertex.**
- ✓ If there is an edge incident from v to v' or incident on v and v', then v and v' are said to be **adjacent/ neighbours.**
- ✓ The minimum of all degrees of the vertices of a graph **G** is denoted by $\delta(G)$, and the maximum of all degrees of the vertices of a graph **G** is denoted by $\Delta(G)$. If $\delta(G) = \Delta(G) = k$, which implies if each vertex of **G** has degree k, then **G** is said to be k-regular or regular of degree k.
- ✓ If $v_1, v_2, \dots, v_n$ are the vertices of G, then the sequence $(d_1, d_2, \dots, d_n)$, where $d_i = degree(v_i)$, is the degree sequence of G. Generally, the vertices are ordered in such a way the degree sequence is monotone increasing $\delta(G) = d_1 \leq d_2 \leq \cdots \leq d_n = \Delta(G)$

Example 2: Refer the diagram 13.1 (a), the vertex c of the graph G has degree 5 and the degree sequence of G is (2, 2, 3, 5) while in diagram 13.1(b) the degree of c in G' is 3 and the degree sequence of G' is (2, 2, 3, 3).

THEOREM: If $V = \{v_1, \dots, v_n\}$ is the vertex set of nondirected graph G, then

$$\sum_{i=1}^{n} deg(v_i) = 2|E|.$$

If G is a directed graph, then

$$\sum_{i=1}^{n} deg^{+}(v_i) = \sum_{i=1}^{n} deg^{-}(v_i) = 2|E|.$$

PROOF: When the degrees are summed, each edge contributes a count of one to the degree of each of the two vertices on which edge is incident.

Corollary 1: In any nondirected graph there is an even number of vertices of odd degree

Proof: Let *V'* be the set of vertices odd degree and let *V''* be the set of vertices of even degree. Then

$$\sum_{v\in V(G)} \deg(v) = \sum_{v\in V\prime} \deg(v) + \sum_{v\in V"} \deg(v) = 2|E|$$

As $\sum_{v\in V"} \deg(v)$ is even then $\sum_{v\in V\prime} \deg(v)$ is also even, indicating that |W| is even and hence the corollary is proved.

Corollary 2: If $k = \delta(G)$ is the minimum degree of all the vertices of a nondirected graph G, then

$$k|V| \leq \sum_{v\in V(G)} \deg(v) = 2|E|$$

In particular, if G is a k-regular graph, then

$$k|V| = \sum_{v\in V(G)} \deg(v) = 2|E|$$

CONCEPTS:

- In a nondirected graph **G** a sequence **P** of zero or more edges of the form $\{v_0, v_1\}$, $\{v_1, v_2\}$,…,$\{v_{n-1}, v_n\}$ also represented as $(v_0 - v_1 - \cdots - v_n)$ is called a **path** from v_0 to v_n; where v_0 is the **initial vertex** and $v_n$is the terminal vertex and they both are called as endpoints of the path P.
- If $v_0 = v_n$, then P is called a **closed path** and if $v_0 \neq v_n$ then P is an **open path.**
- In general, path P is a graph itself where $V(P) = \{v_0, v_1, \dots, v_n\} \subseteq V(G)$ and $E(P) = \{\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{n-1}, v_n\}\} \subseteq E(G)$.
- Also $1 \leq |V(P)| \leq n + 1$ and $0 \leq |E(P) \leq n|$, if there are repeated vertices then |V(P)| may be less than n + 1 and if there are repeated edges then E(P) < n.
- Incase if P has no edges at all that implies the length of P is zero where P is called a trivial path and V(P) is a singleton set $\{v_0\}$.
- A path P is simple if all edges and vertices on the path are distinct except possibly the endpoints. So an open simple path of length of n has n + 1 distinct vertices and n distinct edges, while a closed

simple path of length n has n distinct vertices and n distinct edges.

- A path of length ≥ 1 with no repeated edges and whose endpoints are equal is called a **circuit** and a circuit may have repeated vertices other than the endpoints.
- A **cycle** is a simple circuit with no other repeated vertices except its endpoints and in particular, a loop is a cycle of length 1.
- If two paths in a graph share no common edges then they are said to be **edge-disjoint** and if they share no common vertices then they are known as **vertex-disjoint.**

Example 3: In Fig 13.1 (a) the path {c, c} is cycle of length 1 while the sequence of edges {a, b}, {b, c}, {c, a} and {a, d}, {d, c}, {c, a} form cycles of length 3. The path {a, b}, {b, c}, {c, d}, {d, a} is a cycle of length 4; it is not a cycle because the sequence of vertices a – b – c – c – a includes more than one repeated vertex. Also the sequence of edges {a, b}, {b, c}, {c, a},{a, d}, {d, c}, {c, a}forms a closed path of length 6, but this path is not a circuit because the edge {c, a} is repeated twice.

THEOREM: In a graph G, every *v* – *v'* path contains a simple *v* – *v'*path.

PROOF: If a path is closed path, then it certainly contains the trivial path. Let us assume **P** is an open *v* – *v'* path. We will use induction method. If **P** has length one, then **P** is itself a simple path. Consider that all open *v* – *v'*paths of length *k*, where $1 \leq k \leq n$, contains a simple *v* – *v'*path and **P** is the open *v* – *v'*path $\{v_0, v_1\}, ... \{v_n, v_{n+1}\}$ where $u = v_0$ and $v = v_{n+1}$ incase if P has repeated vertices and if not then **P** is simple *v* – *v'*path.

Other way round if there are repeated vertices in **P**, let *x* and *y* be distinct positive integer where x < y and $v_x = v_y$. If the closed path $v_x - v_y$ is removed from P, an open path P' having length$\leq n$ since atleast the edge $\{v_x, v_{x+1}\}$ was deleted from P. Thus by inductive hypothesis, P' contains a simple path *v* – *v'* path and so does P.

Concept: An **edge labelling** of a graph G is a function $f: E(G) \rightarrow D$, where D is some domain of labels. A **vertex labelling** of G is a function $f: V(G) \rightarrow D$.

CHECK YOUR PROGRESS 1

1. Define in degree and out degree

____

____

____

2. Explain vertex disjoint with example

____

____

____

3. Explain the concept of initial vertex

____

____

____

13.2 TYPES:

13.2.1 SUBGRAPHS:

If **G** and **H** are graphs then **H** is sub-graph of **G** if and only if V(H) is a subset of V(G) and E(H) is a subset of E(G). A subgraph **H** of **G** is called spanning subgraph of **G** if and only if V(H) = V(G). If **W** is any subset of V(G), then the subgraph induced by **W** is the subgraph **H** of **G** obtained by taking V(H) = **W** and E(H) to be those edges of **G** that join pair of vertices in **W**.

Example: Consider the graph shown in figure13.2 as follows:

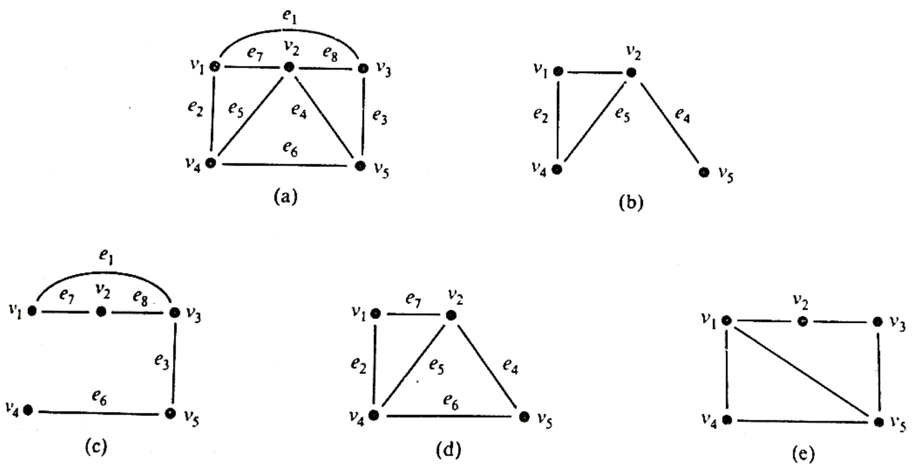


Figure 13.2: Graphs $G, G', G'', G''' and\ G''''$

- ✓ The graph G' as shown in fig (b) is a subgraph of graph G as shown in fig (a) with $V(G') = \{v_1, v_2, v_4, v_5\}$.
- ✓ The graph G'' as shown in fig (c) is a spanning subgraph of G.
- ✓ The graph G''' as shown in fig (d) is the subgraph induced by the set W= $\{v_1, v_2, v_4, v_5\}$.
- ✓ The graph G'''' shown in fig (e) is not a subgraph of G because the edge $\{v_1, v_5\}$ is not in E(G).

A simple nondirected graph with *n* mutually adjacent vertices is called a complete graph on ***n*** vertices, and may be commonly represented as K_n. A complete graph on *n* vertices has n.(n – 1) / 2 edges and n – 1is the degree of each of its vertices.

13.2.2 Complement Of A Graph:

If H is a subgraph of G, the complement of H in G, denoted by $\overline{H}(G)$, is the subgraph $G - E(H)$; which simply means that we subtracted the edges of H from G. If H is a simple graph with n vertices the complement $\overline{H}$ of H is the complement of H in K_n.

It is implied from the above concept that $V(\overline{H}) = V(H)$ and any two vertices are adjacent in $\overline{H}$ if and only if they are not adjacent in H. Note that the degree of vertex in $\overline{H}$ plus its degree in h is n – 1 , where n = |V(H)|.

