

A STUDY ON CRYPTOGRAPHY

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI.

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

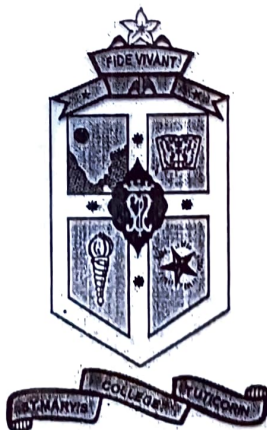
BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NUMBER
A. ADELINE ANISHA	19SUMT01
A. CROSSLIN NIRANJANA	19SUMT08
S. GNANA MALAR	19SUMT12
R. MURUGALAKSHMI	19SUMT21
D. PAVITHRA	19SUMT28

Under the guidance of

Ms. P. SUGANYA M.Sc., M.Phil., SET.,



DEPARTMENT OF MATHEMATICS

St. Mary's College (Autonomous), Thoothukudi.

May-2022

A STUDY ON CRYPTOGRAPHY

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI.

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME

REGISTER NUMBER

A. ADELINE ANISHA

19SUMT01

A. CROSSLIN NIRANJANA

19SUMT08

S. GNANA MALAR

19SUMT12

R. MURUGALAKSHMI

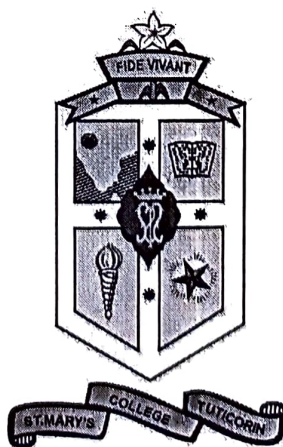
19SUMT21

D. PAVITHRA

19SUMT28

Under the guidance of

Ms. P. SUGANYA M.Sc., M.Phil., SET.,



DEPARTMENT OF MATHEMATICS

St. Mary's College (Autonomous), Thoothukudi.

May-2022

CERTIFICATE

This is to certify that this project work entitled "A STUDY ON CRYPTOGRAPHY" is submitted to St.Mary's College (Autonomous), Thoothukudi affiliated to Manonmaniam Sundaranar University, Tirunelveli in partial fulfilment for the award of degree of Bachelor of Science in Mathematics and is the work done during the year 2021-2022 by the following students.

NAME	REGISTER NUMBER
A. ADELINE ANISHA	19SUMT01
A. CROSSLIN NIRANJANA	19SUMT08
S. GNANA MALAR	19SUMT12
R. MURUGALAKSHMI	19SUMT21
D. PAVITHRA	19SUMT28



Signature of the Guide



Signature of the Coordinator



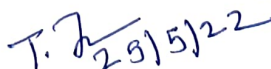
Signature of the Director
Director

Self Supporting Courses
St. Mary's College (Autonomous)
Thoothukudi - 628 001.



Signature of the Principal

Principal
St. Mary's College (Autonomous)
Thoothukudi - 628 001.



Signature of the Examiner

DECLARATION

I here by declare that, the project entitled “A STUDY ON CRYPTOGRAPHY” submitted for the degree of **Bachelor of Science** is our work carried out under the guidance of **Ms. P. Suganya M.Sc., M.Phil., SET.,** Assistant Professor, Department of Mathematics (SSC), **St. Mary's College (Autonomous), Thoothukudi.**

A. Adeline Anisha-
(ADELINE ANISHA. A)

A. Crosslin Niranjana
(CROSSLIN NIRANJANA. A)

S. Gnana Malari
(GNANA MALAR. S)

Murugalakshmi R
(MURUGALAKSHMI. R)

D. Pavithra .
(PAVITHRA. D)

ACKNOWLEDGEMENT

First of all, we thank the Almighty for showering his blessings to undergo this project.

We express our sincere gratitude and heartfelt thanks to our Principal **Rev. Dr. Sr. A. S. J. Lusia Rose M.Sc., PGDCA., M.Phil., Ph.D.**, and to our Director **Rev. Sr. Josephine Jeyarani M.Sc., B.Ed.**, for kindly permitting us to do this project.

We express our gratitude to **Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D.**, Coordinator, Department of Mathematics (SSC) for her inspirational ideas and Encouragement.

We are very thankful to our guide **Ms. P. Suganya M.Sc., M.Phil., SET.**, Assistant Professor, Department of Mathematics (SSC) for her efficient and effective guidance. She played a key role in the preparation of this project.

We also thank our staff members for their encouragement in all our efforts.

Finally, we thank all those who extended their help regarding this project.

Station: Thoothukudi

Date: 17.05.2022

CONTENT

CHAPTER	TOPIC	PAGE NO.
	Introduction	
1	Preliminaries	1
2	Some Simple Cryptosystems	5
3	Discrete Logarithms & Elliptic Curve Discrete Logarithm Problem	17
4	Integer Factorization & RSA	30
5	Applications	42
	Conclusion	
	Reference	

INTRODUCTION

Cryptography is the science of using mathematics to hide data behind encryption. From ancient times to the present, secret messages have been sent. Classically, the need for secret communication has occurred in diplomacy and in military affairs. Now, with electronic communication coming into widespread use, secrecy has become an important use. Just recently, with the advent of electronic banking, secrecy has become necessary even for financial transactions. Hence, there is a great deal of interest in the techniques of making messages unintelligible to everyone except the intended receiver. One of the earliest cryptographic systems was used by around 50 B.C. In this project, you will be introduced to basic mathematical principles and functions that form the foundation for cryptographic methods.

The project consists of five chapters.

In chapter 1, we have given some basic definitions and result on cryptography and mathematical concepts that are needed for the subsequent chapters.

In chapter 2, we have discussed some basic simple cryptosystems.

In chapter 3, we have studied discrete logarithm problem and elliptic curve discrete logarithm problem along with both Diffie Hellman Key Exchange and Elgamal Public Key Cryptosystem.

In chapter 4, we have studied Integer Factorization and RSA Cryptosystem.

In chapter 5, we have discussed some applications of Cryptography especially for chapter 3 & 4.

Chapter 1

CHAPTER 1

PRELIMINARIES

Definition: 1.1

The discipline devoted to secrecy systems is called *cryptology*.

Definition: 1.2

Cryptography is the part of cryptology that deal with the design and implementation of secrecy systems.

Definition: 1.3

The message to be transmitted is called *Plaintext*.

Definition: 1.4

The coded form of the message is called *Ciphertext*.

Definition: 1.5

In cryptography codes are called *Ciphers*.

Definition: 1.6

The process of writing the plaintext in the coded form is called *Encryption*. The process is also called *Enciphering*.

Definition: 1.7

Decryption / Deciphering process is reverse to Encryption.

Definition: 1.8

Alphabets is a collection of symbols. It also referred to as characters.

Definition: 1.9

Let a and b be two integers. We say a is *congruent* to b modulo an integer m if $m \mid a-b$ and denote it as $a \equiv b \pmod{m}$.

Definition: 1.10

A statement like $a \equiv b \pmod{m}$ is called a *congruence* and the integer m is called the *modulus*.

Definition: 1.11

A *cryptosystem* is a structure or scheme consisting of a set of algorithms that converts plaintext to ciphertext to encode or decode messages securely.

Definition: 1.12

Matrix multiplication involves the action of multiplying each row vector of one matrix by each *column vector* of another matrix.

Definition: 1.13

A *Primitive root* mod n is an integer g such that every integer relatively prime to n is congruent to a power of g mod n . That is, the integer g is a primitive root (mod n) if for every number a relatively prime to n there is an integer z such that $a \equiv (g^z \pmod{n})$.

Definition: 1.14

The *discrete logarithm problem* is defined as given a group G , a generator group G . Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups.

Definition: 1.15

ElGamal cryptosystem can be defined as the cryptography algorithm that uses the public and private key concepts to secure communication between two systems. It can be considered the asymmetric algorithm where the encryption and decryption happen by using public and private keys.

Definition: 1.16

Different Hellman Key exchange also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would be code breaker mathematically overwhelming.

Definition: 1.17

One key (*public key*) is used for encrypt the plaintext to convert it into ciphertext and another key (*private key*) is used by receiver to decrypt the ciphertext.

Definition: 1.18

An *elliptic curve* is a mathematical object that can be described by a deceptively simple equation:

$$Y^2 = X^3 + AX + B.$$

Definition: 1.19

Let p be an odd prime number and let a be a number with $p \nmid a$. we say that a is a *quadratic residue modulo p* if a is a square modulo p , i.e., if there is a number

c so that $c^2 \equiv a \pmod{p}$. If a is not a square modulo p , i.e., if there exists no such c , then a is called a *quadratic nonresidue modulo p* .

Definition: 1.20

Let a and b be integers and let b be odd and positive.

The *Jacobi* symbol (a / b) is defined by the formula:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \left(\frac{a}{p_3}\right)^{e_3} \dots \left(\frac{a}{p_t}\right)^{e_t}.$$

Definition: 1.21

In mathematics, particularly in the area of arithmetic, a *modular multiplicative inverse* of an integer a is an integer X such that the product ax is congruent to 1 with respect to the modulus m . In the standard notation of modular arithmetic this congruence is written as

$$ax \equiv 1 \pmod{m}.$$

Definition: 1.22

Laws of exponents states that the base is the variable that is repeatedly multiplied by itself. Exponents show the repeated number of times where the number can be multiplied.

Definition: 1.23

Probabilistic encryption is the use of randomness in an encryption algorithm, so that when encryption the same message several times it will, in general, yield different ciphertexts.

Chapter 2

CHAPTER 2

SOME SIMPLE CRYPTOSYSTEMS

2.1 INTRODUCTION

A need to send and receive confidential information has always been there ever since. There are times when we need to send messages and secret information to a select few without being known to all in general. Number theory has been used very successfully for this purpose. Using the prime numbers and theory of congruences a discipline called Cryptography has evolved that serves the purpose. **Cryptography** is the study of methods used to send messages in disguised form so that only the intended recipient can read it (from the Greek *kryptos* meaning *hidden* and *graphein* meaning *to write*).

In the language of cryptography, where codes are called *ciphers*, the information to be concealed is called *plaintext*. After transformation to a secret form, a message is called *ciphertext*. The process of converting from plaintext to ciphertext is said to be *encrypting* (or *enciphering*), whereas the reverse process of changing from ciphertext back to plaintext is called *decrypting* (or *deciphering*).

2.2 SOME SIMPLE CRYPTOSYSTEMS

In this chapter let us have a look on some simple cryptosystems such as,

- Shift Cipher
- Substitution Cipher
- Hill Cipher
- Vigenere Cipher
- Permutation Cipher

Definition: 2.2.1

Suppose a and b are integers, and m is a positive integer. Then we write $a \equiv b \pmod{m}$ if m divides $b - a$. The phrase $a \equiv b \pmod{m}$ is called a ***congruence***, and it is read as " a is ***congruent*** to b modulo m ". The integer m is called the ***modulus***.

2.3. SHIFT CIPHER

Definition: 2.3.1

Let $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. For $0 \leq K \leq 25$, define

$$e_K(x) = (x + K) \bmod 26$$

and

$$d_K(y) = (y - K) \bmod 26$$

$(x, y \in \mathbb{Z}_{26})$.

Remark: 2.3.2

For the particular key $K = 3$, the cryptosystem is often called the *Caesar Cipher*, which was purportedly used by Julius Caesar.

We would use the *Shift Cipher* (with a modulus of 26) to encrypt ordinary English text by setting up a correspondence between alphabetic characters and residues modulo 26 as follows: $A \leftrightarrow 0, B \leftrightarrow 1, \dots, Z \leftrightarrow 25$. Since we will be using this correspondence in several examples, let's record it for future use:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example: 2.3.3

Suppose the key for a *Shift Cipher* is $K = 11$, and the plaintext is

wewillmeetatmidnight.

We first convert the plaintext to a sequence of integers using the specified correspondence, obtained the following:

22 4 22 8 11 11 12 4 4 19

0 19 12 8 3 13 8 6 7 19

Next, we add 11 to each value, reducing each sum modulo 26:

7 15 7 19 22 22 23 15 15 4

11 4 23 19 14 24 19 17 18 4

Finally, we convert the sequence of integers to alphabetic characters, obtaining the ciphertext:

HPHTWWXPPELEXTTOYTRSE.

To decrypt the ciphertext, Bob will first convert the ciphertext to a sequence of integers, then subtract 11 from each value (reducing modulo 26), and finally convert the sequence of integers to alphabetic characters.

Example: 2.3.3

Using the shift cipher with key = 12, what will be the result after decrypting the message “TQXXA”?

The decryption process is (the y here represents a letter from ciphertext): $(y - K) \bmod 26$

The given data,

Shift cipher with key $K = 12$

Ciphertext = “TQXXA”

The plain text of the letter “T” = $(19 - 12) \bmod 26 = 7 = H$

The plain text of the letter “Q” = $(16 - 12) \bmod 26 = 4 = E$

The plain text of the letter “X” = $(23 - 12) \bmod 26 = 11 = L$

The plain text of the letter “X” = $(23 - 12) \bmod 26 = 11 = L$

The plain text of the letter “A” = $(0 - 12) \bmod 26 = 12 = O$

Hence the correct answer is HELLO.

2.4 SUBSTITUTION CIPHER

Definition: 2.4.1

In a substitution cipher, each numeric equivalent n of plaintext letter is a two digit numerical plaintext. The encryption is done according to the rule

$$E(n) = an + b \pmod{26}, 1 \leq a \leq 25, \gcd(a, 26) = 1, 0 \leq b \leq 25.$$

The pair (a, b) is called encryption key.

Example: 2.4.2

Suppose we have a literal plaintext message: 'I LOVE TO DO MATHEMATICS'. Taking $a = 3$, $b = 2$ as the encryption key, the coding is done as follows:

We first write the numerical equivalent of the message. This is

0811142104191403141200190704120019080218.

Next multiply all these numerics by 3 ($\text{mod } 26$). We have

2407161112051609161000052112100005240602.

Then we add 2 ($\text{mod } 26$) to each of the numerics. This gives

0009181314071811181202072314120207000804.

Once again we go to write literal equivalents. Thus, we have

AJSNOHSLSMCHXOMCHAIE

If we arranged the original message in blocks of 4, the encrypted message reads as

AJSN OHSL SMCH XOMC HAIE.

Example: 2.4.3

Suppose we have the encrypted message: VKYAQVAKEC, where encryption has been done with a linear cipher $E(n) = 17n + 10 \pmod{26}$.

Notice that $C(n) = 23n + 4 \pmod{26}$. For, the inverse of 17 modulo 26 is 23 and if $C(n) = cn + d \pmod{26}$, then $c = 23$ and $d = 4$ as the simple computation shows. To decrypt the message once again we, convert this message into its numerical equivalent which is

21102400162100100402

Next we multiply all these numerics by 23 (mod 26), we have

15220600041500221420

Then we add 4 (mod 26) to each of the resulting numerics, which give

19001004081904001824

Now convert this last set of numerics into literals again to obtain

TAKEITEASY.

Thus the decrypted message is: 'TAKE IT EASY'.

2.5 HILL CIPHER

Definition: 2.5.1

Hill ciphers are block codes, in which every n -letter block of literal plaintext is transformed into n -letter block of ciphertext for some $n \geq 2$. Working again with a 26-letter alphabet A-Z, let M be an invertible matrix over $\frac{\mathbb{Z}}{26\mathbb{Z}}$. Group the plaintext as column vectors C_i of length n . Then the encryption map E is given as

$$E(X) = MX \pmod{26},$$

Where $X = (m_1, m_2, \dots, m_n)^t$ is numeric equivalent of plaintext n -letter column vectors block and a_{ij} , $1 \leq i \leq n$, $1 \leq j \leq n$ are entries of the matrix M . The matrix M is the Encryption key.

Example: 2.5.2

Let us consider the plaintext message: 'HE WHO DARES WINS THE WAR'.

Let the matrix $M = \begin{pmatrix} 5 & 3 \\ 6 & 5 \end{pmatrix}$ be the encryption key.

Clearly, $|M| = 7$ and $\gcd(7, 26) = 1$. The coding rule with Hill cipher for the given encryption key is $E(n_1, n_2) = (5n_1 + 3n_2 \pmod{26}, 6n_1 + 5n_2 \pmod{26})$. The numeric equivalent of the plaintext in pairs is

07 04, 22 07, 14 03, 00 17, 04 18, 22 08, 13 18, 19 07, 04 22, 00 17

To encode, we first notice that there are 10 columns vectors. To find the ciphers, we first compute

$$\begin{aligned} C &= \begin{pmatrix} 5 & 3 \\ 6 & 5 \end{pmatrix} \begin{pmatrix} 07 & 22 & 14 & 00 & 01 & 22 & 13 & 19 & 04 & 00 \\ 04 & 07 & 03 & 17 & 18 & 08 & 18 & 07 & 22 & 17 \end{pmatrix} \\ &= \begin{pmatrix} 21 & 01 & 01 & 25 & 22 & 04 & 15 & 12 & 08 & 25 \\ 10 & 11 & 21 & 07 & 10 & 16 & 12 & 19 & 04 & 07 \end{pmatrix}. \end{aligned}$$

The numeric equivalent of required ciphertext is

21, 10, 01, 11, 01, 21, 25, 07, 22, 10, 04, 16, 15, 12, 12, 19, 08, 24, 25, 07

The literal codes in pairs are

VK, BL, BV, ZH, WK, EQ, PM, MT, IY, ZH

Thus the coded message is VKBLDNZHWKEQPMMTIYZH.

Example: 2.5.3

Let us decrypt the cipher: 'EQPM' where the encryption key is M^{-1} equal to M .

Notice that $M^{-1} = \begin{pmatrix} 23 & 7 \\ 14 & 23 \end{pmatrix}$. Numeric equivalent of 'EQPM' is 04161512.

Since the encryption is to be done in pairs. So, we find

$$P = \begin{pmatrix} 23 & 7 \\ 14 & 23 \end{pmatrix} \begin{pmatrix} 04 & 15 \\ 16 & 12 \end{pmatrix} = \begin{pmatrix} 22 & 13 \\ 08 & 18 \end{pmatrix}$$

Hence the numeric equivalent of the message sent is

22081318

and the literal message is: WINS.

2.6 VIGENERE CIPHER

Definition: 2.6.1

Let m be a positive integer. Define $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. For a key $K = (k_1, k_2, \dots, k_m)$, we define

$$e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$$

and

$$d_K(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m),$$

where all operations are performed in \mathbb{Z}_{26} .

Example: 2.6.2

Suppose $m = 6$ and the keyword is *CIPHER*. This corresponds to the numerical equivalent $K = (2, 8, 15, 7, 4, 17)$. Suppose the plaintext is the string

This cryptosystem is not secure.

We convert the plaintext elements to residues modulo 26, write them in groups of six, and then "add" the keyword modulo 26, as follows:

19 7 8 18 2 17 24 15 19 14 18 24

$$\begin{array}{cccccccccccc}
 20 & 1 & 19 & 19 & 12 & 9 & 15 & 22 & 8 & 25 & 8 & 19 \\
 2 & 8 & 15 & 7 & 4 & 17 & 2 & 8 & 15 & 7 & 4 & 17 \\
 \hline
 18 & 19 & 4 & 12 & 8 & 18 & 13 & 14 & 19 & 18 & 4 & 2 \\
 \\
 20 & 17 & 4 & & & & & & & & & \\
 2 & 8 & 15 & & & & & & & & & \\
 \hline
 22 & 25 & 19 & & & & & & & & &
 \end{array}$$

The alphabetic equivalent of the plaintext string would thus be:

thiscryptosystemisnotsecure.

2.7 PERMUTATION CIPHER

Definition: 2.7.1

Let m be a positive integer. Let $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ and let \mathcal{K} consist of all permutations of $\{1, \dots, m\}$. For a key (i.e., a permutation) π , we define

$$e_{\pi}(x_1, \dots, x_m) = (x_{\pi(1)}, \dots, x_{\pi(m)})$$

and

$$d_{\pi}(y_1, \dots, y_m) = (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(m)}),$$

when π^{-1} is the inverse permutation to π .

Example: 2.7.2

Suppose $m = 6$ and the key is the following permutation π :

X	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Note that the first row of the above diagram lists the values of x , $1 \leq x \leq 6$, and the second row lists the corresponding values of $\pi(x)$. Then the inverse permutation π^{-1} can be constructed by interchanging the two rows, and rearranging the columns so that the first row is in increasing order. Carrying out these operations, we see that the permutation π^{-1} is the following:

X	1	2	3	4	5	6
$\pi(x)$	3	6	1	5	2	4

Now, suppose we are given the plaintext

shesellsseahellsbytheseashore.

We first partition the plaintext into groups of six letters:

shesel | 1sseas | hellsb | ythese | ashore

Now each group of six letters is rearranged according to the permutation π , yielding the following:

EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS

So, the ciphertext is:

EESLSHSALSESLSHBLEHSYEETHRAEOS.

Example: 2.7.3

The ciphertext can be decrypted in a similar fashion, using the inverse permutation π^{-1} as follows:

Let us consider the above cipher text.

Now we partition the cipher text into groups of six letters

EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS

Now each group of six letters is rearranged according to the permutation π^{-1} , yielding the following:

SHESEL | LSSEAS | HELLSB | YTHESE | ASHORE

So, the plaintext is

shesellsseashellsbytheseashore.

Chapter 3

CHAPTER 3

DISCRETE LOGARITHMS & ELLIPTIC CURVE

DISCRETE LOGARITHM PROBLEM

3.1 THE DISCRETE LOGARITHM

The first published public key construction, due to Diffie and Hellman, is based on the discrete logarithm problem in a finite field \mathbf{F}_p , where \mathbf{F}_p is a field with a prime number of elements.

Definition: 3.1.1

Let g be a primitive root for \mathbf{F}_p and let h be a nonzero element of \mathbf{F}_p . The *Discrete Logarithm Problem* (DLP) is the problem of finding an exponent x such that

$$g^x \equiv h \pmod{p}.$$

The number x is called the *discrete logarithm* of h to the base g and is denoted by $\log_g(h)$.

In other words, let G be a group whose group law denoted by $*$. The *Discrete Logarithm Problem* for G is to determine, for any two given elements g and h in G , an integer x satisfying

$$\underbrace{g * g * g * \dots * g}_{x \text{ times}} \equiv h$$

x times

Example: 3.1.2

The number $p = 56509$ is prime, and one can check that $g = 2$ is a primitive root modulo p . How would we go about calculating the discrete logarithm of $h = 38679$? The only method that is immediately obvious is to compute

$$2^2, 2^3, 2^4, 2^5, 2^6, 2^7, \dots \pmod{56509}$$

Until we find some power that equals 38679. It would be difficult to do this by hand, but using a computer, we find that $\log_2(h) = 11235$. We can verify this by calculating $2^{11235} \pmod{56509}$ and checking that is equal to 38679.

3.2 DIFFIE – HELLMAN KEY EXCHANGE

Definition: 3.2.1

Let p be a prime number and g an integer. The *Diffe – Hellman Problem* (DHP) is the problem of computing the value of $g^{ab} \pmod{p}$ from the known values of $g^a \pmod{p}$ and $g^b \pmod{p}$.

The Diffe – Hellman key exchange algorithm is summarized below

Public parameter creation	
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in F_p^* .	

Private computations	
Alice	Bob
Choose a secret integer a .	Choose a secret integer b .

Compute $A \equiv g^a \pmod{p}$.	Compute $B \equiv g^b \pmod{p}$.
-----------------------------------	-----------------------------------

Public exchange of values
Alice sends A to Bob $\rightarrow A$
$B \rightarrow$ Bob sends B to Alice

Further private computations	
Alice	Bob
Compute the number $B^a \pmod{p}$.	Compute the number $A^b \pmod{p}$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$	

Table: 3.2.2 Diffie -Hellman key exchange

Example: 3.2.3

Alice and Bob agree to use the prime $p = 941$ and the primitive root $g = 627$. Alice chooses the secret key $a = 347$ and computes $A \equiv 390 \equiv 627^{347} \pmod{941}$. Similarly, Bob chooses the secret key $b = 781$ and computes $B = 691 \equiv 627^{781} \pmod{941}$. Alice sends Bob the number 390 and Bob sends Alice the number 691. Both of these transmissions are done over an insecure channel, so both $A = 390$ and $B = 691$ should be considered public knowledge. The numbers $a = 347$ and $b = 781$ are not transmitted and remain secret. Then Alice and Bob are both able to compute the number

$$470 \equiv 627^{347 \cdot 781} \equiv A^b \equiv B^a \pmod{941},$$

So 470 is their shared secret.

3.3 THE ELGAMAL PUBLIC KEY CRYPTOSYSTEM

The Elgamal public key encryption algorithm is based on the discrete log problem and is closely related to Diffie – Hellman key exchange. In this section we describe the version of the Elgamal PKC that is based on the discrete logarithm problem for \mathbf{F}_p^* , but the construction works quite generally using the DLP in any group.

Public parameter creation
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.

Alice	Bob
Key creation	
Choose private key $1 \leq a \leq p-1$.	
Compute $A = g^a \pmod{p}$.	
Publish the public key A .	
Encryption	
	Choose plaintext m .
	Choose random element k .
	Use Alice's public key A to compute
	$c_1 = g^k \pmod{p}$ and $c_2 = m A^k \pmod{p}$.
	Send ciphertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1/p)^{-1} \cdot c_2 \pmod{p}$.	

This quantity is equal to m .

Table: 3.3.1 Elgamal key creation, encryption and decryption.

Example: 3.3.2

Alice uses the prime $p = 467$ and the primitive root $g = 2$. She chooses $a = 153$ to be her private key and computes her public key

$$A \equiv g^a \equiv 2^{153} \equiv 224 \pmod{467}.$$

Bob decides to send Alice the message $m = 331$. He chooses a random element, say he chooses $k = 197$, and he computes the two quantities

$$c_1 \equiv 2^{197} \equiv 87 \pmod{467} \quad \text{and} \quad c_2 \equiv 331 \cdot 224^{197} \equiv 57 \pmod{467}$$

The pair $(c_1, c_2) = (87, 57)$ is the ciphertext that Bob sends to Alice.

Alice, knowing $a = 153$, first computes

$$x \equiv (c_1^a)^{-1} \equiv c_1^{p-1-a} \equiv 87^{313} \equiv 14 \pmod{467}.$$

Finally, she computes

$$c_2 x \equiv 57 \cdot 14 \equiv 331 \pmod{467}$$

and recovers the plaintext message m .

3.4 ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Definition: 3.4.1

Let E be an elliptic curve over the finite field \mathbf{F}_p and let P and Q be points in $E(\mathbf{F}_p)$. The *Elliptic Curve Discrete Logarithm Problem* (ECDLP) is the problem of finding an integer n such that $Q = nP$. By analogy with the discrete logarithm problem for \mathbf{F}_p^* , we denote this integer n by

$$n = \log_P(Q)$$

and we call n the *elliptic discrete logarithm* of Q with respect to P .

Example: 3.4.2

Consider the elliptic curve

$$E : Y^2 = X^3 + 8X + 7 \text{ over } \mathbf{F}_{73}.$$

The points $P = (32, 53)$ and $Q = (39, 17)$ are both in $E(\mathbf{F}_{73})$, and it is easy to verify (by computer) that

$$Q = 11P, \quad \text{so} \quad \log_P(Q) = 11.$$

Similarly, $R = (35, 47) \in E(\mathbf{F}_{73})$ and $S = (58, 4) \in E(\mathbf{F}_{73})$, and after some computation we find that they satisfy $R = 37P$ and $S = 28P$, so

$$\log_P(R) = 37 \quad \text{and} \quad \log_P(S) = 28.$$

Finally, we mention that $\# E(\mathbf{F}_{73}) = 82$, but P satisfies $41P = \mathcal{O}$. Thus P has order $41 = 82/2$, so only half of the points in $E(\mathbf{F}_{73})$ are multiples of P .

For example, $(20, 65)$ is in $E(\mathbf{F}_{73})$, but it does not equal a multiple of P .

3.4.3 The Double-and-Add Algorithm

It appears to be quite difficult to recover the value of n from the two points P and $Q = nP$ in $E(\mathbf{F}_p)$, that is difficult to solve the ECDLP. However, in order to use the function

$$\mathbf{Z} \rightarrow E(\mathbf{F}_p), \quad n \mapsto nP,$$

for cryptography, we need to efficiently compute nP from the known values n and P . If n is large, we certainly do not want to compute nP by computing $P, 2P, 3P, 4P, \dots$

However, since the operation on an elliptic curve is written as addition instead of multiplication, we call it "double-and-add".

We first write n binary form as

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + n_3 \cdot 8 + \dots + n_r \cdot 2^r \quad \text{with } n_0, n_1, \dots, n_r \in \{0, 1\}.$$

(We also assume that $n_r = 1$). Next we compute the following quantities:

$$Q_0 = P, \quad Q_1 = 2Q_0, \quad Q_2 = 2Q_1, \dots, Q_r = 2Q_{r-1}.$$

Notice that Q_i is simply twice the previous Q_{i-1} , so

$$Q_i = 2^i P.$$

These points are referred to as 2-power multiples of P , and computing them requires r doublings.

3.5 ELLIPTIC DIFFIE – HELLMAN KEY EXCHANGE

Definition: 3.5.1

Let $E(\mathbf{F}_p)$ be an elliptic curve over a finite field and let $P \in E(\mathbf{F}_p)$. The *Elliptic Curve Diffie – Hellman Problem* is the problem of computing the value of $n_1 n_2 P$ from the known values of $n_1 P$ and $n_2 P$.

Remark: 3.5.2

Elliptic Diffie – Hellman key exchange requires Alice and Bob to exchange points on an elliptic curve.

A point Q in $E(\mathbf{F}_p)$ consists of two coordinates $Q = (x_Q, y_Q)$, where x_Q and y_Q are elements of the finite field \mathbf{F}_p , so it appears that Alice must send Bob two numbers in \mathbf{F}_p . However, those two numbers modulo p do not contain as much information as two arbitrary numbers, since they are related by the formula

$$y_Q^2 = x_Q^3 + Ax_Q + B \quad \text{in } \mathbf{F}_p.$$

Note that Eve knows A and B , so if she can guess the correct value of x_Q , then there are only two possible values for y_Q , and in practice it is not too hard for her to actually compute the two values of y_Q .

There is thus little reason for Alice to send both coordinates of Q_A to Bob, since the y -coordinate contains so little additional information. Instead, she sends Bob only the x -coordinate of Q_A . Bob then computes and uses one of the two possible y -coordinates. If he happens to choose the “correct” y , then he is using Q_A , and if he chooses the “incorrect” y (which is the negative of the correct y), then he is using $-Q_A$. In any case, Bob ends up computing one of

$$\pm n_B Q_A = \pm (n_{AB}) P$$

Similarly, Alice ends up computing one of $\pm (n_{AB})P$. Then Alice and Bob use the x -coordinate as their shared secret value, since that x -coordinate is the same regardless of which y they use.

Public parameter creation
<p>A trusted party chooses and publishes a (large) prime p, an elliptic curve E over \mathbf{F}_p, and a point P in $E(\mathbf{F}_p)$.</p>

Private computations	
Alice	Bob
Chooses a secret integer n_A .	Chooses a secret integer n_B .
Computes the point $Q_A = n_AP$.	Computes the point $Q_B = n_BP$.

Public exchange of values	
Alice sends Q_A to Bob $\rightarrow Q_A$	
$Q_B \leftarrow$ Bob sends Q_B to Alice	

Further private computations	
Alice	Bob
Computes the point n_AQ_B .	Computes the point n_BQ_A .
The shared secret value is $n_AQ_B = n_A(n_BP) = n_B(n_AP) = n_BQ_A$.	

Table: 3.5.3 Diffie-Hellman key exchange using elliptic curves

Example: 3.5.4

Alice and Bob decide to use elliptic Diffie-Hellman with the following prime, curve, and point:

$$p = 3851, \quad E : Y^2 = X^3 + 324X + 1287, \quad P = (920, 303) \in E(\mathbf{F}_{3851}).$$

Alice and Bob choose respective secret values $n_A = 1194$ and $n_B = 1759$, and then

$$\text{Alice computes } Q_A = 1194P = (2067, 2178) \in E(\mathbf{F}_{3851}),$$

$$\text{Bob computes } Q_B = 1759P = (3684, 3125) \in E(\mathbf{F}_{3851}),$$

Alice sends Q_A to Bob and Bob sends Q_B to Alice. Finally,

Alice computes $n_A Q_B = 1194 (3684, 3125) = (3347, 1242) \in E(\mathbf{F}_{3851})$,

Bob computes $n_B Q_A = 1759 (2067, 2178) = (3347, 1242) \in E(\mathbf{F}_{3851})$,

Bob and Alice have exchanged the secret point $(3347, 1242)$. As explained in Remark 3.5.2, they should discard the y -coordinate and treat only the value $x = 3347$ as a secret shared value.

Example: 3.5.5

Alice and Bob decide to exchange another secret value using the same public parameters as in Example: 3.5.4

$$p = 3851, \quad E: Y^2 = X^3 + 324X + 1287, \quad P = (920, 303) \in E(\mathbf{F}_{3851}).$$

However this time they want to send fewer bits to one another. Alice and Bob respectively choose new secret values $n_A = 2489$ and $n_B = 2286$, and as before,

$$\text{Alice computes } Q_A = n_A P = 2489(920, 303) = (593, 719) \in E(\mathbf{F}_{3851}),$$

$$\text{Bob computes } Q_B = n_B P = 2286(920, 303) = (3681, 612) \in E(\mathbf{F}_{3851}).$$

However, rather than sending both coordinates, Alice sends only $x_A = 593$ to Bob and Bob sends only $x_B = 3681$ to Alice.

Alice substitutes $x_B = 3681$ into the equation for E and finds that

$$y_B^2 = x_B^3 + 324 x_B + 1287 = 3681^3 + 324 \cdot 3681 + 1287 = 997.$$

Alice needs to compute a square root of 997 modulo 3851.

Lema: 3.5.6

Let p be a prime satisfying $p \equiv 3 \pmod{4}$. Let a be an integer such that the congruence

$x^2 \equiv a \pmod{p}$ has a solution, that is such that a has a square root modulo p . Then

$$b \equiv a^{(p+1)/4} \pmod{p}$$

is a solution, that is, it satisfies $b^2 \equiv a \pmod{p}$.

Therefore $b^{(p+1)/4}$ is a square root of b modulo p . So Alice sets

$$y_B = 997^{(3851+1)/4} = 997^{963} \equiv 612 \pmod{3851}.$$

It happens that she gets the same point $Q_B = (x_B, y_B) = (3681, 612)$ that Bob used, and she computes $n_A Q_B = 2489(3681, 612) = (509, 1108)$.

Similarly Bob substitutes $x_A = 593$ into the equation for E and takes a square root,

$$y_A^2 = x_A^3 + 324 x_A + 1287 = 593^3 + 324 \cdot 593 + 1287 = 927,$$

$$y_A = 927^{(3851+1)/4} = 927^{963} \equiv 3132 \pmod{3851}.$$

Bob then uses the point $Q_A' = (593, 3132)$, which is not Alice's point Q_A , to compute $n_B Q_A' = 2286(593, 3132) = (509, 2743)$. Bob and Alice end up with points that are negatives of one another in $E(\mathbf{F}_p)$, but that is all right, since their shared secret value is the x -coordinate $x = 509$, which is the same for both points.

3.6 ELLIPTIC ELGAMAL PUBLIC KEY CRYPTOSYSTEM

Alice and Bob agree to use a particular prime p , elliptic curve E , and point $P \in E(\mathbf{F}_p)$. Alice chooses a secret multiplier n_A and publishes the point $Q_A = n_A P$ as her

public key. Bob's plaintext is a point $M \in E(\mathbf{F}_p)$. He chooses an integer k to be his random element and computes

$$C_1 = kP \quad \text{and} \quad C_2 = M + kQ_A.$$

He sends the two points (C_1, C_2) to Alice, who computes

$$C_2 - n_A C_1 = (M + kQ_A) - n_A(kP) = M + k(n_A P) - n_A(kP) = M$$

to recover the plaintext.

The elliptic Elgamal public key cryptosystem is summarized in Table 3.6.1

Public parameter creation

A trusted party chooses and publishes a (large) prime p ,
an elliptic curve E over \mathbf{F}_p , and a point P in $E(\mathbf{F}_p)$.

Alice

Bob

Key creation

Choose a private key n_A .

Compute $Q_A = n_A P$ in $E(\mathbf{F}_p)$.

Publish the public key Q_A .

Encryption

Choose plaintext $M \in E(\mathbf{F}_p)$.

Choose a random element k .

Use Alice's public key Q_A to compute

	$C_1 = kP \in E(\mathbf{F}_p) .$ and $C_2 = M + kQ_A \in E(\mathbf{F}_p) .$ Send ciphertext (C_1, C_2) to Alice.
Decryption	
Compute $C_2 - n_A C_1 \in E(\mathbf{F}_p) .$ This quantity is equal to M .	

Table: 3.6.1 Elliptic Elgamal key creation, encryption and decryption

Chapter 4

CHAPTER 4

INTEGER FACTORIZATION AND RSA

4.1 Fermat's Little Theorem, Euler's Theorem and Roots Module pd

Theorem: 4.1.1 (Fermat's Little Theorem).

It states that $a^p \equiv a \pmod{p}$ for every prime number p and every a .

Proof:

Let us assume that p is positive and not divisible by a . The idea is that if we write down the sequence of numbers

$$a, 2a, 3a, \dots, (p-1)a \quad \text{-----} (1)$$

and reduce each one modulo p , the resulting sequence turns out to be a rearrangement of

$$1, 2, 3, \dots, p-1. \quad \text{-----} (2)$$

Therefore, if we multiply together the numbers in each sequence, the results must be identical modulo p :

$$a \times 2a \times 3a \times \dots \times (p-1)a \equiv 1 \times 2 \times 3 \times \dots \times (p-1) \pmod{p}.$$

Collecting together the a terms yields

$$a^{p-1} (p-1)! \equiv (p-1)! \pmod{p}.$$

Finally, we may "cancel out" the numbers $1, 2, \dots, p-1$ from both sides of this equation,

Obtaining

$$a^{p-1} \equiv 1 \pmod{p}.$$

Theorem: 4.1.2 (Euler's Formula for pq).

Let p and q be distinct primes and let

$$g = \gcd(p-1, q-1).$$

Then

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq} \quad \text{for all } a \text{ satisfying } \gcd(a, pq) = 1.$$

In particular, if p and q are odd primes, then

$$a^{(p-1)(q-1)/2} \equiv 1 \pmod{pq} \quad \text{for all } a \text{ satisfying } \gcd(a, pq) = 1.$$

Proof:

By assumption we know that p does not divide a and that g divides $q-1$,

so we can compute

$$a^{(p-1)(q-1)/g} \equiv (a^{p-1})^{(q-1)/g} \quad \text{since } (q-1)/g \text{ is an integer,}$$

$$\equiv 1^{(q-1)/g} \pmod{p} \quad \text{since } a^{p-1} \equiv 1 \pmod{p}$$

from Fermat's Little theorem

$$\equiv 1 \pmod{p} \quad \text{since } 1 \text{ to any power is } 1!$$

The exact same computation, reversing the roles of p and q , shows that

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod{q}.$$

This proves that $a^{(p-1)(q-1)/g} - 1$ is divisible by both p and by q ; hence it is divisible by pq .

Proposition: 4.2.3

Let p be a prime and let $e \geq 1$ be an integer satisfying $\gcd(e, p-1) = 1$. Since e has an inverse modulo $p-1$, say

$$de \equiv 1 \pmod{p-1}.$$

Then the congruence

$$x^e \equiv c \pmod{p}$$

has the unique solution $x \equiv c^d \pmod{p}$.

Proof:

If $c \equiv 0 \pmod{p}$, then $x \equiv 0 \pmod{p}$ is the unique solution and we are done. So we assume that $c \not\equiv 0 \pmod{p}$. The proof is then an easy application of Fermat's little theorem (Theorem: 4.1.1). The congruence $de \equiv 1 \pmod{p-1}$ means that there is an integer k such that

$$de = 1 + k(p-1).$$

Now we check that c^d is a solution to $x^e \equiv c \pmod{p}$:

$(c^d)^e \equiv c^{de} \pmod{p}$	law of exponents,
$\equiv c^{1+k(p-1)} \pmod{p}$	since $de = 1 + k(p-1)$,
$\equiv c \cdot (c^{p-1})^k \pmod{p}$	law of exponents again,
$\equiv c \cdot 1^k \pmod{p}$	from Fermat's little theorem,
$\equiv c \pmod{p}.$	

This completes the proof that $x = c^d$ is a solution to $x^e \equiv c \pmod{p}$.

In order to see that the solution is unique, suppose that x_1 and x_2 are both solutions to the congruences. We've just proven that $z^{de} \equiv z \pmod{p}$ for any nonzero z , so we find that

$$x_1 \equiv x_1^{de} \equiv (x_1^e)^d \equiv c^d \equiv (x_2^e)^d \equiv x_2^{de} \equiv x_2 \pmod{p}.$$

Thus x_1 and x_2 are the same modulo p , so it has at most one solution.

Proposition: 4.1.4

Let p and q be distinct primes and let $e \geq 1$ satisfy

$$\gcd(e, (p-1)(q-1)) = 1.$$

Since e has an inverse modulo $(p-1)(q-1)$, say

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Then the congruence

$$x^e \equiv c \pmod{pq}$$

has the unique solution $x \equiv c^d \pmod{pq}$.

Proof:

We assume that $\gcd(c, pq) = 1$; Using Euler's Formula (Theorem: 4.1.2).

The congruence $de \equiv 1 \pmod{(p-1)(q-1)}$ means that there is an integer k such that

$$de \equiv 1 + k(p-1)(q-1).$$

Now we check that c^d is a solution to $x^e \equiv c \pmod{pq}$:

$$(c^d)^e \equiv c^{de} \pmod{pq}$$

law of exponents,

$$\equiv c^{1+k(p-1)(q-1)} \pmod{pq}$$

since $de = 1 + k(p-1)(q-1)$,

$$\equiv c \cdot (c^{(p-1)(q-1)})^k \pmod{pq} \quad \text{law of exponents again,}$$

$$\equiv c \cdot 1^k \pmod{pq} \quad \text{from Euler's formula (Theorem 4.1.2),}$$

$$\equiv c \pmod{pq}.$$

This completes the proof that $x = c^d$ is a solution to the congruence. It remains to show that the solution is unique. Suppose that $x = u$ is a solution. Then

$$u \equiv u^{de-k(p-1)(q-1)} \pmod{pq} \quad \text{since } de = 1 + k(p-1)(q-1),$$

$$\equiv (u^e)^d \cdot (u^{(p-1)(q-1)})^{-k} \pmod{pq}$$

$$\equiv (u^e)^d \cdot 1^{-k} \pmod{pq} \quad \text{using Euler's formula (Theorem: 4.1.2),}$$

$$\equiv c^d \pmod{pq} \quad \text{since } u \text{ is a solution}$$

Thus every solution is equal to $c^d \pmod{pq}$, so this is the unique solution.

Remark: 4.1.5

Proposition: 4.1.4 gives an algorithm for solving $x^e \equiv c \pmod{pq}$ that involves first solving $de \equiv 1 \pmod{(p-1)(q-1)}$ and then computing $c^d \pmod{pq}$. We can often make the computation faster by using a smaller value of d . Let $g = \gcd(p-1, q-1)$ and suppose that we solve the following congruence for d :

$$de \equiv 1 \pmod{\frac{(p-1)(q-1)}{g}}$$

Euler's formula (Theorem: 4.1.2) says that $a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq}$. Hence just as in the proof of proposition: 4.1.4. if we write $de = 1 + k(p-1)(q-1)/g$, then

$$(c^d)^e = c^{de} = c^{1 + k(p-1)(q-1)/g} = c \cdot (c^{(p-1)(q-1)/g})^k \equiv c \pmod{pq}.$$

Thus using this smaller value of d , we still find that $c^d \pmod{pq}$ is a solution to

$$x^e \equiv c \pmod{pq}.$$

4.2 The RSA Public Key Cryptosystem

In this section we describe the RSA public key cryptosystem, the first invented and certainly best known such system. RSA is named after its (public) inventors, Ron Rivest, Adi Shamir, and Leonard Adleman.

The security of RSA depends on the following dichotomy:

- **Set up.** Let p and q be large primes, let $N = pq$, and let e and c be integers.
- **Problem.** Solve the congruence $x^e \equiv c \pmod{N}$ for the variable x .
- **Easy.** Bob, who knows the values of p and q , can easily solve for x as described in Proposition 4.1.4.
- **Hard.** Eve, who does not know the values of p and q , cannot easily find x .
- **Dichotomy.** Solving $x^e \equiv c \pmod{N}$ is easy for a person who possesses certain extra information, but it is apparently hard for all other people.

The RSA public key cryptosystem is summarized in Table 4.2.1

Bob	Alice
Key Creation	
Choose secret primes p and q .	
Choose encryption exponent e	
with $\gcd(e, (p-1)(q-1)) = 1$.	
Publish $N = pq$ and e .	
Encryption	
	Choose plaintext m .

	Use Bob's public key (N, e) to compute $c \equiv m^e \pmod{N}$. Send ciphertext c to Bob.
Decryption	
Compute d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. Compute $m' \equiv c^d \pmod{N}$. Then m' equals the plaintext m .	

Table: 4.2.1 RSA key creation, encryption, and decryption

Example: 4.2.2

We illustrate the RSA public key cryptosystem with a small numerical example. Of course, this example is not secure, since the numbers are so small that it would be easy for Eve to factor the modulus N . Secure implementations of RSA use moduli N with hundreds of digits.

RSA Key Creation

- Bob chooses two secret primes $p = 1223$ and $q = 1987$. Bob computes his public modulus

$$N = p \cdot q = 1223 \cdot 1987 = 2430101$$

- Bob chooses a public encryption exponent $e = 948047$ with the property that

$$\gcd(e, (p-1)(q-1)) = \gcd(948047, 948047) = 1.$$

RSA Encryption

- Alice converts her plaintext into an integer

$$m = 1070777$$

satisfying $1 \leq m < N$.

- Alice uses Bob's public key $(N, e) = (2430101, 948047)$ to compute $c \equiv m^e \pmod{N}$, $c \equiv 1070777^{948047} \equiv 14730101 \pmod{2430101}$.
- Alice sends the ciphertext $c = 1473513$ to Bob.

RSA Decryption

- Bob knows $(p-1)(q-1) = 1222 \cdot 1986 = 2426892$, so he can solve $ed \equiv 1 \pmod{(p-1)(q-1)}$, $948047 \cdot d \equiv 1 \pmod{2426892}$, for d and find that $d = 1051235$.

- Bob takes the ciphertext $c = 1473513$ and computes

$$c^d \pmod{N}, \quad 1473513^{1051235} \equiv 1070777 \pmod{2430101}.$$

The value that he computes is Alice's message $m = 1070777$.

4.3 Probabilistic Encryption and the Goldwasser-Micali Cryptosystem.

The Goldwasser-Micali (GM) cryptosystem is an asymmetric key encryption algorithm developed by Shafi Goldwasser and Silvio in 1982. GM has the distinction of being the first probabilistic public-key encryption scheme which is provably secure under standard cryptographic assumptions.

Suppose that Alice wants to use public key cryptosystem to encrypt and send Bob 1 bit, i.e., Alice wants to send Bob one of the values 0 and 1. At first glance such an arrangement seems inherently insecure. All that Eve has to do is to encrypt the two possible plaintext $m = 0$ and $m = 1$, and then she compares the encryptions with Alice's ciphertext. More generally, in any cryptosystem for which the set of possible plaintexts is small. Eve can encrypt every plaintext using Bob's public key until she finds the one that is Alice's.

The idea is that Alice chooses both a plaintext m and a random string of data r , and then she uses Bob's public key to encrypt the pair (m, r) . If the value is random, then Eve will not be able to range of messages and random value used.

Let p and q be (secret) prime numbers and let $N = pq$ be given.

For a given integer a , determine whether a is a square modulo N , i.e., determine whether there exists an integer u satisfying

$$u^2 \equiv a \pmod{N}.$$

Note that Bob, who knows how to factor $N = pq$, is able to solve this problem easily, since

$$a \text{ is a square modulo } pq \quad \text{if and only if} \quad \left(\frac{a}{p}\right) = 1 \text{ and } \left(\frac{a}{q}\right) = 1.$$

Eve, on the other hand, has a harder time, since she knows only the value of N . Eve can compute $\left(\frac{a}{N}\right)$, but suppose that $N = pq$ is a product of two primes.

Then,

$$\left(\frac{a}{N}\right) = \left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right).$$

We see that there are two ways in which $\left(\frac{a}{N}\right)$ can be equal to 1, namely $1 = 1 \cdot 1$ and

$$1 = (-1) \cdot (-1).$$

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1, \quad \text{so } a \text{ is a square modulo } pq.$$

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1, \quad \text{so } a \text{ is not a square modulo } pq.$$

This does not tell her whether a is a square modulo N .

Goldwasser and Micali describe Probabilistic Encryption in Table: 4.3.1

Bob	Alice
Key creation	
Choose secret primes p and q .	.
Choose a with $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$.	
Publish $N = pq$ and a .	
Encryption	
	<p>Choose plaintext $m \in \{0, 1\}$.</p> <p>Choose random value r with $1 < r < N$.</p> <p>Use Bob's public key (N, a) to compute</p> $c = \begin{cases} r^2 \bmod N & \text{if } m = 0, \\ ar^2 \bmod N & \text{if } m = 1. \end{cases}$ <p>Send ciphertext c to Bob</p>
Decryption	
<p>Compute $\left(\frac{c}{p}\right)$. Decrypt to</p> $m = \begin{cases} 0 & \text{if } \left(\frac{c}{p}\right) = 1, \\ 1 & \text{if } \left(\frac{c}{p}\right) = -1. \end{cases}$	

Table: 4.3.1 Goldwasser-Micali probabilistic public key cryptosystem

It is easy to check that the Goldwasser-Micali cryptosystem works as advertised, since

$$\left(\frac{c}{p}\right) = \begin{cases} \left(\frac{r^2}{p}\right) = \left(\frac{r}{p}\right)^2 = 1 & \text{if } m = 0, \\ \left(\frac{ar^2}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{r}{p}\right)^2 = \left(\frac{a}{p}\right) = -1 & \text{if } m = 1. \end{cases}$$

since Alice chooses r randomly, the set of values that Eve sees when Alice encrypts $m = 0$ consists of all possible squares modulo N , and the set of values that Eve sees when Alice encrypts $m = 1$ consists of all possible numbers c satisfying $\left(\frac{c}{N}\right) = 1$ and c is not a square modulo N .

What information does Eve obtain if she computes the Jacobi symbol $\left(\frac{c}{N}\right)$, which she can do since N is a public quantity? If $m = 0$, then $c \equiv r^2 \pmod{N}$, so

$$\left(\frac{c}{N}\right) = \left(\frac{ar^2}{N}\right) = \left(\frac{a}{N}\right) = \left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = (-1) \cdot (-1) = 1$$

is also equal to 1.

(Note that Bob chose a to satisfy $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$.)

Thus $\left(\frac{c}{N}\right)$ is equal to 1, regardless of the value of N , so the Jacobi symbol gives Eve no useful information.

Example: 4.3.2

Bob creates a Goldwasser-Micali public key by choosing

$$p = 2309, \quad q = 5651, \quad N = pq = 13048159, \quad a = 6283665.$$

Note that a has the property that $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$. He publishes the pair (N, a) and keeps the values of the primes p and q secret.

Alice begins by sending Bob the plaintext bit $m = 0$. To do this, she chooses $r = 1642087$ at random from the interval 1 to 13048158. She then computes

$$c \equiv r^2 \equiv 1642087^2 \equiv 8513742 \pmod{13048159},$$

and sends the ciphertext $c = 8513742$ to Bob. Bob decrypts the ciphertext $c = 8513742$ by computing $\left(\frac{8513742}{2309}\right) = 1$, which gives the plaintext bit $m = 0$.

Next Alice decides to send Bob the plaintext bit $m = 1$. She chooses a random value $r = 11200984$ and computes

$$c \equiv ar^2 \equiv 6283665 \cdot 11200984^2 \equiv 2401627 \pmod{13048159}.$$

Bob decrypts $c = 2401627$ by computing $\left(\frac{2401627}{2309}\right) = -1$, which tells him that the plaintext bit $m = 1$.

Finally, Alice wants to send Bob another plaintext bit $m = 1$. She chooses the random value $r = 11442423$ and computes

$$c \equiv ar^2 \equiv 6283665 \cdot 11442423^2 \equiv 4099266 \pmod{13048159}.$$

Notice that the ciphertext for this encryption of $m = 1$ is completely unrelated to the previous encryption of $m = 1$.

Bob decrypts $c = 4099266$ by computing $\left(\frac{4099266}{2309}\right) = -1$ to conclude that the plaintext bit is $m = 1$.

Chapter 5

CHAPTER 5

APPLICATIONS

5.1 SOME IMPORTANT APPLICATIONS OF CRYPTOGRAPHY

5.1.1 Time stamping

Time stamping is a technique that can certify that a certain electronic document or communication existed or was delivered at a certain time. Time stamping uses an encryption model called a blind signature scheme. Blind signature schemes allow the sender to get a message receipted by another party without revealing any information about the message to the other party.

Time stamping is very similar to sending a registered letter through the U.S. mail, but provides an additional level of proof. It can prove that a recipient received a specific document. Possible applications include Patent applications, copyright archives, and contracts. Time stamping is a critical application that will help make the transition to electronic legal documents possible.

5.1.2 Electronic money

The definition of electronic money (also called electronic cash or digital cash) is a term that is still evolving. It includes transactions carried out electronically with a net transfer of funds from one party to another, which may be either debit or credit and can be either anonymous or identified. There are both hardware and software implementations.

Anonymous applications do not reveal the identity of the customer and are based on blind signature schemes. Identified spending schemes reveal the identity of the customer and are based on more general forms of signature schemes. Anonymous

schemes are the electronic analog of cash, while identified schemes are the electronic analog of a debit or credit card. There are also some hybrid approaches where payments can be anonymous with respect to the merchant but not the bank or anonymous to everyone, but traceable (a sequence of purchases can be related, but not linked directly to the spender's identity).

Encryption is used in electronic money schemes to protect conventional transaction data like account numbers and transaction amounts, digital signatures can replace handwritten signatures or a credit-card authorization, and public-key encryption can provide confidentiality. There are several systems that cover this range of applications, from transactions mimicking conventional paper transactions with values of several dollars and up, to various micropayment schemes that batch extremely low cost transactions into amounts that will bear the overhead of encryption and clearing the bank.

5.1.3 Kerberos

Kerberos is an authentication service developed by MIT which uses secret-key ciphers for encryption and authentication. Kerberos was designed to authenticate requests for network resources and does not authenticate authorship of documents.

In a Kerberos system, there is a site on the network, called the Kerberos server, to perform centralized key management and administrative functions. The server maintains a key database with the secret keys of all users, authenticates the identities of users, and distributes session keys to users and servers who need to authenticate one another. Kerberos depends on a trusted third party, the Kerberos server, and if the server were compromised, the integrity of the whole system would be lost. Kerberos is

generally used within an administrative domain across domains the more robust functions and properties of public-key systems are often preferred.

5.1.4 Anonymous remailers

A remailer is a free service that strips off the header information from an electronic message and passes along only the content. It's important to note that the remailer may retain your identity, and rather than trusting the operator, many users may relay their message through several anonymous remailers before sending it to its intended recipient. That way only the first remailer has your identity, and from the end point, it's nearly impossible to retrace.

Here's a typical scenario-the sender intends to post a message to a news group via three remailers. He encrypts the message with the last remailer's public key. He sends the encrypted message to remailer.

1. Which strips away his identity, then forwards it to remailer.
2. Which forwards it to remailer.
3. Remailer 3 decrypts the message and then posts intended newsgroup

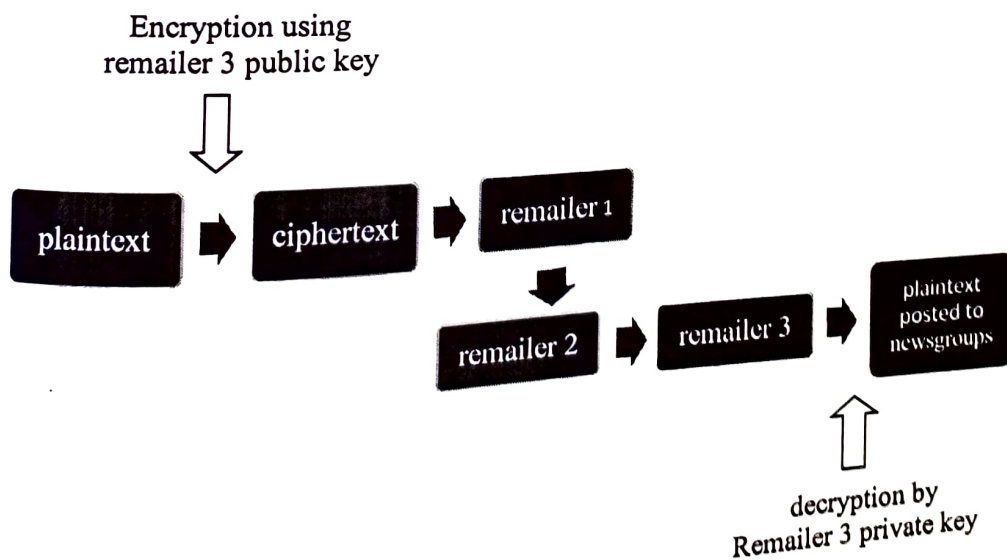


Figure: 5.1.5

5.1.6 Disk encryption

Disk encryption programs encrypt your entire hard disc so that you don't have to worry about leaving any traces of the unencrypted data on your disk.

PGP can also be used to encrypt files. In this case, PGP uses the user's private key along with a user-supplied password to encrypt the file using IDEA. The same password and key are used to unlock the file.

5.2 APPLICATION OF DIFFIE – HELLMAN KEY EXCHANGE

Now, we are going to learn some applications of Diffie Hellman Key Exchange.

5.2.1 Secure socket layer (SSL)

Netscape has developed a public-key protocol called Secure Socket Layer (SSL) for providing data security layered on between TCP/IP and application protocols. SSL supports data encryption, server authentication, message integrity, and client authentication for TCP/IP connection.

The SSL Handshake protocol authenticates each end of the connection with the second of client authentication being optional. In phase 1, the client requests the server's certificate and its cipher preferences. When the client receives this information, it generates a master key and encrypts it with the server's public key, then sends the encrypted master key to the server. The server decrypts the master key with its private key, then authenticates itself to the client by returning a message encrypted with the master key. Following data is encrypted with keys derived from the master key. Phase 2, client authentication, is optional. The server challenges the

client, and the client responds by returning the client's signature on the challenge with its public-key certificate.

SSL uses the RSP public-key cryptosystem for the authentication steps. After the exchange of keys, a number of different cryptosystems are used, including RC2, RC4, IDEA, DES and triple-DES.

5.2.2 Secure shell

SSH is a network security protocol very common for secure remote login on the Internet. The secure shell has come to replace the unsecured Telnet on the network and FTP on the system, mostly because both Telnet and FTP do not encrypt data, and instead send them in plaintext. SSH, on the other hand, can automatically encrypt, authenticate and compress transmitted data.

The key exchange protocol itself is a component of the SSH, as a whole, particularly responsible for parties agreeing upon the keys used by the various primitives later in the SSH protocol. This is the first stage of the SSH algorithm, and it happens before the establishment of session keys.

The protocol proceeds in three stages. The first of these is the "Hello" phase, where the first identification is done. A list of supported algorithms is involved here after the first "Hi" message, and this list details the supported Diffie-Hellman key groups, among other things. The second stage sees the two parties agree upon a shared secret key, session identifier and digest are used to generate the application keys.

Currently, the "diffie-hellman-group1-sha1" method is practiced in the key exchange, prescribing a fixed group on which all operations are performed. The key exchange is then signed with the host key to provide host authentication.

5.2.3 IP Security

IP security is an extension of the Internet Protocol it is a suite of protocols introduced by the Internet Engineering Task Force to aid in configuring a communications channel between multiple machines. Operation at the IP layer of the seven-layer model, it does its job by authenticating and encrypting IP packets.

Like the previous protocol, IPsec uses D.H and asymmetric cryptography to establish identities, preferred algorithms, and a shared secret. Before IPsec can begin encrypting the data stream, some preliminary information exchange is necessary. This is accomplished with the Internet Key Exchange protocol. IKE uses DH to produce a shared secret via the usual mechanisms, and then authenticate each other; after that, the secret key is used for encryption purposes. This shared secret key is ever exchanged over the insecure channel.

5.3 APPLICATION OF ELGAMAL PUBLIC KEY CRYPTOSYSTEM



Source Port		Destination Port	
Sequence		Number	
Acknowledgement		Number	
Data Offset	Reserved	Flags	Window (sliding window)
Checksum			Urgent Pointer
Options			Padding
Data			

The TCP communication portal is the most widely used transport layer protocol for the vast majority of application, with few exceptions. Within figure 1, shown above, the TCP packet structure is displayed with its internal fields labeled. The application that will be discussed exists as an optional feature within the TCP protocol. Besides existing as an option within the protocol, the use of this option will add an additional check some each packet, located at the beginning of the payload section, which will provide additional error – detection capabilities.

During 3-Way Handshake

During the initial 3-way handshake of the TCP protocol, each end of the TCP channel will indicate in the 'options' portion of their handshake packet that it want to use encrypted [Ine]. If you both user's indicate that they want to use encrypted data transport the each user's packed payload which is placed into the 'data' portion of the packet will from this point be encrypted using the public – key received from the other user.

After initialization

The TCP protocol, at this point will begin computing additional checksum after sending each packet, by encrypting the whole data portion of the packet and multiplying each portion of the ciphertext by each other and using that as the checksum (leaving the original checksum portion of the packet, as only a checksum over the non-payload data, allowing the recipient to distinguish between errors in the packet overload and the packet payload). Thus multiplicative checksum will be placed at the front of the 'data' portion of the packet. The homomorphic property comes in handy at this point as it allows for the checksum to be calculated by original senders and intermediate carries directly on the encrypted data, making it simpler to be

handled in embedded hardware settings and allowing the network to find checksum errors in packets as they are traveling to their destination and preemptively dropping them before they waste further bandwidth.

5.4 APPLICATION OF RSA CRYPTOSYSTEM

In this section, we are discussing about a particular RSA Cryptosystem application that is RSA Digital Signatures.

RSA Digital Signature

The original RSA paper described both the RSA encryption scheme and an RSA digital signature scheme. The idea is very simple. The setup is the same as for RSA encryption, Samantha chooses two large secret primes p and q and she publishes their product $N=pq$ and a public verification exponent. Samantha uses her knowledge of the factorization of N to solve the congruence

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

Note that if Samantha were doing RSA encryption, then e would be her encryption exponent and d would be her decryption exponent. However, in the present setup d is her signing exponent and e is her verification exponent.

In order to sign a digital document D , which we assume to be an integer in the range

$1 < D < N$, Samantha computes

$$S = D^d \pmod{N}.$$

Samantha	Victor
Key Creation	

Choose secret primes p and q .	
Choose verification exponent e with $\text{God}(e, (p-1)(q-1)) = 1$.	
Publish $N = pq$ and e .	
Signing	
Compute d satisfying	
$de \equiv 1 \pmod{(p-1)(q-1)}$.	
Sign document D by computing	
$S \equiv D^d \pmod{N}$.	
Verification	
	Compute $S^e \pmod{N}$ and verify that it is equal to D .

Table: 5.4.1

Victor verifies the validity of the signature S on D by computing

$$S^e \pmod{N}$$

And checking that is equal to D . This process works because Euler' formula

$$S^e \equiv D^{de} \equiv D \pmod{N}$$

The RSA digital signature scheme is summarized in the above table

If we can factor N , then she can solve for Samantha's secret signing key d .

However, just as with RSA encryption, the hard problem of factorization. In order to forge a signature on a document D Eve needs to find a eth root of D modulo N . This is

identical to the hard problem underlying RSA decryption, in which the plaintext is the e th root of the ciphertext.

As illustrate the RSA encryption, one can gain a bit of efficiency by choosing d and e to satisfy

$$de \equiv 1 \pmod{\frac{(p-1)(q-1)}{\gcd(p-1, q-1)}}$$

RSA signature key creation

Samantha choose two secret primes $p = 1223$ and $q = 1987$ and computes her public modulus

$$N = p \cdot q = 1223 \cdot 1987$$

Samantha choose a public verification exponent $e = 948047$ with the property that

$$\gcd(e, (p-1)(q-1)) = \gcd(948047, 2426892) = 1$$

RSA signing

Samantha computes her private signing key d using the secret values of p and q to compute $(p-1)(q-1) = 1222 \cdot 1986 = 2426892$ and then solving the congruence

$$ed \equiv 1 \pmod{(p-1)(q-1)}, \quad 948047 \cdot d \equiv 1 \pmod{2426892}.$$

She finds that $d = 1051235$.

Samantha selects a digital document to sign,

$$D = 1070777 \quad \text{with} \quad 1 \leq D < N.$$

She computes the digital signature

$$S \equiv D^d \pmod{N}, \quad S \equiv 1070777^{1051235} \equiv 153337 \pmod{2430101}.$$

Samantha publishes the digital signature

$$D = 1070777 \quad \text{and} \quad S = 153337$$

RSA verification

Verification uses Samantha's public modulus N and verification exponent e to compute

$$S^e \bmod N, \quad 1070777^{948047} \equiv 1070777 \pmod{2430101}.$$

He verifies that the value of S^e modulo N is the same as the value of the digital document $D = 1070777$.

CONCLUSION

In this project we have learned about cryptography. We have proved many theorems and introduced an idea about Diffie Hellman Key Exchange, Elgamal cryptography and RSA Cryptography. And also we have established a deep knowledge and understanding on encryption and decryption. Thus we come to know how our messages are securitized while communicating and mathematics behind its working. Cryptography has more applications in Securing Sensitive Emails, Protecting Confidential Files, Encrypting Database Records, etc.

REFERENCES

- [1] Saroj B. Malik, A Beginner's Course In Number Theory.
- [2] Douglas R. Stinson & Maura B. Paterson, Cryptography Theory And Practice, Fourth Edition.
- [3] Jeffrey Hoffstein , Jill Pipher, Joseph H. Silverman, An Introduction To Mathematical Cryptography, Second Edition.
- [4] Kenneth H. Rosen, Elementary Number Theory and Its Applications

A STUDY ON FIBONACCI AND LUCAS NUMBERS

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

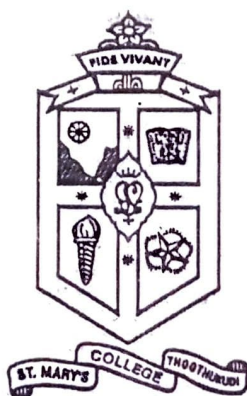
BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NO
B. AMUTHAVALLI	19SUMT02
S. ARTHI	19SUMT06
I. JENIFER SOWMIYA	19SUMT13
A. PRINCY	19SUMT30
S. REETHA SHIVANI	19SUMT34

Under the guidance of

Ms. H. SUJITHA M.Sc., M.Phil.,



DEPARTMENT OF MATHEMATICS

St. Mary's College (Autonomous), Thoothukudi

May-2022

A STUDY ON FIBONACCI AND LUCAS NUMBERS

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NO
B. AMUTHAVALLI	19SUMT02
S. ARTHI	19SUMT06
I. JENIFER SOWMIYA	19SUMT13
A. PRINCY	19SUMT30
S. REETHA SHIVANI	19SUMT34

Under the guidance of

Ms. H. SUJITHA M.Sc., M.Phil.,



DEPARTMENT OF MATHEMATICS


St. Mary's College (Autonomous), Thoothukudi

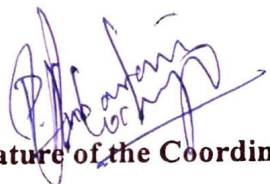
May-2022

CERTIFICATE

This is to certify that this project work entitled "A STUDY ON FIBONACCI AND LUCAS NUMBERS" is submitted to St. Mary's College (Autonomous), Thoothukudi affiliated to Manonmaniam Sundaranar University, Tirunelveli in partial fulfilment for the award of the degree of Bachelor of Science in Mathematics and is the work done during the year 2021-2022 by the following students.

NAME	REGISTER NO
B. AMUTHAVALLI	19SUMT02
S. ARTHI	19SUMT06
I. JENIFER SOWMIYA	19SUMT13
A. PRINCY	19SUMT30
S. REETHA SHIVANI	19SUMT34


Signature of the Guide


Signature of the Coordinator


Signature of the Director
Director
Self Supporting Courses
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Principal
Principal
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Examiner

DECLARATION

We hereby declare that the project entitled “A STUDY ON FIBONACCI AND LUCAS NUMBERS” submitted for the degree of Bachelor of Science is our work carried out under the guidance of Ms. H. SUJITHA M.Sc., M.Phil., Assistant Professor, Department of Mathematics (SSC), St. Mary's College (AUTONOMOUS), Thoothukudi.

B. Amuthavalli
(B. AMUTHAVALLI)

S. Arthi
(S. ARTHI)

I. Jenifer Sowmiya
(I. JENIFER SOWMIYA)

A. Princy
(A. PRINCY)

S. Reetha Shivani
(S. REETHA SHIVANI)

ACKNOWLEDGEMENT

First of all, we thank the Almighty for showering his blessings to undergo this project.

We express our sincere gratitude and heartfelt thanks to our Principal **Rev. Dr. Sr. A. S. J. Lucia Rose M.Sc., PGDCA., M.Phil., Ph.D.**, and to our Director **Rev. Sr. Josephine Jeyarani M.Sc., B.Ed.**, for kindly permitting us to do this project.

We express our gratitude to **Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D.**, Coordinator, Department of Mathematics (SSC) for her inspirational ideas and encouragement.

We are very thankful to our guide **Ms. H. Sujitha M.Sc., M.Phil.**, Assistant Professor, Department of Mathematics (SSC) for her efficient and effective guidance. She played a key role in the preparation of this project.

We also thank our staff members for their encouragement in all our efforts. Finally, we thank all those who extended their help regarding this project.

Place: Thoothukudi

Date: 17.05.2022

CONTENT

CHAPTER	TOPIC	PAGE NO.
	Introduction	1
1	Preliminaries	3
2	Properties of Fibonacci and Lucas Numbers	7
3	Pascal's Triangle	17
4	Fibonacci Matrices	26
5	Applications of Fibonacci and Lucas Numbers	40
	Conclusion	
	Reference	

INTRODUCTION

The concept of Fibonacci numbers was first discovered by Leonardo de Fibonacci depisa. The Fibonacci series was derived from the solution to a problem about rabbits. The problem is: Suppose there are two new born rabbits, one male and the other female. Find the number of rabbits produced in a year if

- 1) Each pair takes one month to become mature
- 2) Each pair produces a mixed pair every month, from the second month
- 3) All rabbits are immortal.

Suppose, that the original pair of rabbits was born on January 1. They take a month to become mature, so there is still only one pair on February 1. On March 1, they are two months old and produce a new mixed pair, so total is two pair. By continuing like this, there will be 3 pairs in April, 5 pairs in May and so on. The numbers 1,1,2,3,5,8,... are Fibonacci numbers. They have fascinating property: Any Fibonacci number, except the first two, is the sum of the two immediately preceding Fibonacci numbers. (At the given rate, there will be 144 pairs rabbit on December 1).

This yields the following recursive definition of the n th Fibonacci number F_n

$$F_1 = 1$$

$$F_2 = 1$$

$$\vdots$$

$$F_n = F_{n-1} + F_{n-2}, n \geq 3$$

Closely related to Fibonacci numbers are the Lucas numbers 1,3,4,7,11,... named after Lucas. Lucas number L_n are defined recursively as follows

$$L_1 = 1$$

$$L_2 = 3$$

$$\vdots$$

$$L_n = L_{n-1} + L_{n-2}, n \geq 3$$

There is a huge interest of modern science in the application of the Golden Section and Fibonacci numbers. The Fibonacci numbers F_n and the term of the sequence 0,1,2,3,5..... Where in each term is the sum of the two previous terms, beginning with the values $F_0 = 0$, and $F_1 = 1$. On the other-hand the ratio of two consecutive Fibonacci numbers converges to Golden mean or Golden section,

$$\varphi = \frac{1+\sqrt{5}}{2}$$

Chapter 1

CHAPTER -1

Preliminaries

1.1 Division Algorithm

Let a and b be two integers, where $b > 0$. Then there exist unique integers q and r such that $a = bq + r, 0 \leq r < b$

Definition: 1.2

An integer a is said to be **divisible** by an integer $d \neq 0$ if there exists some integer c such that $a = dc$

Definition: 1.3

If a and b are integers, not both zero, then the greatest common divisor of a and b , denoted by $\gcd(a, b)$ is the positive integer d satisfying

1. $d|a$ and $d|b$
2. If $c|a$ and $c|b$ then $c|d$

Theorem:1.4 (Divisibility)

For any integers a, b, c

1. If $a|b$ and $c|d$, then $ac|bd$
2. If $a|b$ and $b|c$, then $a|c$
3. If $a|b$ and $a|c$, then $a|(bx + cy)$ for arbitrary integers x and y

Definition: 1.5

Two integers a and b , not both of which are zero, are said to be **relatively prime** whenever $\gcd(a, b) = 1$

1.6 Euclidean Algorithm

Euclidean algorithm is a method of finding the greatest common divisor of two given integers. This is a repeated application of division algorithm.

Let a and b two integers whose greatest common divisor is required.

Since $\gcd(a, b) = \gcd(|a|, |b|)$, it is enough to assume that a and b are positive integers. Without loss of generality, we assume $a > b > 0$. Now by division algorithm, $a = bq_1 + r_1$, where $0 \leq r_1 < b$. If it happens that $r_1 = 0$, then $b|a$ and $\gcd(a, b) = b$. If $r_1 \neq 0$, by division algorithm $b = r_1q_2 + r_2$, where $0 \leq r_2 < r_1$. If $r_2 = 0$, then process stops. If $r_2 \neq 0$ by division algorithm $r_1 = r_2q_3 + r_3$, where $0 \leq r_3 < r_2$. The process continues until some zero remainder appears. This must happen because the reminders r_1, r_2, r_3, \dots forms a decreasing sequence of integers and since $r - 1 < b$, the sequence contains at most b non-negative integers. Let us assume that $r_{n+1} = 0$ and r_n is the last non-zero remainder. We have the following relation: .

$$a = bq_1 + r_1, 0 < r_1 < b$$

$$b = r_1q_2 + r_2, 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1} + 0$$

Then, $\gcd(a, b) = r_n$

Theorem: 1.7 (Fundamental Theorem of Arithmetic)

Any positive integer is either 1 or prime, or it can be expressed as a product of primes, the representation being unique except for the order of the prime factors.