Example: A graph and its complement is as shown in figure 13.3

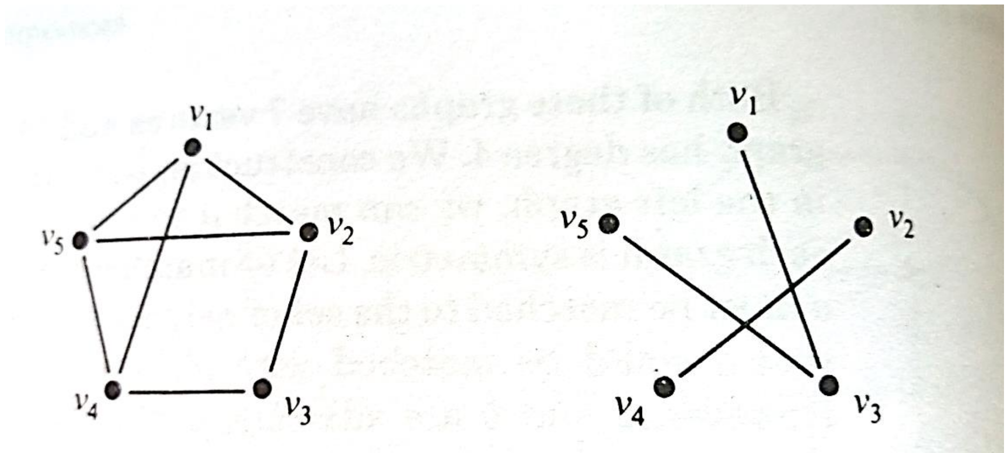


Figure 13.3: A graph and its complement

13.2.3 Intersection Of A Graph:

Let G and G'be two graphs. The intersection of G and G', written as $G \cap G'$, is the graph whose vertex set is $V(G) \cap V(G')$ and whose edge set is $E(G) \cap E(G')$. Similarly, the union of G and G', is the graph with vertex set $V(G) \cup V(G')$ and edge set $E(G) \cup E(G')$.

If G is a simple graph with ***n*** vertices, then $G \cup \bar{G}$ is a complete graph on n vertices.

13.2.4: Cycles And Wheels:

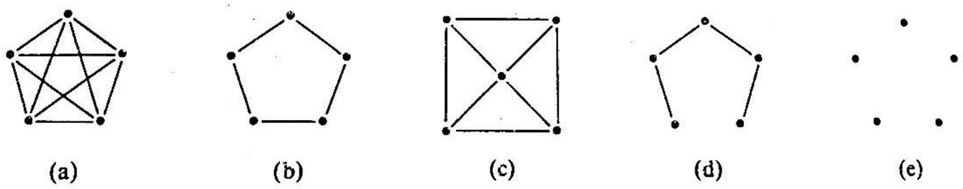
A **cycle graph** of order ***n*** is a connected graph whose edges form a cycle of length n and they are represented as C_n.

A **wheel** of order ***n*** is a graph obtained by joining a single new vertex (the 'hub') to each vertex of a cycle graph of order n – 1 and are denoted by W_n.

A **path graph** of order ***n*** is obtained by removing an edge from a C_n graph and denoted by P_n.

A **null graph** of order ***n*** is a graph with ***n*** vertices and no edges.

Example: Graphs of classes K_5, C_5, W_5, P_5 and N_5 are shown in Figure



13.4

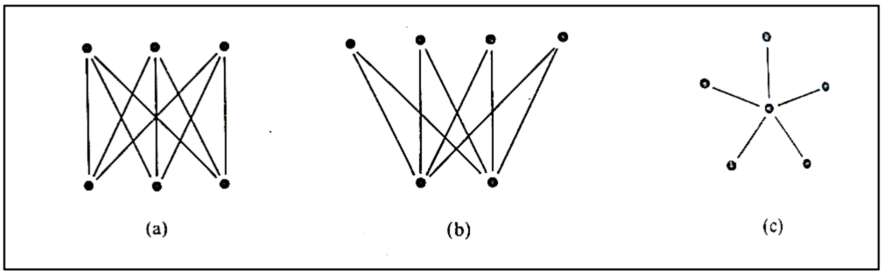
Figure 13.4: K_5, C_5, W_5, P_5 and N_5

13.2.5: Bipartite Graph:

It is a non-directed graph whose set of vertices can be partitioned into two sets X and Y in such a way that each edge joins a vertex in X to a vertex in Y. A complete bipartite graph is a bipartite graph in which every vertex of X is adjacent to every vertex of Y. The complete bipartite graphs which may be partitioned into X and Y as above such that $|X| = x$ and $|Y| = x$ are denoted by $K_{x,y}$ (where $x \leq y$).

Any graph like $K_{1,y}$ is called a **star graph**.

Example: Figure 13.5 (a), (b) and (c) represents the graph of $K_{3,3}$, $K_{2,4}$and $K_{1,5}$



13.3 GRAPH ISOMORPHISM:

Two graphs G and G' are isomorphic if there is a function $f: V(G) \rightarrow V(G')$ from the vertices of G to the vertices of G' such that

(i) *f* is one-to-one

(ii) *f* is onto, and

(iii) for each pair of vertices***u***and***v***of G, $\{u, v\} \in \boldsymbol{E}(\boldsymbol{G})$if and only if$\{f(u), f(v) \in E(G')\}$

Any function f with the above three properties is called an isomorphism from G to G'. The condition (iii) implies that vertices **u** and **v** are adjacent in G if and only if *f(u)* and *f(v)* are adjacent in G' and function *f* preserves adjacency.

If the graphs G and G' are isomorphic and *f* is an isomorphism of G to G', then the only difference between them is the only name of the vertices. If we change the names of the vertices of G' from f(v) to v for each $v \in V(G)$, then G' with the new vertices name would be identical to the graph G as they both would have same vertices and edges.

If several isomorphism *f* between G and G' exists then we can make following conclusions:

i. $|V(G)| = |V(G')|$

ii. $|E(G)| = |E(G')|$

iii. If $v \in V(G)$ then $deg_G(v) = deg_G\big(f(v)\big)$, and the degree sequence of G and G' are the same.

iv. If {***v, v***} is a loop in G, then {*f(v),f(v)}* is a loop in G', and if $v_0 - v_1 - v_2 - \cdots - v_{k-1} - v_k = v_0$ is a cycle of length *k* in G, then $f(v_0) - f(v_1) - f(v_2) - \cdots - f(v_{k-1}) - f(v_k)$ is a cycle of length k in G'. The cycle vectors of G and G' are equal, where the cycle vector of G is by definition the vector $(c_1, c_2, \dots c_n)$ where $c_i$is the number of cycles in G of length i. The value $c_1 = 0$ for simple graphs and c_2 is non-zero only for multigraphs.

Discovering Isomorphism:

To determine whether the two given graphs are isomorphic or not is known as the isomorphic problem and for arbitrary graphs approximately 2^n operations are required to resolve the isomorphic problem and $\boldsymbol{n}$ indicates the number of vertices.

Once we have one-to-one onto map $f: V(G) \rightarrow V(G')$ where G and G' are two graphs with same number of vertices, the process of verifying an isomorphism is quite simple. Also the adjacency matrix can be employed as a bookkeeping tool for recording all the adjacencies.

Consider $v_1, v_2, \dots, v_n$ are the vertices of G, then the adjacency matrix for this ordering of the vertices of G is the $n \times n$ matrix A, where ijth entry $A(i,j)$ of A is 1 if the edge $\{v_i, v_j\}$ is an edge of G; otherwise, $A(i,j) = 0$. Thus, A is symmetric matrix each of whose entries is either 0 or 1. If there is a loop at v_i 1 will appear on the ith position of the diagonal of A. Entries of A can be rearranged by changing the ordering of the vertices of G. The following fact is implied from the above discussion as follows: Suppose that G and G' are two graphs and that $f: V(G) \rightarrow V(G')$ is one-to-one onto function. Let A be the adjacency matrix for the vertex ordering $v_1, v_2, \dots, v_n$ of the vertices of G.Let A' be the adjacency matrix for the vertex ordering $f(v_1), f(v_2), \dots f(v_n)$. Then f is an isomorphism from V(G) to V(G') if the adjacency matrices A and A' are equal.

Example: The graph G and G' of figure 13.6 are isomporphic.

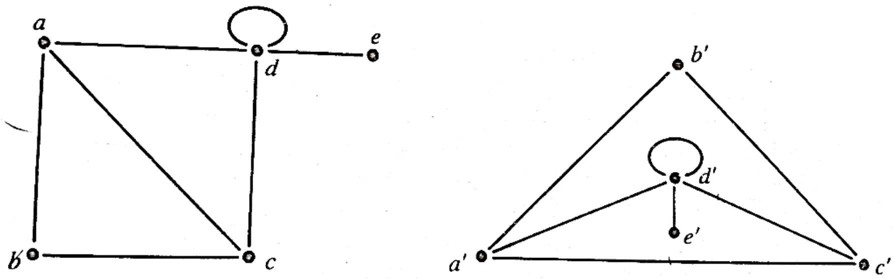


Figure 13.6: Isomorphic Graphs

The above given graphs G and G' are isomorphic, then the vertices b, d and e must be mapped to the vertices b', d' and e' as these are the unique vertices of degree 2, 5 and 1. We have only 2 maps to consider instead of 5! maps. We can verify the map f which maps a to c', b to b, c to a', d to d' and e to e' is an isomorphism because the adjacency matrix for G' is as given below for the ordering $f(a) = c', f(b) = b', f(c) = a', f(d) = d', f(e) = e'$ is

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

[NOTE: In some cases at least, the degree sequence of a graph can be used to shorten the search for isomorphisms. If the simple graphs G and G' each have vertices of degree **i**, then there are $(V_0!)$,$(V_1!)$ ... $(V_{n-1}!)$ one-to-one onto maps from V(G) to V(G') that will map the V_i vertices of degree **i** to vertices of degree **i** which is more manageable than n!.]

Determining when graphs are not isomorphic:

We need to figure out such property of the isomorphic graphs which other graphs do not share and we can easily state that they are not isomorphic. Like if we consider two graphs G and G' which had different number of vertices or different degree sequences then they are not an isomorphic. But in certain cases even though two graphs have the same degree sequences but still they are not an isomorphic.