Definition: 1.8

Let m be fixed positive integer. Two integers a and b are said to be **congruent modulo m** if $a - b$ is divisible by m and symbolically this is denoted by $a \equiv b \pmod{m}$. We also used to say a is congruent to b modulo m

Theorem: 1.9

1. $a \equiv a \pmod{m}$
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$
3. If $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$
4. If $a \equiv b \pmod{m}$, then for any integer c ,
 $(a + c) \equiv (b + c) \pmod{m}$; $ac \equiv bc \pmod{m}$

Definition: 1.10

Fibonacci Numbers are the numbers in the integer sequence defined by the recurrence relation $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$ with $F_0 = 0$ and $F_1 = 1$

Definition: 1.11

Lucas Numbers are the numbers in the integer sequence defined by the recurrence relation $L_n = L_{n-1} + L_{n-2}$ for all $n > 1$ and $L_0 = 2$ and $L_1 = 1$

1.12 Golden Ratio

The Golden Ratio denoted by φ , is an irrational mathematical constant, approximately 1.61803398874989. In mathematics two quantities are in the golden ratio of the sum of quantities to the larger quantity is equal to the ratio of the larger quality to the smaller one. Two quantities a and b are said to be in the golden ratio if

$$\frac{a+b}{a} = \frac{a}{b} = \varphi$$

$$\text{Then } \frac{a+b}{a} = 1 + \frac{a}{b}$$

$$= 1 + \frac{1}{\varphi}$$

$$1 + \frac{1}{\varphi} = \varphi$$

$$\varphi^2 = \varphi + 1$$

$$\varphi^2 - \varphi - 1 = 0$$

$$\varphi = \frac{1+\sqrt{5}}{2}$$

$$\varphi = 1.61803398874989$$

$$\varphi \approx 1.618$$

Definition: 1.13

A **golden rectangle** is one whose side lengths are in golden ratio, that is approximately $1:\frac{1+\sqrt{5}}{2}$

Construction of Golden Rectangle

A Golden Rectangle can be constructed with only straightedge and compass by this technique

1. Construct a single square.
2. Draw a line from the midpoint of one side of the square to an opposite corner.
3. Use the line as radius to draw an arc that defines the height of the rectangle.
4. Complete the golden rectangle

1.12 Golden Spiral

In a Golden rectangle, starting with the smallest one on the right connect the lower corner to the upper right corner with an arc that is one fourth of a circle. Then continue the line into the second square with an arc that is one fourth of a circle. Continue this process until each square has an arc inside it, with all or them connected as a continuous line. This line looks like a spiral.

Chapter 2

CHAPTER 2

PROPERTIES OF FIBONACCI AND LUCAS NUMBERS

2.1 THE SIMPLEST PROPERTIES OF FIBONACCI NUMBERS

Theorem:2.1.1 The sum of the first n Fibonacci numbers is equal to

$$F_{n+2} - 1$$

Proof: We have

$$F_1 = F_3 - F_2,$$

$$F_2 = F_4 - F_3,$$

$$\vdots$$

$$F_{n-1} = F_{n+1} - F_n,$$

$$F_n = F_{n+2} - F_{n+1}$$

Adding up these equations term by term, we get

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - F_2 = F_{n+2} - 1$$

Theorem: 2.1.2 The sum of first n Fibonacci with odd suffices is equal to F_{2n}

Proof: We know

$$F_1 = F_2,$$

$$F_3 = F_4 - F_2,$$

$$F_5 = F_6 - F_4,$$

$$\vdots$$

$$F_{2n-1} = F_{2n} - F_{2n-2}$$

Adding up these equations term by term, we obtain

$$F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$$

Theorem: 2.1.3 $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$

Proof: We know that

$$F_k F_{k+1} - F_{k-1} F_k = F_k (F_{k+1} - F_{k-1}) = F_k^2$$

$$F_1^2 = F_1 F_2,$$

$$F_2^2 = F_2 F_3 - F_1 F_2,$$

$$\vdots$$

$$F_n^2 = F_n F_{n+1} - F_{n-1} F_n$$

Adding up these equations term by term, we get

$$F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$$

Theorem: 2.1.4 $F_{n+m} = F_{n-1} F_m + F_n F_{m+1}$.

Proof: We shall prove the theorem by the method of induction on m .

For $m = 1$, we get

$$F_{n+1} = F_{n-1} F_1 + F_n F_{1+1} = F_{n-1} + F_n \text{ which is true.}$$

Suppose that it is true for $m = k$ and $m = k + 1$

We shall prove it is also true that $m = k + 2$.

$$\text{Let } F_{n+k} = F_{n-1} F_k + F_n F_{k+1} \quad \text{and}$$

$$F_{n+(k+1)} = F_{n-1} F_{k+1} + F_n F_{k+2}$$

Adding these two equations, we get

$$F_{n+(k+2)} = F_{n-1} F_{k+2} + F_n F_{k+3}$$

$$\text{Hence } F_{n+m} = F_{n-1} F_m + F_n F_{m+1}$$

Theorem: 2.1.5 $F_{n+1}^2 = F_n F_{n+2} + (-1)^n$

Proof: We shall prove the theorem by induction on n

We have since, $F_2^2 = F_1 F_3 - 1 = 1$, the assertion is true for $n = 1$

Let us assume that the theorem is true for $n = 1, 2, \dots, k$

Then adding $F_{n+1} F_{n+2}$ to both sides, we get

$$F_{n+1}^2 + F_{n+1} F_{n+2} = F_{n+1} F_{n+2} + F_n F_{n+2} + (-1)^n$$

Which implies that

$$F_{n+1} (F_{n+1} + F_{n+2}) = F_{n+2} (F_n + F_{n+1}) + (-1)^n$$

This simplifies to $F_{n+1}F_{n+3} = F_{n+2}^2 + (-1)^n$

Finally, we have, $F_{n+2}^2 = F_{n+1}F_{n+3} + (-1)^{n+1}$

2.2 NUMBER-THEORETIC PROPERTIES OF FIBONACCI NUMBERS

Theorem: 2.2.1

For the Fibonacci sequence $\gcd(F_n, F_{n+1}) = 1$ for every $n \geq 1$

Proof: Let $\gcd(F_n, F_{n+1}) = d > 1$. Then $d|F_n$ and $d|F_{n+1}$

Then $F_{n+1} - F_n = F_{n-1}$ will also be divided by d

Again, we know that $F_n - F_{n-1} = F_{n-2}$

This implies $d|F_{n-2}$

Working backwards, the same argument shows that $d|F_{n-3}, d|F_{n-4} \dots$ and finally that $d|F_1 = 1$. This is impossible.

Hence $\gcd(F_n, F_{n+1}) = 1$ for every $n \geq 1$

Theorem: 2.2.2 For $m \geq 1, n \geq 1, F_{nm}$ is divisible by F_m

Proof: We shall prove the theorem by induction on n

For $n = 1$ the theorem is true.

Let us assume that $F_m|F_{nm}$, for $n = 1, 2, 3 \dots, k$

Now $F_{m(k+1)} = F_{mk} + F_m = F_{mk-1}F_m$

$$= F_{mk}F_{m+1} + F_m$$

The right-hand side of the equation is divisible by F_m

Hence $d|F_{m(k+1)}$

Lemma: 2.2.3 If $m = nq + r$, then $\gcd(F_m, F_n) = \gcd(F_r, F_n)$

Proof: Observe that $\gcd(F_m, F_n) = \gcd(F_{nq+r}, F_n)$

$$= \gcd(F_{nq-1}F_r + F_{qn}F_{r+1}, F_n)$$

$$= \gcd(F_{nq-1}F_r, F_n)$$

Now, we claim that $\gcd(F_{nq-1}, F_n) = 1$

Let $d = \gcd(F_{nq-1}, F_n)$

Then $d|F_{nq-1}$ and $d|F_n$

Also, that $F_n|F_{nq}$

Therefore $d|F_{nq}$

This d is the positive common divisor of F_{nq} and F_{nq-1}

But $\gcd(F_{nq-1}, F_{nq}) = 1$. This is an absurd.

Hence $d = 1$

Theorem: 2.2.4 The greatest common divisor of two Fibonacci number is again a Fibonacci number.

Proof: Let F_m and F_n be two Fibonacci number.

Let us assume that $m \geq n$.

Then by applying Euclidian Algorithm to m and n ,

We get the following system of equations

$$m = q_1n + r_1, 0 \leq r_1 < n$$

$$n = q_2r_1 + r_2, 0 \leq r_2 < r_1$$

$$r_1 = q_3r_2 + r_3, 0 \leq r_3 < r_2, \dots$$

$$r_{n-2} = q_nr_{n-1} + r_n, 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1}r_n + 0$$

Then from the previous lemma

$$\gcd(F_m, F_n) = \gcd(F_{r_1}, F_n)$$

$$= \gcd(F_{r_1}, F_{r_1})$$

\vdots

$$= \gcd(F_{r_{n-2}}, F_{r_n})$$

Since $r_n | r_{n-1}$, then $F_{r_n} | F_{r_{n-1}}$

Therefore $\gcd(F_{r_{n-1}}, F_{r_n}) = F_{r_n}$

But r_n being the last non-zero remainder Euclidian Algorithm for m and n is equal to $\gcd(m, n)$

Thus $\gcd(F_m, F_n) = F_d$, where $d = \gcd(m, n)$

Theorem: 2.2.5 In a Fibonacci sequence $F_m | F_n$ if and only if $m | n$

Proof: If $F_m | F_n$, then $\gcd(F_m, F_n) = F_m$

But we know that $\gcd(F_m, F_n) = F_{\gcd(m, n)}$

This implies that $\gcd(m, n) = m$

Hence $m | n$

Theorem: 2.2.6 The sequence of ratio of successive Fibonacci numbers $F_{n+1} | F_n$

converges to a Golden ratio i. e., $\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \varphi$

Proof:

We consider the sequence $r_n = \frac{F_{n+1}}{F_n}$, for $n = 1, 2, 3 \dots$

Then by definition of Fibonacci Numbers, we have

$$\begin{aligned} r_n &= \frac{F_{n+1}}{F_n} \\ &= \frac{F_n + F_{n-1}}{F_n} \\ &= 1 + \frac{1}{r_{n-1}} \end{aligned}$$

When $n \rightarrow \infty$, then we can write the above equation in limits

$$\begin{aligned} x &= 1 + \frac{1}{x} \\ x^2 &= 1 + x \\ &= x^2 - x - 1 \\ &= 0 \end{aligned}$$

$$x = \frac{1+\sqrt{5}}{2} = \varphi$$

$$\text{Hence, } \lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \varphi$$

2.3 BINET'S FORMULA FOR FIBONACCI AND LUCAS NUMBERS

Lemma: 2.3.1 Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, so that α and β are both roots of the equation $x^2 = x + 1$. Then, $F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$, for all $n \geq 1$

Proof: When $n = 1$, $F_1 = 1$ which is true.

Let us assume that it is true for $n = 1, 2, 3, \dots, n$

$$\text{Then } F_{k-1} = \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}} \text{ and } F_k = \frac{\alpha^k - \beta^k}{\sqrt{5}}$$

Adding these two equations, we get

$$F_k + F_{k-1} = \frac{\alpha^k}{\sqrt{5}}(1 + \alpha^{-1}) + \frac{\beta^k}{\sqrt{5}}(1 + \beta^{-1})$$

$$\text{Then } F_{k+1} = \frac{\alpha^{(k+1)} + \beta^{(k+1)}}{\sqrt{5}}$$

Lemma: 2.3.2 Let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, so that α and β are both roots of the equation $x^2 = x + 1$. Then $L_n = \alpha^n + \beta^n$, for all $n \geq 1$.

Proof: For $n = 1$, $L_1 = 1$.

Then the theorem is true for $n = 1$.

Let us assume that it is true for $n = 1, 2, 3, \dots, k$

We have to prove that it is true for $n = k + 1$

$$\text{Now, } L_k + L_{k-1} = \alpha^k + \alpha^{k-1} + \beta^k + \beta^{k-1}$$

$$L_{k+1} = \alpha^k(1 + \alpha^{-1}) + \beta^k(1 + \beta^{-1})$$

$$L_{k+1} = \alpha^k(1 + \alpha - 1) + \beta^k(1 + \beta - 1)$$

$$L_{k+1} = \alpha^{k+1} + \beta^{k+1}$$

2.4 RELATION BETWEEN FIBONACCI AND LUCAS NUMBERS

Theorem: 2.4.1 $L_n = F_{n-1} + F_{n+1}$, for $n > 1$

Proof: We know that $L_{k+1} = L_k + L_{k-1}$

$$L_{k+1} = (F_{k-1} + F_{k+1}) + (F_{k-2} + F_k)$$

$$\begin{aligned} L_{k+1} &= (F_{k-1} + F_{k-2}) + (F_k + F_{k+1})L_{k+1} \\ &= F_k + F_{k+2} \end{aligned}$$

Theorem: 2.4.2 For all $n \geq 1$, $F_{2n} = L_n F_n$

Proof: Now

$$L_n F_n = \frac{1}{\sqrt{5}} (\alpha^n - \beta^n) (\alpha^n + \beta^n)$$

$$L_n F_n = \frac{1}{\sqrt{5}} (\alpha^{2n} - \beta^{2n})$$

$$L_n F_n = F_{2n}$$

Lemma: 2.4.3 $L_n^2 - L_{n-1} L_{n+1} = 5(-1)^n$ for $n \geq 1$.

Proof: Induction $L_{n+1}^2 - L_n L_{n+2} = L_{n-1} L_{n+1} - L_n^2$
 $= 5(-1)^n$

Lemma: 2.4.4 $2F_{m+n} = F_m L_n + F_n L_m$

Proof: By induction

$$\begin{aligned} F_{n+m+1} &= F_{n+m} + F_{n+m-1} \\ &= \frac{1}{2} (F_n L_m + F_m L_n) + \frac{1}{2} (F_n L_{m-1} + F_{m-1} L_n) \\ &= \frac{1}{2} (F_n (L_m + L_{m-1})) = L_n (F_m + F_{m-1}) \\ &= \frac{1}{2} (F_n L_{m+1} + L_n F_{m+1}) \end{aligned}$$

Theorem: 2.4.5 Further two relations

$$(a) L_n^2 - 5F_n^2 = 4(-1)^n$$

$$(b) L_{n+1} L_n - 5F_{n+1} F_n = 2(-1)^n$$

Proof: $(a) L_n^2 - 4((-1)^n + F_n^2) = (F_{n+1} + F_{n-1})^2 - 4(F_{n-1} F_{n+1})$

$$= (F_{n+1} - F_{n-1})^2$$

$$= F_n^2$$

$$\begin{aligned} (b) L_{n+2}L_{n+1} - 5F_{n+2}F_{n+1} &= (L_{n+1} + L_n)L_{n+1} - 5(F_{n+1}F_n)F_{n+1} \\ &= L_{n+1}^2 + L_nL_{n+1} - 5F_{n+1}^2 - 5F_nF_{n+1} \\ &= L_{n+1}^2 - 5F_{n+1}^2 + 2(-1)^n \\ &= 4(-1)^{n+1} + 2(-1)^n = 2(-1)^n \end{aligned}$$

2.5 FIBONACCI AND LUCAS IDENTITIES

Theorem: 2.5.1 $\sum_1^n F_i = F_{n+2} - 1$

Proof: Using the Fibonacci recurrence relation, we have

$$F_1 = F_3 - F_2$$

$$F_2 = F_4 - F_3$$

$$F_3 = F_5 - F_4$$

$$\vdots$$

$$F_{n-1} = F_{n+1} - F_n$$

$$F_n = F_{n+2} - F_{n+1}$$

Adding these equations, we get

$$\sum_1^n F_i = F_{n+2} - F_2 = F_{n+2} - 1$$

Theorem: 2.5.2 $\sum_1^n F_{2i-1} = F_{2n}$

Proof: Using the Fibonacci recurrence relation, we have

$$F_1 = F_2 - F_0$$

$$F_3 = F_4 - F_2$$

$$F_5 = F_6 - F_4$$

$$\vdots$$

$$F_{2n-3} = F_{2n-2} - F_{2n-4}$$

$$F_{2n-1} = F_{2n} - F_{2n-2}$$

Adding these equations, we get $\sum_1^n F_{2i-1} = F_{2n} - F_0 = F_{2n}$

For example, $\sum_1^{10} F_{2i-1} = F_{20} = 6765$

Corollary: 2.5.3 $\sum_1^n F_{2i} = F_{2n+1} - 1$

Proof: $\sum_1^n F_{2i} = \sum_1^n F_i - \sum_1^n F_{2i-1}$
 $= (F_{2n} - 1) - F_{2n}$ (by theorem)
 $= (F_{2n+2} - F_{2n}) - 1$
 $= F_{2n+1} - 1$ (by the Fibonacci recurrence relation)

Corollary: 2.5.4 $\beta^n = \beta F_n + F_{n-1}$, where $n \geq 0$

Proof: Let $u_n = (\alpha^n - \beta^n)/\sqrt{5}$, where $n \geq 1$

$$\text{Then } u_1 = \frac{\alpha - \beta}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 \text{ and}$$

$$u_2 = \frac{\alpha^2 - \beta^2}{\sqrt{5}} = \frac{(\alpha + \beta)(\alpha - \beta)}{\sqrt{5}} = 1$$

Suppose $n \geq 3$. Then

$$\begin{aligned} u_{n-1} + u_{n-2} &= \frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{5}} + \frac{\alpha^{n-2} - \beta^{n-2}}{\sqrt{5}} \\ &= \frac{\alpha^{n-2}(\alpha + 1) - \beta^{n-2}(\beta + 1)}{\sqrt{5}} \\ &= \frac{\alpha^{n-2} \cdot \alpha^2 - \beta^{n-2} \cdot \beta^2}{\sqrt{5}} \\ &= \frac{\alpha^n - \beta^n}{\sqrt{5}} = u_n \end{aligned}$$

Thus, u_n satisfies the Fibonacci recurrence relation and the two initial conditions.

This gives us an explicit formula for $F_n : F_n = u_n$

Theorem: 2.5.5 $\sum_1^n F_i^2 = F_n F_{n+1}$

Proof: When $n = 1$,

$$LHS = \sum_1^1 F_i^2 = F_1^2 = 1 = 1 \cdot 1 = F_1 \cdot F_2 = RHS$$

So, the result is true when $n = 1$

Assume it is true for an arbitrary positive integer k :

$$\sum_1^k F_i^2 = F_k F_{k+1}$$

$$\text{Then, } \sum_1^{k+1} F_i^2 = \sum_1^k F_i^2 + F_{k+1}^2$$

$$= F_k F_{k+1} + F_{k+1}^2$$

$$= F_{k+1}(F_k + F_{k+1})$$

$$= F_{k+1} F_{k+2} \text{ (by the Fibonacci recurrence relation)}$$

So, the statement is true when $n = k + 1$. Thus it is true for every positive integer n

For example,

$$\sum_1^{25} F_i^2 = F_{225} F_2 = 75,025.121,393 = 9,107,509,825$$

Chapter 3

CHAPTER 3

PASCAL'S TRIANGLE

3.1 BINOMIAL COEFFICIENTS

Let n and k be non-negative integers. The binomial coefficient $\binom{n}{k}$ is defined by

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{if } 0 \leq k \leq n \\ 0 & \text{otherwise} \end{cases}$$

Theorem: 3.1.1

Let $0 \leq k \leq n$. Then $\binom{n}{k} = \binom{n}{n-k}$

For Example, $\binom{25}{20} = \binom{25}{25-20} = \binom{20}{5} = 53,130$

The next theorem gives a recurrence satisfied by binomial coefficients. It is called Pascal's identity.

Theorem: 3.1.2 (Pascal's identity). Let n and k be positive integers, where $k \leq n$.

Then $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

3.2 PASCAL'S TRIANGLE

The various binomial coefficients $\binom{n}{k}$, where $0 \leq k \leq n$, can be arranged as a triangular array, called Pascal's triangle.

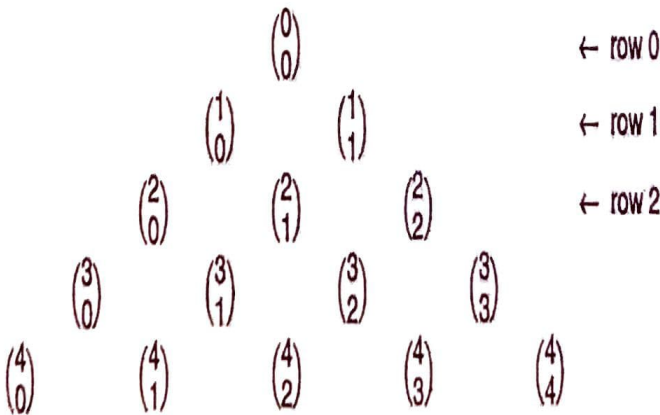


Figure 3.1

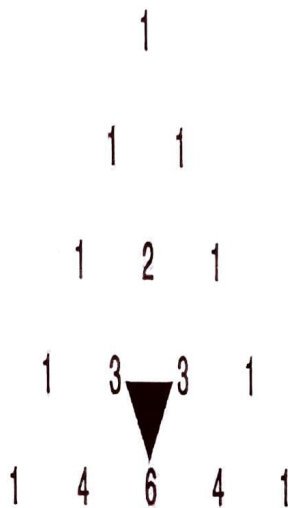


Figure 3.2

Pascal's triangle has many intriguing properties. Some of them are:

- 1) Every row begins with and ends in 1.
- 2) Pascal's triangle is symmetric about a vertical line through the middle. This is so by Theorem 3.1.1
- 3) Any interior number in each row is the sum of the numbers immediately to its left and right in the preceding row. This is true by virtue of Pascal's identity.
- 4) The sum of the numbers in row n is 2^n

The next theorem shows how the binomial coefficients can be used to find the Binomial Expansion of $(x + y)^n$. It can be proved using PMI or Combinatorics the former is a bit long, while the latter is short.

Theorem: 3.2.1 (The Binomial Theorem).

Let x and y be any real numbers and n any non-negative integers.

$$\text{Then } (x + y)^n = \sum_{r=0}^n \binom{n}{r} x^{n-r} y^r$$

The binomial theorem has some interesting and useful by products. They are given in the next two corollaries.

Corollary: 3.2.2

$$(1+x)^n = \sum_{r=0}^n \binom{n}{r} x^r$$

$$(1-x)^n = \sum_{r=0}^n (-1)^r \binom{n}{r} x^r$$

Corollary: 3.2.3

$$\sum_{r=0}^n \binom{n}{r} = 2^n$$

$$\sum_{r=0}^n (-1)^r \binom{n}{r} = 0$$

$$\sum_{r \text{ odd}} \binom{n}{r} = \sum_{r \text{ even}} \binom{n}{r}$$

3.3 FIBONACCI NUMBERS AND PASCAL'S TRIANGLE

How can Fibonacci Numbers be extracted from Pascal's triangle? To see this, consider the array. Now add the numbers along the northeast diagonals. The sums are 1,1,2,3,5,8,.....; and they seem to be Fibonacci Numbers. In fact, they are, as the next theorem, discovered by Lucas in 1876, confirms.

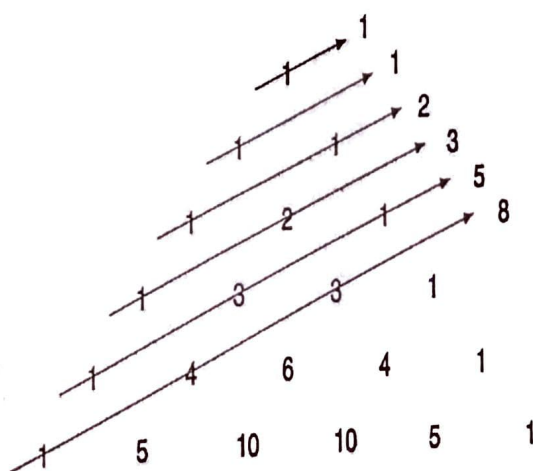


Figure 3.3 Pascal's Triangle

Theorem: 3.3.1(Lucas, 1876)

Let $n \geq 1$. Then, $F_n = \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n-i-1}{i}$

Proof: We will prove the result using the strong version of PMI. Since $\binom{0}{0} = 1 = F_1$, the statement is true when $n = 1$

Now assume it is true for all positive integers $\leq k$, where $k \geq 1$. By Pascal's identity,

we then have $\sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i}{i} = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i-1}{i-1} + \sum_{i=0}^{k/2} \binom{k-i-1}{i}$.

Suppose k is even. Then

$$\begin{aligned} \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i}{i} &= \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i-1}{i-1} + \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i-1}{i} \\ &= \sum_{i=0}^{(k-1)/2} \binom{k-i-2}{i-1} + \sum_{i=0}^{\frac{k}{2}-1} \binom{k-i-1}{i} + \binom{\frac{k}{2}-1}{\frac{k}{2}} \\ &= \sum_{i=0}^{\lfloor \frac{k-2}{2} \rfloor} \binom{k-i-2}{i} + \sum_{i=0}^{\lfloor \frac{(k-1)}{2} \rfloor} \binom{k-i-1}{i} - 0 \\ &= F_{k-1} + F_k \\ &= F_{k+1} \end{aligned} \dots\dots\dots(3.1)$$

So, the formula works when k is even.

It can similarly be shown that it works when n is odd.

Consequently, it is true when $n = k + 1$

Thus, by the strong version of PMI, the formula is true for all positive integers n .

For Example, $F_6 = \sum_{i=0}^2 \binom{5-i}{i} = 1 + 4 + 3 = 8$

$$F_7 = \sum_{i=0}^3 \binom{6-i}{i} = 1 + 5 + 6 + 1 = 13$$

It follows by the Lucas formula in Theorem 3.3.1 that $K_n = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-i}{i}$

Satisfies Fibonacci recurrence, where $K_1 = 1 = F_2$ and $K_2 = 2 = F_3$

The Lucas formula is a special case of an interesting result derived in 1950 by Steven Vajda to see this, we use a bit of operator theory.

Let $S_n = S_n(x) = \sum_{i \geq 0} \binom{n-i}{i} x^i$ and $\Delta S_n = S_{n+1} - S_n$.

$$\begin{aligned}
\text{Then, } \Delta S_n &= \sum_{i \geq 0} \left[\binom{n+1-i}{i} - \binom{n-i}{i} \right] x^i \\
&= \sum_{i \geq 0} \binom{n-i}{i-1} \\
&= \sum_{j \geq 0} \binom{n-j-1}{j} x^{j+1}
\end{aligned}$$

$$\begin{aligned}
\Delta^2 S_n &= \Delta(\Delta S_n) \\
&= \Delta S_{n+1} - \Delta S_n \\
&= \sum_{i \geq 0} \left[\binom{n+1-i}{i-1} - \binom{n-i}{i-1} \right] x^i \\
&= \sum_{i \geq 0} \binom{n-i}{i-2} x^i \\
&= \sum_{j \geq 0} \binom{n-j-1}{j-1} x^{j+1}
\end{aligned}$$

$$\begin{aligned}
\text{Then, } \Delta^2 S_n - \Delta S_n &= \sum_{j \geq 0} \left[\binom{n-j-1}{j} + \binom{n-j-1}{j-1} \right] x^{j+1} \\
S_{n+2} - S_{n+1} &= \sum_{j \geq 0} \binom{n-j}{j} x^{j+1} \\
&= x S_n
\end{aligned}$$

Thus, S_n satisfies the recurrence $S_{n+2} - S_{n+1} - x S_n = 0$, where $S_0 = 1 = S_1$

Its characteristic equation is $t^2 - t - x = 0$ with roots $r = \frac{1+\sqrt{1+4x}}{2}$ and

$$s = \frac{1-\sqrt{1+4x}}{2}$$

So, the general solution of the recurrence is $S_n = A r^n + B r^n$, where A and B are constants.

It follows by the initial conditions $S_0 = 1 = S_1$ that $A = \frac{r}{r-s}$ and $B = \frac{s}{s-r}$

$$\begin{aligned}
\text{Thus, } S_n(x) &= \frac{r^{n+1} - s^{n+1}}{r-s} \\
&= \frac{1}{\sqrt{1+4x}} \left[\left(\frac{1+\sqrt{1+4x}}{2} \right)^{n+1} + \left(\frac{1-\sqrt{1+4x}}{2} \right)^{n+1} \right] \dots\dots\dots(3.2)
\end{aligned}$$

In particular, $S_n(1)$ gives Binet's formula for F_{n+1}

Formula (3.2) has other interesting by products.

Suppose, for example, $x = 2$

Then, $\sum_{i \geq 0} \binom{n-i}{i} 2^i = \frac{2^{n+1} - (-1)^{n+1}}{3}$

Numbers of the form $J_{n+1} = \frac{2^{n+1} - (-1)^{n+1}}{3}$ are the well-known Jacobsthal numbers, named after the German mathematics Ernst Jacobsthal, where $n \geq 0$. Formula (3.2) is Binet's formula for the Jacobsthal polynomial $J_{n+1}(x) = S_n(x)$, where $n \geq 0$;

$$J_{n+1}(x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-i}{i} x^i$$

So Jacobsthal numbers and polynomial can be computed from Pascal's triangle with appropriate weights.

When $x = -1$, formula (3.2) yield another interesting case

$$\text{Then } r = \frac{1+\sqrt{3}i}{2} = e^{i\pi/3} \text{ and } S = \frac{1-\sqrt{3}i}{2} = e^{-i\pi/3},$$

$$\begin{aligned} \text{so } \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i \binom{n-i}{i} &= \frac{1}{\sqrt{3}i} [e^{(n+1)i\pi/3} - e^{-(n+1)i\pi/3}] \\ &= \frac{2 \sin(n+1)\pi/3}{\sqrt{3}} \\ &= \begin{cases} 0, & \text{if } n \equiv 2 \pmod{3} \\ (-1)^{\lfloor \frac{n}{3} \rfloor}, & \text{otherwise} \end{cases} \end{aligned}$$

Where $i\sqrt{-1}$ and $\lfloor t \rfloor$ denotes the floor of the real number t .

The case $x = -1/4$ is also an intersecting one. We leave it for the curious-minded to pursue. It follows by the identity $L_n = F_{n+1} + F_{n-1}$ and Theorem 3.4 that Lucas numbers also can be extracted from Pascal's triangle. Each L_n is the sum of the diagonal sums on rising diagonals $n+1$ and $n-1$

3.4 ANOTHER EXPLICIT FORMULA FOR L_n

Using Theorem 3.3.1 and the identity $L_n = F_{n+1} + F_{n-1}$, we can develop another explicit formula for L_n

$$L_n = F_{n+1} + F_{n-1}$$

$$\begin{aligned}
&= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k} + \sum_{k=0}^{\lfloor (n-2)/2 \rfloor} \binom{n-k-2}{k} \\
&= \sum_k^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k} + \sum_{k=0}^{(n/2)} \binom{n-k-2}{k} \\
&= \sum_k^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{k} + \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k-1}{k-1} \\
&= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \left[\binom{n-k}{k} + \binom{n-k-1}{k-1} \right] \\
&= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-k} \binom{n-k}{k}
\end{aligned}$$

For example, $L_5 = \sum_{k=0}^2 \frac{5}{5-k} \binom{5-k}{k}$

$$\begin{aligned}
&= \frac{5}{5} \binom{5}{0} + \frac{5}{4} \binom{4}{1} + \frac{5}{3} \binom{3}{2} \\
&= 1+5+5 = 11
\end{aligned}$$

3.5 CATALAN'S FORMULA

In lieu of using the rising diagonal of Pascal's triangle, we can use its rows to computer Fibonacci numbers. To see this, we expand Binet's formula using the binomial theorem:

$$\begin{aligned}
F_n &= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right] \\
&= \frac{1}{2^{n-1}} \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 5^k
\end{aligned}$$

Catalan discovered this formula in 1846.

But, by Corollary 3.2.3, $2^{n-1} = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k}$

Consequently, we can rewrite Catalan formula with a more aesthetic appeal

$$F_n = \frac{\binom{n}{1} + \binom{n}{3}5 + \binom{n}{5}5^2 + \binom{n}{7}5^3 + \dots}{\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \dots}$$

We can similarly show that

$$L_n = \frac{\binom{n}{0} + \binom{n}{2}5 + \binom{n}{4}5^2 + \binom{n}{6}5^3 + \dots}{\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \dots}$$

For example,

$$F_7 = \frac{\binom{7}{1} + \binom{7}{3} 5 + \binom{7}{5} 5^2 + \binom{7}{7} 5^3}{\binom{7}{0} + \binom{7}{2} + \binom{7}{4} + \binom{7}{6}} = \frac{832}{64} = 13$$

$$L_7 = \frac{\binom{7}{0} + \binom{7}{3} 5 + \binom{7}{5} 5^2 + \binom{7}{7} 5^3}{\binom{7}{1} + \binom{7}{3} + \binom{7}{5} + \binom{7}{7}} = \frac{1856}{64} = 29$$

Additional Identities

We can use Binet's and Lucas formula with the binomial theorem in tandem to derive an array of Fibonacci and Lucas identities.

To begin with, notice that

$$\begin{aligned} \sum_{i=0}^5 \binom{5}{i} F_i &= \binom{5}{0} F_0 + \binom{5}{1} F_1 + \binom{5}{2} F_2 + \binom{5}{3} F_3 + \binom{5}{4} F_4 + \binom{5}{5} F_5 \\ &= 0 + 5 + 10 + 20 + 15 + 5 = 35 \\ &= F_{10} \end{aligned}$$

More generally, we have the following identity

Theorem: 3.5.1 (Lucas) Let $n \geq 0$. Then $\sum_{i=0}^n \binom{n}{i} F_i = F_{2n}$

Proof: Since $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$, by Binet's formula, we have

$$\begin{aligned} (\alpha - \beta) \sum_{i=0}^n \binom{n}{i} F_i &= \sum_{i=0}^n \binom{n}{i} (\alpha^i - \beta^i) \\ &= \sum_{i=0}^n \binom{n}{i} \alpha^i - \sum_{i=0}^n \binom{n}{i} \beta^i \\ &= (1 + \alpha)^n - (1 + \beta)^n \\ &= \alpha^{2n} - \beta^{2n} \end{aligned}$$

$$\sum_{i=0}^n \binom{n}{i} F_i = F_{2n}$$

A similar argument yields yet another identity by Lucas, when $n \geq 0$

$$\sum_{i=0}^n \binom{n}{i} L_i = L_{2n} \quad \dots\dots\dots(3.3)$$

For example, $\sum_{i=0}^4 \binom{4}{i} L_i = \binom{4}{0} L_0 + \binom{4}{1} L_1 + \binom{4}{2} L_2 + \binom{4}{3} L_3 + \binom{4}{4} L_4$

$$= 2 + 4 + 18 + 16 + 7 = 47$$

$$= L_8$$

Theorem: 3.5.2 Let $n \geq 0$, Then, $\sum_{i=0}^n (-1)^{i+1} \binom{n}{i} F_i = F_n$

Proof: By Binet's formula and Corollary 3.2.2,

$$\begin{aligned} \text{we have } (\alpha - \beta) \text{ LHS} &= -\sum_{i=0}^n \binom{n}{i} [(-\alpha)^i - (-\beta)^i] \\ &= -[(1 - \alpha)^n - (1 - \beta)^n] \\ &= \alpha^n - \beta^n \\ \text{LHS} &= F_n \end{aligned}$$

For example,

$$\begin{aligned} \sum_{i=0}^5 (-1)^{i+1} \binom{5}{i} F_i &= -\binom{5}{0} F_0 + \binom{5}{1} F_1 - \binom{5}{2} F_2 + \binom{5}{3} F_3 - \binom{5}{4} F_4 + \binom{5}{5} F_5 \\ &= 0 + 5 - 10 + 20 - 15 + 5 = 5 = F_5 \end{aligned}$$

We can show similarly that

$$\sum_{i=0}^n (-1)^i \binom{n}{i} L_i = L_n \tag{3.4}$$

where $n \geq 0$

For example,

$$\begin{aligned} \sum_{i=0}^4 (-1)^i \binom{4}{i} L_i &= \binom{4}{0} L_0 - \binom{4}{1} L_1 + \binom{4}{2} L_2 - \binom{4}{3} L_3 + \binom{4}{4} L_4 \\ &= 2 - 4 + 18 - 16 + 7 = L_4 \end{aligned}$$

Chapter 4

CHAPTER 4

FIBONACCI MATRICES

4.1 THE Q-MATRIX

First, we will demonstrate a close link between matrices and Fibonacci numbers.

To this, consider the matrix

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

Notice that $|Q| = -1$, where $|M|$ denotes the determinant of the square matrix M .

$$\begin{aligned} \text{Then } Q^2 &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \end{aligned}$$

$$\begin{aligned} Q^3 &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} \end{aligned}$$

$$\text{Similarly, } Q^4 = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

Theorem: 4.1.1 Let $n \geq 1$. Then $Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$

Proof: Clearly, the result is true when $n = 1$. Now assume it is true for an arbitrary positive integer k :

$$Q^k = \begin{bmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{bmatrix}$$

$$\text{Then } Q^{k+1} = Q^k Q^1$$

$$\begin{aligned} &= \begin{bmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} F_{k+2} & F_{k+1} \\ F_{k+1} & F_k \end{bmatrix} \end{aligned}$$

So, the result is true when $n = k + 1$ also

Thus, by PMI, the result is true for all positive integers n .

It follows by Theorem 4.1.1 that trace (sum of the diagonal elements) of the matrix

$$Q^n \text{ is } F_{n+1} + F_{n-1} = L_n$$

4.2 CASSINI'S FORMULA REVISITED

Theorem 4.1.1 yields Cassini's formula as a delightful dividend: see the next corollary.

Corollary: 4.2.1 Let $n \geq 1$. Then, $F_{n+1} F_{n-1} - F_n^2 = (-1)^n$

Proof: Since $|Q| = -1$, it follows by $|Q^n| = (-1)^n$

$$\text{But, by Theorem 4.1.1, } |Q^n| = F_{n+1} F_{n-1} - F_n^2$$

$$\text{Thus, } F_{n+1} F_{n-1} - F_n^2 = (-1)^n$$

Interestingly, the Cassini-like formula $L_{n+1} L_{n-1} - L_n^2 = 5(-1)^{n-1}$ also follows by

Theorem 4.1.1 To see this, first notice that

$$Q^2 + I = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}$$

So $|Q^2 + I| = 5$. Since $F_{n+1} + F_{n-1} = L_n$, then we have

$$Q^{n+1} + Q^{n-1} = \begin{bmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix} + \begin{bmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{bmatrix}$$

$$Q^{n-1} (Q^2 + I) = \begin{bmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{bmatrix}$$

$$|Q^{n-1} (Q^2 + I)| = L_{n+1} L_{n-1} - L_n^2$$

$$\text{Since } |Q^{n-1} (Q^2 + I)| = |Q^{n-1}| \cdot |(Q^2 + I)|$$

$$= 5(F_n F_{n-2} - F_{n-1}^2) = 5(-1)^{n-1},$$

this implies $L_{n+1} L_{n-1} - L_n^2 = 5(-1)^{n-1}$

4.3 FIBONACCI ADDITION FORMULA

Using Theorem 4.1.1, we can develop an addition formula for Fibonacci numbers, as the next corollary shows. Although the corollary lists four addition formulas, they are basically the same.