So in such situation we classify the vertices into classes according to the properties related to isomorphism. If the two graphs are isomorphic the vertices of a given class in one graph must correspond to the vertices of the same class in the other graph. If the vertices in these classes do not correspond, then the graphs are not isomorphic.

Check Your Progress 2

1. Define the following terms a.wheel

b. complement of graph

2. What do you understand by Graph Isomorphism?

13.4 REACHABILITY AND CONNECTEDNESS:

REACHABILITY:

Concept: A vertex y in a digraph D = (V, A) is said to be reachable from a vertex x if there is a directed walk from x to y.

Remark. It is possible for a vertex to be not reachable from itself.

Example: In the below figure, the vertices 2 and 3 are reachable from the vertex 1, while the vertex 5 is reachable from the vertices 4 and 5.

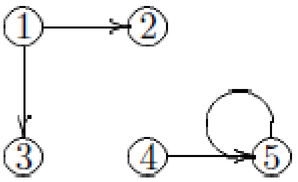


Figure 13.7: Diagraph

CONNECTEDNESS: It consist of following sub points

Connected Components: Two vertices in a graph are said to be *connected* when there is a path that begins at one and ends at the other. By convention, every vertex is considered to be connected to itself by a path of length zero. The diagram in Figure 7.8 looks like a picture of three graphs, but is intended to be a picture of *one* graph. This graph consists of three pieces (subgraphs). Each piece by itself is connected, but there are no paths between vertices in different pieces.

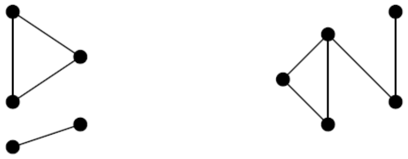


Figure 13.8: One graph with 3 connected components

A graph is said to be ***connected*** when every pair of vertices are connected. These connected pieces of a graph are called its *connected components*. In other words, a connected component is the set of all the vertices connected to some single vertex. So a graph is connected if it has exactly one connected component. The empty graph on n vertices has n connected components.

How Well Connected?

Imagine a graph as modelling cables in a telephone network, or oil pipelines, or electrical power lines, then we are interested in connectivity that survives component failure as well. A graph is called k-*edge connected* if it takes at least k "edge-failures" to disconnect it. Let us define this concept as follows:

Concept: Two vertices in a graph are k-*edge connected* if they remain connected in every subgraph obtained by deleting k – 1 edges. A graph with at least two vertices is ***k-edge*** connectedif every two of its vertices are ***k-edge*** connected.

So 1-edge connected is the same as connected for both vertices and graphs. In other word a graph is k-edge connected is that every subgraph obtained from it by deleting at most k – 1 edges is connected.

Consider the graph in the below figure 7.9, the vertices B and E are 2-edge connected, G and E are 1-edge connected, and no vertices are 3-edge connected. The graph as a whole is only 1-edge connected. More generally, any simple cycle is 2-edge connected, and the complete graph, $K_n$is (n – 1) edge connected.

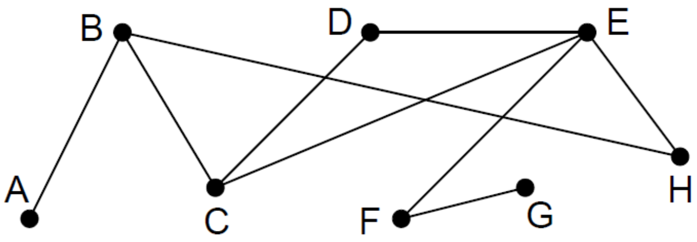


Figure 13.9: A graph with 3- simple cycles

If two vertices are connected by k edge-disjoint paths (that is, no two paths traverse the same edge), then they are obviously k-edge connected.

Connection by Simple Path

LEMMA: *If vertex* u *is connected to vertex* v *in a graph, then there is a simple path from* u *to* v.

PROOF*:*Since there is a path from u to v, there must, by the Well-ordering Principle, be a minimum length path from u to v. If the minimum length is zero or one, this minimum length path is itself a simple path from u to v. Otherwise, there is a minimum length path

$$v_0, v_1, \dots, v_k$$

from $u = v_0$to $v = v_k$where$k \geq 0$. We claim this path must be simple. To prove the claim, suppose to the contrary that the path is not simple, that is, some vertex on the path occurs twice. This means that there are integers i,j such that $0 \leq i \leq j \leq k$with$v_i = v_j$. Then deleting the subsequence

$$v_{i+1}, \dots v_j$$

yields a strictly shorter path

$$v_0, v_1, \dots, v_i, v_{j+1}, v_{j+2}, \dots v_k$$

from u to v, contradicting the minimality of the given path.

COROLLARY: *For any path of length* k *in a graph, there is a simple path of length* at most k *with the same endpoints.*

The Minimum Number of Edges in a Connected Graph:

THEOREM: *Every graph with* v *vertices and* e *edges has at least* $v - e$*connected components.*

PROOF:

We use induction on the number of edges, e.

Let P(e) be the proposition that for every v, every graph with v vertices and e edges has at least $v - e$ connected components.

Base case (e =0): In a graph with 0 edges and v vertices, each vertex is itself a connected component, and so there are exactly $v = v - 0$connected components. So P(e) holds.

Inductive step: Now we assume that the induction hypothesis holds for every e-edge graph in order to prove that it holds for every (e + 1)-edge graph, where$e \geq 0$. Consider a graph, G, with e+1 edges and k vertices. We want to prove that G has at least $v - (e + 1)$connected components. To do this, remove an arbitrary edge a—b and the resulting graph is G'. By the induction assumption, G' has at least $v - e$connected components. Now add back the edge a—b to obtain the original graph G. If a and b were in the same connected component of G', then G has the same connected components as G', so G has at least $v - e > v - (e + 1)$components.

Otherwise, if a and b were in different connected components of G', then these two components are merged into one in G, but all other components remain unchanged, reducing the number of components by 1. Therefore, G has at least $(v - e) - 1 = v - (e + 1)$connected components. So in either case, P(e+1) holds. And thus the theorem now follows by induction.

COROLLARY: *Every connected graph with* v *vertices has at least* $v - 1$*edges.*

13.5 EULER & HAMILTON PATH

Euler Path:

An Euler path in a multigraph is a path that includes each edge of the multigraph exactly once and intersects each vertex of the multigraph at least once. A multigraph is said to be traversable if it has an Euler path. An Euler circuit is an Euler path whose endpoints are identical. (If an Euler path is a sequence of edges $e_1, e_2, \ldots, e_k$ corresponding to the sequence of pairs of vertices $(x_1, x_2), (x_2, x_3), \ldots, (x_{k-1}, x_k)$, then the $e_{i's}$ are all distinct, and $x_1 = x_k$)

A multigraph is said to be an Eulerian multigraph if it has an Euler circuit.

THEOREM: A non-directed multigraph has an Euler path if and only if it is connected and has 0 or exactly 2 vertices of odd degree. In the latter case, the two vertices of odd degree are the endpoints of every Euler path in the multigraph.

PROOF: Let a multigraph G have an Euler path, so G must be connected. Every time the Euler path meets a vertex it traverses two edges which are incident on the vertex and which have not been traced before. The degree of all other vertices must be even except for the two endpoints of the path. The degree is odd if the endpoints are distinct. If the two endpoints coincide, their degrees are even and the path becomes an Euler circuit.

Let us construct an Euler path by starting at one of the vertices of odd degree and traversing each edge of G exactly once. Let us start at an arbitrary vertex as there are no vertices of odd degree. For every vertex of an even degree the path will enter the vertex and leave the vertex by tracing an edge that was not traced before. Thus, the construction will return to the vertex where it started or terminate at a vertex with an odd degree and such tracing will produce an Euler path if all edges in G are traced exactly once this way.

If all the edges in G are not traced, we will remove the traced edges and obtain the subgraph G’ induced by the remaining edges. The degrees of all vertices in this subgraph must be even and at least one vertex must intersect with the path, since G is connected. We can construct a new path which will be a cycle starting from one of the vertices as all the degrees are even. This path can joined into the previous path. The argument can be repeated until a path that traverses all edges in G is obtained.

Corollary: A non-directed multigraph has an Euler circuit if it is connected and all of its vertices are of even degree.

Corollary: A directed multigraph G has an Euler path if it is unilaterally connected and the in-degree of each vertex is equal to its out-degree, with the possible exception of two vertices, for which it may be that the in-degree of one is larger than its out-degree and the in-degree of the other is one less than its out-degree.

Corollary: A directed multigraph G has an Euler circuit if G is unilaterally connected and the in-degree of every vertex in G is equal to its out-degree.

Hamiltonian Graphs:

Concept: A graph G is said to be Hamiltonian if there exist a cycle containing every vertex of G. Such a cycle is referred to as Hamiltonian cycle. Thus, a Hamiltonian graph is a graph containing a Hamiltonian cycle.

Hamiltonian path is a simple path that contains all the vertices of G but where the end points may be distinct.

A graph is a Hamiltonian if its underlying simple graph is Hamiltonian.

A Hamiltonian cycle always provide a Hamiltonian path upon deletion of any edge while a Hamiltonian path may not lead to a Hamiltonian cycle (which depends upon whether or not the end points of the path happen to be joined by an edge in the graph).

For example, the graph in figure 13.10 is Hamiltonian as we can find a Hamiltonian cycle by inspection i.e. by following the numbering and omitting the edge $\{v_4, v_8\}$.