Corollary: 4.3.1

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n \quad \dots\dots\dots(4.1)$$

$$F_{m+n} = F_{m+1}F_n + F_mF_{n-1} \quad \dots\dots\dots(4.2)$$

$$F_{m+n} = F_mF_{n+1} + F_{m-1}F_n \quad \dots\dots\dots(4.3)$$

$$F_{m+n-1} = F_mF_n + F_{m-1}F_{n-1} \quad \dots\dots\dots(4.4)$$

Proof:

$$Q^{m+n} = Q^m Q^n$$

$$\begin{aligned} \begin{bmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{bmatrix} &= \begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix} \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \\ &= \begin{bmatrix} F_{m+1}F_{n+1} + F_mF_n & F_{m+1}F_n + F_mF_{n-1} \\ F_mF_{n+1} + F_{m-1}F_n & F_mF_n + F_{m-1}F_{n-1} \end{bmatrix} \end{aligned}$$

Equating the corresponding elements yields the given identities.

In particular, let $m = n$. Then identity (4.1) yields Lucas' formula

$$F_n^2 + F_{n+1}^2 = F_{2n+1}$$

Likewise, identity (4.2) yields

$$\begin{aligned} F_{2n} &= F_{n+1}F_n + F_nF_{n-1} \\ &= F_n(F_{n+1} + F_{n-1}) \\ &= F_nL_n \end{aligned}$$

F_{2n} also equals

$$(F_{n+1} - F_{n-1})(F_{n+1} + F_{n-1}) = F_{n+1}^2 - F_{n-1}^2$$

Addition formula (4.2), coupled with the charming identity $F_{2n} = F_nL_n$ can be used to evaluate an interesting infinite product, studied in 1980 by J. Shallit of Palo Alto, California.

Example: 4.3.2 Evaluate the infinite product

$$P = (1 + \frac{1}{2})(1 + \frac{1}{13}) \left(1 + \frac{1}{610}\right) \dots\dots\dots$$

Solution: Notice that $P = \prod_{n=1}^{\infty} \left(1 + \frac{1}{F_{2^{n+1}-1}}\right)$. To evaluate this product, we will first prove two results.

1) To prove that $F_{2^n-1} L_{2^n} = F_{2^{n+1}-1} + 1$

Using the identity $F_{m+1} + F_{m-1} = L_m$, Cassini's formula, and the Fibonacci addition formula, we have

$$\begin{aligned}
 F_{2^n-1} L_{2^n} &= F_{2^n-1} (F_{2^{n+1}} + F_{2^{n-1}}) \\
 &= F_{2^n-1} F_{2^{n+1}} + F_{2^{n-1}}^2 \\
 &= F_{2^n-1} F_{2^{n+1}} + [F_{2^n} F_{2^{n-2}} - (-1)^{2^{n-1}}] \\
 &= (F_{2^n-1} F_{2^{n+1}} + F_{2^n} F_{2^{n-2}}) + 1 \\
 &= F_{2^n+(2^n-1)} + 1 \\
 &= F_{2^{n+1}-1} + 1
 \end{aligned}$$

2) To prove that $\prod_{i=1}^n L_{2^i} = F_{2^{n+1}}$

When $n = 1$, $LHS = L_2 = 3 = F_4 = RHS$, so the result is true when $n = 1$.

Now, assume it is true for an arbitrary positive integer k .

Then using the identity $F_{2m} = F_m L_m$ we have

$$\begin{aligned}
 \prod_{i=1}^{k+1} L_{2^i} &= \prod_{i=1}^k L_{2^i} \cdot L_{2^{k+1}} \\
 &= F_{2^{k+1}} L_{2^{k+1}} \\
 &= F_{2^{k+2}}
 \end{aligned}$$

So, the result is true for all positive integers n by PMI

With this machinery at our disposal, we are now ready to evaluate the given product.

$$\text{Let } P_m = \prod_{n=1}^m \left(1 + \frac{1}{F_{2^{n+1}-1}}\right)$$

$$\text{Then, } P_m = \prod_{n=1}^m \frac{1 + F_{2^{n+1}-1}}{F_{2^{n+1}-1}}$$

$$= \prod_{n=1}^m \frac{F_{2^n-1} L_{2^n}}{F_{2^{n+1}-1}}$$

$$\begin{aligned}
&= \prod_{n=1}^m \frac{F_{2^{n+1}}}{F_{2^{n+1}-1}} F_{2^{m+1}} \\
&= \frac{F_{2^{m+1}}}{F_{2^{m+1}-1}} \\
P &= \lim_{m \rightarrow \infty} \frac{F_{2^{m+1}}}{F_{2^{m+1}-1}} \\
&= \alpha, \text{ the golden ratio}
\end{aligned}$$

Another immediate consequence of the addition formula is a fact that

$$F_{mn} > F_m F_n, \text{ Where } m > n > 1.$$

Consequently, $F_{nm} > F_n^m$, where $m > n > 1$. It also follows by the addition formula that $F_{mn} | F_n$

Next, we will develop an addition formula for the Lucas family.

Corollary: 4.3.3 $L_{m+n} = F_{m+1}L_n + F_mL_{n-1}$ (4.5)

Proof: Using the identities (4.1) and (4.4), we have

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n$$

$$F_{m+n-1} = F_{m+1}F_{n-1} + F_mF_{n-2}$$

$$\text{Adding, } F_{m+n+1} + F_{m+n-1} = F_{m+1}(F_{n+1} + F_{n-1}) + F_m(F_n + F_{n-2})$$

$$L_{m+n} = F_{m+1}L_n + F_mL_{n-1}$$

Corollary 4.3.1 can be used to derive two additional formulas linking the Fibonacci and Lucas families.

Corollary: 4.3.4

$$2F_{m+n} = F_mL_n + F_nL_m \quad \text{.....(4.6)}$$

$$2L_{m+n} = L_mL_n + 5F_mF_n \quad \text{.....(4.7)}$$

Using the fact that $Q^{m-n} = Q^mQ^{-n}$, we can derive another Fibonacci identity:

$$F_mF_{n+1} - F_nF_{m+1} = (-1)^nF_{m-n} \quad \text{.....(4.8)}$$

It is also called *d'Ocagne's identity*, after the French mathematician Philbert Maurice d'Ocagne. Clearly, it is generalization of Cassini's formula.

d'Ocagne's identity has an interesting Lucas counterpart

$$L_m L_{n+1} - L_n L_{m+1} = 5(-1)^{n+1} F_{m-n} \dots\dots\dots(4.9)$$

For example, $L_7 L_5 - L_4 L_8 = 29 \cdot 11 - 7 \cdot 47 = 5(-1)^5 F_{7-4}$

Identity (4.7) has an interesting by product. To see this, it follows from the identity

$$2L_{m+n} \equiv L_m L_n \pmod{5}$$

that

Let $i + j = h + k$. Then $L_i L_j \equiv 2L_{i+j} \equiv 2L_{h+k}$

$$\equiv L_h L_k \pmod{5}$$

For example, $L_5 L_7 = 11 \cdot 29$

$$\equiv 47 \cdot 7$$

$$\equiv L_8 L_4 \pmod{5}$$

4.4 The M -Matrix

Closely related to the Q -matrix is the M -matrix, studied by Sam Moore of the Community College of Allegheny County, Pennsylvania:

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

We can show by PMI that $M^n = \begin{bmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{bmatrix}$,

Where $n \geq 1$; then

$$\frac{M^n}{F_{2n-1}} = \begin{bmatrix} 1 & F_{2n}/F_{2n-1} \\ F_{2n}/F_{2n-1} & F_{2n+1}/F_{2n-1} \end{bmatrix}$$

Since $\left(\frac{F_k}{F_{k-1}}\right) = \alpha$, it follows that

$$\lim_{n \rightarrow \infty} \frac{M^n}{F_{2n-1}} = \begin{bmatrix} 1 & \alpha \\ \alpha & \alpha^2 \end{bmatrix} = \begin{bmatrix} 1 & \alpha \\ \alpha & 1 + \alpha \end{bmatrix}$$

Thus, the sequence of Fibonacci matrices $\{M_n/F_{2n-1}\}$ converges to the matrix

$A = \begin{bmatrix} 1 & \alpha \\ \alpha & 1 + \alpha \end{bmatrix}$, where $n \geq 1$.

Likewise, sequence $\{Q^n/F_{2n-1}\}$ also converges to the matrix $\begin{bmatrix} 1 & \alpha \\ \alpha & 1 + \alpha \end{bmatrix}$

Next, we will investigate a generalized version of the M -matrix

4.5 A Generalized M -Matrix

Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 1+x \end{bmatrix}$. We will compute its power, scale them to make their leading entries 1, and then find the limit of the resulting sequence of scaled matrices.

The characteristic equation of A is given by $|A - \lambda I| = 0$; that is,

$$\begin{bmatrix} 1-\lambda & 1 \\ 1 & 1+x-\lambda \end{bmatrix} = 0$$

$$\lambda^2 - (x+2)\lambda + x = 0.$$

So, the characteristics roots are $r(x) = 1 + \frac{1}{2}(x - \sqrt{x^2 + 4})$ and

$$s(x) = 1 + \frac{1}{2}(x + \sqrt{x^2 + 4})$$

Next, we will find a characteristic vector $\begin{pmatrix} u \\ v \end{pmatrix}$ associated with r . To this end, we solve

the equation $A \begin{pmatrix} u \\ v \end{pmatrix} = r \begin{pmatrix} u \\ v \end{pmatrix}$. We can easily choose $\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 \\ r-1 \end{pmatrix}$

Similarly, we can choose the characteristic vector associated with s to be $\begin{pmatrix} 1 \\ s-1 \end{pmatrix}$. Then

$$A = \begin{bmatrix} 1 & 1 \\ r-1 & s-1 \end{bmatrix} \begin{bmatrix} r & 0 \\ 0 & s \end{bmatrix} \begin{bmatrix} 1 & 1 \\ r-1 & s-1 \end{bmatrix}^{-1}.$$

The expression $\alpha(x) = \frac{x+\sqrt{x^2+4}}{2}$ and $\beta(x) = \frac{x-\sqrt{x^2+4}}{2}$ will play a significance role in the study of Fibonacci and Lucas polynomials.

Since $(r-1)(s-1) = -1$, we then have

$$\begin{aligned} A^n &= \begin{bmatrix} 1 & 1 \\ r-1 & s-1 \end{bmatrix} \begin{bmatrix} r^n & 0 \\ 0 & s^n \end{bmatrix} \begin{bmatrix} 1 & 1 \\ r-1 & s-1 \end{bmatrix}^{-1} \\ &= \frac{1}{s-r} \begin{bmatrix} 1 & 1 \\ r-1 & s-1 \end{bmatrix} \begin{bmatrix} r^n & 0 \\ 0 & s^n \end{bmatrix} \begin{bmatrix} s-1 & -1 \\ 1-r & 1 \end{bmatrix} \\ &= \frac{1}{s-r} \begin{bmatrix} (s-1)r^n - (r-1)s^n & s^n - r^n \\ s^n - r^n & (s-1)s^n - (r-1)r^n \end{bmatrix} \end{aligned}$$

Scaling this matrix to make its leading entry 1 gives the matrix

$$\begin{aligned}
 B_n &= \begin{bmatrix} 1 & \frac{s^n - r^n}{(s-1)r^n - (r-1)s^n} \\ \frac{s^n - r^n}{(s-1)r^n - (r-1)s^n} & \frac{s^n - r^n}{(s-1)r^n - (r-1)s^n} \end{bmatrix} \\
 &= \begin{bmatrix} 1 & \frac{1 - (r/s)^n}{(s-1)(r/s)^n - (r-1)} \\ \frac{1 - (r/s)^n}{(s-1)(r/s)^n - (r-1)} & \frac{1 - (r/s)^n}{(s-1)(r/s)^n - (r-1)} \end{bmatrix}
 \end{aligned}$$

Since $x > 0$, $(r/s)^n \rightarrow 0$ as $n \rightarrow \infty$

$$\begin{aligned}
 \text{So, } \lim_{n \rightarrow \infty} B_n &= \begin{bmatrix} 1 & \frac{1}{1-r} \\ \frac{1}{1-r} & \frac{s-1}{1-r} \end{bmatrix} \\
 &= \begin{bmatrix} 1 & s-1 \\ s-1 & (s-1)^2 \end{bmatrix}
 \end{aligned}$$

In particular, let $x = 1$

Then $s = \alpha + 1 = \alpha^2$

So $\lim_{n \rightarrow \infty} M^n = \begin{bmatrix} 1 & \alpha \\ \alpha & \alpha^2 \end{bmatrix}$, as found earlier.

Next, we will find the eigenvalues of the Q^n . In the process, we will employ the well-known formula $L_n^2 - 5F_n^2 = 4(-1)^n$

4.6 EIGENVALUES OF Q^n

Let $A = (a_{ij})$ and I the identity matrix of the same size. Then the equation $|A - \lambda I| = 0$ is the characteristic equation of matrix A . Its solution are the eigenvalues.

To find the eigenvalues of Q^n , first we will find its characteristic equation

Using Cassion's Formula, We have

$$\begin{aligned}
 |Q^n - \lambda I| &= \begin{vmatrix} F_{n+1} & F_n \\ F_n & F_{n+1} \end{vmatrix} \\
 &= (F_{n+1} - \lambda)(F_{n+1} - \lambda) - F_n^2 \\
 &= \lambda^2 - (F_{n+1} + F_{n+1})\lambda + F_{n+1}^2 - F_n^2 \\
 &= \lambda^2 - L_{n+1}\lambda + (-1)^{n+1}
 \end{aligned}$$

So, the characteristic equation of Q^n is

$$\lambda^2 - L_n \lambda + (-1)^n = 0 \dots\dots\dots(4.10)$$

Using the quadratic formula, the eigenvalues of Q^n are given by

$$\begin{aligned} \lambda &= \frac{L_n \pm \sqrt{L_n^2 - 4(-1)^n}}{2} \\ &= \frac{L_n \pm \sqrt{5} F_n}{2} \\ &= \alpha^n, \beta^n \end{aligned}$$

Thus, we have the following result.

Theorem: 4. 6. 1 The eigenvalues of Q^n are α^n and β^n

Corollary: 4.6.2 The eigenvalues of Q are α and β

When $n = 1$, equation (4.10) becomes $\lambda^2 - \lambda - 1 = 0$, which is the characteristic equation of Q . But $Q^2 - Q - I = 0$. Thus Q satisfies its characteristic equation, illustrating the well-known Cayley-Hamilton Theorem: “ Every square matrix satisfies its characteristic equation ”

Since $Q^2 = Q + 1$, it follows by the binomial theorem that

$$\begin{aligned} Q^{2n} &= (Q + 1)^n \\ &= \sum_{k=0}^n \binom{n}{k} Q^k \end{aligned}$$

Equating the corresponding elements from both sides, We get

$$\begin{aligned} F_{2n} &= \binom{n}{1} F_1 + \binom{n}{2} F_2 + \dots + \binom{n}{n} F_n \\ F_{2n+1} &= \binom{n}{0} F_1 + \binom{n}{1} F_2 + \dots + \binom{n}{n} F_{n+1} \end{aligned}$$

Next, we will see how I.D. Ruggles and Hoggatt in 1963 derived summation formula using the Q -matrix

SUMMATION FORMULA

Using PMI, we can use establish that

$$(1 + Q + Q^2 + \dots + Q^n)(Q - 1) = Q^{n+1} - 1 \dots\dots\dots (4.11)$$

Since $|Q - I| = -1 \neq 0$, $Q - I$ is invertible.

since $Q^2 = Q + 1$, $Q^2 - Q = 1$ that is, $Q(Q - 1) = I$

Thus, by equation (4.1), we have

$$\begin{aligned} I + Q + Q^2 + \dots + Q^n &= (Q^{n+1} - I)Q \\ &= Q^{n+2} - Q \end{aligned}$$

Equating the upper right-hand element in this matrix equation, we get the desired summation formula,

$$\sum_{k=1}^n F_k = F_{n+2} - 1$$

Next, we will verify study four 2×2 matrices related to the Q -matrix. Joseph Ercolano of Baruch College, New York, investigated them. They too, have interesting Fibonacci and Lucas implications.

We will begin with a definition. Let A and B be two $n \times n$ matrices. Then A is similar to B if there exist an invertible matrix M such that $A = MBM^{-1}$, that is, $AM = MB$

1) The first matrix we will study is $A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$. How are A and Q related Both have the same characteristic polynomial. $x^2 - x - 1$, and hence the same eigen-values α and β . Both have the same determinant: $|A| = -1 = |Q|$. Both have the same trace $\alpha + \beta = 1$. Finally, Q is similar to A , since $Q = MAM^{-1}$ where $M = \begin{bmatrix} \alpha & 1 \\ 1 & -\alpha \end{bmatrix}$

This is true, since

$$QM = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha & 1 \\ 1 & \alpha \end{bmatrix} = \begin{bmatrix} \alpha^2 & \beta \\ \alpha & 1 \end{bmatrix} = \begin{bmatrix} \alpha & 1 \\ 1 & -\alpha \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ \alpha & \beta \end{bmatrix} = MA$$

Since $Q = MAM^{-1}$, it follows that $Q^n = MAM^{-1}$.

So Q^n is similar to $A^n = \begin{bmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{bmatrix}$. Since similar matrices have the same trace and determinant, it follows that trace

$$A^n = \alpha^n + \beta^n = L_n = F_{n+1} + F_{n+1} = \text{trace}(Q^n)$$

Likewise, $|A^n| = |Q^n|$ yields Cassini's formula for Fibonacci numbers.

We can extract additional properties using the similarity of Q^n and A^n .

Since $Q^n M = M A^n$, we have

$$\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n+1} \end{bmatrix} \begin{bmatrix} \alpha & 1 \\ 1 & -\alpha \end{bmatrix} = \begin{bmatrix} \alpha & 1 \\ 1 & -\alpha \end{bmatrix} \begin{bmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{bmatrix}$$

$$\begin{bmatrix} \alpha F_{n+1} + F_n & F_{n+1} - \alpha F_n \\ \alpha F_n + F_{n+1} & F_n - \alpha F_{n-1} \end{bmatrix} = \begin{bmatrix} \alpha^{n+1} & \beta^n \\ \alpha^n & \beta^{n-1} \end{bmatrix}$$

This implies

$$\alpha F_{n+1} + F_n = \alpha^{n+1} \tag{4.12}$$

$$F_{n+1} - \alpha F_n = \beta^n \tag{4.13}$$

$$\alpha F_n + F_{n+1} = \alpha^n \tag{4.14}$$

$$F_n - \alpha F_{n-1} = \beta^{n-1} \tag{4.15}$$

Notice that Binet's formula for F_n follows from equation (4.14) and (4.13) and also from equations (4.14) and (4.15)

2) The next matrix we will study is $B = \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{5}{4} & \frac{1}{2} \end{bmatrix}$. Then

$$B = \begin{bmatrix} \frac{1}{2} L_1 & F_1 \\ \frac{5}{4} F_1 & \frac{1}{2} L_1 \end{bmatrix}$$

$$B^2 = \begin{bmatrix} \frac{1}{2} L_2 & F_2 \\ \frac{5}{4} F_2 & \frac{1}{2} L_2 \end{bmatrix}$$

$$B^3 = \begin{bmatrix} \frac{1}{2}L_3 & F_3 \\ \frac{5}{4}F_3 & \frac{1}{2}L_3 \end{bmatrix}$$

More generally, we can confirm that

$$B^n = \begin{bmatrix} \frac{1}{2}L_n & F_n \\ \frac{5}{4}F_n & \frac{1}{2}L_n \end{bmatrix}$$

The trace invariance between β^n and A^n yields Binet's formula for L_n . Since Q^n and β^n are similar, they have the same trace; this implies $L_n = F_{n+1} + F_{n-1}$.

$$\frac{1}{4}L_n^2 - \frac{5}{4}F_n^2 = F_{n+1}F_{n-1} - F_n^2;$$

$$\text{That is } L_n - 5F_n^2 = 4(1)^n$$

Similarly, between Q^n and B^n yields the same result.

3) Next, we will investigate the matrix $C = \begin{bmatrix} -1 & 1 \\ -1 & 2 \end{bmatrix}$

$$\text{Then } C^n = \begin{bmatrix} -F_{n-2} & F_n \\ -F_n & F_{n+2} \end{bmatrix}$$

Matrices C^n, Q^n, A^n , and all similar. Similarity with Q^n yields

$$F_{n+2} - F_{n-2} = L_n$$

$$F_{n+2}F_{n-2} = (-1)^{n+1}$$

Trace invariance between C^n and A^n gives $F_{n+2} - F_{n-2} = \alpha^n + \beta^n = L_n$ and the determinant invariance between C^n and B^n gives the identity

$$F_n^2 - F_{n+2}F_{n-2} = \frac{1}{4}L_n^2 - \frac{5}{4}F_n^2$$

$$\text{That is, } L_n^2 = 9F_n^2 - 4F_{n+2}F_{n-2}$$

4) Finally, Consider the matrix $D = \begin{bmatrix} 3 & 1 \\ -5 & -2 \end{bmatrix}$

$$\text{Then } D^n = \begin{bmatrix} L_{n+1} & F_n \\ -5F_n & -L_{n-1} \end{bmatrix}$$

Its similarity with Q^n, A^n, B^n , and C^n yields the following results. You may confirm them.

$$L_{n+1}L_{n-1} + F_{n+1}F_{n-1} = 6F_n^2$$

$$L_{n+1}L_{n-1} - 5F_n^2 = (-1)^{n+1}$$

$$L_n^2 + 4L_{n+1}L_{n-1} = 25F_n^2$$

$$L_{n+2} - L_{n-2} = F_{n+2}F_{n-2}$$

$$L_{n+1}L_{n-1} - F_{n+2}F_{n-2} = 4F_n^2$$

Consequently, both $L_n^2 + 4L_{n+1}L_{n-1}$ and $L_{n+1}L_{n-1} - F_{n+2}F_{n-2}$ are squares.

Next, we introduce another 2×2 matrix R, introduced by Hoggatt and Ruggles in 1964. Coupled with the Q-matrix, it will give us Cassini's formula for Lucas numbers.

4.7 R-MATRIX

The R-matrix is given by $R = \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}$

Using the identities $L_{n+1} = F_{n+1} + 2F_n$, $L_n = 2F_{n+1} - F_n$, $5F_{n+1} = L_{n+1} + 2L_n$ and $5F_n = 2L_{n+1} - L_n$, it follows that

$$\begin{aligned} RQ^n &= \begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \\ &= \begin{bmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{bmatrix} \end{aligned}$$

This implies $\begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} L_{n+1} & L_n \\ L_n & L_{n-1} \end{bmatrix}$; that is

$$\begin{aligned} L_{n-1} - L_n^2 &= (-5)(F_{n+1}F_{n-1} - F_n^2) \\ &= 5(-1)^{n-1} \end{aligned}$$

$$\text{Thus, } L_{n+1}L_{n-1} - L_n^2 = 5(-1)^{n-1} \dots\dots\dots(4.16)$$

This is Cassini's formula for the Lucas family

Next, we will re-derive Cassini's formula for Fibonacci numbers, using Cramer's rule for 2×2 linear systems.

4.8 CASSINI'S FORMULA REVISITED

We will first review Cramer's rule. The 2×2 linear system

$$ax + by = e$$

$$cx + dy = f$$

has a unique solution if and only if $ad - bc \neq 0$.

$$\text{It is given by } x = \frac{\begin{bmatrix} e & b \\ f & d \end{bmatrix}}{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}, \quad y = \frac{\begin{bmatrix} a & e \\ c & f \end{bmatrix}}{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}$$

In particular, consider the linear system

$$F_n x + F_{n-1} y = F_{n+1} \text{ and}$$

$$F_{n-1} x + F_n y = F_{n+2}$$

Since $(F_k, F_{k+1}) = 1$, it follows by the Fibonacci recurrence that $x = 1 = y$ is the unique solution to this system.

$$\text{By Cramer's rule, we then have } y = \frac{\begin{bmatrix} F_n & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix}}{\begin{bmatrix} F_n & F_{n-1} \\ F_{n+1} & F_n \end{bmatrix}} = 1$$

Thus, $F_n F_{n+2} - F_{n+1}^2 = F_n^2 - F_{n-1} F_{n+1}$; that is $F_{n+2} F_n - F_{n+1}^2 = -(F_{n+1} F_{n-1} - F_n^2)$

Let $p_n = F_{n+1} F_{n-1} - F_n^2$. Then this equation yields the recurrence $p_n = -p_{n-1}$ where

$$p_1 = F_2 F_0 - F_1^2 = -1$$

Solving this recurrence, we get $p_n = (-1)^n$

$$\text{Thus, } F_{n+1} F_{n-1} - F_n^2 = (-1)^n$$

Chapter 5

CHAPTER 5

APPLICATION OF FIBONACCI AND LUCAS NUMBERS

5.1 FLOWERS

Fibonacci numbers also appear in plants and flowers. Some plants branch in such a way that they always have a Fibonacci number of growing points. Flowers often have a Fibonacci number of petals, daisies can have 34, 55 or even as many as 89 petals. The number of petals in a flower consistently follows the Fibonacci sequence.

Famous examples include

- 1 petal: White Cally Lily
- 3 petals: Lily, Iris
- 5 petals: Buttercup, Wild Rose, Larkspur, Columbine (Aquilegia)
- 8 petals: Delphiniums
- 13 petals: Ragwort, Corn Marigold, Cineraria,
- 21 petals: Aster, Black-eyed susan, chicory
- 34 petals: Plantain, Pyrethrum
- 55, 89 petals: Michaelmas Daisies



A particularly beautiful appearance of Fibonacci numbers is in the spirals of seeds in a seed head. In sunflower the arrangement of the seeds at its centre appears to be spiralling outwards both to the left and right direction. The pattern of seeds within a sunflower follows the Fibonacci sequence as 1,2,3,5,8,13,21,34,55,89,144.....

Each number in the sequence is the sum of the previous two numbers. In sunflowers, the spirals you see in the centre are generated from this sequence – there are two series of curves winding in opposite directions, starting at the centre and stretching out to the petals with each seed starting at a certain angle from the neighbouring seeds to create the spiral.

At the edge of a sunflower if we count those curves of seeds spiralling to the left as we go outwards, there are 55 spirals. At the same point there are 34 spirals of seeds spiralling to the right. A little further towards the centre and you can count 34 spirals to the left and 21 spirals to the right. The pair of numbers are neighbours in the Fibonacci series.

5.2 FIBONACCI SPIRAL

The Fibonacci numbers are found in the arrangement of seeds on flower heads. There are 55 spirals spiraling outwards and 34 spirals spiraling inwards in most daisy or sunflower blossoms. Pinecones clearly show the Fibonacci spirals. Fibonacci spiral can be found in cauliflower. The Fibonacci numbers can also be found in Pineapples and Bananas (Lin and Peng). Bananas have 3 or 5 flat sides and Pineapple scales have Fibonacci spirals in sets of 8, 13, and 21. Inside the fruit of many plants we can observe the presence of Fibonacci order.



8 parallel rows of
scales spiralling
gradually

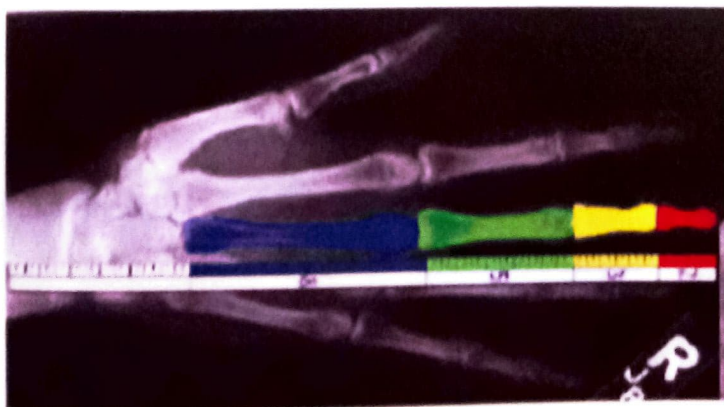
13 parallel rows of
scales spiralling at
a medium slope

21 parallel rows of
scales spiralling
at a steep slope

Fibonacci spiral are also found in various fields associated in nature. It is seen in snail, sea shells, waves, combination of colours; roses etc in so many things created in nature.

5.3 HUMAN HAND AND FINGERS

Humans exhibit Fibonacci characteristics. Every human has two hands, each one of these has five fingers and each finger has three parts which are separated by two knuckles. All of these numbers fit into the sequence. More over the lengths of bones in a hand are in Fibonacci numbers.



Our hand creates a golden section in relation to our arm, as the ratio of our forearm to our hand is 1.618, the Divine Proportion

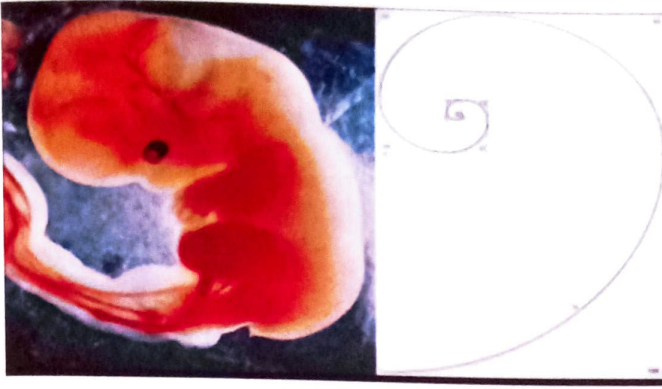


Golden spiral even found in the finger prints of the human.



5.4 HUMAN EMBRYO

During the human embryo development, the human embryo gradually unfolds itself in such a way that it is exactly similar to the golden spiral unfolds itself as it spins farther away from its centre.



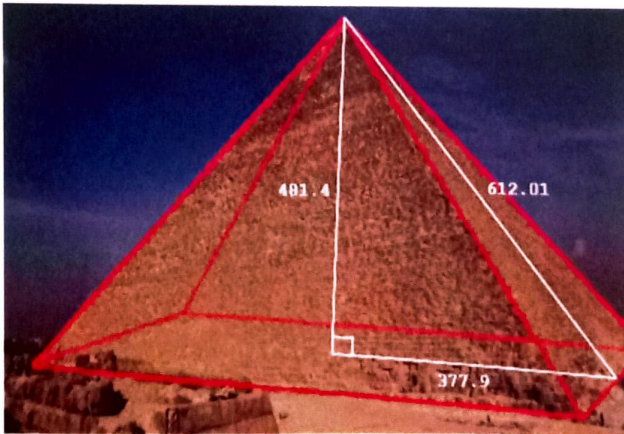
5.5 ARCHITECTURE

One of the earliest examples can be found in the Great Pyramid of Giza

Let b be the base of a triangle which goes from the midpoint of a side of a pyramid to the centre of the square base. Let a be the diagonal up the side of the pyramid from the same midpoint of the side to the very top of the pyramid. For the Great Pyramid, the approximate lengths of a and b are 612.01 feet and 377.9 feet approximately respectively.

$$\frac{a}{b} = \frac{612.01}{377.9}$$

$$= 1.62 \text{ which is very close to the golden ratio}$$



5.6 HUMAN TEETH

The front two incisor teeth form a golden rectangle with a phi ratio in the height to the width. The ratio of the width of the first tooth to the second tooth from the centre is phi. The ratio of the width of the smile to the third tooth from the centre is phi.



5.8 IN POETRY

A limerick, according to Webster's dictionary, is a nonsensical poem of 5 lines, of which the first, second, and fifth have 3 beats, and the other two have 2 beats and rhyme. The following limerick, for example, is made up of 5 lines; they contain 2 groups of 2 beats and 3 groups of 3 beats, a total of 13 beats. Once again, all numbers involved are Fibonacci numbers.

A fly and a flea in a flue	3 beats
Were imprisoned, so what could they do?	3 beats
Said the fly, "Let us flee!"	2 beats
"Let us fly!" said the flea	2 beats
So they fled through a flaw in the flue.	3 beats

Total = 13 beats

G.E. Duckworth analysed the Aeneid, an epic poem written in Latin by Virgil, the "greatest poet of ancient Rome and one of the outstanding poets of the world". Duckworth discovered frequent occurrences of the Fibonacci numbers and several variations in this masterpiece

1, 3, 4, 7, 11, ... ← Lucas sequence

1, 4, 5, 9, 14, ...

1, 5, 6, 11, 17, ...

1, 6, 7, 13, 20, ...

2, 3, 5, 8, 13, ...

3, 7, 10, 17, 27, ...

4, 9, 13, 22, 35, ...

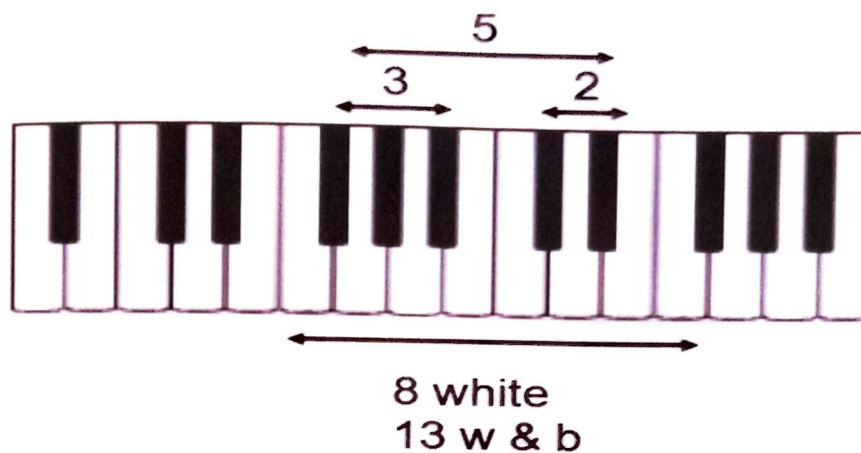
6, 13, 19, 32, 61, ...

The mathematical symmetry Virgil consciously employed in composing the Aeneid brings the harmony and aesthetic balance of music to the ear, since ancient poetry was written to be read out loud. According to Duckworth's investigations into Virgil's structural patterns and proportions, there is evidence that even Virgil's contemporary poets, such as Catullus, Lucretius, Horace and Lucan used the Fibonacci sequence in the structure of their poems. Duckworth's study lends credibility to the theory that the Fibonacci sequence and the Golden Section were known to the ancient Greeks and Romans.

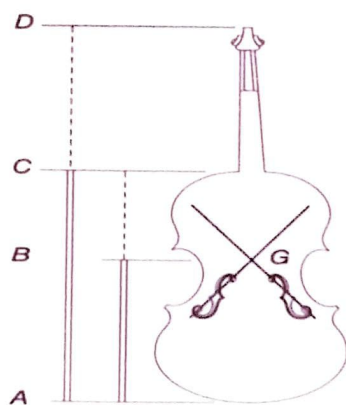
5.9 FIBONACCI IN MUSIC

The Fibonacci sequence of numbers and the golden ratio are manifested in music widely. The numbers are present in the octave, the foundational unit of melody and harmony. Stradivarius used the golden ratio to make the greatest string instruments ever created. Howat's research on Debussy's works shows that the composer used the golden ratio and Fibonacci numbers to structure his music. The Fibonacci Composition reveals the inherent aesthetic appeal of this mathematical phenomenon. Fibonacci numbers harmonize naturally and the exponential growth which the Fibonacci sequence typically defines in nature is made present in music by using

Fibonacci notes. The intervals between keys on a piano of the same scales are Fibonacci numbers.



The golden ratio plays a significant role in the design of the violin, one of the beautiful orchestral instruments. The point B where the two lines through the centres of the f holes intersect, divides the body in the golden ratio $\frac{AB}{BC} = \alpha$



Besides, $\frac{AC}{CD} = \alpha$, so the body and the neck are in the golden proportion.

It now follows that

$$\frac{AD}{AC} = \frac{AC}{AB} = \frac{CD}{BC} = \alpha$$

CONCLUSION:

In this Project, we discussed about the Fibonacci and Lucas numbers and its wide range of applications. We have presented the link between the Matrix and Fibonacci and Lucas numbers. Happily our project revealed that the Fibonacci and Lucas numbers is not only a concept in mathematics but also occurs in our day-to-day life.

REFERENCE:

- [1] Adam, J. A. (2003). Mathematics in nature: Modelling patterns in the natural world, NJ: Princeton University Press.
- [2] Brousseau Alfred (1971), Linear Recursion and Fibonacci Sequence. San Jose: The Fibonacci Association
- [3] Fu. X, Zhou.X(2008), On matrices related with Fibonacci and Lucas numbers, Appl. Math. Compute 100–960.
- [4] Horadam. A. F., (1961), A generalized Fibonacci sequence, Math. Mag. 68 page. 455–459.
- [5] Kalman. D and Mena. R (2003). The Fibonacci Numbers – exposed. Math Magazine.
- [6] Livio. M,(2002) The Golden Ratio: The Story of Phi, The World's Most Astonishing Number, Broadway Books, New York.
- [7] Thomas Koshy, Fibonacci and Lucas numbers with applications Volume One (Second Edition) Framingham State University.
- [8] Thomas Koshy, Fibonacci and Lucas numbers with applications Volume Two (Second Edition) Framingham State University.
- [9] Vajda. S., (1989), Fibonacci & Lucas Numbers and the Golden Section, Theory and Applications, Ellis Horwood Limited.

ORDINARY DIFFERENTIAL EQUATIONS

A project submitted to

ST.MARY'S COLLEGE (Autonomous), THOOTHUKUDI.