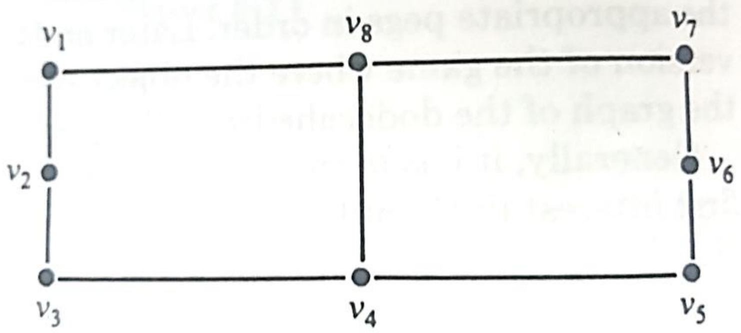


Figure 13.10: Hamiltonian Graph

There are some basic rules for constructing Hamiltonian paths and cycles which help to prove the existence or nonexistence of a Hamiltonian path and the basic idea behind this rules is that a Hamiltonian cycle must contains exactly two edges incident at each vertex and a Hamiltonian path must contain at least one of the edges.

Rule 1: If G has n vertices, then a Hamiltonian path must contain exactly n – 1 edges, and a Hamiltonian cycle must contain exactly n edges.

Rule 2: If a vertex *v* in G has degree *k*, then Hamiltonian path must contain at least one edge incident on v and at most two edges incident on v. A Hamiltonian cycle will contain exactly two edges incident on v. Both edges incident on a vertex of degree two will be contained in every Hamiltonian cycle. It implies that there cannot be three or more edges incident with one vertex in a Hamiltonian cycle.

Rule 3: No cycle that does not contain all the vertices of G can be formed when building a Hamiltonian path or cycle.

Rule 4: Once the Hamiltonian cycle has passed through a vertex v on its construction, then all other unused edges incident on v can be deleted because only two edges incident on v can be included in Hamiltonian cycle.

Example: In the below figure 13.11, the path through the vertices of G_1 in the order of appearance in the English alphabets forms a Hamiltonian path. G_1 has no Hamiltonian cycle since if so, any Hamiltonian cycle must contains edges {a, b}, {a, e}, {c, d}, {d, e}, {f, g} and {e, g}. But then there would be three edges of a cycle incident on the vertex e.

Similarly, G_2 has neither a Hamiltonian path nor a cycle for following reasons:

The vertex ***l*** has degree 5 so in that case three edges incident on ***l*** cannot be included in any Hamiltonian path. The same is true in the case of vertices ***h*** and ***j***. There are 13 vertices of degree 3 and in particular, b, d, f and n are such that at least one of the three edges incident on each of these vertices cannot be included in a Hamiltonian path. Thus, atleast 9 + 4 = 13 of the 27 edges of G_2 cannot be included in any Hamiltonian path.

Hence there are not enough edges to form a Hamiltonian path on the 16 vertices of G_2. Thus, G_2 has no Hamiltonian path.

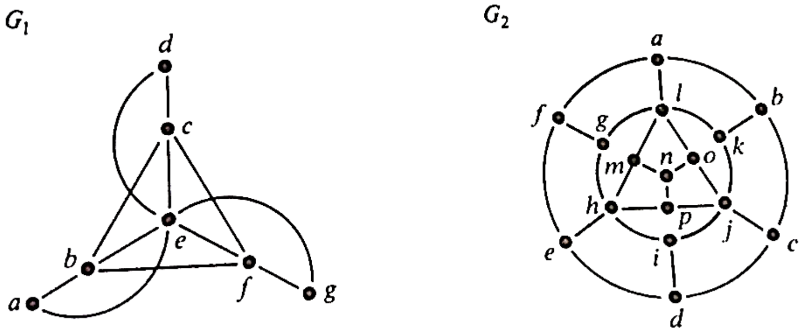


Figure 13.11

Check Your Progress 2

1. What is Euler Graph?

2. Enumerate the concept of connectedness.

13.6 SUMMING UP

Graph theory has got wide application in number of fields including computer science. It helps to represent structural model in Chemistry, Biology, Sociology, Operation Research, Computer Algorithm, Transport & Activity networks and Theory of Games.

13.7 KEYWORDS

1. Vertex - "**Vertex**" is a synonym for a node of a **graph**, i.e., one of the points on which the **graph** is defined and which may be connected by **graph** edges.

2. Edge - For an undirected **graph**, an unordered pair of nodes that specify a line joining these two nodes are said to form an **edge**. For a directed **graph**, the **edge** is an ordered pair of nodes

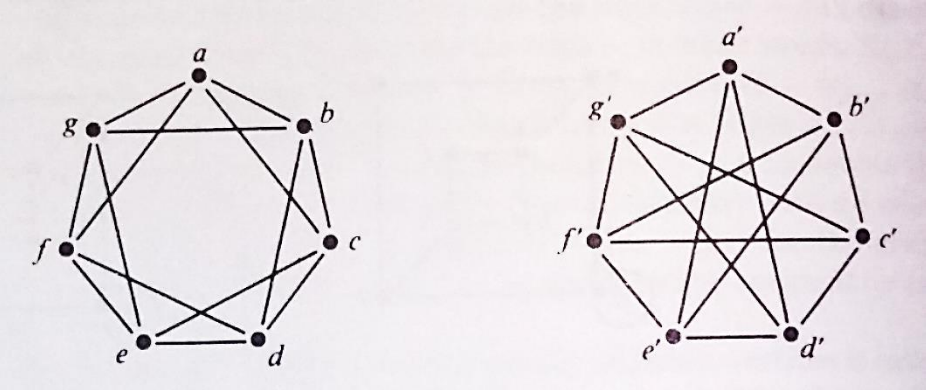
3. A **traceable graph** is a **graph** that possesses a Hamiltonian path.

4. Unilaterally - A digraph is **unilaterally** connected if for every pair of points there is a path from one to the other (but not necessarily the other way around)

13.7 MODEL EXAMINATION QUESTION

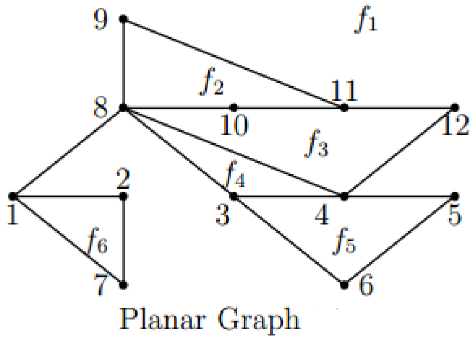
1. What is the largest possible number of vertices in a graph with 35 edges and all vertices of degree at least 3?

2. The graphs in the below figure are isomorphic. Discuss.



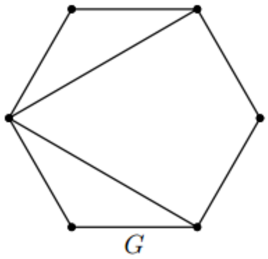
3. Is it necessary that a plane graph G should contain a vertex of degree less than 5?

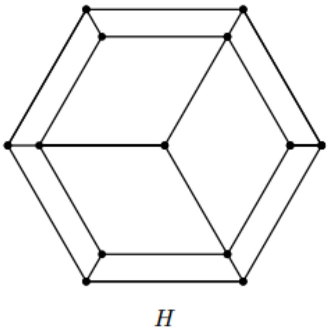
4. Determine the faces of the planar graph and their corresponding edges.



Planar Graph

5. Consider the graphs shown below.





(a) Determine the closure of G.

(b) Show that H is not Hamiltonian.

13.8 SUGGESTED READINGS

1. Kenneth H. Rosen - Discrete Mathematics and Its Applications, Tata Mc-Graw-Hill, 7th Edition, 2012.
2. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross-Discrete Mathematical Structures-Prentice Hall, 3rd Edition, 1996.
3. Grimaldi R-Discrete and Combinatorial Mathematics. 1-Pearson, Addison Wesley, 5th Edition, 2004.
4. C. L. Liu – Elements of Discrete Mathematics, McGraw-Hill, 1986.
5. F. Harary – Graph Theory, Addition Wesley Reading Mass, 1969.
6. N. Deo – Graph Theory With Applications to Engineering and Computer Science, Prentice Hall of India, 1987.
7. K. R. Parthasarathy – Basic Graph Theory, Tata McGraw-Hill, New Delhi, 1994.

8. G. Chartand and L. Lesniak – Graphs and Diagraphs, wadsworth and Brooks, 2nd Ed.,
9. Clark and D. A. Holton – A First Look at Graph Theory, Allied publishers.
10. D. B. West – Introduction to Graph Theory, Pearson Education Inc.,2001, 2nd Ed.,
11. J. A. Bondy and U. S. R. Murthy – Graph Theory with applications, Elsevier, 1976
12. J. P. Tremblay & R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co. 1997
13. S. Witala, Discrete Mathematics - A Unified Approach, McGraw Hill Book Co

13.9 ANSWER TO CHECK YOUR PROGRESS

1. In a directed graph (*v, v'*) is said to be **incident from** *v*, and to be **incident to***v'.* In a particular graph, the number of edges incident to a vertex is called the **in-degree** of the vertex and it is denoted by $degree_G{}^{+}(v)$ and the number of edges incident from it is called its **out-degree** and it is denoted by $degree_G{}^{-}(v)$. **---13.1**
2. If two paths in a graph share no common vertices then they are known as **vertex-disjoint & give example. ---13.1**
3. In a nondirected graph **G** a sequence **P** of zero or more edges of the form $\{v_0, v_1\}$, $\{v_1, v_2\}$,…,$\{v_{n-1}, v_n\}$ also represented as $(v_0 - v_1 - \cdots - v_n)$ is called a **path** from v_0 to v_n; where v_0 is the **initial vertex ---13.1**
4. Provide the definition (a) --- 13.2.4 & (b) ---13.2.2
5. Explain the concept–13.3
6. Explain the concept–13.5
7. Explain the concept–13.4.2

UNIT 14: GRAPH THEORY II

STRUCTURE

14.0 OBJECTIVES

- Concept and types of Trees

14.1 CONCEPT:

- A **tree** is a simple graph G such that there is a unique simple nondirected path between each pair of vertices of G.
- A **rooted tree** is a tree in which there is one designated vertex, called a **root**.
- A **rooted tree** is a **directed tree** if there is a root from which there is a directed path to each vertex. In such case there is exactly one such root.
- The **level** of a vertex ***v*** in a rooted tree is the length of the path to ***v*** from the root.
- A tree T with only one vertex is called a **trivial tree**; otherwise it is a **nontrivial tree**.