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

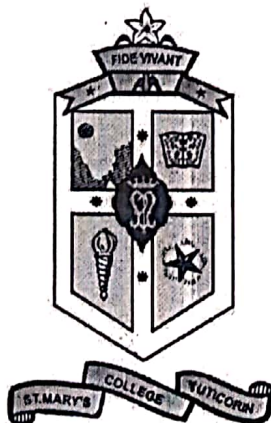
BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NO
J.AUNCY FERDINA	19SUMT03
M.BHAVADHARSHINI	19SUMT07
B.FLORENCE STEFFY	19SUMT11
S.KARTHIGAI DURGA	19SUMT15
K.KAVIYA	19SUMT16

Under the guidance of

Dr. P. ANBARASI RODRIGO M.Sc., B.Ed., Ph.D.,



DEPARTMENT OF MATHEMATICS

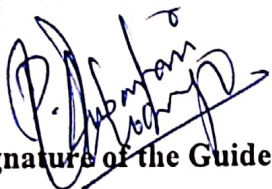
St.Mary's College (Autonomous), Thoothukudi.

May-2022

CERTIFICATE


This is to certify that this project work entitled "ORDINARY DIFFERENTIAL EQUATIONS" is submitted to St.Mary's College (Autonomous), Thoothukudi affiliated to Manonmaniam Sundaranar University, Tirunelveli in partial fulfilment for the award of degree of Bachelor of Science in Mathematics and is the work done during the year 2021-2022 by the following students.

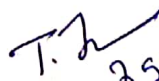
NAME	REGISTER NO
J.AUNCY FERDINA	19SUMT03
M.BHAVADHARSHINI	19SUMT07
B.FLORENCE STEFFY	19SUMT11
S.KARTHIGAI DURGA	19SUMT15
K.KAVIYA	19SUMT16


Signature of the Guide


Signature of the Coordinator


Signature of the Director
Director
Self Supporting Courses
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Principal
Principal
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Examiner
25/5/22

DECLARATION

We hereby declare that the project entitled "ORDINARY DIFFERENTIAL EQUATIONS" submitted for the degree of Bachelor of Science is our work carried out under the guidance of Dr.P.Anbarasi Rodrigo M.Sc., B.Ed., Ph.d., , Department of Mathematics (SSC), St.Mary's College(AUTONOMOUS), Thoothukudi.

J.Auncy Ferdina.
(AUNCY FERDINA. J)

M. Bhavadharshini
(BHAVADHARSHINI. M)

B. Florence Steffy
(FLORENCE STEFFY. B)

S. Karthigai Durga
(KARTHIGAI DURGA. S)

B. Kaviya
(KAVIYA. K)

ACKNOWLEDGEMENT

First of all, we thank the Almighty for showering his blessings to undergo this project.

We express our sincere gratitude and heartfelt thanks to our Principal Rev. Dr. Sr. A. S. J. Lusia Rose M.Sc., PGDCA., M.Phil., Ph.D., and to our Director Rev. Sr. Josephine Jeyarani M.Sc., B.Ed., for kindly permitting us to do this project.

We express our gratitude to Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D., Coordinator, Department of Mathematics (SSC) for her inspirational ideas and Encouragement.

We are very thankful to our guide Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D., Coordinator, Department of Mathematics (SSC) for her efficient and effective guidance. She played a key role in the preparation of this project.

We also thank our staff members for their encouragement in all our efforts. Finally, we thank all those who extended their help regarding this project.

Place: Thoothukudi

Date: 17.05.2022

CONTENT

CHAPTER	TOPIC	PAGE NO.
	Introduction	
1	Preliminaries	1
2	First Order Equations	5
3	Second Order Equations	11
4	Power Series	25
5	Special Functions of Power Series	36
	Conclusion	
	References	

INTRODUCTION

The field of Mathematics plays a vital role in various fields. The place of differential equations in Mathematics. Analysis has been the dominant branch for 300 years and differential equations are the heart of Analysis. In Mathematics the term "Ordinary Differential Equations" also termed as **ODE** is an equation that contains only one independent variable and one or more of its derivatives with respect to the variable. Ordinary Differential Equations have important applications and are a powerful tool in the study of many problems in the natural sciences and in technology and they are exclusively employed in mechanics, astronomy, physics, and in many problems of chemistry and biology. Differentiation can help us solve many types of real world problems.

The Project consists of five chapters.

In chapter 1 , we have given some basic definitions and results on ordinary differential equations that are needed for the subsequent chapters.

In chapter 2 , we have discussed about the first order differential equations.

In chapter 3 , we have discussed about the second order differential equations.

In chapter 4 , we have discussed about the power series of ODE

In chapter 5 , we have discussed about the special functions of power series like regular singular points ,derivation of Frobenius series , Bessel's equation and series and the theorems and problems o

CHAPTER 1

Chapter 1

Preliminaries

Definition: 1.1

A differential equation of the form $f(x,y)dy = g(x,y)dx$ is said to be **homogeneous differential equation** if the degree of $f(x,y)$ and $g(x,y)$ is same.

Definition: 1.2

A function of form $F(x,y)$ which can be written in the form $t^n f(x,y)$ is said to be a homogeneous function of **degree n**, for $k \neq 0$ the differential equation

$M(x,y)dx + N(x,y)dy = 0$ is said to be homogeneous if M and N are **homogeneous function** of the same degree.

Definition: 1.3

The equation $p(x,y)dx + Q(x,y)dy = 0$ is an exact differential equation if there exists a function f of two variables x and y having continuous partial derivatives such that the **exact differential equation** is separated as follows

$$u_x(x,y) = p(x,y) \text{ and } u_y(x,y) = Q(x,y)$$

Therefore, the general solution of the equation is $u(x,y) = c$

Where "C" is an arbitrary constant.

Definition: 1.4

An **integrating factor** is a function by which an ordinary differential equation can be multiplied in order to make it integrable. For example a linear first-order ordinary differential equation of type

$$\frac{dy}{dx} + P(x)y(x) = q(x), \quad \text{-----(1)}$$

Where P and Q are given continuous function, can be made integrable by letting $v(x)$ be a function such that

$$V(x) = \int p(x) dx \text{ and } \frac{dv(x)}{dx} = p(x) \quad \text{-----(2)}$$

Then $e^{v(x)}$ would be the integrating factor such that multiplying by $y(x)$ gives the expression

$$\begin{aligned} \frac{d}{dx} [e^{v(x)}y(x)] &= e^{v(x)} \left[\frac{dy(x)}{dx} + p(x)y(x) \right] \quad \text{-----(3)} \\ &= e^{v(x)}q(x) \end{aligned}$$

Definition: 1.5

Linear Differential Equations is an equation having a variable, a derivative of this variable and a few other functions. The standard form of a linear differential equation is $\frac{dy}{dx} + Py = Q$ and it contains the variable y and its derivatives.

Definition: 1.6

A point x_0 is a **singular point** of the differential equation

$y'' + P(x)y' + Q(x)y = 0$ if one or both of the coefficient function $P(x)$ and $Q(x)$ are not analytic at x_0 .

Definition: 1.7

One of a class of transcendental functions expressible as infinite series and occurring in the solution of the differential equation is called as **Bessel function**.

$$x^2 d^2 y/dx^2 + x dy/dx = (n^2 - x^2)y$$

Definition: 1.8

$$e^{2x-t^2} = \sum_{n=0}^{\infty} \frac{H_n(x)}{n!} t^n = H_0(x) + H_1(x)t + \frac{H_2(x)t^2}{2!} + \dots$$

The function e^{2x-t^2} is called the **generating function of the Hermite polynomial**.

Definition: 1.9

The **Radrigues Formula** for the Hermite Polynomial is given by

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} (e^{-x^2})$$

Definition: 1.10

An **Indicial equation** also called as characteristic equation is a recurrence equation obtained during application of the frobenius series method of solving a second order differential equation.

Definition: 1.11

If two functions $f(x)$ and $g(x)$ are defined on an interval $[a, b]$ and have the property that one function is a constant multiple of the other, then they are said to be **linearly dependent function** on $[a, b]$

If $f(x) = kg(x)$ then $f(x)$ and $g(x)$ are linearly dependent.

Definition: 1.12

If neither of the functions $f(x)$ and $g(x)$ is a constant multiple of the other than they are called **linearly independent**.

Definition: 1.13

An infinite series of the form $y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots$

is called a power series in x . In general $y = \sum_{n=0}^{\infty} a_n (x - x_0)^n$ is a power series in $(x - x_0)$.

Definition: 1.14

For every power series $\sum_{n=0}^{\infty} a_n x^n$ there exists a positive real number R such that series $\sum_{n=0}^{\infty} a_n x^n$ is convergent if $|x| < R$ and divergent if $|x| > R$. The

number R is called **radius of convergent** where $R = \lim_{n \rightarrow \infty} \left(\frac{a_n}{a_{n+1}} \right)$

Definition: 1.15

$f(x) = \sum_{n=0}^{\infty} \frac{f^n(x_0)}{n!} (x - x_0)^n$ is Taylor series of $f(x)$ at x_0

$f(x) = \sum_{n=0}^{\infty} \frac{f^n(0)}{n!} x^n$ is Taylor series in $x_0 = 0$

Definition: 1.16

The point $x = a$ of the interval I is said to an **ordinary point** of the differential equation (1) if each x is analytic at $x = a$.

CHAPTER 2



Chapter 2

First Order Equations

2.1 Homogeneous Equations

Definition: 2.1.1

A differential equation of the form $f(x,y)dy = g(x,y)$ is said to be homogeneous differential equation if the degree of $f(x,y)$ and $g(x,y)$ is same.

Definition: 2.1.2

A function of form $F(x,y)$ which can be written in the form $t^n F(x,y)$ is said to be a homogeneous function of degree n , for $k \neq 0$. The differential equation

$$M(x,y)dx = N(x,y)dy = 0$$

is said to be homogeneous if M and N are homogeneous function of the same degree.

This equation can be written in the form $\frac{dy}{dx} = f(x,y)$ -----(1)

where $f(x,y) = \frac{-M(x,y)}{N(x,y)}$ is clearly homogeneous of degree 0. The procedure for solving

(1) rests on the fact that it can always be changed into an equation with separable variables by mean of the substitution $z = y/x$, regardless of the form of the function $f(x,y)$. To see this we note the relation

$$f(tx,ty) = t^0 f(x,y) = f(x,y)$$

permits us to set $t = 1/x$ and obtain

$$f(x,y) = f(1, \frac{y}{x}) = f(1,z).$$

Then, since $y = zx$ and

$$\frac{dy}{dx} = z + x \frac{dz}{dx'}$$

equation (1) becomes

$$z + x \frac{dz}{dx} = f(1, z),$$

and the variables can be separated :

$$\frac{dz}{f(1, z) - z} = \frac{dx}{x}.$$

We now complete the solution by integrating and replacing z by y/x .

Example: 2.1.3

Solve $(x + y) dx - (x - y) dy = 0$.

Solution:

We begin by writing the equation in the form suggested by the above discussion:

$$\frac{dy}{dx} = \frac{x+y}{x-y}.$$

Since the function on the right is clearly homogeneous of degree 0, we know that it can be expressed as a function of $z = \frac{y}{x}$. This is easily accomplished by dividing numerator and denominator by x :

$$\frac{dy}{dx} = \frac{1 + \frac{y}{x}}{1 - \frac{y}{x}} = \frac{1 + z}{1 - z}$$

We next introduce equation (2) and separate the variables, which gives

$$\frac{(1 - z) dz}{1 + z^2} = \frac{dx}{x}$$

On integration this yields

$$\tan^{-1}z - \frac{1}{2}\log(1 + z^2) = \log x + c ;$$

and when z is replaced by $\frac{y}{x}$, we obtain

$$\tan^{-1}\frac{y}{x} = \log\sqrt{x^2 + y^2} + c \text{ as the desired solution.}$$

2.2 Exact Equations

If we start with a family of curves $f(x, y) = c$, then its differential equation can be written in the form $df = 0$ or

$$\frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy = 0.$$

For example, the family $x^2y^3 = c$ has $2xy^3 dx + 3x^2y^2dy = 0$ as its differential equation. Suppose we turn this situation around, and begin with the differential equation

$$M(x,y)dx + N(x,y)dy = 0. \quad \text{-----}(1)$$

If there happens to exist a function $f(x, y)$ such that

$$\frac{\partial f}{\partial x} = M \quad \text{and} \quad \frac{\partial f}{\partial y} = N, \quad \text{-----}(2)$$

then (1) can be written in the form

$$\frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy = 0 \quad \text{or} \quad df = 0$$

and its general solution is

$$f(x,y) = c.$$

In this case the expression $M dx + N dy$ is said to be an **exact differential**, and (1) is called an **exact differential equation**.

Example : 2.2.1

Test the equation $e^y dx + (xe^y + 2y) dy = 0$ for exactness, and solve it if it is exact. Here we have

$$M = e^y \quad \text{and} \quad N = xe^y + 2y$$

$$\frac{\partial M}{\partial y} = e^y \quad \text{and} \quad \frac{\partial N}{\partial x} = e^y$$

Thus condition (4) is satisfied, and the equation is exact. This tells us that

there exists a function $f(x, y)$ such that

$$\frac{\partial f}{\partial x} = e^y \quad \text{and} \quad \frac{\partial f}{\partial y} = xe^y + 2y$$

Integrating the first of these equations with respect to x gives

$$f = \int e^y dx + g(y) = xe^y + g(y), \text{ so}$$

$$\frac{\partial f}{\partial x} = xe^y + g'(y).$$

Since this partial derivative must also equal $xe^y + 2y$, we have $g'(y) = 2y$, so $g(y) = y^2$ and $f = xe^y + y^2$. All that remains is to note that $xe^y + y^2 = c$ is the desired solution of the given differential equation.

2.3 Integrating Factors

An **integrating factor** is a function used to solve differential equations. It is a function in which an ordinary differential equation can be multiplied to make the function integrable

2.4 Integrating Factor Method

When the given differential equation is of the form $\frac{dy}{dx} + P(x)y = Q(x)$

then the integrating factor is defined as $\mu = e^{\int P(x)dx}$

Example : 2.4.1

Solve the differential equation using the integrating factor: $\frac{dy}{dx} - (3\frac{y}{x} + 1) = (x+1)^4$

Solution:

$$\text{Given: } \frac{dy}{dx} - (3\frac{y}{x} + 1) = (x+1)^4$$

First, find the integrating factor:

$$\mu = e^{\int p(x) dx}$$

$$\mu = e^{\int (-3/(x+1)) dx}$$

$$\int (-3/(x+1)) dx = -3 \int (x+1)^{-1} = -3 \ln(x+1)$$

Hence, we get

$$\mu = e^{-3 \ln(x+1)}$$

$$\mu = 1/(x+1)^3$$

Now, multiply the integrating factor on both the sides of the given differential equation:

$$[1/(x+1)^3] \left[\frac{dy}{dx} - \left[\frac{3y}{(x+1)^4} \right] \right] = (x+1)$$

Integrate both the sides, we get:

$$\left[\frac{y}{(x+1)^3} \right] = \left[\left(\frac{1}{2} \right) x^2 + x + c \right]$$

Here, c is a constant

Therefore, the general solution of the given differential equation is

$$y = [(x+1)^3] \left[\left(\frac{1}{2} \right) x^2 + x + c \right].$$

2.5 Linear Equations

The most important type of differential equation is the linear equation, in which the derivative of highest order is a linear function of the lower order derivatives. Thus the general first order linear equation is $\frac{dy}{dx} = p(x)y + q(x)$ and the general second order linear equation is $\frac{d^2y}{dx^2} = p(x)\frac{dy}{dx} + q(x)y + r(x)$

Example: 2.5.1

Solve the following differential equation: $\frac{dy}{dx} + (\sec x)y = 7$

Solution:

Comparing the given equation with : $\frac{dy}{dx} + Py = Q$

We see, $P = \sec x$, $Q = 7$

Now let's find out the integrating factor using the formula $e^{\int P dx}$

$$\Rightarrow e^{\int \sec x dx} = \text{I.F.}$$

$$e^{\int |\sec x + \tan x|} = \sec x + \tan x$$

Now we can also rewrite the L.H.S as

$$\frac{d(y \times \text{I.F})}{dx}$$

$$\text{i.e. } d(y \times (\sec x + \tan x))$$

$$\Rightarrow \frac{d(y \times (\sec x + \tan x))}{dx} = 7(\sec x + \tan x)$$

Integrating both the sides w. r. t. x , we get,

$$\Rightarrow y = \frac{7|\sec x + \tan x| + \log|\sec|}{(\sec x + \tan x)} + c$$

CHAPTER 3



CHAPTER 3

Second Order Partial Derivatives

3.1 Introduction

In this chapter we discuss an important class of equations. The general second order linear differential equation of the form,

$$\frac{d^2 y}{dx^2} + P(x) \frac{dy}{dx} + Q(x)y = R(x)$$

it be written as $y'' + P(x)y' + Q(x)y = R(x)$ -----(1)

Here $P(x), Q(x), R(x)$ are the functions of x alone. (1) cannot be solved explicitly in

terms of known elementary functions even in terms of indicated integrations. For that we

state the following existence and uniqueness theorem.

Note :

1. If a and b are real numbers such that $a < b$, then the interval consisting of all real numbers x that satisfy the inequalities $a \leq x \leq b$. This is called closed because it contains its endpoints.
2. In the second order equation $y'' + P(x)y' + Q(x)y = R(x)$ if $R(x) = 0$ (identically zero),

then the equation (1) reduces to the homogeneous equation,

$$y'' + P(x)y' + Q(x)y = 0 \dots\dots\dots(2)$$

Theorem: 3.1.1

If y_g is the general solution of the equation (2) and y_p is any particular solution of the complete equation (1), then $y_g + y_p$ is the general equation of $y'' + P(x)y' + Q(x)y = R(x)$

Proof:

The general second order differential equation is

$$y'' + P(x)y' + Q(x)y = R(x) \text{-----(1)}$$

If $R(x) = 0$, then

$$y'' + P(x)y' + Q(x)y = 0 \text{-----(2)}$$

In that y_g is the general solution of (2)

$$y_g'' + P(x)y_g' + Q(x)y_g = 0 \text{------(A)}$$

y_p is the particular solution of (1)

$$y_p'' + P(x)y_p' + Q(x)y_p = R(x) \text{------(B)}$$

Adding (A) and (B), we get,

$$\begin{aligned} y_p'' + y_g'' + P(x)[y_p' + y_g'] + Q(x)[y_p + y_g] &= R(x) \\ (y_p'' + P(x)y_p' + Q(x)y_p) + (y_g'' + P(x)y_g' + Q(x)y_g) &= R(x) \end{aligned} \text{------(3)}$$

$y_p + y_g$ is the solution of (1)

Theorem: 3.1.2

If $y_1(x)$ and $y_2(x)$ are any two solutions of (2), then $c_1y_1(x) + c_2y_2(x)$ ----- (4)

is also a solution for any constants c_1 and c_2

Proof:

The homogeneous equation is

$$y'' + P(x)y' + Q(x)y = 0 \quad \text{-----(1)}$$

$y_1(x)$ be the solution of (1)

$$y_1''(x) + P(x)y_1'(x) + Q(x)y_1(x) = 0$$

And $y_2(x)$ be the solution of (1)

$$y_2''(x) + P(x)y_2'(x) + Q(x)y_2(x) = 0$$

To prove

$c_1y_1 + c_2y_2$ is the solution of (1)

Consider,

$$(c_1y_1 + c_2y_2)'' + P(x)(c_1y_1 + c_2y_2)' + Q(x)(c_1y_1 + c_2y_2) = (c_1y_1'' + c_2y_2'') +$$

$$P(x)(c_1y_1' + c_2y_2') + Q(x)(c_1y_1 + c_2y_2)$$

$$= c_1(y_1'' + P(x)y_1' + Q(x)y_1) + c_2(y_2'' + P(x)y_2' + Q(x)y_2)$$

$$= c_1y_1(x) + c_2y_2(x)$$

$$= c_1(0) + c_2(0)$$

$$= 0 \text{ is the solution of (1)}$$

where the multiples of c_1 and c_2 are zero, because by assumption, y_1 and y_2 are solutions of (2)

Corollary :

Above theorem can be restated as follows: any linear combination of two solutions of the homogeneous equation (2) is also the solution .

Note :

- i) If either y_1 or y_2 is a constant multiple of the other, (i.e.)

$$y_1 = ky_2; \quad y_2 = ky_1$$

Take $y_1 = ky_2$, then

$$c_1 y_1 + c_2 y_2 = c_1 k y_2 + c_2 y_2$$

$$= y_2 (k c_1 + c_2) = c y_2$$

Where $c_1 k + c_2$ is the solution of the homogeneous equation.

- ii) If neither y_1 nor y_2 is a constant multiple of the other ,then

$c_1 y_1(x) + c_2 y_2(x)$ is the general equation of the homogeneous equation (2)

Example: 3.1.3

By inspection ,find the general solution of $y'' = e^x$

Solution:

$$\text{Given } y'' = e^x$$

Integrating both sides ,we get

$$\frac{dy}{dx} = e^x + c_1 \dots (1)$$

where c_1 is a constant ,

Again integrating, $y = c_1 x + c_2 + e^x$ is the general solution of $y'' = e^x$

Example: 3.1.4

Find the particular solution for each following : $x^3y'' + x^2y' + xy = 1$

Solution :

Given equation is $x^3y'' + x^2y' + xy = 1$ (1)

Let y_p be a particular solution of (1)

Take $y_p = \frac{1}{2x}$

$$y_p' = \frac{-1}{2x^2}, y_p'' = \frac{1}{x^3}$$

$$x^3 \cdot \frac{1}{x^3} + x^2 \left[\frac{-1}{2x^2} \right] + x \cdot \left(\frac{1}{x^3} \right) = 1 - \frac{1}{2} + \frac{1}{2} = 1$$

$$y = \frac{1}{2x}$$

Example: 3.1.5

Find the particular solution of the following equation : $y'' - 2y' = 6$

Solution:

Given equation is $y'' - 2y' = 6$ -----(1)

Let y_p the particular solution of (1)

Take $y_p = -3x$

$$y_p' = -3, y_p'' = 0$$

$$y_p'' - 2y_p' = 0 - 2(-3) = 6$$

$$Y = -3x$$

Example: 3.1.6

If a solution of the homogeneous equation on an interval $[a, b]$ is a tangent to the x-axis at any point of this interval, then it must be identically zero. why?

Solution:

Equation of the homogeneous equation is

$$y'' + P(x)y' + Q(x)y = 0 \quad \text{-----(1)}$$

let us take $y(x)$ be the solution of (1) on $[a, b]$.given that it is tangent to the x- axis at any point on $[a, b]$.

Tangent to the x-axis $\Rightarrow y=0$

$$\Rightarrow y'(x)=0$$

$$\Rightarrow y'(x)=0 \text{ on } [a, b]$$

$$(1) \Rightarrow Q(x) y(x) = 0$$

$$\Rightarrow y(x)=0 \text{ (therefore, } Q(x) \neq 0)$$

Since $y(x)$ is the solution of the given equation.

Example: 3.1.7

By eliminating the constants c_1 and c_2 . find the differential equation of the families of the curve, $y = c_1 e^{kx} + c_2 e^{-kx}$

Solution:

Given equation is

$$y = c_1 e^{kx} + c_2 e^{-kx} \quad \text{-----(1)}$$

differentiating (1) both sides

$$y' = c_1 e^{kx} \cdot k + c_2 e^{-kx} \cdot k \quad \text{-----}(2)$$

again differentiating (2) on both sides

$$y'' = c_1 k^2 e^{kx} + c_2 k^2 e^{-kx}$$

$$= k^2(c_1 e^{kx} + c_2 e^{-kx})$$

$$= k^2(y)$$

$$y'' - k^2 y = 0$$

Example: 3.1.8

By eliminating the constants c_1 and c_2 , find the differential equation of the following families of curves : $y = c_1 x + c_2 x^2$

Solution:

$$\text{Given equation is } y = c_1 x + c_2 x^2 \quad \text{-----}(1)$$

Differentiating on both sides,

$$y' = c_1 + 2c_2 x \quad \text{-----}(2)$$

again differentiate,

$$y'' = 2c_2 \quad \text{-----}(3)$$

$$c_2 = \frac{y''}{2}$$

$$y' = c_1 + 2\frac{y''}{2}x = c_1 + y''x$$

$$c_1 = y' - y''x$$

$$y = (y' - y''x)x + \frac{y''}{2}x^2$$

$$= x y' - x^2 y'' + \frac{y''}{2}x^2$$

$$x^2 y'' - 2xy' + 2y = 0$$

Example: 3.1.9

Find the particular solution of the following equation : $y'' - 2y = \sin x$

Solution :

$$y'' - 2y = \sin x \dots (1)$$

let y_p be the particular solution of the equation (1)

$$\text{take } y_p = \frac{-1}{3} \sin x$$

$$y_p' = -\frac{1}{3} \cos x ; y_p'' = \frac{1}{3} \sin x$$

$$y_p'' - 2y_p = \frac{1}{3} \sin x + \frac{2}{3} \sin x = \sin x$$

$$y = -\frac{1}{3} \sin x$$

3.2 The General Solution of a Homogeneous Equations:

Theorem: 3.2.1

Let $y_1(x)$ and $y_2(x)$ be linearly independent solution of the homogeneous equation,

$$y'' + P(x)y' + Q(x)y = 0$$

on the interval $[a, b]$. Then,

$$c_1 y_1(x) + c_2 y_2(x)$$

is the general solution of the equation (1) on this interval $[a, b]$, in the sense that every solution of (1) on this interval can be obtained from (2) by a suitable choice of the arbitrary constants c_1 and c_2 .

Proof:

Let us prove the theorem by means of several lemmas and auxiliary ideas.

Lemma: 1

If $y_1(x)$ and $y_2(x)$ are any two solutions of equation (1) on $[a, b]$, then their wronskian $W = W(y_1, y_2)$ is either identically zero or never zero on $[a, b]$

Proof:

Given that y_1 and y_2 are two solutions of the homogeneous equation (1)

$$\Rightarrow y_1'' + P(x)y_1' + Q(x)y_1 = 0 \quad \text{-----(2)}$$

$$\text{and } y_2'' + P(x)y_2' + Q(x)y_2 = 0 \quad \text{-----(3)}$$

$$W' = W(y_1, y_2)$$

$$= y_1 y_2' - y_2 y_1' \quad \text{-----(A)}$$

$$W' = y_1 y_2'' + y_1' y_2' - y_2 y_1'' - y_1' y_2'$$

$$= y_1 y_2'' - y_2 y_1'' \quad \text{-----(B)}$$

On multiplying the first equation by y_2

$$\Rightarrow y_1'' y_2 + P(x)y_2 y_1' + Q(x)y_2 y_1 = 0 \quad \text{-----(4)}$$

On multiplying the second equation by y_1

$$\Rightarrow y_1 y_2'' + P(x)y_2' y_1 + Q(x)y_1 y_2 = 0 \quad \text{-----(5)}$$

Subtracting the first, from second, we obtain

$$\Rightarrow y_1''y_2 - y_1y_2'' + P(x)(y_2y_1' - y_2'y_1) = 0$$

$$\Rightarrow -W' - P(x)W = 0$$

$$\Rightarrow W' = -P(x)W$$

$$\Rightarrow \frac{W'}{W} = -P(x)$$

$$\Rightarrow \frac{dW}{dx} + P(x)W = 0$$

Integrating both sides

$$\log_e W = \int P(x)dx + \log c$$

$$W = e^{\log W} = e^{-\int P(x)dx + c}$$

$$= c e^{-\int P(x)dx}$$

The general solution of this first order equation is

$$W = c e^{-\int P(x)dx}$$

And since the exponential factor is never zero, we see that W is identically zero, if the constant $c = 0$ on $[a, b]$ and never zero if $c \neq 0$ on $[a, b]$ and the proof is complete.

Lemma: 2

If y_1 and y_2 two solutions of (1) on $[a, b]$, then they are linearly dependent on this interval iff their Wronskian $W(y_1, y_2) = y_1y_2' - y_2y_1'$ is identically zero.

Proof:

Suppose that y_1 and y_2 are the solutions of (1) on $[a, b]$ are linearly dependent.

To prove :

$$W=0 \text{ (i.e.) } y_1 y_2' - y_2 y_1' = 0$$

=> Either of one is a constant multiple of other (or) either one is a zero function.

Case (i)

Suppose that $y_1(x) = 0 \Rightarrow y_1'(x) = 0$

Now, $W(y_1, y_2) = 0$

Case (ii)

Suppose y_2 is the constant multiple of y_1

(i.e.) $y_2 = k y_1$

For some constant $k \Rightarrow y_2' = k y_1'$

$$= y_1 y_2' - y_2 y_1' = y_1 (k y_1') - (k y_1') y_1 = 0$$

$$W(y_1, y_2) = W(y_1, k y_1) = y_1 (k y_1') - y_1 k y_1' = 0$$

Thus if y_1 and y_2 are linearly dependent then their wronskian $W \approx 0$

Conversely suppose that the wronskian is identically zero. (i.e.)

Proof of the main theorem :

y_1 and y_2 are linearly dependent.

If any one of the function is zero, y_1 is identically zero (say) on the interval $[a, b]$, then

$y_1 = 0, y_2$ which is a constant multiple of y_2 .

y_1 and y_2 are linearly dependent.

Assume that y_1 is not identically zero on the interval $[a, b]$.

(i.e.) to prove one is the constant multiple of other.

$y_1 = 0$ on some sub interval $[c,d]$ of $[a,b]$.

since the wronskian is identically zero $[W=0]$ on $[a,b]$, we can divide it by y_1^2 to get,

$$\Rightarrow W=0 \text{ on } [c,d]$$

$$\Rightarrow \frac{W/(y_1^2)}{y_1^2} = 0$$

$$\Rightarrow y_1 y_2' - y_1' y_2 + y_1^2 = 0 \text{ on } [c]$$

thus can be written in the form, $(y_2/y_1)' = 0$ or $y_2(x) = k y_1(x)$

for some constant k and all x in $[c,d]$

y_1 and y_2 are linearly dependent on $[c,d] \Rightarrow W=0$

y_1 and y_2 are linearly dependent on $[a,b]$

since $y_2(x)$ and $k y_1(x)$ have equal values in $[c,d]$, they have equal derivatives.

$$y_2'(x) = k y_1'(x)$$

for all x in $[a,b]$, which concludes the argument

Proof of the main theorem :

From the above lemma 1,2 we get y_1 and y_2 are linearly dependent iff $W=0$

Let $y(x)$ be any solution of the homogeneous equation (1) on $[a,b]$. We must show that constants c_1 and c_2 can be found so that

$$y = c_1 y_1 + c_2 y_2 \text{ and}$$

$$y(x) = c_1 y_1(x) + c_2 y_2(x) \text{ for all } x \text{ in } [a,b]$$

since $c_1 y_1(x) + c_2 y_2(x)$ and $y(x)$ are both solutions of homogeneous equations on $[a,b]$. it suffices to show that for some point x_0 in $[a,b]$, we can find c_1 and c_2 so that

$$y(x_0) = c_1 y_1(x_0) + c_2 y_2(x_0) \quad \text{-----(1)}$$

differentiate on both sides,

$$y'(x_0) = c_1 y_1'(x_0) + c_2 y_2'(x_0) \quad \text{-----(2)}$$

these two equations (1), (2) in c_1 and c_2 have unique solutions when the coefficient of the determinant has a value different from zero,

$$\begin{vmatrix} y_1(x_0) & y_2(x_0) \\ y_1'(x_0) & y_2'(x_0) \end{vmatrix} \neq 0$$

$$\Rightarrow y_1(x_0)y_2'(x_0) - y_1'(x_0)y_2(x_0) \neq 0$$

This leads to investigating the function of x defined by

$$W(y_1, y_2) \neq 0$$

So we get a unique value of c_1 and c_2 corresponding to any point $x_0 \in [a, b]$

Hence the general solution of the differential equation is

$$y = c_1 y_1 + c_2 y_2$$

Example: 3.2.2

Show that e^x and e^{-x} are linearly independent solutions of $y'' - y = 0$

Solution:

$$y'' - y = 0 \quad \text{-----(1)}$$

$$y_1(x) = e^x, \quad y_2(x) = e^{-x}$$

$$y_1'(x) = e^x, \quad y_2'(x) = -e^{-x}$$

$$y_1''(x) = e^x, \quad y_2''(x) = e^{-x}$$

$$y_1'' - y_1 = 0 \quad ; y_2'' - y_2 = 0$$

$$W = \begin{vmatrix} y_1 & y_2 \\ y_1' & y_2' \end{vmatrix}$$

$$= \begin{vmatrix} e^x & e^{-x} \\ e^x & -e^{-x} \end{vmatrix}$$

$$= -e^x e^{-x} - e^{-x} e^x = -2 \neq 0$$

y_1 and y_2 are linearly independent .

e^x and e^{-x} are linearly independent solutions of the given equation.

CHAPTER 4



CHAPTER 4

Power Series

4.1 POWER SERIES:

Definition: 4.1.1

An infinite series of the form $y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots$ is called a power series in x . In general $y = \sum_{n=0}^{\infty} a_n (x - x_0)^n$ is a power series in $(x - x_0)^n$.

Definition: 4.1.2

For every power series $\sum_{n=0}^{\infty} a_n x^n$ there exists a positive real number R such that $\sum_{n=0}^{\infty} a_n x^n$ is convergent, if $|x| < R$ if divergent is $|x| > R$. The number R is called radius of convergent

$$R = \lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right|$$

Derivative of power series:

$$y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$$

The series converges for $|x| < R$ with $R > 0$.

$$\therefore y' = \sum_{n=1}^{\infty} n a_n x^{n-1}$$

$$= a_1 + 2a_2 x + 3a_3 x^2 + \dots + n a_n x^{n-1} + \dots$$

$$y'' = \sum_{n=2}^{\infty} n(n-1) a_n x^{n-2}$$

$$= 2a_2 + 6a_3 x + \dots + n(n-1) a_n x^{n-2} + \dots$$

$\therefore y', y'', y''', \dots, y^n$ is also converges for all $|x| < R$.

Problem: 4.1.3

Find the radius of convergence of given series e^x .

Solution:

$$e^x = 1 + x + \frac{x^2}{2!} + \dots + \frac{x^n}{n!} + \dots$$

$$\text{Here } a_n = \frac{1}{n!}, a_{n+1} = \frac{1}{(n+1)!}$$

$$R = \lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right|$$

$$= \lim_{n \rightarrow \infty} \left| \frac{(n+1)!}{n!} \right|$$

$$= \lim_{n \rightarrow \infty} \left| \frac{(n+1)n!}{n!} \right| = \infty$$

\therefore There series e^x converges for all x .

Problem: 4.1.4

If P is not zero ($P \neq 0$) or a positive integer, show that the

series $\sum_{n=0}^{\infty} \frac{p(p-1)(p-2)\dots(p-n+1)}{n!} x^n$ converges for $|x| < 1$ and diverges for $|x| > 1$.

Solution:

$$a_n = \frac{p(p-1)(p-2)\dots(p-n+1)}{n!}$$

$$a_{n+1} = \frac{p(p-1)(p-2)\dots(p-n)}{(n+1)!}$$

$$R = \lim_{n \rightarrow \infty} \left| \frac{a_n}{a_{n+1}} \right|$$

$$= \lim_{n \rightarrow \infty} \left| \frac{p(p-1)\dots(p-n+1)}{n!} \times \frac{(n+1)!}{p(p-1)\dots(p-n+1)(p-n)} \right|$$

$$= \lim_{n \rightarrow \infty} \left| \frac{(n+1)!}{n!(p-n)} \right|$$

$$= \lim_{n \rightarrow \infty} \left| \frac{(n+1)(n)!}{n!(p-n)} \right|$$

$$= \lim_{n \rightarrow \infty} \left| \frac{n \left(1 + \frac{1}{n}\right)!}{n \left(\frac{p}{n} - 1\right)} \right|$$

$$= 1$$

\therefore This series converges for $|x| < 1$ and diverges for $|x| > 1$.

Definition: 4.1.5

$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!} (x - x_0)^n$ is Taylor Series of $f(x)$ at x_0 .

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n \text{ Taylor Series in } x_0 = 0$$

Example: 4.1.6

Find the Taylor series of $\sin x$

Solution:

$$f(x) = \sin x \quad f(0) = 0$$

$$f'(x) = \cos x \quad f'(0) = 1$$

$$f''(x) = -\sin x \quad f''(0) = 0$$

$$f'''(x) = -\cos x \quad f'''(0) = -1$$

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \dots + \frac{f^{(n)}(0)}{n!}x^n + \dots$$

$$= 0 + \frac{1}{1!}x - \frac{1}{3!}x^3 + \frac{x^5}{5!} - \dots$$

$$\therefore f(x) = \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

4.2 Series Solutions of First Order Differential Equation:

Problem: 4.2.1

Solve $y' = y$ by direct method and power series method and explain any discrepancy.

Solution:

$$\text{Given } y' = y$$

Direct method

$$\frac{dy}{dx} = y \Rightarrow \frac{dy}{y} = dx$$

Integrating both sides we get

$$\log_e y = x + c$$

$$\therefore y = ce^x$$

Power series method

Assume $y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$ is the power series

solution of given differential equation.

$$\text{Given } y' = y$$

$$y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$$

$$y' = a_1 + 2a_2 x + 3a_3 x^2 + \dots + na_n x^{n-1} + (n+1)a_{n+1} x^n + \dots$$

$$a_1 + 2a_2 x + 3a_3 x^2 + \dots + na_n x^{n-1} + (n+1)a_{n+1} x^n + \dots$$

$$y = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$$

Equating the constant term

$$a_1 = a_0$$

Equating the coefficient of x term

$$2a_2 = a_1$$

$$a_2 = \frac{a_1}{2} = \frac{a_0}{2!}$$

Equating the coefficient of x^2 term

$$3a_3 = a_2$$

$$a_3 = \frac{a_2}{3} = \frac{a_0}{2 \cdot 3} = \frac{a_0}{3!}$$

Equating the coefficient of x^n term

$$(n+1)a_{n+1} = a_n$$

$$a_{n+1} = \frac{a_n}{n+1} = \frac{a_0}{(n+1)!}$$

$$\therefore y = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$$

$$= a_0 + a_0 x + \frac{a_0 x^2}{2!} + \dots$$

$$= a_0 \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots + \frac{x^n}{n!} + \dots \right)$$

$$y = a_0 e^x$$

Problem: 4.2.2

Solve $y'x = y$

Solution:

Direct method

$$y'x = y \Rightarrow y = \frac{y}{x} \Rightarrow \frac{dy}{dx} = \frac{y}{x} \Rightarrow \frac{dy}{y} = \frac{dx}{x}$$

Integrating both sides, we get

$$\log y = \log x + \log c$$

$$y = cx$$

Power series method

Assume $y = \sum_{n=0}^{\infty} a_n x^n$ is a solution of the given equation.

$$y' = \sum_{n=1}^{\infty} n a_n x^{n-1}$$

Given $y'x = y$

$$x \sum_{n=1}^{\infty} n a_n x^{n-1} = \sum_{n=0}^{\infty} a_n x^n$$

$$\sum_{n=0}^{\infty} n a_n x^n = \sum_{n=0}^{\infty} a_n x^n$$

$$y = a_1 x + 2a_2 x^2 + \dots$$

$$= a_0 + a_1 x + a_2 x^2 + \dots$$

Equating the constant term

$$a_0 = 0$$

Equating the coefficient of x term

$$a_1 = a_1$$

Equating the coefficient of x^2 term

$$2a_2 = a_2 \Rightarrow a_2 = 0$$

Equating the coefficient of x^3 term

$$3a_3 = a_3 \Rightarrow a_3 = 0$$

Equating the coefficient of the n^{th} term

$$n a_n = a_n \Rightarrow a_n = 0$$

$$\therefore y = a_0 + a_1 x + a_2 x^2 + \dots$$

$$\Rightarrow y = a_1 x$$

From this no change.

4.3 Second Order Differential Equation (Ordinary Points):

Definition: 4.3.1

The point $x = a$ of the interval I is said to an ordinary point of the differential equation I if each $b_1(x)$ is analytic at $x = a$.

Theorem: 4.3

Let x_0 be an ordinary point of the differential equation

$$y'' + P(x)y' + Q(x)y = 0$$

And let a_0 and a_1 be arbitrary constants. Then there exists a unique function $y(x)$ that is analytic at x_0 , is a solution of equation (1) in a certain neighborhood of this point, and satisfies the initial conditions $y(x_0) = a_0$ and $y'(x_0) = a_1$. Furthermore, if the power series expansions of $P(x)$ and $Q(x)$ are valid on an interval $|x - x_0| < R$, $R > 0$, then the power series expansion of this solution is also valid on the same interval.

Proof.

For the sake of convenience, we restrict our argument to the case in which at $x_0 = 0$. This permits us to work with power series in x rather than $x - x_0$ and involves no real loss of generality. With this slight simplification, the hypothesis of the theorem is that $P(x)$ and $Q(x)$ are analytic at the origin and therefore have power series expansions.

$$P(x) = \sum_{n=0}^{\infty} p_n x^n = p_0 + p_1 x + p_2 x^2 + \dots \quad \text{-----(2)}$$

$$Q(x) = \sum_{n=0}^{\infty} q_n x^n = q_0 + q_1 x + q_2 x^2 + \dots \quad \text{-----(3)}$$

that converge on an interval $|x| < R$, for some $R > 0$. Keeping in mind the specified initial conditions, we try to find a solution for (1) in the form of a power series

$$y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots \quad \text{-----(4)}$$

with radius of convergence at least R . Differentiation of (4) yields

$$y' = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n = a_1 + 2a_2 x + 3a_3 x^2 + \dots \quad \text{-----(5)}$$

$$y'' = \sum_{n=0}^{\infty} (n+1)(n+2) a_{n+2} x^n = 2a_2 + 2.3a_3 x + 3.4a_4 x^2 + \dots \quad \text{-----(6)}$$

It now follows from the rule for multiplying power series that

$$\begin{aligned}
 p(x)y' &= \left(\sum_{n=0}^{\infty} p_n x^n \right) \left[\sum_{n=0}^{\infty} (n+1) a_{n+1} x^n \right] \\
 &= \sum_{n=0}^{\infty} \left[\sum_{k=0}^{\infty} p_{n-k} (k+1) a_{k+1} \right] x^n
 \end{aligned}
 \tag{7}$$

$$\begin{aligned}
 q(x)y &= \left(\sum_{n=0}^{\infty} q_n x^n \right) \left(\sum_{n=0}^{\infty} a_n x^n \right) \\
 &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^n q_{n-k} a_k \right) x^n
 \end{aligned}
 \tag{8}$$

On substituting (6), (7), and (8) into (1) and adding the series term by term, we obtain

$$\sum_{n=0}^{\infty} \left[(n+1)(n+2) a_{n+2} + \sum_{k=0}^n p_{n-k} (k+1) a_{k+1} + \sum_{k=0}^n q_{n-k} a_k \right] x^n = 0$$

so we have the following recursion formula for the a_n

$$(n+1)(n+2) a_{n+2} = - \sum_{k=0}^n \left[(k+1) p_{n-k} a_{k+1} + q_{n-k} a_k \right] \tag{9}$$

For $n=0, 1, 2, \dots$ this formula becomes

$$2a_2 = -(p_0 a_0 + q_0 a_0),$$

$$2.3a_3 = -(p_1 a_1 + 2p_0 a_2 + q_1 a_0 + q_0 a_1),$$

$$3.4a_4 = -(p_2 a_1 + 2p_1 a_2 + 3p_0 a_3 + q_2 a_0 + q_1 a_1 + q_0 a_2)$$

Problem: 4.3.3

Find the ordinary point of the differential equation

$$y'' + xy' + (x^2 + 2)y = 0$$

Solution:

$P(x) = x$, $Q(x) = x^2 + 2$ are analytic at all points.

$$\therefore P'(x) = 1, \quad Q'(x) = 2x$$

Every point is an ordinary point.

Using power series method to find the general solution of $y'' = y = 0$

Solution:

$$\text{Given } y'' + 0y' + y = 0$$

$P(x) = 0$ and $Q(x) = 1$ are analytic of all points.

$\Rightarrow P(x)$ and $Q(x)$ are analytic at $x = 0$

$\Rightarrow x = 0$ is an ordinary points.

Assume $y = \sum_{n=0}^{\infty} a_n x^n$ is the solution of the given differential equation.

$$y' = \sum_{n=1}^{\infty} n a_n x^{n-1}$$

$$y'' = \sum_{n=2}^{\infty} n(n-1) a_n x^{n-2}$$

$$y'' + y = 0$$

$$\sum_{n=2}^{\infty} n(n-1) a_n x^{n-2} + \sum_{n=0}^{\infty} a_n x^n = 0$$

$$\sum_{n=0}^{\infty} (n+2)(n+1) a_{n+2} x^n + \sum_{n=0}^{\infty} a_n x^n = 0$$

Equating the coefficient of x^n term

$$(n+2)(n+1) a_{n+2} = -a_n \Rightarrow a_{n+2} = \frac{-a_n}{(n+1)(n+2)}$$

$$n = 3, a_5 = \frac{-a_3}{20} - \frac{a_1}{5!}$$

$$n = 4, a_6 = \frac{-a_4}{30} - \frac{-a_0}{6!}$$

$$\therefore y(x) = a_0 + a_1 x - \frac{a_0 x^2}{2!} - \frac{a_1 x^3}{3!} + \frac{a_0 x^4}{4!} + \dots$$

$$= a_0 \left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots \right) + a_1 \left(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots \right)$$

$$y(x) = a_0 \cos x + a_1 \sin x.$$

Problem: 4.3

Solve the legendre equation by power series method.

Solution:

Legendre's equation is

$$(1-x^2)y'' - 2xy' + P(P+1)y = 0.$$

$$y'' - x^2y'' - 2xy' + P(P+1)y = 0. \quad (1)$$

Divide (1) by $(1-x^2)$, we get

$$y'' - \frac{2x}{1-x^2} y' + \frac{P(P+1)}{1-x^2} y = 0$$

$$P(x) = \frac{-2x}{1-x^2}, \quad Q(x) = \frac{P(P+1)}{1-x^2}$$

$P(x)$ and $Q(x)$ are analytic at $x = 0$

$\therefore x = 0$ is an ordinary point.

Assume $y = \sum_{n=0}^{\infty} a_n x^n$ is the solution of the given differential equation

$$y' = \sum_{n=1}^{\infty} n a_n x^{n-1}$$

$$y'' = \sum_{n=2}^{\infty} n(n-1) a_n x^{n-2} = \sum_{n=0}^{\infty} (n+2)(n+1) a_{n+2} x^n$$

$$y'' - x^2y'' - 2xy' + P(P+1)y = 0$$

$$\sum_{n=0}^{\infty} (n+2)(n+1) a_{n+2} x^n - x^2 \sum_{n=2}^{\infty} n(n-1) a_n x^{n-2}$$

$$- 2x \sum_{n=0}^{\infty} n a_n x^{n-1} + P(P+1) \sum_{n=0}^{\infty} a_n x^n = 0$$

$$\sum_{n=0}^{\infty} [(n+1)(n+2)a_{n+2} + 2 - n(n-1)a_n - 2na_n + P(P+1)a_n] a^n = 0$$

Equating the coefficient of x^n term

$$(n+1)(n+2)a_{n+2} + 2 - n(n-1)a_n - 2na_n + P(P+1)a_n = 0$$

$$(n+1)(n+2)a_{n+2} + 2 = n(n-1)a_n + 2na_n - P(P+1)a_n$$

$$a_n + 2 = \frac{n(n-1)a_n + 2na_n - P(P+1)a_n}{(n+1)(n+2)}$$

$$= \frac{[n(n-1) + 2n - P(P+1)]}{(n+1)(n+2)} a_n$$

$$= \frac{n(n-1+2) - P(P+1)}{(n+1)(n+2)} a_n$$

$$= \frac{n(n+1) - P(P+1)}{(n+1)(n+2)} a_n$$

$$= \frac{n(n+1) - P(P+n+1-n)}{(n+1)(n+2)} a_n$$

$$= \frac{n(n+1) - P(P+n+1)}{(n+1)(n+2)} a_n$$

$$a_n + 2 = \frac{(P+n+1) - (n-P)}{(n+1)(n+2)} a_n$$

$$n=0, a_2 = \frac{-P(P+1)}{2!} a_0$$

$$n=1, a_3 = \frac{(P+2)(1-P)}{6} a_1 = \frac{-(P+2)(P-1)}{3!} a_1$$

$$n=2, a_4 = \frac{(P+3)(2-P)}{12} a_2 = \frac{(P+3)(P-2)(P+1)}{4!} a_2$$

$$n=3, a_5 = \frac{(P+4)(3-P)}{20} a_3 = \frac{(P+4)(P-3)(P+2)(P-1)}{120} a_1$$

$$= \frac{(P+4)(P+2)(P-3)(P-1)}{5!} a_1$$

$$y = a_0 \left[1 - \frac{P(P+1)}{2!} x^2 + \frac{P(P+3)(P+1)(P-2)}{4!} x^4 + \dots \right] + a_1 \left[x - \frac{(P+2)(P-1)}{3!} x^3 + \frac{(P+4)(P+2)(P-3)(P-1)}{5!} x^5 + \dots \right]$$

CHAPTER 5

Special Functions of Power series

5.1 Regular Singular Points

Definition: 5.1.1

- If the functions defined by the product $(x-x_0)P(x)$ and $(x-x_0)^2Q(x)$ are analytic at x_0 . Then x_0 is called the regular singular point of the differential equation.
- If either of the function $(x-x_0)P(x)$ and $(x-x_0)^2Q(x)$ are not analytic at x_0 , then x_0 is called the irregular singular points of the differential equation.

Theorem: 5.1.2

Let x_0 be an ordinary point of the differential equation $y'' + P(x)y' + Q(x)y = 0$ and let a_0 and a_1 be arbitrary constants. Then there exists a unique function $y(x)$ that is analytic at x_0 , is a solution of given equation in a certain neighbourhood of this point, and satisfies the initial conditions $y(x_0) = a_0$ and $y'(x_0) = a_1$. Furthermore, if the power series expansions of $P(x)$ and $Q(x)$ are valid on an interval $|x - x_0| < R$, $R > 0$, then the power series expansion of this solution is also valid on the same interval.

Proof:

For the sake of convenience, we restrict our argument to the case in which $x_0 = 0$. This permits us to work with power series in x rather than $x - x_0$, and involves no real loss of generality. With this slight simplification, the hypothesis of the theorem is that $P(x)$ and $Q(x)$ are analytic at the origin and therefore have power series expansions

$$P(x) = \sum_{n=0}^{\infty} p_n x^n = p_0 + p_1 x + p_2 x^2 + \dots \quad (1)$$

and

$$Q(x) = \sum_{n=0}^{\infty} q_n x^n = q_0 + q_1 x + q_2 x^2 + \dots \quad (2)$$

that converge on an interval $|x| < R$ for some $R > 0$. Keeping in mind the specified initial conditions, we try to find a solution for given equation in the form of a power series

$$y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \dots \quad (3)$$

with radius of convergence at least R . Differentiation of (3) yields

$$y' = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n = a_1 + 2a_2 x + 3a_3 x^2 + \dots \quad (4)$$

$$\text{and } y'' = \sum_{n=0}^{\infty} (n+1)(n+2) a_{n+2} x^n = 2a_2 + 2 \cdot 3a_3 x + 3 \cdot 4a_4 x^2 + \dots \quad (5)$$

It now follows from the rule for multiplying power series that

$$\begin{aligned} P(x)y' &= \left(\sum_{n=0}^{\infty} p_n x^n \right) \left[\sum_{n=0}^{\infty} (n+1) a_{n+1} x^n \right] \\ &= \sum_{n=1}^{\infty} \left[\sum_{k=0}^n p_{n-k} (k+1) a_{k+1} \right] x^n \end{aligned} \quad (6)$$

$$\text{And } Q(x)y = \left(\sum_{n=0}^{\infty} q_n x^n \right) \left(\sum_{n=0}^{\infty} a_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n q_{n-k} a_k \right) x^n \quad (7)$$

On substituting (5), (6), and (7) into given equation and adding the series term by term, we obtain

$$\sum_{n=0}^{\infty} [(n+1)(n+2) a_{n+2} + \sum_{k=0}^n [(k+1) p_{n-k} a_{k+1} + q_{n-k} a_k]] x^n = 0$$

So we have the following recursion formula for the a_n :

$$(n+1)(n+2) a_{n+2} = - \sum_{k=0}^n [(k+1) p_{n-k} a_{k+1} + q_{n-k} a_k] \quad (8)$$

For $n = 0, 1, 2, \dots$ this formula becomes

$$2a_2 = -(p_0a_1 + q_0a_0)$$

$$2 \cdot 3a_3 = -(p_1a_1 + 2p_0a_2 + q_1a_0 + q_0a_1)$$

$$3 \cdot 4a_4 = -(p_2a_1 + 2p_1a_2 + 3p_0a_3 + q_2a_0 + q_1a_1 + q_0a_2)$$

.....

These formulae determine a_2, a_3, \dots in terms of a_0 and a_1 so the resulting series (3) which formally satisfies the given equation and the given initial conditions is uniquely determined by these requirements. Suppose now that we can prove that the series (3), with its coefficients defined by formula (8), actually converges for $|x| < R$. Then by the general theory of power series it will follow that the formal operations by which (3) was made to satisfy the given equation termwise differentiation, multiplication, and term-by-term addition—are justified, and the proof will be complete.

Example 5.1.3

Locate and classify its singular point on the x-axis of the differential equation

$$x^3(x-1)y'' - 2(x-1)y' + 3xy = 0$$

Solution:

$$x^3(x-1)y'' - 2(x-1)y' + 3xy = 0$$

$$y'' - \frac{2}{x^3}y' + \frac{3}{x(x-1)}y = 0$$

$$P(x) = \frac{-2}{x^3} \quad \text{and} \quad Q(x) = \frac{3}{x^2(x-1)}$$

$P(x)$ and $Q(x)$ are not analytic at $x=0$ and $x=1$

Therefore, $x=0$ and $x=1$ are the singular points.

Case (i)

When $x=0$ is a singular point, $xP(x) = \frac{2}{x^3}$ and $x^2Q(x) = \frac{3}{(x-1)}$

Therefore, $x=0$ is an irregular singular point. [Since, $xP(x)$ are not analytic at $x=0$ and $x^2Q(x)$ are analytic at $x=0$]

Case (ii)

When $x=1$ is a singular point, $(x-1)P(x) = \frac{-2(x-1)}{x^3}$ and $(x-1)^2Q(x) = \frac{3(x-1)}{x^2}$

$(x-1)P(x)$ and $(x-1)^2Q(x)$ are analytic at $x=1$ Therefore, $x=1$ is a regular singular point.

[Since, $(x-1)P(x)$ is analytic at $x=1$]

Example : 5.1.4

Determine the nature of the point $x=0$ for $x^3y'' - \sin xy = 0$

Solution:

$$P(x) = 0 \quad \text{and} \quad Q(x) = \frac{\sin x}{x^3}$$

$P(x)$ is analytic at $x=0$ and $Q(x)$ is analytic at $x=0$

$xP(x)$ is analytic at $x=0$ and $x^2Q(x)$ is analytic at $x=0$. Therefore, $x=0$ is an irregular singular point.

5.2 FROBENIUS SERIES:

It is a way to find an infinite series solution for a second order ordinary differential equation of the form $z^2 u'' + p(z)zu' + q(z)u = 0$ in the vicinity of the regular singular point $z=0$

$$y = x^m (a_0 + a_1 x + a_2 x^2 + \dots) = a_0 x^m + a_1 x^{m+1} + \dots$$

$$y' = m a_0 x^{m-1} + a_1 (m+1) x^m + a_2 (m+2) x^{m+1} + \dots$$

$$y'' = m(m-1) a_0 x^{m-2} + a_1 (m+1) m x^{m-1} + a_2 (m+2)(m+1) x^m + \dots$$

$$2x^2 [m(m-1)a_0 x^{m-2} + a_1 (m+1) m x^{m-1} + a_2 (m+2)(m+1) x^m + \dots] + 2x^2 [m a_0 x^{m-1} + a_1 (m+1) x^m + a_2 (m+2) x^{m+1} + \dots] + x [m a_0 x^{m-1} + a_1 x^{m+1} + a_2 x^{m+2} + \dots] - [a_0 x^m + a_1 x^{m+1} + \dots] = 0$$

$$2[m(m-1)a_0 x^m + a_1 (m+1) m x^{m+1} + a_2 (m+1)(m+2) x^{m+2} + \dots] + 2[m a_0 x^{m+1} + a_1 (m+1) x^{m+2} + \dots] + [m a_0 x^m + a_1 x^{m+1} + \dots] - [a_0 x^m + a_1 x^{m+1} + \dots] = 0$$

$$[m(m-1)a_0 + a_1 (m+1) m x + a_2 (m+1)(m+2) x^2 + \dots] + [m a_0 x + a_1 (m+1) x^2 + \dots] + \frac{1}{2} [m a_0 + (m+1) a_1 x + a_2 (m+2) x^2 + \dots] - \frac{1}{2} [a_0 + a_1 x + a_2 x^2 + \dots] = 0$$

$$[m(m-1)a_0 + a_1 (m+1) m x + a_2 (m+1)(m+2) x^2 + \dots] + (\frac{1}{2} + x) [m a_0 + (m+1) a_1 x + (m+2) a_2 x^2 + \dots] - \frac{1}{2} [a_0 + a_1 x + a_2 x^2 + \dots] = 0$$

Equating the constant term,

$$\Rightarrow a_0 m(m+1) + \frac{1}{2} a_0 m - \frac{1}{2} a_0 = 0 \quad \text{--- (1)}$$

We combine corresponding powers of x and equating the coefficient of each power of x to zero,

$$\Rightarrow a_0 m + a_1 \left[(m+1) \left(m + \frac{1}{2} \right) - \frac{1}{2} \right] = 0$$

$$a_0 m + a_1 (m+1)m + \left[\frac{1}{2} (m+1) - \frac{1}{2} \right] a_1 = 0 \quad \text{--- (2)}$$

$$a_2 \left[(m+2)(m+1) + \frac{1}{2} (m+2) - \frac{1}{2} \right] + a_1 (m+1) = 0$$

$$a_0 \neq 0 \Rightarrow (m-1) + \frac{1}{2} m - \frac{1}{2} = 0 \quad \text{--- (3)}$$

This is called the **INDICIAL EQUATION** of the differential equation. Its roots are

$$m^2 - m + \frac{1}{2} m - \frac{1}{2} = 0$$

$$2m^2 - m - 1 = 0$$

$$(m-1) \left(m + \frac{1}{2} \right) = 0$$

$$m = 1 ; m = -\frac{1}{2}$$

For each of this values of m , we now using the remaining (2) to calculate a_1, a_2, \dots in terms of a_0 . For $m=1$ in (2), we get the equation,

$$a_0 + a_1 \left[(1+1) + \frac{1}{2} (1+1) - \frac{1}{2} \right] = 0$$

$$a_0 + 2a_1 + a_1 - \frac{1}{2} a_1 = 0$$

$$\Rightarrow a_0 = \frac{-5}{2} a_1 \quad \text{and} \quad a_1 = \frac{-2}{5} a_0$$

When $m = -\frac{1}{2}$ in (2) we get, $a_1 = -a_0$ and when $m = 1$ in (3) we get, $a_2 = \frac{4}{35} a_0$

When $m = -\frac{1}{2}$ in (3) we get, $a_2 = \frac{1}{2} a_0$

Therefore. We have the following two frobenius seies solution, we put $a_0 = 1$,

$$y_1 = x \left(1 - \frac{2}{5}x + \frac{4}{35}x^2 + \dots \right) \text{ and } y_2 = x^{\frac{-1}{2}} \left(1 - x + \frac{1}{2}x^2 + \dots \right)$$

Example: 5.2.1

Find the indicial equation and the solution of the following equation

$$4x^2 y'' + (2x^4 - 5x)y' + (3x^2 + 2)y = 0$$

Solution:

$$y'' + \frac{2x^4 - 5x}{4x^2} y' + \frac{3x^2 + 2}{4x^4} y = 0$$

$$P(x) = \frac{2x^4 - 5x}{4x^2} = \frac{2x^3 - 5}{4x} \text{ and } Q(x) = \frac{3x^2 + 2}{4x^2}$$

$$xP(x) = \frac{2x^3 - 5}{4} \text{ and } x^2 Q(x) = \frac{3x^2 + 2}{4}$$

When $x=0$, $xP(x)$ and $x^2 Q(x)$ both are analytic at $x=0$. Therefore, $x=0$ is regular singular point.

The initial equation is $m(m-1) + pm + q = 0$

$$m(m-1) - \frac{5}{4}m + \frac{1}{2} = 0$$

$$m^2 - m - \frac{5}{4}m + \frac{1}{2} = 0$$

$$m^2 - \frac{9}{4}m + \frac{1}{2} = 0$$

$$4m^2 - 9m + 2 = 0$$

$$(4m - 1)(m - 2) = 0$$

$$4m = 1 ; m = 2$$

$$= \int_{-\infty}^{\infty} e^{-x^2} [H_n(x)]^2 dx$$

$$= \int_{-\infty}^{\infty} e^{-x^2} [(-1)^n e^{x^2} \frac{d^n(e^{-x^2})}{dx^n}] H_n(x) dx$$

[Since, by RODRIGUES FORMULA, $H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}$]

$$= \int_{-\infty}^{\infty} [(-1)^n \frac{d^n}{dx^n} e^{-x^2}] H_n(x) dx$$

$$u = H_n(x)$$

$$dv = \frac{d^n}{dx^n} (e^{-x^2}) dx$$

$$du = H_n'(x) dx$$

$$v = \frac{d^{n-1}}{dx^{n-1}} e^{-x^2}$$

$$\int u dv = uv - \int v du$$

$$= (-1)^n \left\{ \left[H_n(x) \frac{d^{n-1}}{dx^{n-1}} e^{-x^2} \right]_{-\infty}^{\infty} - \int_{-\infty}^{\infty} H_n'(x) \frac{d^{n-1}}{dx^{n-1}} e^{-x^2} dx \right\}$$

$$= (-1)^{n+1} \int_{-\infty}^{\infty} \frac{d^{n-1}}{dx^{n-1}} e^{-x^2} H_n'(x) dx \quad \text{—————(1)}$$

[Since, $e^{-x^2} \rightarrow 0$ as $x \rightarrow \pm \infty$]

$$\text{Take } u = H_n'(x)$$

$$dv = \frac{d^{n-1}}{dx^{n-1}} e^{-x^2} dx$$

$$du = H_n''(x) dx$$

$$v = \frac{d^{n-1}}{dx^{n-1}} e^{-x^2}$$

Therefore from (1) we get

$$\Rightarrow (-1)^{n+1} \left\{ \left[H_n'(x) \frac{d^{n-2}}{dx^{n-2}} e^{-x^2} \right]_{-\infty}^{\infty} - \int_{-\infty}^{\infty} \frac{d^{n-2}}{dx^{n-2}} e^{-x^2} H_n''(x) dx \right\}$$

Proceeding like this we get,

$$\int_{-\infty}^{\infty} W_m W_n dx = (-1)^{n+n} \int_{-\infty}^{\infty} \frac{d^{n-n}}{dx^{n-n}} e^{-x^2} H_n^{(n)}(x) dx = \int_{-\infty}^{\infty} e^{-x^2} H_n^{(n)}(x) dx$$

$H_n(x)$ is a polynomial of degree n with highest power term as $2^n x^n$

Therefore, $H_n^{(n)}(x) = 2^n n!$

$$\text{Therefore, } \int_{-\infty}^{\infty} W_m W_n dx = \int_{-\infty}^{\infty} e^{-x^2} 2^n n! dx = n! 2^n \int_{-\infty}^{\infty} e^{-x^2} dx$$

$$\int_{-\infty}^{\infty} W_m W_n dx = n! 2^n \sqrt{\pi} \quad (\text{Since, } \int_{-\infty}^{\infty} e^{-x^2} dx = \sqrt{\pi})$$

$$\text{Thus } m = n, \quad \int_{-\infty}^{\infty} W_m W_n dx = n! 2^n \sqrt{\pi}$$

$$\text{When } m \neq n, \quad \int_{-\infty}^{\infty} W_m W_n dx = 0$$

CONCLUSION

In this project, we have learned about Ordinary Differential Equations. Ordinary Differential Equations have important applications and are a powerful tool in the study of many problems in the natural science and technology. They are a very natural way to describe many things in the universe. We have proved many theorems using many concepts in differential equations which are having applications in various fields. These definitions and theorems can be extended to other field of mathematics. They have applications in the variety of fields like Engineering field, Medical fields etc. These equations can be typically solved using either analytical or numerical methods. It is a truism that nothing is permanent except change; and the primary purpose of differential equations is to serve as a tool for the study of change in the physical world.

REFERENCES

- [1] Differential Equations with Historical Applications Third edition , George Simmons.F.,CRC Press Taylor & Francis Group , New York.
- [2] Hale.J , Ordinary Differential Equations , Dover Publications , 2009.
- [3] Hydon P.E , Symmetry Methods for Differential Equations , Cambridge University Press , Cambridge.
- [4] Jordon.D and Smith.P , Nonlinear Ordinary Differential Equations, Third Edition , Oxford University Press , Oxford, 1999.

A STUDY ON GAME THEORY

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

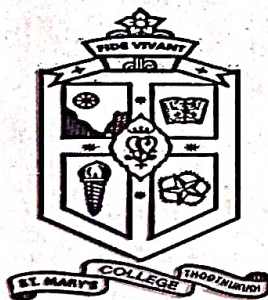
BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NUMBER
M. ANNAMALAI	19SUMT04
G. MUTHU JEROME	19SUMT22
R. MUTHU MARI	19SUMT24
S. RAJA RAJESHWARI	19SUMT33
V. SELVA ANUSHYA BEUVIN	19SUMT36

Under the guidance of

Ms. I. ANBU RAJAMMAL M.Sc., M.Phil., B.Ed., SET.,



DEPARTMENT OF MATHEMATICS

St. Mary's College (Autonomous), Thoothukudi

May - 2022

A STUDY ON GAME THEORY

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

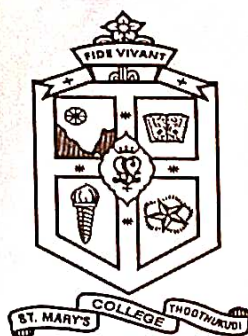
BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NUMBER
M. ANNAMALAI	19SUMT04
G. MUTHU JEROME	19SUMT22
R. MUTHU MARI	19SUMT24
S. RAJA RAJESHWARI	19SUMT33
V. SELVA ANUSHYA BEUVIN	19SUMT36

Under the guidance of

Ms. I. ANBU RAJAMMAL M.Sc., M.Phil., B.Ed., SET.,



DEPARTMENT OF MATHEMATICS

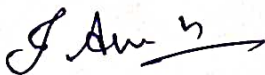
St. Mary's College (Autonomous), Thoothukudi

May - 2022


CERTIFICATE

This is to certify that this project work entitled "A STUDY ON GAME THEORY" is submitted to St. Mary's College (Autonomous), Thoothukudi affiliated to Manonmaniam Sundaranar University, Tirunelveli in partial fulfilment for the award of the degree of Bachelor of Science in Mathematics and is the work done during the year 2021 - 2022 by the following students:

NAME	REGISTER NUMBER
M. ANNAMALAI	19SUMT04
G. MUTHU JEROME	19SUMT22
R. MUTHU MARI	19SUMT24
S. RAJA RAJESHWARI	19SUMT33
V. SELVA ANUSHYA BEUVIN	19SUMT36



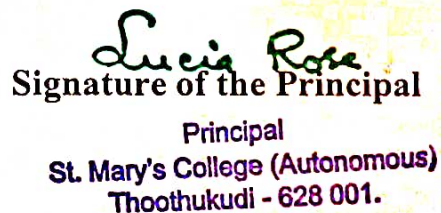
Signature of the Guide



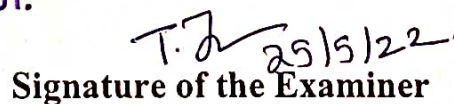
Signature of the Coordinator



Self Supporting Courses
St. Mary's College (Autonomous)
Thoothukudi - 628 001.



Principal
St. Mary's College (Autonomous)
Thoothukudi - 628 001.



Signature of the Examiner

DECLARATION

We hereby declare that, the project entitled "A STUDY ON GAME THEORY" submitted for the degree of Bachelor of Science is our work carried out under the guidance of Ms. I. ANBU RAJAMMAL M.Sc., M.Phil., B.Ed., SET., Assistant Professor, Department of Mathematics (SSC), St. Mary's College (Autonomous), Thoothukudi.

M. Annamalai^o
(ANNAMALAI. M)

P. Muthu Jerome
(MUTHU JEROME. G)

R. Muthu Mari.
(MUTHU MARI. R)

S. Raja Rajeshwari
(RAJA RAJESHWARI. S)

V. Selva Anushya Beuvin.
(SELVA ANUSHYA BEUVIN. V)

ACKNOWLEDGEMENT

First of all, I thank the Almighty for showering his blessing to undergo this project.

We express my sincere gratitude and heartfelt thanks to our Principal **Rev. Dr. Sr. A.S.J. Lucia Rose M.Sc., PGDCA., M.Phil., Ph.D.**, and to our Director **Rev. Sr. Josephine Jeyarani M.Sc., B.Ed.**, for kindly permitting me to do this project.

We express my gratitude to **Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D.**, Coordinator, Department of Mathematics (SSC) for her inspirational ideas and encouragement.

We are very thankful to my guide **Ms. I. Anbu Rajammal M.Sc., M.Phil., B.Ed., SET.**, Assistant Professor, Department of Mathematics (SSC) for her efficient and effective guidance. She played a key role in the preparation of this project.

We also thank my staff members for their encouragement in all our efforts. Finally, we thank all those who extended their help regarding this project.

Place: Thoothukudi

Date: 17.05.2022

CONTENT

CHAPTER	TOPIC	PAGE NUMBER
	Introduction	1
1	Preliminaries	2
2	Two player zero sum games	5
3	Games without saddle point	12
4	Coalitional form of games	35
5	Applications of game theory	45
	Conclusion	49
	References	50

INTRODUCTION

Game theory is an approach to modelling behaviour in situations where the outcome of your decisions depends on the decisions of others. Game theory is the study of strategic, interactive decision making among rational individuals or organizations. Game theory is a branch of applied mathematics that provides tools for analyzing situations in which parties (called players) make decisions that are interdependent. This interdependence causes each player to consider the other player's possible decisions (or strategies) in formulating strategy. In addition, a player need not be an individual; it may be a nation, a corporation, or a team comprising many people with shared interests. A solution to a game describes the optimal decisions of the players, who may have similar, opposed, or mixed interests, and the outcomes that may result from these decisions. Game theory is applied for determining different strategies in the business world. It offers valuable tools for solving strategy problems.

Game theory is not just theory it's also applied in many areas. The use of game theory has expanded and applied to economics, business, biology, computer science, political science, psychology and philosophy. Game theory can describe a number of specific phenomena: interpersonal relations, competition, war and political affairs. From a historical aspects game theory can be identified in the works of ancient philosophers. It is applied to develop theories of ethical or normative behavior. Economists and philosophers have applied game theory to understand rational behavior.

CHAPTER 1

CHAPTER 1

PRELIMINERIES

Definition: 1.1

Game theory is a Mathematical subject that is commonly used in practical life. It is applied to various other non-mathematical fields too. Game theory explains how a strategic game is played. It determines the way or order in which the players should make moves. It considers the information for the players at each decision point.

Definition: 1.2

A competitive situation is called as a **game** if it has the following properties:

1. There are finite number of participants called players.
2. Each player has finite number of strategies available to him.
3. Every game results in an outcome.

Definition: 1.3

In game theory, an **outcome** is a situation which results from a combination of player's strategies. Formally, a path through the game tree, or equivalently a terminal node of the game tree. A primary purpose of game theory is to determine the outcomes of games according to a solution concept.

Definition: 1.4

The expected outcome per play when players follow their optimal strategy is called the **Value of the game**.

Definition: 1.5

If the value of the game is zero (there is no loss or gain for any player), the game is called **Fair game**.

Definition: 1.6

The **Strategy** for a player is the list of all possible actions (or moves or courses of action) that he will take for a every pay-off (outcome) that might arise. It is assumed that the rules governing the choice are known in advance to the players. The outcome resulting from a particular choice is also known to the players in advance and is expressed in terms of numerical values. Here, it is not necessary that players have a definite information about each other strategy.

Definition: 1.7

The particular strategy (or complete plan) by which a player optimises his gains or losses without knowing the competitor's strategies is called **Optimal strategy**. In other word's the strategy that puts the player in the most preferred position irrespective to the strategy of his opponents is called as optimal strategy.

Definition: 1.8

A decision rule which is always used by the player to select the particular course of action. Thus, each player known in advance of all the strategies out of which he always select only one particular strategy irrespective of the strategy others may choose and the objective of the players is to maximize gains or minimize losses. It is known as **pure strategy**.

Definition: 1.9

When both players one guessing as to which course of action is to be selected on a particular occasion with some fixed probability it is a **Mixed strategies game**. Thus, there is a probability situation and objective of the players is to maximize expected gains or to minimize expected losses by making a solution among pure strategies with fixed probabilities.

Definition: 1.10

The pay-off I terms if gains or losses, when players selected their particular can be represented in the form of a matrix, called the **Pay-off matrix**.

Definition: 1.11

A **Saddle point** of a pay- off matrix is that is that position in the pay-off matrix where maximum of row minima coincides with the minima of the column maximal. The saddle point need not be unique.

Definition: 1.12

If in a game the gains of one player are exactly the losses to another player, such that sum of the gains and losses equals zero, then the game is said to be **Zero-sum game**. Otherwise it is said to be **non-zero sum game**.

Definition: 1.13

If a game involves only two players (competitors), then it is called a **two-person game**. However, if the number of players are more than two the game is known as **n-person game**.

Definition: 1.14

A game in coalitional form is said to be of **constant sum** if $v(S) + v(X \setminus S) = v(X)$ For all $S \in P(X)$. If additionally, $v(X) = 0$, the game is described instead as **zero-sum**

Definition: 1.15

A game in coalitional inessential if $\sum_{i=1}^n v(\{i\}) = v(X)$. Otherwise, the game is essential.

Result: 1.16

Any Two Person Zero-Sum game is inessential.

Definition 1.1

A game is a situation in which two or more players must make a decision. The players are called *players* and the decisions are called *moves*.

1.1.1 The Game of *Rock-Paper-Scissors*

The game of *Rock-Paper-Scissors* is a game in which two players, Player 1 and Player 2, must make a decision. The players are called *players* and the decisions are called *moves*. The moves are *Rock*, *Paper*, and *Scissors*. The game is played by two players, Player 1 and Player 2, who must make a decision simultaneously. The game is played by two players, Player 1 and Player 2, who must make a decision simultaneously.

The game is played by two players, Player 1 and Player 2, who must make a decision simultaneously. The game is played by two players, Player 1 and Player 2, who must make a decision simultaneously.

This game is played by two players, Player 1 and Player 2, who must make a decision simultaneously. The game is played by two players, Player 1 and Player 2, who must make a decision simultaneously. The game is played by two players, Player 1 and Player 2, who must make a decision simultaneously.

If the total is odd, Player 1 wins; otherwise, Player 2 wins (giving rise to the negative entries in the above payoff matrix).