Example: Two trees, G_1 and G_2 are shown in figure 7.12. $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ where

$$V = \{a, b, c, d, e, f, g, h, i, j\}$$

$E_1 = \{\{a,c\},\{b,c\},\{c,d\},\{c,e\},\{e,g\},\{f,g\},\{g,i\},\{h,i\},\{i,j\}\}$ and
$E_2 = \{\{c,a\},\{c,b\},\{c,d\},\{c,f\},\{f,e\},\{f,i\},\{g,d\},\{h,e\},\{j,g\}\}$

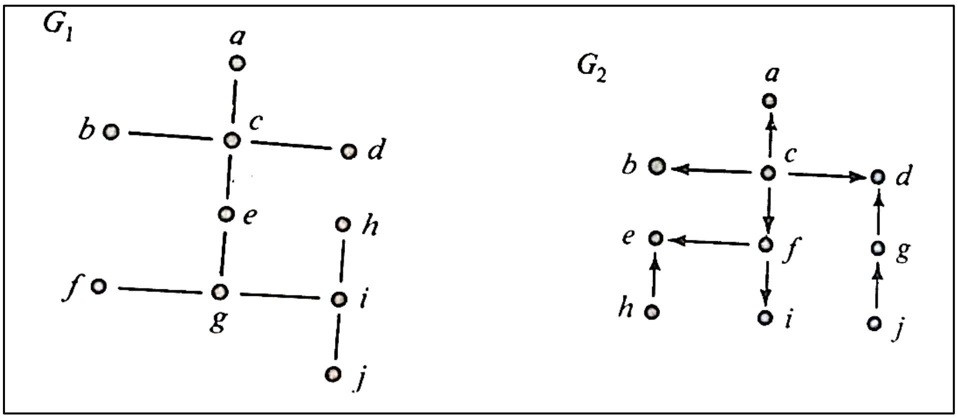


Figure 14.1: Two kinds of nondirected trees

Neither of these trees is a directed tree. If vertex c is designated as the root of each tree, vertex j is at level 4 in G_1 and at level 3 inG_2.

Example: A directed tree T is shown in figure 7.13.
$T = (V, E)$ where $V = \{a, b, c, d, e, f, g, h\}$ and
$E = \{(a,b),(a,c),(a,d),(b,e),(d,f),(e,g),$
$(e,h)\}$. The root of T is the vertex a and the vertices at level 2 are *e* and *f*.

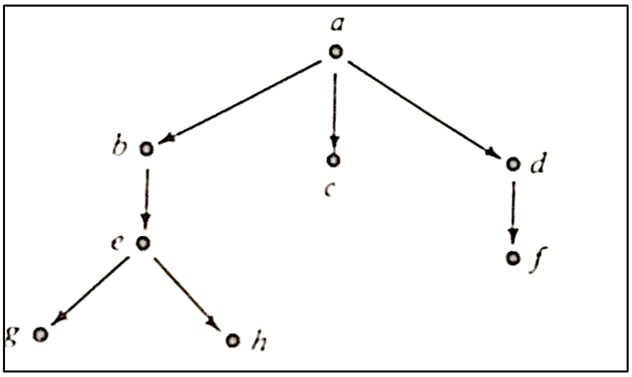


Figure 14.2: A directed tree

Concept:

Two vertices suppose a and b of a graph are said to be connected if there is a nondirected path from a to b in G and then the graph G is connected if each pair of its vertices is connected. If we define a Relation R on the vertices of a graph G by aRb if a and b are connected then R is an equivalence relation. We can partitioned the vertices of G into disjoint nonempty sets $V_1, V_2, \dots, V_n$ and the subgraphs $H_1, H_2, \dots, H_n$ of G induced by $V_1, V_2, \ldots and\ V_n$, respectively are called the connected components of G or simply the components of G and it is generally denoted by C(G) and if C(G)=1 it implies G is connected. A connected subgraph H of a graph G is a component of G if for each connected subgraph F of G where $H \subseteq F \subset G, V(H) \subseteq V(F)$ and $E(H) \subseteq E(F)$, then it follows that H = F.

If a graph **G** is connected and e is an edge such that $G - e$ is not connected, then ***e*** is said to be a bridge or a cut edge. If v is a vertex of **G** such that $G - v$ is not connected, then ***v*** is a cut vertex.

Example: Let G be the graph depicted in figure 7.11. This graph G has 3 components; the vertices a and d are connected as are i and g and j and k are not connected. Moreover, c is a cut vertex of the first component.

THEOREM: A simple non-directed graph **G** is a tree if **G** is connected and contains no cycles.

PROOF: Suppose that **G** is a tree. Since each pair of vertices are joined by a path, **G** is connected. If **G** contains a cycle containing distinct vertices **u** and **v**, then **u** and **v** are joined by at least two simple paths, the one along one portion of the cycle and the other part completing the cycle. The above discussion contradicts the hypothesis which states that there is a unique path between u and v, and thus a tree has no cycles.
Conversely, assume that **G** is connected and contains no cycles. Let **a** and **b** be any pair of vertices of **G**. If there are two different simple paths, P_1 and P_2 from **a** to **b**, then we can find cycle in **G** as follows:
Since P_1 and P_2 are different paths there must be a vertex v_1 (like $v_1 = a$) on both paths such that the vertex following v_1 on P_1 is not the same as the vertex following v_1 on P_2. Since P_1 and P_2 terminate at b, there is a first vertex after v_1, call its v_2, which P_1 and P_2 have common (possibly $v_2 = b$). Thus, the part of P_1 from v_1 to v_2 form a cycle in **G**. This contradicts the assumption that **G** has no cycles. Therefore, **G** has exactly one path joining **a** and **b**.

THEOREM: In every nontrivial tree there is at least one vertex of degree one.

PROOF: Let us start at any vertex say v_1. If $\deg(v_1) \neq 1$, move along any edge to vertex v_2 incident with v_1. If $\deg(v_2) \neq 1$ continue to vertex v_3 along a different edge and continue it to produces a path $v_1 - v_2 - v_3 - v_4$ ... (it indicates that there is an edge from v_1 to v_2, one from v_2 to v_3 and so on.) None of the $v_i's$ is repeated in this path since then we would have circuit – which a tree may not have. Since the number of vertices in the graph is finite, the graph must end somewhere and there should be a vertex of degree 1 as we can enter this vertex but cannot leave it.

THEOREM: A tree with n vertices has exactly n – 1 edges.

PROOF: We will use mathematical induction on the number of vertices. If n = 1, there are no edges. Hence, the result is trivial for n = 1. Assume, then, for $n \geq 1$ that all the trees with n vertices have exactly n – 1. Now consider an arbitrary tree with n + 1 edges. With reference to the previous theorem, there is a vertex v in T of degree 1. Let us consider the figure 7.14 where let us prune this tree by removing this vertex v and its associated edge e from T and consider it as $T' = T - v$.

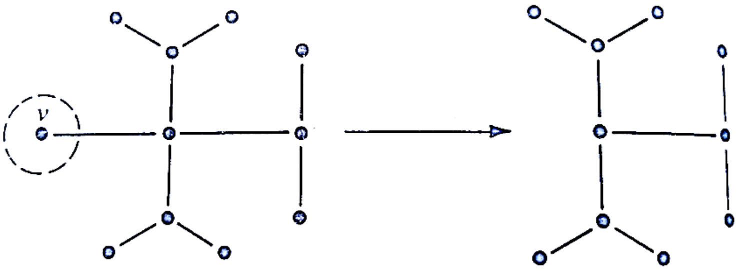


Figure 14.3

T’ has n vertices and one edge less than T. Also T’ is connected as for any pair of vertices say a and b in T’, there is a unique simple path from a to b in T and this path is not affected by the removal of the vertex v and edge e. There are no cycles in T’ as there were none in T. Thus, T’ is a tree and inductive hypothesis implies that it has n – 1 edges and so T must have n edges as it has one more edge as compare to T’.

COROLLARY: If G is a nontrivial tree then G contains at least two vertices of degree 1.

PROOF: Let n be the number of vertices of graph G. By the sum of degrees formula,

$$\sum_{i=1}^{n} \deg(v_i) = 2|E| = 2(n-1) = (2n-2)$$

Now if there is only one vertex, say v_1, of degree 1, then

$\deg(v_i) \geq 2$ for $i = 2, \dots, n$

And $\sum_{i=1}^{n} \deg(v_i) = 1 + \sum_{i=2}^{n} \deg(v_i) \geq 1 + 2n - 2 = 2n - 1$

But then

$$2n - 2 \geq 2n - 1 \; or \; -2 \geq -1, a\ contradiction$$

Example: There are 6 non-isomorphic trees with 6 vertices as depicted in Figure 7.15 as below.

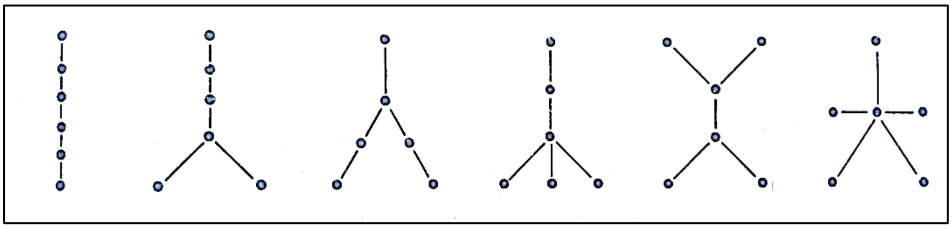


Figure 14.4 The trees of 6 vertices

THEOREM: If 2 non adjacent vertices of a tree T are connected by adding an edge, then the resulting graph will contain a cycle.