The purpose of studying the strategic form is to attempt to determine a strategy for each player that is optimal to each player. The first question for Player 1 is that there is a strategy that always yields the best result for each player of the game. The second question is that there is a strategy that always yields the best result for each player of the game. The third question is that there is a strategy that always yields the best result for each player of the game.

However, we can make a further observation. If Player 1 chooses *Rock*, then Player 2 can choose *Paper* and win. If Player 1 chooses *Paper*, then Player 2 can choose *Scissors* and win. If Player 1 chooses *Scissors*, then Player 2 can choose *Rock* and win. Therefore, there is no strategy for Player 1 that is optimal to each player. The game is a *zero-sum game*.

CHAPTER 2

TWO PLAYER ZERO-SUM GAMES

Definition: 2.1

A game with only two persons is said to be two-person zero-sum game if the gain of one player is equal to the loss of the other.

2.2 2×2 PAYOFF MATRICES

We consider initially the simplest case a 2×2 payoff matrix where each player is presented with a single choice. As a motivational example, consider the game of two finger Morra, described by

$$\begin{pmatrix} -2 & 3 \\ 3 & -4 \end{pmatrix}$$

This game is related to an ancient Roman guessing/gambling game, micare digitis (to flash with fingers); however, in this simple formulation, it is the parity of the total, rather than a successful guess of its value, which determines the victor. Each player reveals either 1 or 2 fingers, with the winnings being the total number of fingers shown. If the total is odd, Player 1 wins; otherwise Player 2 wins (giving rise to the negative entries in the above payoff matrix).

The purpose of studying the strategic form is to attempt to determine a strategy for each player that is in some sense optimal. The ideal scenario for Player 1 is that there is a strategy that always enables him to win any given play of the game. However, such games are likely to be few and far between, and willing participants for the role of Player 2 even rarer.

However, we can more usefully tackle a refinement of this question, namely determining whether there is a strategy for player 1 which, in the long run, they might expect to profit from. For any play of the game, Player 1 can pick either option 1, or option 2. Their return will then depend on the strategy employed by Player 2 for that

particular play. We may suppose that Player 1 chooses option 1 with probability p_1 , either in accordance with some plan or simply by chance; choosing option 2 the rest of the time, i.e., with probability $p_2 = 1 - p_1$. We will refer to this as a mixed strategy, although it is worth nothing the special case of a pure strategy, where $\{p, q\} = \{0, 1\}$ and thus only one options ever used.

The objective for Player 1, therefore, is to devise a mixed strategy that maximizes their payoff. At the same time, Player 2 is trying to minimize the payoff of Player 1, since this maximizes their own pay off (by the zero-sum condition). Whilst neither player is aware of the particular option the other intends to take in a given play of the game, their calculations can take into account this motivation on the part of their opponent. Perhaps surprisingly, this does not descend into endless second- guessing, and should Player 1 find an optimal mixed strategy, they can even safely pre-declare the mix (although not a given move) without giving an advantage to Player 2. We shall illustrate how this arises for 2 finger Morra, then consider generalizations to any 2×2 game. Note, however, that we have once again sidestepped some considerations of utility theory in our acceptance of expected pay out as a good measure of the worth of a game, especial if the number of plays is to be small.

2.2.1 A STRATEGY FOR PLAYER 1

Can Player 1 guarantee a certain minimum (and preferably positive) pay off? Note that if she employs the mixed strategy (p_1, p_2) , then her return depends on the strategy of Player 2;

- If Player 2 opts for '1', then the return for Player 1 is -2 (if she played) or 3 (if she played 2). Thus on average, she may expect a payoff of $-2p_1 + 3p_2$
- If Player 2 opts for '2', then Player 1's expectation is $3p_1 - 4p_2$

If, therefore, we seek an expected payoff of at least V regardless of Player 2's strategy, then we require

$$\bullet -2p_1 + 3p_2 \geq V$$

$$\bullet 3p_1 - 4p_2 \geq V$$

As a first attempt, consider the case of equality:

$$V = -2p_1 + 3p_2 = 3p_1 - 4p_2$$

$$7p_2 = 5p_1$$

$$7(1 - p_1) = 5p_1$$

$$7 = 12p_1$$

$$\frac{7}{12} = p_1$$

Thus we have a mixed strategy $\frac{7}{12}, \frac{5}{12}$ where the expected payoff is $-2\frac{7}{12} + 3\frac{5}{12} = \frac{1}{12} = 3\frac{7}{12} - 4\frac{5}{12}$. So Player 1 can guarantee an expected return of $\frac{1}{12}$ per play (over a large number of plays).

2.2.2 A STRATEGY FOR PLAYER 2

Analogously to the duality theorem in linear programming, we may determine whether it is possible for Player 1 to ensure a greater expectation by seeing whether Player 2 is able to cap their losses at the $\frac{1}{12}$ per play presented above.

In fact, Player 2 can minimize their losses in this way (and thus Player 1 must be content with the value of $\frac{1}{12}$) by the same strategy. For Player 2 the expected payoffs are $2p_1 - 3p_2$ when Player 1 opts for '1' and $-3p_1 + 4p_2$ when she opts for '2'; so with a mixed strategy of $\frac{7}{12}, \frac{5}{12}$ Player 2 expects $-\frac{1}{12}$ in either case.

So, on average, Player 1 values the game as being good for at least $\frac{1}{2}$ per play, whilst Player 2 can ensure it is not worse than $-\frac{1}{2}$ per play for them, i.e., it is at best worth $\frac{1}{2}$ to Player 1. This is an example of general behaviour.

2.3 GAMES WITH SADDLE POINT

A point at which a function of two variables has partial derivatives equal to zero but at which the function has neither a maximum nor a minimum value.

2.3.1 MINIMAX AND MAXIMIN PRINCIPLE:

Consider the pay matrix of a game which represents payoff of player A. Now, the objective of the study is to know how these players must elect their respective strategies so that they may optimize their pay off such a decision making criterion is referred to as the minimax-maximin principle.

For player A minimum value in each row represents the least gain (pay-off) to him if he chose his particular strategy.

These are written in the matrix by row minima. He will then select the strategy that gives largest gain among the row minimum values.

This choice of player A is called the maximin principle, and the corresponding gain is called the maximin value of the game denoted by v .

For player B (who is assumed to be the loser), the maximum value in each column represents the maximum loss to him if he chooses his particular strategy.

These are written in the pay-off by column minima. He will then select the strategy that gives minimum loss among the column maximum values.

This choice of player B is called the minimax principle, and the corresponding loss is the minimax value of the game denoted by v .

Theorem 2.3.2 (Minimax Theorem for a game with a saddle point).

Let a_{ij} be a saddle point for a game in strategy form given by X , Y and A . Then the game has value a_{ij} , achieved when Player 1 plays the pure strategy x_i and Player 2 the pure strategy y_j .

Proof:

Player 1 is guaranteed a payoff of at least a_{ij} by using strategy x_i since for any strategy choice y_j , by Player 2, $A(x_i, y_j) = a_{ij} \geq a_{ij}$ since a_{ij} is the minimum of row i . Thus $V \geq a_{ij}$.

Player 2 is guaranteed a payoff of at least $-a_{ij}$ by using strategy y_j since for any strategy choice x_i by Player 1, the payoff to Player 2 is $-A(x_i, y_j) = -a_{ij} \geq -a_{ij}$ as $a_{ij} \geq a_{ij}$ by virtue of being the maximum of column j .

Thus $-V \geq -a_{ij}$ and so $V \leq a_{ij}$. Hence $V = a_{ij}$ and the pure strategies are x_i, y_j .

2.3.3 Procedure to determine saddle point:

Step 1:

Select the minimum element in each row and enclose it in a rectangle

Step 2:

Select the maximum element in each column and enclose it in a circle

Step 3:

Find out the element which is enclosed by the rectangle as well as the circle.

Such element is the value of the game and that position is called as the saddle point.

Example: 2.3.4

Find the optimal plan for both the player

Player A	Player B				
		I	II	III	IV
	I	-2	0	0	5
	II	4	2	1	3
	III	-4	-3	0	-2
	IV	5	3	-4	2

Solution:

We use maxmin-minimax principle for solving the game.

Player A	Player B					Row Minimum
		I	II	III	IV	
	I	-2	0	0	5	-2
	II	4	2	①	3	1
	III	-4	-3	0	-2	-4
	IV	5	3	-4	2	-6
Column Maximum		5	3	①	5	

Select minimum from the column maximum values.

i.e. Minimax = 1, (marked as circle)

Select maximum from the row minimum values

i.e. Maximin = 1, (marked as rectangle)

Player A will choose strategy II,

which yields the maximum payoff of 1

Player B will choose strategy III,

The value of game is 1, which indicates that player A will gain 1 unit and player B will sacrifice 1 unit.

Since the maximin value = the minimax value = 1. Therefore, the game has saddle point and the game is not fair game (since value of the game is non zero)

Also $\text{maxmin} = \text{minimax} = \text{value of game}$, therefore the game is strictly determinable.

It is a pure strategy game and the saddle point is (A-II, B-III)

The optimal strategies for both players given by pure strategy, Player A must select strategy II and player B must select strategy III.

CHAPTER 3

CHAPTER 3

GAMES WITHOUT SADDLE POINT

Two person zero sum game is a basic model in game theory. There are two players, each with an associated set of strategies, while one player aims to maximize her pay-off, the other player attempts to take an action to minimize this pay-off. In fact, there are several methods for finding solution of games without saddle points.

3.1 MIXED STRATEGIES

There are some games for which no saddle point exists. In such cases both the players must determine an optimal combination of strategies to find a saddle (equilibrium) point. The optimal strategy combination for each player may be determined by assigning to each strategy its probability of being chosen. The strategies so determined are called mixed strategies because they are probabilistic combination of available choices of strategy.

The value of game obtained by the use of mixed strategies represents least pay-off which player (A) can expect to win and the least which player (B) can lose. The expected pay-off to a player in a game with arbitrary pay-off matrix $[a_{ij}]$ of order $m \times n$ is defined as

$$\begin{aligned} E(p, q) &= \sum_{i=1}^m \sum_{j=1}^n p_i a_{ij} q_{ij} \\ &= P^T A Q \text{ (in matrix notation)} \end{aligned}$$

Where, $P = (p_1, p_2, \dots, p_m)$ and $Q = (q_1, q_2, \dots, q_n)$ denotes the mixed strategies for player A and B.

Also, $p_1 + p_2 + \dots + p_m = 1$ and $q_1 + q_2 + \dots + q_n = 1$.

A particular strategy with particular probability a player chooses can also be interpreted as the relative frequency with which a strategy is chosen from the number of strategies of the game.

3.1.1 DOMINANCE PROPERTY OF REDUCING THE SIZE OF THE GAME

We can sometimes reduce the size of a game's pay-off matrix by eliminating a course of action which is so inferior to another as never to be used. Such a course of action is said to be dominated by the other. The concept of dominance is especially useful for the evaluation two – person zero sum games where a saddle point does not exist.

3.1.2 GENERAL RULE

1. If all the elements of a row, say k^{th} are less than or equal to the corresponding elements of any other row, say r^{th} then k^{th} row is dominated by the r^{th} row
2. If all the elements of a column, say k^{th} are greater than or equal to the corresponding elements of any other column, say r^{th} , then k^{th} column is dominated by r^{th} column.
3. Omit dominated rows or columns.
4. If some linear combination of some rows dominates r^{th} row, then r^{th} row will be deleted. Similar argument follows for columns.

Example: 3.1.3

Reduce the size of the game whose matrix is given by

		Player B		
		I	II	III
Player A	I	-4	6	3
	II	-3	-3	4
	III	2	-3	4

Solution:

$\boxed{-4}$	$\textcircled{6}$	3
$\boxed{-3}$	$\boxed{-3}$	$\textcircled{4}$
$\textcircled{2}$	$\boxed{-3}$	$\textcircled{4}$

We observe that no saddle point exists. Consider I^{st} and III^{rd} column's from the player B's point of view we observe that pay-off in the III^{rd} column is greater than the corresponding element in the I^{st} column regardless of player A's strategy.

Evidently, the choice of III^{rd} strategy by the player B will always result in the greater loss compared to that of selecting the I^{st} strategy.

Hence, deleting the III^{rd} column which is dominated by I , the reduced size pay-off matrix is obtained.

	I	II
I	-4	6
II	-3	-3
III	2	-3

Again, if the reduced matrix is looked at from player A's point of view, it is seen that the player A will never use the II^{nd} strategy which is dominated by III .

Hence, the size of the matrix can be reduced further by deleting the II^{nd} row, Hence the reduced matrix is

	I	II
I	-4	6
II	2	-3

3.1.4 DIFFERENT SOLUTION METHODS

A mixed strategies game can be solved by different solution methods such as

1. Algebraic method
2. Arithmetic method
3. Analytical or Matrix method
4. Graphical Method and
5. Linear programming method

These methods will be discussed in detail in the next section

3.2 ALGEBRIC METHOD

This method can be used to determine probability value by using different strategies by players A and B. This method becomes quite lengthy when number of strategies for both are large.

Consider the game where pay-off matrix is $[a_{ij}]_{m \times n}$

Let (p_1, p_2, \dots, p_m) and (q_1, q_2, \dots, q_n) be the probabilities with which players A and B adopt their mixed strategies (A_1, A_2, \dots, A_m) and (B_1, B_2, \dots, B_n) respectively.

If V is the value of game, then the expected gain to player A for this game when player B select strategies one by one is given by left hand side of simultaneous equations respectively.

Since player A is the gainer and expects at least V, we must have where,

$$a_{11}p_1 + a_{12}p_2 + \dots + a_{1m}p_m \geq V$$

$$a_{21}p_1 + a_{22}p_2 + \dots + a_{2m}p_m \geq V$$

⋮

$$a_{n1}p_1 + a_{n2}p_2 + \dots + a_{nm}p_m \geq V$$

where,

$$p_1 + p_2 + \dots + p_m = 1 \text{ and } p_i \geq 0 \forall i$$

Similarly, the expected loss to player B when player A adopts strategies (A_1, A_2, \dots, A_m) can be determined since player B is the loser we must have where,

$$a_{11}q_1 + a_{21}q_2 + \dots + a_{n1}q_1 \geq V$$

$$a_{12}q_1 + a_{22}q_2 + \dots + a_{n2}q_2 \geq V$$

⋮

$$a_{1m}q_1 + a_{2m}q_2 + \dots + a_{nm}q_n \geq V$$

Where, $a_1 + q_2 + \dots + q_n = 1$ and $q_j \geq 0 \forall j$ values of p_i 's and q_j 's from (1) and (2), these inequalities are considered as equations and then solved for given unknowns.

However, if the system of equations so obtained is inconsistent, then at least one of the inequalities must hold as strict inequality. The solution can now be obtained only by applying trial and error method.

Example: 3.2.1

In a game of matching coins with two players, suppose A wins one unit of value when there are two tails and loses $1/2$ unit of value when there is one head and one tail. Determine the pay-off matrix, the best strategies for each player and the value of the game to A

Solution:

The pay-off matrix for the given matching coin game is

PLAYER B

$$\text{PLAYER A} \begin{bmatrix} -1 & -1/2 \\ -1/2 & 0 \end{bmatrix}$$

As the pay-off matrix does not have a saddle point, the game can be solved by algebraic method for player A, let P_1 and P_2 be probabilities of selecting a strategy A_1 and A_2 , respectively.

Then the expected gain to player A when player B uses its B_1 and B_2 strategies is given by,

$$-P_1 - 1/2 P_2 \geq V \quad \text{----- (1)}$$

$$-1/2 P_1 + 0 \cdot P_2 \geq V \quad \text{----- (2)}$$

Where,

$$P_1 + P_2 = 1 \quad \text{----- (3)}$$

From (2) we get $P_1 = -2V$

Substituting the value in (1) we get $P_2 = -6V$

Substituting the value of P_1 and P_2 in (3) we get $P_1 = 0.25, P_2 = 0.75$, and $V = -1/8$

For player B, let q_1 and q_2 be the probabilities of selecting strategies B_1 and B_2 respectively. Then, the expected loss to player B when player A uses its strategies A_1 and A_2 is given by

$$q_1 - 1/2 q_2 \geq V \quad \text{----- (4)}$$

$$-1/2 q_1 + 0 \cdot q_2 \geq V \quad \text{----- (5)}$$

$$q_1 + q_2 = 1 \quad \text{----- (6)}$$

We get, $q_1 = 2V, q_2 = -6V$ substituting the values of q_1 and q_2 in (6). We get $V = -1/8, q_1 = 0.25, q_2 = 0.75$.

Hence the optimal strategies for players A and B are $(0.25, 0.75)$ and $(0.25, 0.75)$ respectively and the value of the game $V = -1/8$.

3.3 ARITHMETIC METHOD

Arithmetic method provides an easy technique for obtaining the optimum strategies for each player in (2×2) games without saddle point this method consists of the following steps.

Step 1

Find the difference of two number in column I put it under the column II neglecting the negative sign if occurs.

Step 2

Find the difference of two numbers in column II, and put it under the column I, neglecting the negative sign if occurs.

Step 3

Repeat the above two steps for the two rows also, the values thus obtained are called the oddments, these are the frequencies with which the players must use their courses of action in their optimum strategies.

Example: 3.3.1

Two players A and B showing each other, put on a table a coin, with head or tail up. A wins ₹ 8 when both the coins show head and ₹ 1 when both are tails. B wins ₹ 3 when the coins do not match. Given the choice of being matching player (A) or non-matching player (B) which one would you choose and what would be your strategy?

Solution:

The pay-off matrix for player A is given by

		Player B	
		H	T
Player A	H	8	-3
	T	-3	1

Since no saddle point, is found that the optimal strategies will be mixed strategies.

Step 1

Taking the difference of two numbers in column I we find $8 - (-3) = 11$ and put it under column II.

Step 2

Taking the difference of two numbers in column II we find $-3 - 1 = -4$ and put number 4 (neglecting negative sign) under column I.

Step 3

Repeat the above two steps for the two rows also, thus for optimum gains, player A musts use strategy H with probability $11/15$ and strategy T with probability $4/15$, while player B musts use strategy H with probability $4/15$ and strategy T with probability $11/15$.

Step 4

To obtain the value of game any of following expressions may be used.

Using B's oddments

$$\begin{aligned} \text{B plays H, value of the game, } V &= ₹ \frac{4 \times 8 + 11 \times (-3)}{11 + 4} \\ &= ₹ \frac{-1}{15} \end{aligned}$$

$$\begin{aligned} \text{B plays T, value of the game, } V &= ₹ \frac{4 \times (-3) + 11 \times 1}{11 + 4} \\ &= ₹ \frac{-1}{15} \end{aligned}$$

Using A's oddments

$$\begin{aligned} \text{A plays H, value of game, } V &= ₹ \frac{4 \times 8 + 11 \times 1}{4 + 11} \\ &= ₹ \left(\frac{-1}{15} \right) \end{aligned}$$

$$\begin{aligned} \text{A plays T, value of game, } V &= ₹ \frac{4 \times (-3) + 11 \times 1}{4 + 11} \\ &= ₹ \left(\frac{-1}{15} \right) \end{aligned}$$

The above values of V are equal only if the sum of the oddments vertically and horizontally are equal cases in which it not so will be discussed later thus, the complete solution of the game is

1. Optimum strategy for A is $\left(\frac{4}{15}, \frac{11}{15} \right)$
2. Optimum strategy for B is $\left(\frac{4}{15}, \frac{11}{15} \right)$
3. Value of the game A is $V = ₹ \frac{-1}{15}$

Thus the player gains $₹ \left(\frac{-1}{15} \right)$, i.e., he loses $₹ \frac{1}{15}$ which B, is turn gets.

Remark: 3.3.2

Even though arithmetic method is easier than the algebraic method but it cannot be applied to larger games.

3.4 MATRIX METHOD

If the pay-off matrix of a game is a square matrix, then optimal strategy mixture as well as value of the game obtained by the matrix method.

The solution of a two person zero sum game with mixed strategies with a square pay-off matrix may be found by using the following formulae.

$$\frac{[1 \ 1] P_{adj}}{[1 \ 1] P_{cof} \begin{bmatrix} 1 \\ 1 \end{bmatrix}} = \text{Player A's optimal strategy}$$

$$\frac{[1 \ 1] P_{cof}}{[1 \ 1] P_{adj} \begin{bmatrix} 1 \\ 1 \end{bmatrix}} = \text{Player B's optimal strategy}$$

Value of the game = (Player A's optimal strategies) \times (Pay-off matrix P_{ij}) \times (Player B's optimal strategies) Where P_{adj} = adjoint matrix.

P_{cof} = cofactor matrix. Player A's optimal strategies are in the form of a row vector and B's optimal strategies are in a form of a column vector.

This method can be used for finding a solution of a game with size more than 2×2 . However, in rare cases, the solution violates.

The solution violates, the nonnegative condition of probabilities that is $p_i \geq 0, q_i \geq 0$ although the requirement $p_1 + \dots + p_m = 1$ or $q_1 + \dots + q_n = 1$ is satisfied.

Example: 3.4.1

Solve the following game after reducing it to a 2×2 game.

Solution:

		Player B		
		B_1	B_2	B_3
Player A	A_1	1	7	2
	A_2	6	2	7
	A_3	5	1	6

Reduction to 2×2 matrix:

In the given Pay-off matrix, the third row is dominated by second row and third column is dominated by the first column.

Hence, by the dominance property, the matrix is reduced in to

		Player B	
		1	7
Player A	2	-6	2
	1		

Calculation of P_{adj} and P_{cof}

$$P_{adj} = \begin{bmatrix} 2 & -7 \\ -6 & 1 \end{bmatrix} \quad \text{and} \quad P_{cof} = \begin{bmatrix} 2 & -6 \\ 7 & 1 \end{bmatrix}$$

$$\text{Player A's optimal strategies} = \frac{[1 \ 1] \begin{bmatrix} 2 & -7 \\ -6 & 1 \end{bmatrix}}{[1 \ 1] \begin{bmatrix} 2 & -7 \\ -6 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix}} = \frac{[-4 \ -6]}{-10} = \frac{[4 \ 6]}{10}$$

This solution can be broken into the optimal strategy combination for player A as $P_1=4/10=2/5$ and $P_2=6/10=3/5$, where P_1 and P_2 represents the probabilities of player A's using his strategies A_1 and A_2 respectively.

Similarly, the optimal strategy combination for player B's optimal strategies.

$$= \frac{\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & -6 \\ -7 & 1 \end{bmatrix}}{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 2 & -6 \\ -6 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix}} = \frac{\begin{bmatrix} -5 & -5 \\ -10 & -10 \end{bmatrix}}{-10} = \frac{\begin{bmatrix} 5 & 5 \\ 10 & 10 \end{bmatrix}}{10}$$

This solution can also be broken down into the optimal strategy combination for player B is obtained as player B as $q_1 = 5/10=1/2$ and $q_2=5/10=1/2$, where q_1 and q_2 represent the probabilities of player B's using the strategies B_1 and B_2 , respectively

Value of the game

$$v = \begin{bmatrix} 2/3 & 3/5 \end{bmatrix} \begin{bmatrix} 1 & 7 \\ 6 & 2 \end{bmatrix} \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} = 4$$

3.4.2 ANOTHER FORM OF MATRIX METHOD: (matrix oddment method for $n \times n$ games)

Algorithm:

Step 1

Let $A = (a_{ij})_{n \times n}$ be a pay-off matrix of a game.

Obtain a new matrix C, whose first column is obtained from A by subtracting the second column from the first.

The second column is obtained by subtracting A's third column from the second column and so on until the last column of A is taken care of.

Thus, c is an $n \times (n-1)$ matrix.

Step 2

Obtain a new matrix R, from A, by subtracting its successive rows from the preceding ones, in exactly the same manner as was done for columns in step 1.

Thus R is an $(n-1) \times n$ matrix.

Step 3

Determine the magnitude of oddments corresponding to each row and each column of A .

The oddment corresponding to the i_{th} row of A is defined as the determinant $|C_i|$ where C_i is obtained from C by deleting the i_{th} row.

Similarly,

the oddment corresponding to the j_{th} column of $A = |R_j|$ is defined as the determinant where R_j is obtained from R by deleting the j_{th} column.

Step 4

Write the magnitude of oddments (after ignoring negative signs, if any against their respective rows and columns).

Step 5

Check whether the sum of the row oddments is equal to the sum of column oddments.

If so, the oddments expressed as fractions of the grand total yields the optimum strategies.

If not, the method fails.

Step 6

Calculate the expected value of the game corresponding to the optimum mixed strategies determine above for the row player (against any move of the column player).

Example: 3.4.3

Solve the following problem by the method of matrices

$$\begin{matrix} & & & B \\ A & \begin{bmatrix} 1 & 0 & 2 \\ 3 & 0 & 0 \\ 0 & 2 & 1 \end{bmatrix} \end{matrix}$$

Solution:

The matrices C and R are as follows

$$C = \begin{bmatrix} 1 & -2 \\ 3 & 0 \\ -2 & 1 \end{bmatrix} \quad R = \begin{bmatrix} -2 & 0 & 2 \\ 3 & -2 & -1 \end{bmatrix}$$

Now,

$$C_1 = \begin{vmatrix} 3 & 0 \\ -2 & 1 \end{vmatrix} = 3 - 0 = 3$$

$$C_2 = \begin{vmatrix} 1 & -2 \\ -2 & 1 \end{vmatrix} = 1 - 4 = -3$$

$$C_3 = \begin{vmatrix} 1 & -2 \\ 3 & 0 \end{vmatrix} = 0 + 6 = 6$$

$$R_1 = \begin{vmatrix} 0 & 2 \\ -2 & -1 \end{vmatrix} = 0 + 4 = 6$$

$$R_2 = \begin{vmatrix} -2 & 2 \\ 3 & -1 \end{vmatrix} = 2 - 6 = -4$$

$$R_3 = \begin{vmatrix} -2 & 0 \\ 3 & -2 \end{vmatrix} = 4 - 0 = 4$$

The augmented pay-off matrix is

				Row oddments
	1	0	2	3
	3	0	0	3
	0	2	1	6
Column oddments	4	4	4	12

Sum of columns oddments = Sum of row oddments

Thus optimum strategies for Player A are $\left(\frac{3}{12}, \frac{3}{12}, \frac{6}{12}\right)$ or $\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{2}\right)$

The optimum strategies for Player B are $\left(\frac{4}{12}, \frac{4}{12}, \frac{4}{12}\right)$ or $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$

The value of the game, $v = 1 \times \frac{1}{4} + 3 \times \frac{1}{4} + 0 \times \frac{1}{2} = 1$.

3.5 GRAPHICAL METHOD

The Graphical method is useful for the game where the pay-off matrix is of the size $2 \times n$ or $m \times 2$. That is, the game with mixed strategies that only two pure strategies for one of the players in the Two Person Zero-sum game.

Optimal strategies for both the players assign non-zero Probabilities to the same number of pure strategies. Therefore, if one player has only two strategies, the other will also use the same number of strategies.

Hence, this method is useful in finding out which of the two strategies can be used. Consider the $2 \times n$ pay-off matrix of a game without saddle points

$$\begin{array}{c} \text{Player B} \\ B_1 \quad B_2 \dots B_n \\ \text{Player A} \quad \begin{bmatrix} A_1 & a_{11} & a_{12} \dots & a_{1n} \\ A_2 & a_{21} & a_{22} \dots & a_{2n} \end{bmatrix} \end{array}$$

Let the mixed strategy for player A is given by $S_A = \begin{bmatrix} A_1 & A_2 \\ P_1 & P_2 \end{bmatrix}$,

Where $P_1 + P_2 = 1$ and $P_1 \geq 0, P_2 \geq 0$

Now for each of the pure strategies available to B, expected pay-off for player A would be as follow

B's pure move	A's expected pay-off E(P)
B_1	$E_1(P) = a_{11}P_1 + a_{21}P_2$
B_2	$E_2(P) = a_{12}P_1 + a_{22}P_2$
\vdots	\vdots
B_n	$E_n(P) = a_{1n}P_1 + a_{2n}P_2$

The player B would be like to choose that pure move B_j against for which $E_j(P)$ is a minimum for $j = 1, \dots, n$. Let us denote this minimum expected pay-off for A by,

$$v = \min\{E_j(P), j = 1, \dots, n\}$$

The objective of player A is select P_1 and hence P_2 in such a way that v is as large as possible.

This may be done by plotting the straight lines. $E_j(P) = a_{1j}P_1 + a_{2j}P_2 = (a_{1j} - a_{2j})P_1 + a_{2j} (j = 1, 2, \dots, n)$ as linear function of P_1 .

The highest point on the lower boundary of these lines will give maximum expected pay-off among the minimum expected pay-off's on the lower boundary (lower envelope) and the optimum value of the probability P_1 and P_2 .

Now the two strategies for player B corresponding to those lines which pass through the maximum point can be determined.

It helps in reducing the size of the game to (2×2) .

The $(m \times 2)$ games are also treated in the same way except that the upper boundary (upper envelope) of the straight lines corresponding to B's expected pay-off will give a maximum expected pay-off to player B and the lowest point on this boundary will then give the minimum expected pay-off (minimax value) and the optimum value of probability q_1 and q_2 .

Example: 3.5.1

Solve the following 2×5 graphically

	Player B					
	B_1	B_2	B_3	B_4	B_5	
Player A	A_1	2	-1	5	-2	6
	A_2	-2	4	-3	1	0

Solution:

The game does not have a saddle point. Let the probability of player A playing A_1 and A_2 in the strategy combination is denoted by P_1 and P_2 , respectively where $P_2 = 1 - P_1$.

Then, the expected pay-off (gain) to player A will be

B's pure strategy	A's expected pay-off (EI)
B_1	$P_1 - 2P_2$
B_2	$-P_1 + 4P_2$
B_3	$5P_1 - 3P_2$
B_4	$-2P_1 + P_2$
B_5	$6P_1 + 0P_2$

This five expected pay-off lines are plotted on the graph below.

Here, P_1 is measured on the x-axis. Since, P_1 cannot exceed 1, the x-axis is cut-off at $P = 1$.

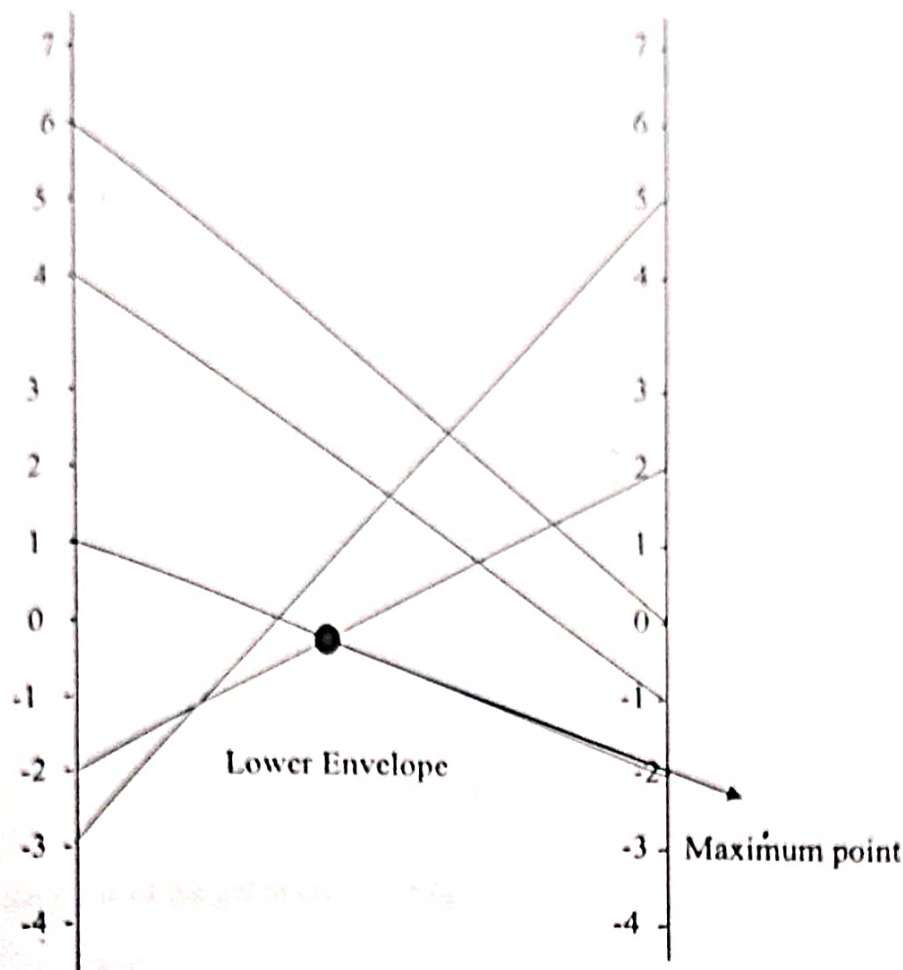
The expected pay-off of player A is measured along y-axis.

From the game matrix, if player B plays B_1 , the expected pay-off of player A is 2 when A plays A_1 with P_1 and -2 when A plays A_2 with $P_1 = 0$.

These two extreme points are connected by a straight line, which shows the expected pay-off of A when B plays B_1 .

Four other straight lines are similarly drawn for B_2, B_3, B_4 and B_5 .

GRAPH



The maximum point shows that the reduced pay-off matrix is for player A is

Player B

B_1 B_2

$$\text{Player A } \begin{matrix} A_1 \\ A_2 \end{matrix} \begin{bmatrix} 2 & -2 \\ -2 & 1 \end{bmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Let $S_A = \begin{pmatrix} A_1 & A_2 \\ P_1 & P_2 \end{pmatrix}$ be the mixed strategy for player A. Then, the strategies

for player A. Then,

$$P_1 = \frac{a_{22} - a_{21}}{(a_{11} + a_{22}) - (a_{12} + a_{21})} = \frac{1 - (-2)}{(2 + 1) - (-2 - 2)} = \frac{3}{7} \quad \text{and,}$$

$$P_2 = 1 - P_1 = 1 - \frac{3}{7} = \frac{4}{7}$$

Let,

$S_B = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 & B_5 \\ q_1 & 0 & 0 & q_2 & 0 \end{pmatrix}$ be the optimum strategies for player B. The

$$q_1 = \frac{a_{22} - a_{12}}{(a_{11} + a_{22}) - (a_{12} + a_{21})} = \frac{1 - (-2)}{(2+1) - (-2-2)} = 3/7 \text{ and}$$

$$q_2 = 1 - q_1 = 4/7$$

Value of the game

$$v = \frac{a_{11}a_{22} - a_{21}a_{12}}{(a_{11} + a_{22}) - (a_{12} + a_{21})} = \frac{2(1) - (-2)(-2)}{(2+1) - (-2-2)} = -2/7$$

The optimum strategies are given by

$$S_A = \begin{pmatrix} A_1 & A_2 \\ 3/7 & 4/7 \end{pmatrix}$$

$$S_B = \begin{pmatrix} B_1 & B_2 & B_3 & B_4 & B_5 \\ 3/7 & 0 & 0 & 4/7 & 0 \end{pmatrix}$$

And the value of the game is $v = -2/7$

Remark: 3.5.2

We observe that by using graphical method, the $2 \times n$ game is converted into a 2×2 game and then solved by using standard method

3.6 LINEAR PROGRAMMING METHOD

A two person zero sum game can also be solved by linear programming approach. The major advantage of using linear programming technique is that it solves mixed strategy of any size.

To illustrate the connection between a game problem and linear programming.

Let us consider $(m \times n)$ pay-off matrix (a_{ij}) for player A

Let $S_A = \begin{bmatrix} A_1 & \dots & A_m \\ A_1 & \dots & A_m \end{bmatrix}$ and $S_B = \begin{bmatrix} B_1 & \dots & B_n \\ q_1 & \dots & q_n \end{bmatrix}$ be the optimum strategies for

player A and player B.

Then, $\sum_{i=1}^m p_i = \sum_{j=1}^n q_j = 1$.

Then the expected gains $g_j (j = 1, \dots, n)$ of player A against B 's pure strategies will be

$$g_1 = a_{11}p_1 + a_{21}p_2 + \dots + a_{m1}p_m$$

$$g_2 = a_{12}p_1 + a_{22}p_2 + \dots + a_{m2}p_m$$

\vdots

$$g_m = a_{1n}p_1 + a_{2n}p_2 + \dots + a_{mn}p_m$$

And the expected loss $l_i (i = 1, \dots, n)$ player B against A 's pure strategies will be

$$l_1 = a_{11}q_1 + a_{12}q_2 + \dots + a_{1n}q_n$$

$$l_2 = a_{21}q_1 + a_{22}q_2 + \dots + a_{2n}q_n$$

\vdots

$$l_n = a_{n1}q_1 + a_{n2}q_2 + \dots + a_{nn}q_n$$

The objective of player A is to select $P_i (i = 1, 2, \dots, m)$ such that he can maximise his minimum expected gains and the player B desires to select $q_j (j = 1, 2, \dots, n)$ that will minimize his expected loss. Thus if we left,

$$U = \min_j \sum_{i=1}^m a_{ij} p_i \quad (j = 1, 2, \dots, n) \text{ and}$$

$$V = \max_i \sum_{j=1}^n a_{ij} q_j \quad (i = 1, 2, \dots, m)$$

The problem of two players could be

Player A: Maximise $u = \minimize \frac{1}{u} = \sum_{i=1}^m \frac{p_i}{u}$ subject to the constraints

$$\sum_{i=1}^m a_{ij} p_i \geq u \text{ and } \sum p_i = 1$$

$$P_i \geq 0 (i = 1, 2, \dots, m)$$

Player B: Minimize $v = \maximize \frac{1}{v} = \sum_{j=1}^n \frac{q_j}{v}$ subject to the constraints

$$\sum_{i=1}^m a_{ij} q_j \leq v \text{ and } \sum q_i = 1$$

$$q_j \geq 0 (j = 1, 2, \dots, n)$$

Assuming $u > 0, v > 0$, introduce a new variable defined by

$$p_i^1 = \frac{p_i}{u} \text{ and } q_j^1 = \frac{q_j}{v} \quad (i = 1, 2, \dots, m, j = 1, 2, \dots, n)$$

Then, the pair of linear programming can be written as

Player A: Minimise

$$P_0 = p_1^1 + p_2^1 + p_3^1 + \dots + p_m^1 \text{ subject to}$$

$$a_{1j}p_1^1 + a_{2j}p_2^1 + \dots + a_{mj}p_m^1 \geq 1$$

$$p_i^1 \geq 0 \quad (i = 1 \text{ to } m \text{ and } j = 1 \text{ to } n)$$

It is easy to note that the LPPs of the 2 players represent a primal dual pair.