PROOF: If T has n- vertices then T has n – 1 edges and if additional edge is added to the edges of T the resulting graph G has n vertices and n edges. Hence G cannot be a tree by previous theorem. In case, if the addition of an edge has not affected the connectivity. Hence G must have cycle.

Example: As shown in below figure 7.16 if any of the dotted line is added to the tree it will create a cycle.

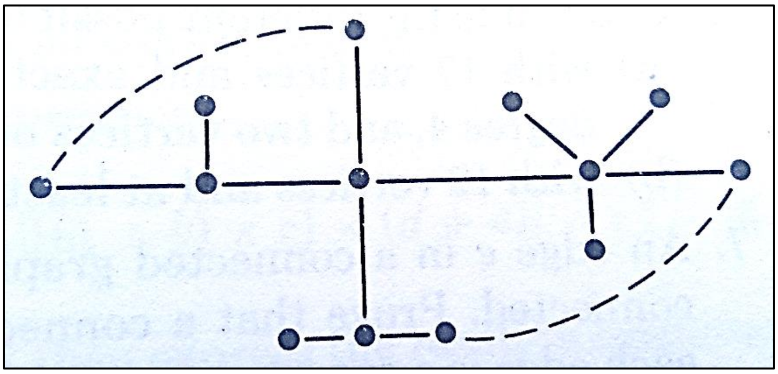


Figure 14.5

THEOREM: A graph G is a tree if and only if G has no cycles and $|E| = |V| - 1$.

PROOF: We are interested to show that if G has no cycles and $|E| = |V| - 1$, then G is connected. Let us consider the components of the G and denote it by $G_1, G_2, \dots, G_n$ where $n \geq 1$. Assume $|V_i|$= the number of vertices of G_i. Now each G_i is a tree which contains no cycles and hence they are connected. Thus, $G_i$has $|V_i| - 1$ edges .Hence G has $(|V_1| - 1) + (|V_2| - 1) + \cdots + (|V_n| - 1) = |V_1| + |V_2| + \cdots + |V_n| - n = |V| - n$ edges. Thus, k = 1, and G is connected.

14.2 ORDERED ROOTED TREES:

An ordered rooted tree is a rooted tree wherethe children of each internal vertex are ordered. For example, in an ordered binary tree (just called binary tree), if an internal vertex has twochildren,

− the first child is called the left child and thesecond is called the right child.

− the tree rooted at the left child is called the leftsubtree, and at the right child, the right subtree

[**NOTE**: Ordered rooted trees can be defined recursively.]

Example:

a

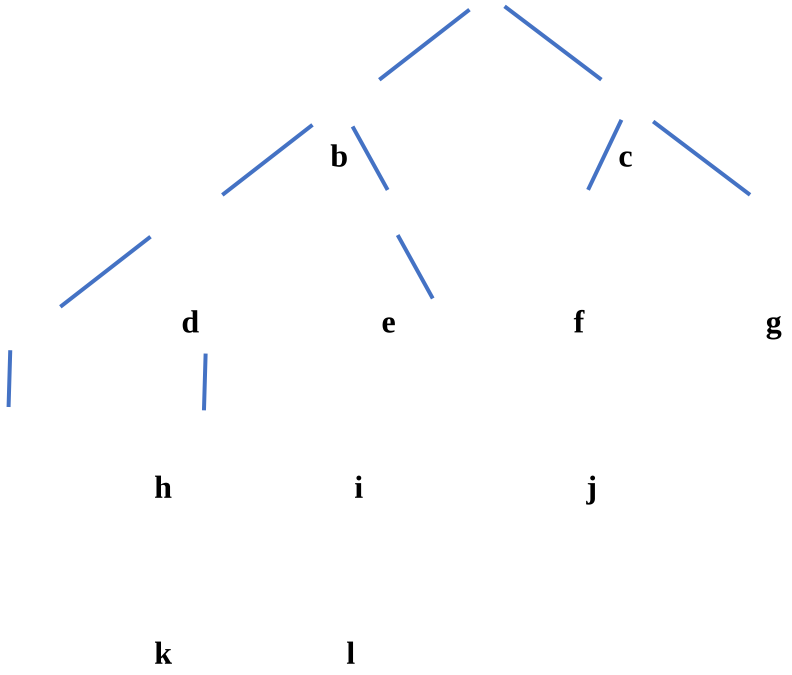


Figure: 14.6: Ordered Rooted Tree

In the above ordered rooted tree, we observe the following things:

- b is the left child of vertex a
- c is the right child of vertex a
- {e, j} is the right subtree of the vertex b
- {d, h, i, k, l} is the left subtree of the vertex b

Check Your Progress 1:

1. What is rooted tree?

____

____

____

2. Explain directed tree.

____

____

____

14.3 TREE TRAVERSAL:

Procedures for systematically visiting every vertex of an ordered rooted tree are called traversal algorithms.

a. Pre-order traversal:

Let T be an ordered rooted tree with root r. If T consists only of r, then r is the preorder traversal of T. Otherwise, suppose that $T_1, T_2, \ldots, T_n$are the subtrees at r from left to right in T. The preorder traversal begins by visiting r. It continues by traversing T_1 in preorder, then T_2 in preorder, and so on, until T_n is traversed in preorder.

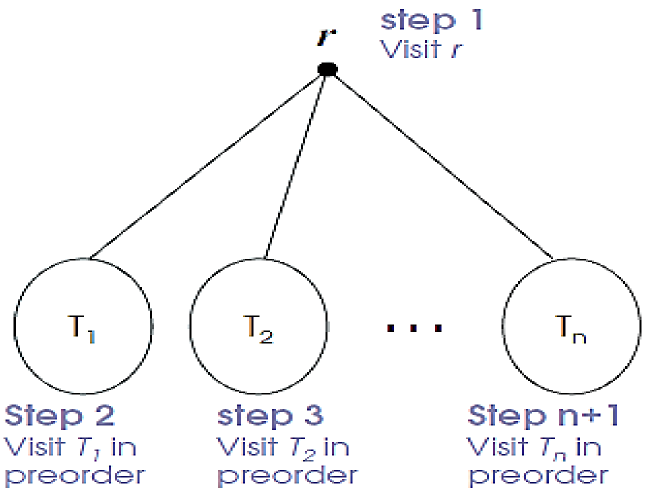


Figure 14.7: Pre-order Traversal

b. Inorder traversal

Let T be an ordered rootedtree with root r.If T consists only of r, then r isthe inorder traversal of T.Otherwise, suppose that $T_1, T_2, \ldots, T_n$are the subtrees at rfrom left to right. The inordertraversal begins by traversingvisiting T_1 in inorder, thenvisiting r. It continues bytraversing T_2 in inorder, thenT_3 in inorder, …, and finallyT_n in inorder.

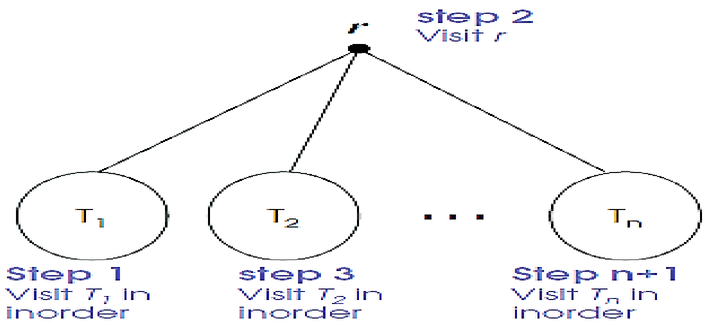


Figure 14.8: Inorder Traversal

c. Postorder Traversal:

Let T be an ordered rootedtree with root r.If T consists only of r, then r isthe postorder traversal of T.Otherwise, suppose that $T_1, T_2, \ldots, T_n$are the subtrees at rfrom left to right. The postordertraversal begins by traversingT_1in postorder, then T_2inpostorder, …, then $T_n$inpostorder, and ends byvisiting r.

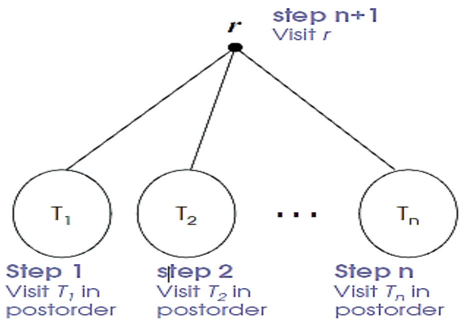
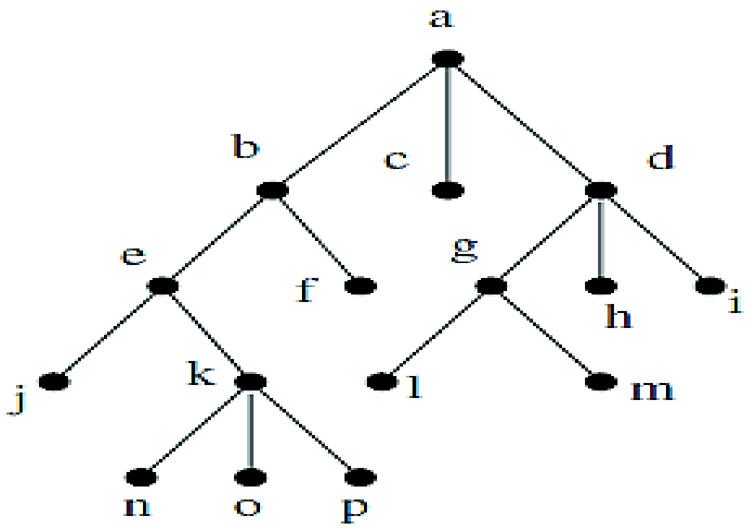


Figure 14.9: Post order Traversal

Example: In the below figure 14.10



Preorder: a, b, e, j, k, n, o, p, f, c, d, g, l, m, h, I

Inorder: j, e, n, k, o, p, b, f, a, c, l, g, m, d, h, i

Postorder: j, n, o, p, k, e, f,b, c, l, m, g, h, i, d, a

14.4 SPANNING TREES:

Concept: A subgraph **H** of a graph **G** is called a spanning tree of G if

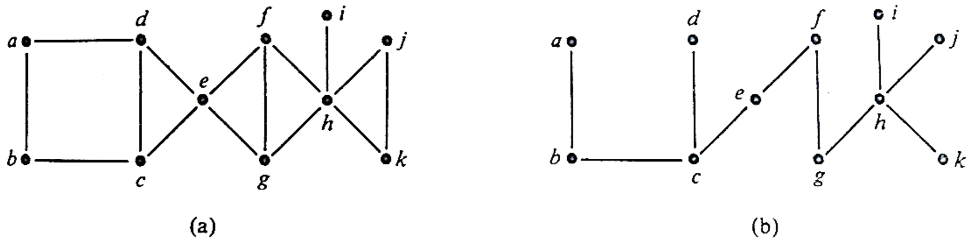
(i) **H** is a tree

(ii) **H** contains all the vertices of **G**.

A spanning tree that is a directed tree is called a **directed spanning tree** of **G.**

Example: Consider the graph G in Figure 7.22 (a) and let this graph represents a communication network in which vertices resembles the stations and edges resembles the communication links. Now we need to find out the largest number of edges that can be deleted while still allowing the station to communicate with each other.

After close observation, the cycle $d - c - e - d$ gives two ways for d and e to communicate. Along the path $d - c - e$ or directly from d to e. If the edge {d, e} is deleted, d and e can still communicate via c. One edge of each cycle in G can be deleted and the leftover edges are sufficient to maintain communication between all stations. This is depicted in figure 7.22 (b) and the result is the spanning tree for the graph of figure 7.22 (a). We can obtain other spanning tree by deleting another sequence of edges to eliminate cycles. The graph G has 15 edges and the spanning tree for G has 10 edges so 5 edges have to be deleted. In general, if a graph G is connected graph with n vertices and m edges, a spanning tree of G must have n – 1 edges. Hence, the number of edges that must be removed before a spanning tree is obtained must be $m - (n - 1) = m - n + 1$ which is also called as circuit rank of graph



G.

Figure 14.11

THEOREM: A non-directed graph **G** is connected if and only if **G** contains a spanning tree. Indeed if we successively delete edges of cycles until no further cycles remain, then the result is the spanning tree of **G**.

PROOF: If **G** has a spanning tree T, there is a path between any pair of vertices in **G** along the tree T. Thus **G** is connected.
We can prove it conversely that a connected graph G has a spanning tree by mathematical induction on the number ***k*** of the cycles in G. If k = 0, then G is connected with no cycles and hence **G** is a tree. Now let us assume that all connected graphs with fewer than ***k*** cycles have a spanning tree. Now consider that **G** is connected graph with ***k*** cycles. Remove an edge ***e*** from one of the cycles. Then G – e is still connected and has a spanning tree for G by the inductive hypothesis because G – e has fewer cycles than **G**. But since G – e has all vertices of G, the spanning tree for G – e is also one for **G** and the results followed by mathematical induction.

Concepts: Let **T** be a rooted tree with designated root v_0. Suppose that ***u*** and ***v*** are vertices in T and that $v_0 - v_1 - \cdots - v_n$ is a simple path in **T**. Then

i. v_{n-1} is the **parent** of v_n
ii. $v_0, v_1, \dots, v_{n-1}$ are the **ancestor** of v_n
iii. v_n is the **child** of v_{n-1}
iv. If u is an **ancestor** of v, then v is **descendan**t of u
v. If u has no children, then u is a **leaf** of T
vi. If v is not a leaf of T, then v is an **internal vertex** of T
vii. The subgraph of T consisting of ***v*** and all its descendants, with v designated as a root, is the **subtree** of T rooted at ***v***.

Example: Refer the figure 7.23, if ***a*** is designated as the root,
then ***b, d, f, h*** and ***j*** are leaves of T,
i is the parent of ***h*** and ***j***;
f, h, i and ***j*** are descendants of ***g***;
a and ***c*** are the ancestors of ***e***;
and the children of ***c*** are ***b, d*** and ***e***.

also the vertices ***a, c, e, g*** and ***i*** are the internal vertices to the tree rooted at ***a***.

Incase if we consider ***c*** as a root, then ***a*** becomes a leaf, and ***c*** is the parent of ***a***.

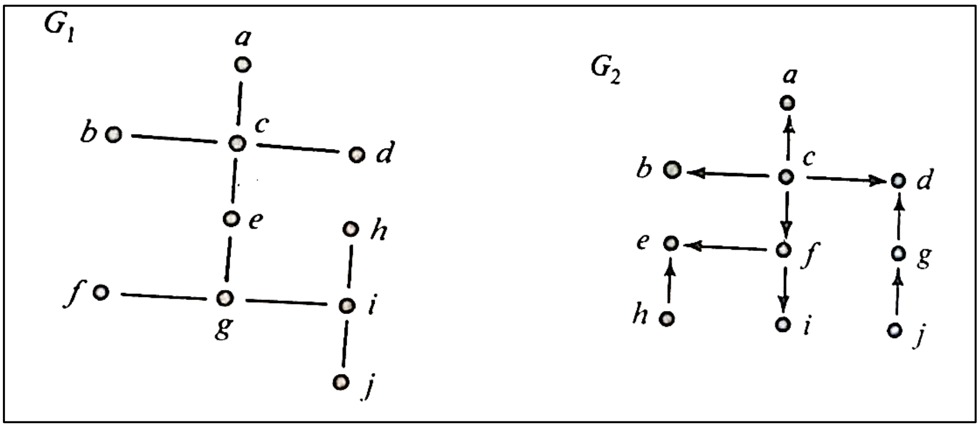


Figure 14.12

Minimal Spanning Trees:

Consider the collection of k cities, and we wish to construct a transportation network connecting all the cities and also assume that the cost of building links between each pair of cities is known and we wish to construct it as cheaply as possible.

We can represent the desired network with the help of graph by considering each city as a vertex and placing an edge between vertices if a link runs between the two corresponding cities. If the cost for constructing a link between cities say v_a and v_b, the weights like c_{ab} can be assigned to the edge $\{v_a, v_b\}$. So the main issue is to design such network at minimum cost of construction. If M is the graph of a network with minimal cost , it is essential that M be connected for all cities are to be connected by links. Also there would not be any circuit in the graph M, otherwise we can remove an edge from a circuit and thereby reduce the total cost by the cost of construction of that edge. Hence the graph of minimal cost M must be a spanning tree of the k vertices.

We can state the above problem in general terms as follows:

Let G be the graph of all possible links between the cities with the non-negative cost of construction C(e) assigned to each edge e in G. Then if H is any subgraph of G with edges $e_{1,} \dots, e_m$ the total cost of constructing the network H is $C(H) = \sum_{i=1}^{m} C(e_i)$. A spanning tree T where C(T) is minimal is called **minimal spanning tree**.

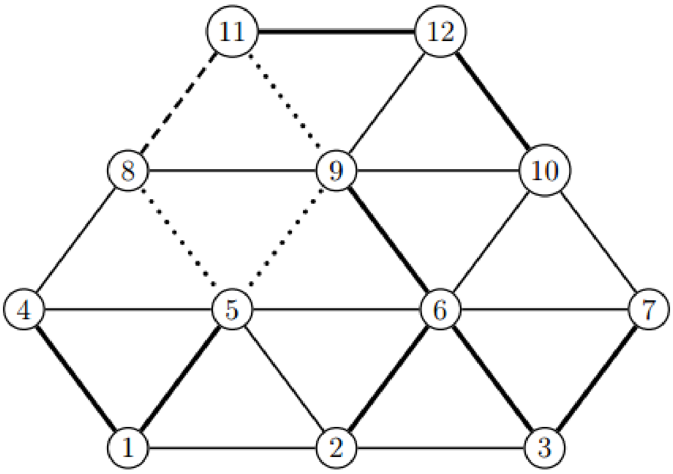
Minimum (or Maximum) Weight Spanning Trees

Definition : A *weighted graph* is a finite graph without loops, $G = (V, E, st)$, together with a function, c: $E \to$ R, called a *weight function* (or *cost function*). We will denote a weighted graph by (G, c). Given any set of edges, $E \subseteq E$, we define the *weight (or cost)* of E by

$$c(E') = \sum_{e \in E'} c(e).$$

Given a weighted graph, (G, c), an important problem is to find a spanning tree, T such that $c(T)$ is maximum (or minimum). This problem is called the *maximal weight spanning tree* (resp. *minimal weight spanning tree*). Actually, it is easy to see that any algorithm solving any one of the two problems can be converted to an algorithm solving the other problem. For example, if we can solve the maximal weight spanning tree, we can solve the mimimal weight spanning tree by replacing every weight, $c(e)$, by $-c(e)$, and by looking for a spanning tree, T , that is a maximal spanning tree, since

$$\min_{T \subseteq G} c(T) = -\max_{T \subseteq G} -c(T).$$



The set C_e associated with an edge $e \in G - T$

Since every spannning tree of a given graph, G = (V, E, st), has the same number of edges (namely, $|V|-1$), adding the same constant to the weight of every edge does not affect the maximal nature a spanning tree, that is, the set of maximal weight spanning trees is preserved. Therefore, we may assume that all the weights are non-negative.

$$C_{\{8,11\}} = \{\{8,5\},\{5,9\},\{9,11\}\}.$$

In order to justify the correctness of Kruskal's algorithm, we need two definitions. Let G = (V, E, st) be any connected weighted graph and let T be any spanning tree of G. For every edge, $e \in E - T$, let Ce be the set of edges belonging to the unique chain joining the endpoints of e (the vertices in $st(e)$). For example, in the graph shown in above Figure. the set $C_{\{8,11\}}$ associated with the edge {8, 11} (shown as a dashed line) corresponds to the following set of edges (shown as dotted lines) in T:

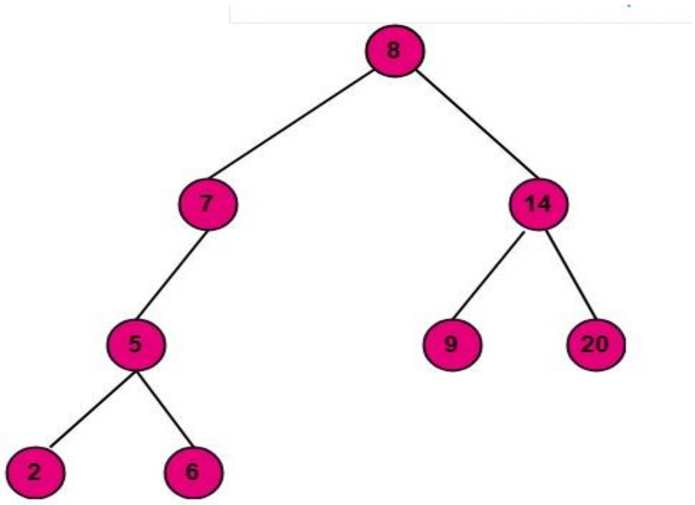
Also, given any edge, $e \in T$, observe that the result of deleting e yields a graph denoted
$T - e$ consisting of two disjoint subtrees of T. We let Ωe be the set of edges, $e \in G - T$,
such that if $st(e)$ = {u, v}, then u and v belong to the two distinct connected components of T − {e}. For example, in above figure, deleting the edge {5, 9} yields the set of edges (shown as dotted lines)

$$\Omega_{\{5,9\}} = \{\{1,2\},\{5,2\},\{5,6\},\{8,9\},\{8,11\}\}.$$

14.5 BINARY SEARCH TREE

Binary search trees have the property that the node to the left contains a smaller value than the node pointing to it and the node to the right contains a larger value than the node pointing to it.
It is not necessary that a node in a 'Binary Search Tree' point to the nodes whose value immediately precede and follow it.

Example: The tree shown in fig is a binary search tree

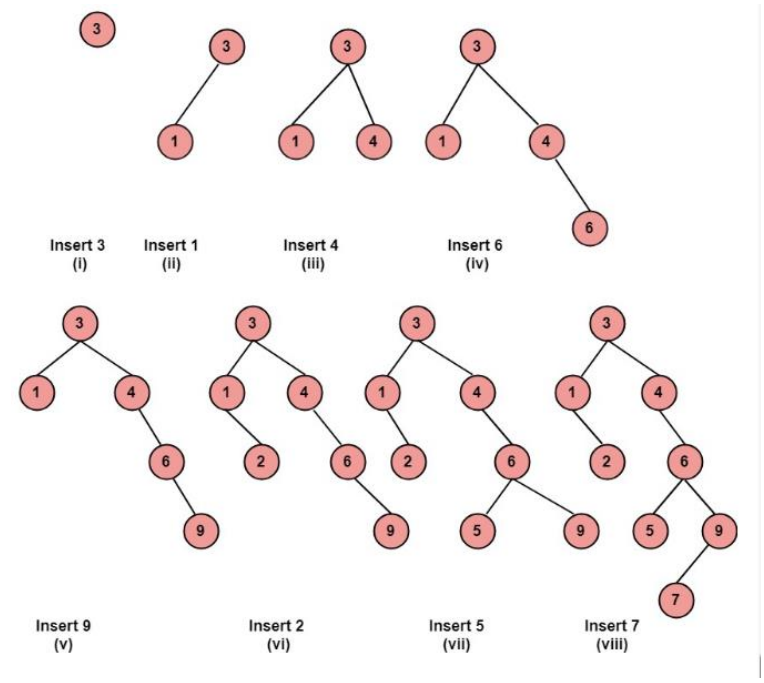


Inserting into a Binary Search Tree: Consider a binary tree T, and suppose we have given an ITEM of information to insert in T. The ITEM is inserted as a leaf in the tree. The following steps explain a procedure to insert an ITEM in the binary search tree T.

1. Compare the ITEM with the root node.
2. If ITEM > ROOT NODE, proceed to the right child, and it becomes a root node for the right subtree.
3. If ITEM < ROOT NODE, proceed to the left child.
4. Repeat the above steps until we meet a node which has no left and right subtree.
5. Now if the ITEM is greater than the node, then the ITEM is inserted as the right child, and if the ITEM is less than the node, then the ITEM is inserted as the left child.
6.

Example: Show the binary search tree after inserting 3, 1,4,6,9,2,5,7 into an initially empty binary search tree.

Solution: The insertion of the above nodes in the empty binary search tree is shown in fig:



Insert 3 (i) Insert 1 (ii) Insert 4 (iii) Insert 6 (iv)

Insert 9 (v) Insert 2 (vi) Insert 5 (vii) Insert 7 (viii)

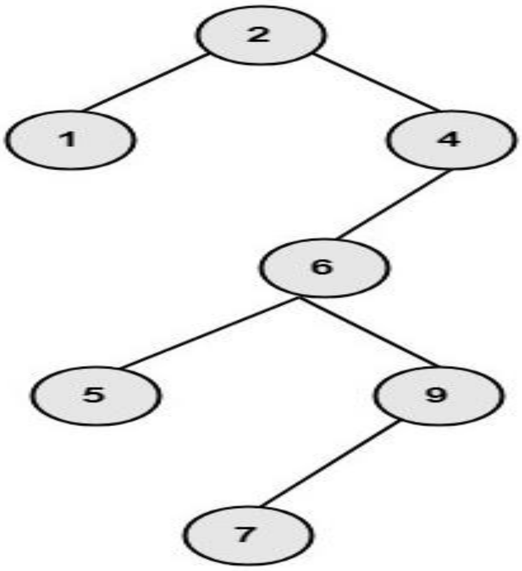
Deletion in a Binary Search Tree: Consider a binary tree T. Suppose we want to delete a given ITEM from binary search tree. To delete an ITEM from a binary search tree we have three cases, depending upon the number of children of the deleted node.

1. **Deleted Node has no children:** Deleting a node which has no children is very simple, as replace the node with null.
2. **Deleted Node has Only one child:** Replace the value of a deleted node with the only child.
3. **Deletion node has only two children:** In this case, replace the deleted node with the node that is closest in the value to the deleted node. To find the nearest value, we move once to the left and then to the right as far as possible. This node is called the immediate predecessor. Now replace the value of the deleted node with the immediate predecessor and then delete the replaced node by using case1 or case2.

Example: Show that the binary tree shown in fig (viii) after deleting the root node.

Solution: To delete the root node, first replace the root node with the closest elements of the root. For this, first, move one step left and then to the right as far as possible to the node. Then delete the replaced node.

The tree after deletion shown in fig:



Check Your Progress 2:

1. Explain tree traversal.

2. Explain deletion in binary search tree

3. What is minimal spanning tree?

14.6 SUMMING UP

Graph theory has got wide application in number of fields including computer science. It helps to represent structural model in Chemistry, Biology, Sociology, Operation Research, Computer Algorithm, Transport & Activity networks and Theory of Games.

14. 7 KEYWORDS

1. Adjacent: Two vertices are adjacent if they are connected by an edge.

2. Arc: A synonym for edge

3. Complete graph: A complete graph with n vertices (denoted Kn) is a graph with n vertices in which each vertex is connected to each of the others

4. Degree: The degree (or valence) of a vertex is the number of edge ends at that vertex. For example, in this graph all of the vertices have degree three.

14.8 QUESTIONS FOR REVIEW

1. Let G be a graph with k components, where each component is a tree. Obtain a formula for |E| in terms of |V| and k

2. A forest is a simple graph with no circuits. Show that the connected components of a forest are trees.

3. Draw a binary tree to represent *((a-b). c) + (d/e)v*

4. Use a binary tree to sort the following list of numbers

15, 7, 24, 11, 27, 13, 18, 19, 9 .

We note that when a binary tree is used to sort a list, the in order traversal will be automatically assumed in this unit.

14.9 SUGGESTED READINGS

1. Kenneth H. Rosen - Discrete Mathematics and Its Applications, Tata Mc-Graw-Hill, 7th Edition, 2012.

2. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross-Discrete Mathematical Structures-Prentice Hall, 3rd Edition, 1996.
3. Grimaldi R-Discrete and Combinatorial Mathematics. 1-Pearson, Addison Wesley, 5th Edition, 2004.
4. C. L. Liu – Elements of Discrete Mathematics, McGraw-Hill, 1986.
5. F. Harary – Graph Theory, Addition Wesley Reading Mass, 1969.
6. N. Deo – Graph Theory With Applications to Engineering and Computer Science, Prentice Hall of India, 1987.
7. K. R. Parthasarathy – Basic Graph Theory, Tata McGraw-Hill, New Delhi, 1994.
8. G. Chartand and L. Lesniak – Graphs and Diagraphs, wadsworth and Brooks, 2nd Ed.,
9. Clark and D. A. Holton – A First Look at Graph Theory, Allied publishers.
10. D. B. West – Introduction to Graph Theory, Pearson Education Inc.,2001, 2nd Ed.,
11. J. A. Bondy and U. S. R. Murthy – Graph Theory with applications, Elsevier, 1976
12. J. P. Tremblay & R. Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill Book Co. 1997
13. S. Witala, Discrete Mathematics - A Unified Approach, McGraw Hill Book Co.

14.10 ANSWER TO CHECK YOUR PROGRESS

1. A **rooted tree** is a tree in which there is one designated vertex, called a **root**.

   ---14.1
2. A **rooted tree** is a **directed tree** if there is a root from which there is a directed path to each vertex. In such case there is exactly one such root.---14.1
3. Explain the concept**---14.3**
4. Explain deletion of spanning tree with steps --- 14.5
5. Explain the concept–14.4.