Therefore, by fundamental theorem of duality one can read the optimum solution of one player, just from the optimum simplex table of the opponent.

That is, solve one player's LPP.

Remark: 3.6.1

In case there are negative elements in the pay-off matrix and suitable constant, then value of the game = value of the game – constant.

Example: 3.6.2

Solve the following game by using simplex method

	Player B		
Player A	1	-1	3
	3	5	-3
	6	2	-2

Solution:

Since, some of the entries in the pay-off matrix are negative, we add a suitable constant, say $c=4$ to each element.

	Player B		
Player A	5	3	7
	7	9	1
	10	6	2

Let the strategies for 2 players be

$$S_A = \begin{bmatrix} A_1 & A_2 & A_3 \\ P_1 & P_2 & P_3 \end{bmatrix}$$

$$S_B = \begin{bmatrix} B_1 & B_2 & B_3 \\ q_1 & q_2 & q_3 \end{bmatrix}$$

Where, $P_1 + P_2 + P_3 = 1, q_1 + q_2 + q_3 = 1$.

The linear programming problem for B is

Minimise $v =$ Maximize $\frac{1}{v} = y_1 + y_2 + y_3$ subject to

$$5y_1 + 3y_2 + 7y_3 \leq 1,$$

$$7y_1 + 9y_2 + y_3 \leq 1,$$

$$10y_1 + 6y_2 + 2y_3 \leq 1$$

$y_{ij} \geq 0$ for $j = 1, 2, 3$ where $y_j = \frac{q_j}{v}$ $j = 1, 2, 3$ introduce slack variable $S_1 \geq$

$0, S_2 \geq 0$ and $S_3 \geq 0$

Starting table:

Table 1

We observe that y_3 enters in to the basis and S_1 leaves the basis

		C_j	1	1	1	0	0	0	
C_B	Y_B	X_B	y_1	y_2	$y_3 \downarrow$	s_1	s_2	s_3	Min ratio
0	S_1	1	5	3	7	1	0	0	$1/7$
0	S_2	1	7	9	1	0	1	0	$1/1$
0	S_3	1	10	6	2	0	0	1	$1/2$
$Z_j - C_j$			-1	-1	-1	0	0	0	

First iteration:

Introduce and drop S_3

Table 2

		C_j	1	1	1	0	0	0	
C_B	Y_B	X_B	y_1	y_2	y_3	s_1	s_2	s_3	Min ratio
-1	y_3	$1/7$	$5/7$	$3/7$	1	$1/7$	0	0	$1/3$
0	$S_2 \leftarrow$	$6/7$	$44/7$	$60/7$	0	$-1/7$	1	0	$1/10$
0	S_3	$5/7$	$60/7$	$36/7$	0	$-2/7$	0	1	$5/36$
$Z_j - C_j$			$-2/7$	$-4/7$	0	$1/7$	1	0	

We observe that y_2 enters the basis and S_1 leaves the basis.

Second iteration:

			1	1	1	0	0	0
C_B	Y_B	X_B	y_1	y_2	y_3	s_1	s_2	s_3
1	y_3	$1/10$	$2/5$	0	1	$3/20$	$-1/20$	0
1	y_2	$1/10$	$11/15$	1	0	$-1/60$	$7/60$	0
0	s_3	$1/5$	$24/5$	0	0	$-1/5$	$-3/5$	1
$Z_j - C_j$		$1/5$	$2/5$	0	0	$2/15$	$1/15$	0

Since all the $Z_j - C_j \geq 0$, current solution is optimum

$$1/v = 1/5, v = 5$$

The value of the game, $v = 5 - 4 = 1 = v - 4$

Optimum strategies for B are

$$q_1 = 0, q_2^1 = 1/10 \times 5 = 1/2$$

$$q_3^1 = 1/10 \times 5 = 1/2$$

Making use of duality, the optimum strategies for player A are obtained.

$$p_1^1 = \frac{2}{15} \times 5 = 2/3,$$

$$p_2^1 = \frac{1}{10} \times 5 = 1/2,$$

$$p_3^1 = 0.$$

CHAPTER 4

CHAPTER 4

COALITIONAL FORM OF GAMES

4.1 COALITIONAL FORM FOR n -PLAYER GAMES

We now examine cooperative games, that is, ones in which players may enter into binding arrangements. Each remains motivated by their individual utility payoff, and thus can be expected to only enter an agreement that is personally beneficial to them. However, we will also allow for transferable utility. That is, the participants in a coalition may redistribute the total return to the coalition amongst themselves, rather than keeping to the individual returns prescribed by the game. In effect, this allows for side payments from one player to another, to give the second an incentive to join a coalition with the first. This, of course, assumes that the payoffs to each player are inequivalent units, and represent a transferable commodity. In a genuine prisoner's dilemma, for instance, neither participant can accept jail time for the other; although mutual cooperation will still arise as their best strategy.

We thus require two things: a rule for determining the return to any coalition; and a means to decide which players will enter into the coalition. Broadly speaking, the payoffs to the coalitions constitute the rules of the game, analogous to the payoff matrices/functions in strategic form games; whilst the formation of coalitions represent the plays (strategies).

Example: 4.1.1.

The bi matrix form of Two-finger Morra. As a two player game, there are four possible coalitions- \emptyset , $\{1\}$, $\{2\}$ or $\{1, 2\}$. $v(\emptyset) = 0$ is given, and since Two-finger Morra is zero-sum the value gives that $v(\{1\}) = 1/12$ and $v(\{2\}) = -1/12$. Interpreted directly, $v(\{1, 2\})$ is the total return to the coalition when, working together, the players

are able to select any entry in the bi matrix. Since the game is zero-sum, this is always zero (which can be verified by inspection)

Solution:

Notice that super additivity holds, and the grand coalition offers a return of 0.

Since Player 1 receives a payoff of $1/12$ by not entering the grand coalition, Player 2 would have to offer a side payment of at least $1/12$ to entice Player 1 into a coalition.

But it would be irrational for Player 2 to offer any more than $1/12$ to create the coalition, since going it alone only costs him $1/12$.

Hence the distribution within the grand coalition would be the same as if it did not form players are indifferent to the formation of a coalition, and the coalitional form precisely mimics the strategic form.

This motivates some additional Definitions.

Example: 4.1.2

Individual payoffs in the simple majority game with symmetric distribution can be described by the following table, where the rows denote the options for Player 1 and the columns the options for Players 2 and 3 (as an ordered pair):

	(1, 1)	(1, 2)	(3, 1)	(3, 2)
2	$(1/2, 1/2, -1)$	$(1/2, 1/2, -1)$	$(0, 0, 0)$	$(-1, 1/2, 1/2)$
3	$(1/2, -1, 1/2)$	$(0, 0, 0)$	$(1/2, -1, 1/2)$	$(-1, 1/2, 1/2)$

Solution:

The value $v(\{1, 2, 3\})$ is determined by free choice of any of the 8 strategy combinations, but for any such choice the sum of the payoffs is 0.

As always, $v(\emptyset) = 0$.

To determine $v(\{1\})$ (and by symmetry $v(\{2\})$ and $v(\{3\})$) we can consider players 2 and 3 as acting as a single entity against Player 1; the return to their coalition being the sum of the individual returns, which they are motivated to drive as high as possible.

It should be clear then that they will form a couple to ensure a return of 1, forcing a payoff of -1 onto Player 1, ensuring that $v(\{1\}) = -1$.

However, it is enlightening to see precisely why this occurs.

By treating Players 2 and 3 as a single player with strategy set A, B, C, D the above table reduces to

	A	B	C	D
2	$(1/2, -1/2)$	$(1/2, -1/2)$	$(0, 0)$	$(-1, 1)$
3	$(1/2, -1/2)$	$(0, 0)$	$(1/2, -1/2)$	$(-1, 1)$

This is a bi matrix for a 2 player strategic form game; more over it is the bi matrix of the zero-sum game given by

$$\begin{pmatrix} 1/2 & 1/2 & 0 & -1 \\ 1/2 & 0 & 1/2 & -1 \end{pmatrix}$$

Further, column 4 dominates all other columns, so the strategic form reduces to that column- giving the game a value of -1 for Player 1 (and hence of 1 for the coalition of Players 2 and 3).

So the simple majority game is described in coalitional form by

- $v(\emptyset) = v(X) = 0$
- $v(\{1\}) = v(\{2\}) = v(\{3\}) = -1$
- $v(\{1, 2\}) = v(\{1, 3\}) = v(\{2, 3\}) = 1$

Super additivity holds,

since $v(\{i\}) + v(\{j, k\}) = -1 + 1 = 0 \leq 0 = v(\{i, j, k\})$ for any permutation i, j, k of the players.

Further, the game is zero-sum; but it is essential,

$$\text{since } v(\{1\}) + v(\{2\}) + v(\{3\}) = -3 < v(X).$$

Hence Any two person zero-sum game is inessential does not generalise to any zero-sum game; it is specific to the two-player case.

4.1.3 COALITIONAL FORM OF A STRATEGIC FORM GAME

The construction of the characteristic function used in the preceding example can be used, after suitable generalisation, for any strategic form game.

Given a coalition $S \in P(X)$, we consider a two-player zero-sum game between two team S and $X \setminus S$.

The strategy sets for each team consists of the cartesian product of the strategy sets of the individual members of each team.

The payoff to the coalition for any given combination of strategies is then determined by the sum of the payoffs to its members from those strategies.

$v(S)$ is then determined by the value of the game, which (due to the Minimax theorem) exists and can be found.

4.1.4 S-VETO GAMES

Of particular interest are the class of coalitional games known as S -veto games. In these, a coalition is only effective if some subset S of the players are all members.

Thus this gives rise to characteristic functions of the form

$$w_s(T) = \begin{cases} 1 & S \subseteq T \\ 0 & S \not\subseteq T \end{cases}$$

For instance, $S = \{1\}$ gives rise to a dictatorship by Player 1 (an inessential game) whereas $S = X$ forces the grand coalition to form for any player to receive a payoff- or, considered as a voting system, a unanimous verdict.

More complicated voting arrangements can be built upon veto systems, such as the United Nations Security Council system of "great power unanimity" which requires the support of all five permanent members (and any four of the ten non-permanent members) to pass major resolutions.

4.2 SHAPLEY VALUE

Given a coalitional form game (X, v) we seek to construct a value $\Phi(X, v) \in \mathbb{R}^n$ for the game, where the component $\Phi_i(X, v)$ denotes the payoff to player i .

This can be interpreted as a measure of the power of player i in the game, since it indicates their contribution to the grand coalition, were one to form.

An example of such a value is the Shapley value, constructed as follows. Given a permutation $\pi \in (i.e., a bijection from X to X) we can consider the players as forming the coalition one by one, in accordance with the ordering created by π .$

Thus the coalition is built by considering first the coalition consisting of Player $\pi(1)$, then of players $\pi(1)$ and $\pi(2)$, and so on.

By super additivity, the value at each step either increases or remains constant, so we may assign to each player a non-negative payoff equal to this increase. Let p_π^i denote the set of players who joined the coalition before Player i .

Therefore $p_\pi^i = \{j | \pi(j) < \pi(i)\}$.

Then the value of Player i to the coalition is given by

$$v(p_\pi^i \cup \{i\}) - v(p_\pi^i).$$

However, it is unlikely that the payoff constructed in this way will be independent of the ordering π .

Thus we consider the value of a player to be their average contribution to the formation of a coalition; where any ordering of players is equally likely. That is,

$$\Phi_i(X, v) = \frac{1}{n!} \sum_{\pi \in S_n} v(p_\pi^i \cup \{i\}) - v(p_\pi^i)$$

since the size of S_n is the number of permutations of the set of players X , namely $n!$, and for any given permutation we may determine Player i 's contribution by the method in the previous paragraph.

4.3 SHAPLEY AXIOMS

The above construction, determining average contributions to a coalition, is intuitively fair.

However, the notion of fairness can be made rigorous by requiring the satisfaction of a number of axioms, some of which have been hinted at in earlier discussion.

A number of desirable properties for a value can be advanced.

For group rationality, the total value of the players should be the value of the grand coalition. Thus, to assign a value to each player in X we require that

$$\sum_{i=0}^n \Phi_i(X, v) = v(X)$$

A value should not a priori favour any particular player over another.

That is, should the return to any coalition featuring Player i and not Player j be the same as the return to the coalition with Player i replaced by Player j , then the values of players i and j should be equal.

Any player whose presence in a coalition does not alter its payoff should receive a value of 0.

Given games (X, v) and (X, w) , then we can define the game $(X, v + w)$ as $(v + w)(S) = v(S) + w(S)$.

Logically, we should require that

$$\Phi(X, v + w) = \Phi(X, v) + \Phi(X, w),$$

i.e., that the return of playing the sum of two games is the sum of the returns of each game.

Theorem 4.3.1.

A function satisfying the Shapley axioms always exists

Proof:

The function Φ constructed in section 4.2 satisfies the Shapley axioms: We can recursively define p_π^i via

$$p_\pi^i = \begin{cases} \emptyset & i = 1 \\ p_\pi^{i-1} \cup \{i\} & i \geq 2 \end{cases}$$

Further, we can consider $q_\pi^i = p_\pi^i \cup \{i\}$; in particular, $q_\pi^n = X$. Thus

$$\begin{aligned} \Phi_i(X, v) &= \frac{1}{n!} \sum_{\pi \in S_n} v(q_\pi^i) - v(p_\pi^i) \\ \sum_{i=0}^n \Phi_i(X, v) &= \sum_{i=0}^n \frac{1}{n!} \sum_{\pi \in S_n} v(q_\pi^i) - v(p_\pi^i) \\ &= \frac{1}{n!} \sum_{\pi \in S_n} \sum_{i=1}^n (v(q_\pi^i) - v(p_\pi^i)) \\ &= \frac{1}{n!} \sum_{\pi \in S_n} (\sum_{i=2}^n (v(q_\pi^i) - v(p_\pi^i)) + (v(q_\pi^1) - v(p_\pi^1))) \\ &= \frac{1}{n!} \sum_{\pi \in S_n} (\sum_{i=2}^n v(q_\pi^i) - \sum_{i=2}^n v(q_\pi^{i-1}) + (v(q_\pi^1) - v(p_\pi^1))) \\ &= \frac{1}{n!} \sum_{\pi \in S_n} (v(q_\pi^n) - v(q_\pi^{n-1}) + v(q_\pi^1) - v(\emptyset)) \\ &= \frac{1}{n!} \sum_{\pi \in S_n} (v(X) - v(q_\pi^1) + v(q_\pi^1) - 0) \\ &= \frac{1}{n!} \sum_{\pi \in S_n} v(X) \\ &= \frac{1}{n!} n! v(X) \\ &= v(X) \end{aligned}$$

Thus efficiency holds. Symmetry and the dummy axioms are immediate from the Definition of $\Phi_i(X, v)$, whilst additivity follows from the linearity of \sum and the averaging process.

Theorem 4.3.2.

The Shapley function is unique.

Proof:

The S -veto games described in section 4.1.4 are a basis for the set of coalitional games:

Note First that the value of an S -veto game is completely determined from the Shapley axioms.

For a given characteristic function w_S the dummy axiom ensures that

$$\Phi_i(X, w_S) = 0 \text{ for any } i \notin S;$$

whilst the symmetry axiom ensures that if $i, j \in S$ then

$$\Phi_i(X, w_S) = \Phi_j(X, w_S),$$

that is, the members of the veto set S have equal value. Since (by the efficiency axiom) the sum of their values is the grand coalition payoff $w_S(X) = 1$ it follows that the individual values for members of S are $\frac{1}{|S|}$.

By the same reasoning for $W_S(X) = c$ for an arbitrary constant c , we deduce

$$\Phi_i(X, cw_S) = \begin{cases} \frac{c}{|S|} & i \in S \\ 0 & i \notin S \end{cases}$$

Now for an arbitrary characteristic function v , consider the set of constants c_T for $T \in \mathcal{P}(X)$ constructed inductively on the size of T by $c_\emptyset = 0$ and

$$c_T = v(T) - \sum_{S \subset T, S \neq T} c_S$$

Then

$$\sum_{S \in \mathcal{P}(X)} c_S w_S(T) = \sum_{S \subset T} c_S = c_T + \sum_{S \subset T, S \neq T} c_S = v(T)$$

Hence v is uniquely determined by the coefficients c_S and S -veto games w_S as

$v = \sum_{S \in \mathcal{P}(X)} c_S w_S(T)$. By the additivity axiom.

$$\Phi_i(X, v) = \Phi_i(X, \sum_S c_S w_S) = \sum_{S \in \mathcal{P}(X)} \Phi_i(X, c_S w_S) = \sum_{S \in \mathcal{P}(X)} \frac{c_S}{|S|}$$

So $\Phi_i(X, v)$, and thus $\Phi(X, v)$, are uniquely determined by the constants c_S .

4.4 SHAPLEY'S THEOREM

There exists a unique value $\Phi(X, v)$ satisfying the Shapley axioms from the Shapley axioms, given by the random arrival formula

$$\Phi_i(X, v) = \frac{1}{n!} \sum_{\pi \in S_n} v(p_\pi^i \cup \{i\}) - v(p_\pi^i)$$

Hence a unique value function, the Shapley value, exists. Further, the coefficients c_S provide an alternative mean of calculating the value.

Example: 4.4.1.

Consider three companies A, B and C, which seek to invest in a combined project. The project requires five million pounds in funding to be successful; the three companies have investment budgets of 2, 3 and 4 million pounds respectively. What is the worth of each company in terms of Shapley value?

Solution:

By considering the coalitions with sufficient funding, we observe that

$$v\{A\} = v\{B\} = v\{C\} = v\{\emptyset\} = 0$$

$$v\{A, B\} = v\{A, C\} = v\{B, C\} = v\{A, B, C\} = 1$$

Following the construction in theorem 4.3.2, we determine the values c_T . c_\emptyset is zero by assumption, and so for each $L \in \{A, B, C\}$,

$$c_{\{L\}} = v(\{L\}) - c_\emptyset = 0 - 0 = 0$$

i.e.,

$$c_{\{A\}} = c_{\{B\}} = c_{\{C\}} = 0$$

Thus

$$c_{\{A, B\}} = v(\{A, B\}) - (c_\emptyset + c_{\{A\}} + c_{\{B\}}) = 1 - (0 + 0 + 0) = 1$$

By symmetry,

$$c_{\{A,B\}} = c_{\{A,C\}} = c_{\{B,C\}} = 1$$

Finally, this gives

$$\begin{aligned} c_{\{A,B,C\}} &= v(\{A, B, C\}) - (c_{\emptyset} + c_{\{A\}} + c_{\{B\}} + c_{\{C\}} + c_{\{A,B\}} + c_{\{A,C\}} + c_{\{B,C\}}) \\ &= 1 - (0 + 0 + 0 + 0 + 1 + 1 + 1) \\ &= -2 \end{aligned}$$

So

$$\begin{aligned} \Phi_i(\{A, B, C\}, v) &= c_{\{A\}}/1 + c_{\{A,B\}}/2 + c_{\{A,C\}}/2 + c_{\{A,B,C\}}/3 \\ &= \frac{0}{1} + \frac{1}{2} + \frac{1}{2} + \frac{-2}{3} \\ &= \frac{1}{3} \end{aligned}$$

By the same argument,

$$\Phi_1(\{A, B, C\}, v) = \Phi_2(\{A, B, C\}, v) = \Phi_3(\{A, B, C\}, v) = 1/3.$$

That is, no one company has more influence (or right to the profits) than any of the others.

This is intuitively obvious from the problem formulation, since it is the simple majority game.

No one company can afford the project, but any two can.

This can also be seen from the random arrival formula, as the value of a coalition will only be increased when a second company joins, which, across the set of all participations, is equally likely for any particular company.

CHAPTER 5

CHAPTER 5

APPLICATIONS OF GAME THEORY

5.1 ECONOMICS AND BUSSINESS

Game theory is an important tactics applied in mathematical economics and business for modeling the patterns of behavior of interacting agents. According to P.A. Samuelson and W. D. Nordhaus:

“Economic life contains many situations with strategic interaction among firms, households, governments or others. Game theory analyzes the way that two or more parties, who interact in an arena such as a market, choose actions or strategies that jointly affect all Participants.”

Economists use ‘Game Theory’ as a tool to analyze economic competition, economic phenomena such as bargaining, mechanism design, auctions, voting theory; experimental economics, political economy, behavioral economics etc.

Game theory is applied for determining different strategies in the business world. It offers valuable tools for solving strategy problems. Many business strategies are short or long-term plans to achieve sustainable profitability. A business can often successfully position in the market with right strategy and a business will suffer in the long run with wrong strategy.

Strategic behavior occurs regularly among executives, manager and investors in business world. They must decide to enter into new markets, launch new products, invest now or lose the opportunity to invest and make pricing and purchasing decisions. Game-theoretic models are very potential tools for analyzing firm decisions. Game theory models forces each player to consider the actions of others when picking their strategy, in which one player may respond to the moves of his competitor. It provides significant benefit to a decision maker.

5.2 GAME THEORY IN POLITICS

Game theory is widely used in political affairs, which is focused on the areas of international politics, war strategy, war bargaining, social choice theory, Strategic voting, political economy etc. Game theory is an effective tool in the hands of diplomats and politicians to analysis any situation of conflict between individuals, companies, states, political parties. Rationality of actors and the choice of strategies are one of the basic assumptions of game theory. Game theory seems to be useful tool for research on terrorism because it captures the interaction between attacked subject and terrorist organization, when the steps are interdependent and therefore cannot be analyzed separately.

5.3 EVOLUTION OF COOPERATION

Game theory is applied to analyze many seemingly anomalous natural phenomena in biology. The evolution of cooperation is a fundamental problem in biology because unselfish, altruistic actions apparently contradict Darwinian selection. Game theory offers to an evolutionary context, has become an invaluable tool to address the evolution of cooperation. The most noted mechanisms of cooperation are direct and indirect reciprocity and spatial structure.

5.4 GAME THEORY AND PHILOSOPHY

Game theory and Philosophy are connected in many ways. Game theory has been used as a tool in philosophical discussions. Philosophers have promisingly attracted in game theory as it offers a way of interpreting the conception of Philosophers. There are different areas of Philosophy that interact in a fruitful way with game theory.

5.5 EPISTEMOLOGY

Epistemology, the study of knowledge, which inquires about the nature, source, status and extent of knowledge. Game theory challenged philosophers to think in terms of interactive epistemology. It covers players have common knowledge of the structure of the game and their mutual rationality.

5.6 RATIONAL BEHAVIOR AND DECISION THEORY

Game theory is a useful and potential tool for the understanding of human affairs. Game theory has been expounded as a part of a general theory of Rational Behavior. Rationality is a normative concept, which indicates to what we should do in order to attain a given end or objective. When we are thinking of behavior involving a choice of the best means available for achieving a given end that is 'rational behavior'. Rational behavior models are widely used in game theory. According to Von Neumann and Morgenstern: 'We wish to find the mathematically complete principles which define 'rational behavior' for the participants in a social economy, and to derive from them the general characteristics of that behavior'. Game theory as a theory of rationality advises what agents (players) should do in specific interactive situations, given their preferences.

Decision theory is the analysis of the human behavior, which concentrates on identifying the 'best' decision option to decision maker. Decision theory provides the rationality of decisions in the light of preferences over outcomes and beliefs about the likelihood of outcomes. Game theory is closely related to decision theory, which studies inter-actions between self-interested players. Game theory along with decision theory analyzes interdependent decision problems between rational, strategic agents. The basic difference between the two that: Decision theory treats all outcomes as exogenous events, 'moves of nature'; whereas in Game theory the prime source of uncertainty for

an agent is the way other agents will behave. After analyzing some of the application of the game theory in philosophy we assumed that, game theory has been the object of philosophical inquiry.

CONCLUSION

Game theory is the formal study of conflict and cooperation between intelligent rational decision-makers. It has been a powerful analytical tool to help us understand the phenomena that can be observed when decision makers interact. Game theoretic models have become increasingly sophisticated and in consequence, much more powerful and useful. It has been successfully applied to a wide variety of disciplines including economics, sociology, psychology, philosophy. Game theory has helped sharpen our intuitions, allowing a 'rational reconstruction' of different ideas, norms and values among agents (players) for significant philosophical expositions. Thus it can be seen that the techniques of Game Theory provide numerous insights into questions of decision making and strategy. The more recent theorems described (Shapley values) are particularly far reaching, generalising to arbitrary player or strategy sets without modification; yet even the simplest of problems (such as the iterated prisoner's dilemma) can yield complex behaviour.

REFERENCES:

- [1] Axelrod. R (1980) 'Effective choice in the prisoner's dilemma' Journal of Conflict Resolution Vol 24 No. 1 (March).
- [2] Ferguson. S. T- Lecture notes for Mathematics 167, Game Theory, Fall 2000, University of California Los Angeles (UCLA).
- [3] Grossman. W 'New tack to wins prisoner's dilemma'.
- [4] Rasmusen. E - Games and Information, Blackwell Publishers.
- [5] Von Neumann and Morgenstern - Theory of Games and Economic Behaviour, Princeton University Press.
- [6] Yuval Peres - Lecture notes for STAT 155: Game Theory (Fall 2005), Berkeley University of California.
- [7] Winter. E - The Shapley Value

MATHEMATICS IN MACHINE LEARNING

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

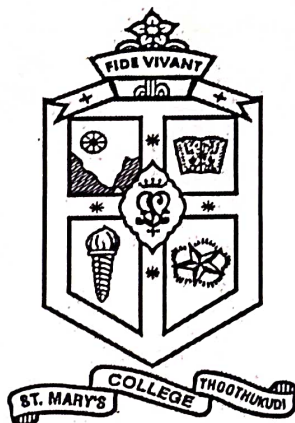
BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NO
S. ANUSHYA DEVI	19SUMT05
K. MARIA VIJILIOUS MANCY	19SUMT20
S. POORANA PRIYADARSHINI	19SUMT29
M. RAGAVI	19SUMT32
VHARSHA THIRUMENINATHAN	19SUMT39

Under the guidance of

Dr. C. REENA M.Sc., B.Ed., M. Phil., SET., Ph.D.,



DEPARTMENT OF MATHEMATICS


St. Mary's College (Autonomous), Thoothukudi

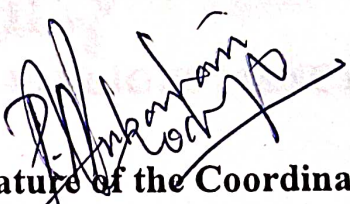
May-2022

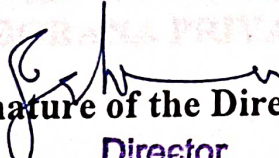
CERTIFICATE


This is to certify that this project work entitled "MATHEMATICS IN MACHINE LEARNING" is submitted to St. Mary's College (Autonomous), Thoothukudi affiliated to Manonmaniam Sundaranar University, Tirunelveli in partial fulfilment for the award of the degree of Bachelor of Science in Mathematics and is the work done during the year 2021-2022 by the following students.

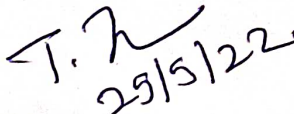
NAME	REGISTER NO
S. ANUSHYA DEVI	19SUMT05
K. MARIA VIJILIOUS MANCY	19SUMT20
S. POORANA PRIYADARSHINI	19SUMT29
M. RAGAVI	19SUMT32
VHARSHA THIRUMENINATHAN	19SUMT39


Signature of the Guide


Signature of the Coordinator

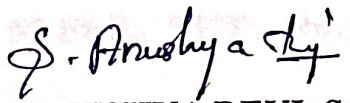

Signature of the Director
Director
Self Supporting Courses
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Principal
Principal
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Examiner

DECLARATION

We hereby declare that the project entitled "MATHEMATICS IN MACHINE LEARNING" submitted for the degree of Bachelor of Science is our work carried out under the guidance of Dr.C.Reena M.Sc., B.Ed., M.Phil., SET., Ph.D., Assistant Professor , Department of Mathematics (SSC), St.Mary's College(AUTONOMOUS), Thoothukudi.


(ANUSHYA DEVI. S)


(MARIA VIJILIOUS MANCY. K)


(POORANA PRIYADARSHINI. S)


(RAGAVI. M)


(VHARSHA THIRUMENINATHAN)

ACKNOWLEDGEMENT

First of all, we thank the Almighty for showering his blessings to undergo this project.

We express our sincere gratitude and heartfelt thanks to our Principal **Rev. Dr. Sr. A. S. J. Lucia Rose M.Sc., PGDCA., M.Phil., Ph.D.**, and to our Director **Rev. Sr. Josephine Jeyarani M.Sc., B.Ed.**, for kindly permitting us to do this project.

We express our gratitude to **Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D.**, Coordinator, Department of Mathematics (SSC) for her inspirational ideas and encouragement.

We are very thankful to our guide **Dr. C. Reena M.Sc., B.Ed., M.Phil., SET., Ph.D.**, Assistant Professor, Department of Mathematics (SSC) for her efficient and effective guidance. She played a key role in the preparation of this project.

We also thank our staff members for their encouragement in all our efforts. Finally, we thank all those who extended their help regarding this project.

Place: Thoothukudi

Date: 17.05.2022

CONTENT

CHAPTER	TOPIC	PAGE NO.
	Introduction	
1	Preliminaries	1
2	Analytic Geometry	4
3	Orthogonal Projection	18
4	Rotation	36
	Conclusion	
	Reference	

INTRODUCTION

The field of Mathematics plays a vital role in various fields. One of the important areas in Mathematics is Machine Learning. Machine learning is the latest in a long line of attempts to distill human knowledge and reasoning into a form that is suitable for constructing machines and engineering automated systems.

As machine learning becomes more ubiquitous and its software packages become easier to use, it is natural and desirable that the low-level technical details are abstracted away and hidden from the practitioner. However, this brings with it the danger that a practitioner becomes unaware of the design decisions and, hence, the limits of machine learning algorithms. Primarily we focus on machine learning algorithms and methodologies in basic mathematics related to machine learning such as analytical geometry, Vector space, Matrices, etc.

The project consists of four chapters.

In chapter 1, we have given some basic definitions on analytic geometry needed for the subsequent chapters.

In chapter 2, we have discussed the concepts and basic theorem of analytic geometry.

In chapter 3, we have discussed the different types of orthogonal projection.

In chapter 4, we have discussed the concepts of rotation and their properties.

Chapter 1

CHAPTER 1

PRELIMINARIES

Definition: 1.1

A **norm** is a function from a real or complex vector space to the non-negative real numbers that behaves in certain ways like the distance from the origin, it commutes with scaling, obeys a form of the triangle inequality, and is zero only at the origin. In particular, the origin is a norm, called the Euclidean norms, or 2-norms, which may also be defined as the square root of the inner product of a vector with itself.

Definition: 1.2

Inner products allow formal definitions of initiative geometric notations, such as length, angles and orthogonality (zero inner product) of vectors. Inner product space in which the inner product is the dot product or scalar product of Cartesian co-ordinates. This concept of angles, length and distance turn \mathbb{R}^2 or \mathbb{R}^3 into Euclidean spaces. We want to define these notions abstractly, for any V . The key ingredient is the inner product.

Definition: 1.3

The product of the Euclidean magnitude of the two vectors and the cosine of the angle between them. However inner product as the **dot product** are more general concepts with specific properties, $\mathbf{x}^T \mathbf{y} = \sum_{i=1}^n x_i y_i$

Definition: 1.4

A **bilinear mapping** Ω is a mapping with two arguments, and it is linear in each argument, i.e.). When we look at a vector space V then it holds that for all $x, y, z \in V, \lambda, \psi \in \mathbb{R}$ that

$$\Omega(\lambda x + \psi y, z) = \lambda \Omega(x, z) + \psi \Omega(y, z) \quad \dots\dots\dots(1)$$

$$\Omega(x, \lambda y + \psi z) = \lambda \Omega(x, y) + \psi \Omega(x, z) \dots\dots\dots(2)$$

Here (1) asserts that Ω is linear in the first argument and (2) asserts that Ω is linear in the second argument.

Definition: 1.5

A symmetric $A \in \mathbb{R}^{n \times n}$ that satisfies $\forall x \in V \setminus \{0\} : x^T A x > 0$ is called symmetric, positive definite or just positive definite. If only \geq holds then A is called symmetric positive semi definite.

Definition: 1.6

The length of V is $\sqrt{(v_1^2 + \dots + v_n^2)}$ by Pythagoras theorem, so the norm defined by the standard inner product on \mathbb{R}^2 (or) \mathbb{R}^3 gives the familiar length of a vector in Euclidean space.

Definition: 1.7

Consider an inner product space $(V, \langle \cdot, \cdot \rangle)$. Then $d(x, y) = \|x - y\| = \sqrt{\langle x - y, x - y \rangle}$ is called the distance between x and y for $x, y \in V$. If we use the dot product as the inner product then the distance is called **Euclidean distance**.

Definition: 1.8

The distance between two vectors, inner products also capture the geometry of a vector space by defining the angle w between two vectors. We use Cauchy Schwarz inequality to define **angle** w in inner product spaces between two vectors x, y and this notion coincides with our intuition in \mathbb{R}^2 and \mathbb{R}^3 . Assume that $x \neq 0, y \neq 0$ then

$$-1 \leq \frac{\langle x, y \rangle}{\|x\| \|y\|} \leq 1.$$

Therefore, there exists a unique $w \in [0, \pi]$,

$$\cos w = \frac{\langle x, y \rangle}{\|x\| \|y\|}.$$

Definition: 1.9

A subspace of R_n is a subset V of R_n satisfying:

1. Non-emptiness: The zero vector is in V .
2. Closure under addition: If u and v are in V , then $u+v$ is also in V .
3. Closure under scalar multiplication: If v is in V and c is in R , then cv is also in V .

Definition: 1.10

A subspace of a vector space consisting of vectors that under a given linear transformation are mapped onto zero is called a null space

Chapter 2

CHAPTER 1

ANALYTIC GEOMETRY

1.1 Introduction

In this chapter, we will introduce some basic concepts and definitions related to vector spaces. In particular, we will look at geometric vectors and discuss their properties. We will also introduce the concept of a scalar product (or inner product) and show how it relates to the geometry of the vector space. We will then discuss the concept of a norm and show how it relates to the geometry of the vector space. Finally, we will discuss the concept of a metric and show how it relates to the geometry of the vector space.

1.2 Norms

Definition 1.2.1

Let V be a vector space. A norm on V is a function $\| \cdot \| : V \rightarrow \mathbb{R}$ satisfying the following properties:

$$\|x\| \geq 0$$

$$\|x\| = 0 \iff x = 0$$

For every $x \in V$ and $\alpha \in \mathbb{R}$, $\|\alpha x\| = |\alpha| \|x\|$.

For every $x, y \in V$,

$$\|x + y\| \leq \|x\| + \|y\|$$

$$\|x - y\| \leq \|x\| + \|y\|$$

$$\|x\| \leq \|x\| + \|y\| \iff \|y\| \geq 0$$

Proposition 1.2.2

Let V be a vector space. If $\| \cdot \|$ is a norm on V , then $\| \cdot \|$ is a metric on V .

Proof. Let $x, y, z \in V$. Then

CHAPTER 2

ANALYTIC GEOMETRY

2.1 Introduction

In this chapter, we will add some geometric interpretation and intuition to all of these concepts. In particular, we will look at geometric vectors and compute their lengths and distances or angles between two vectors. To be able to do this, we equip the vector space with an inner product that induces the geometry of the vector space. Inner products and their corresponding norms and metrics capture the intuitive notions of similarity and distances, which we use to develop the support vector machine in Classification with support vector machines.

2.2 Norms

Definition: 2.2.1

Let V be an inner product space define for every $v \in V$. $\|v\| = \sqrt{\langle v, v \rangle}$, $\|v\|$ is called the norm of v , and V is called a normed space. A norm on a vector space V is function

$$\|\cdot\|: V \rightarrow \mathbb{R},$$

$$x \mapsto \|x\|,$$

Which assign each vector x its length $\|x\| \in \mathbb{R}$, such that for all $\lambda \in \mathbb{R}$ and $x, y \in V$ the following holds:

- Absolutely homogeneous: $\|\lambda x\| = |\lambda| \|x\|$
- Triangle inequality: $\|x+y\| \leq \|x\| + \|y\|$
- Positive definite: $\|x\| \geq 0$ and $\|x\| = 0 \iff x=0$.

Remark: 2.2.2

- (i) By axiom of \langle, \rangle we know that $\langle v, v \rangle \geq 0$ and therefore $\|v\|$ is well defined.

(ii) $\|v\|$ coincides with the usual Euclidean length, in $\mathbb{R}^2/\mathbb{R}^3$.

Theorem: 2.2.3

$\|v\| = \sqrt{\langle v, v \rangle}$ is indeed a norm, ie). Satisfies the following three axioms:

- (i) $\|\alpha v\| = |\alpha| \|v\|$
- (ii) $\|v\| \geq 0, \|v\| = 0 \Leftrightarrow v = 0$
- (iii) $\|u + v\| \leq \|u\| + \|v\|$ (triangle inequality)

Proof :

$$(i) \quad \|\alpha v\| = \sqrt{\langle \alpha v, \alpha v \rangle}$$

$$= \sqrt{\alpha \langle v, v \rangle}$$

$$= \sqrt{|\alpha|^2 \langle v, v \rangle}$$

$$= |\alpha| \sqrt{\langle v, v \rangle}$$

$$= |\alpha| \|v\|$$

(ii) We will see now it follows from Cauchy Schwarz inequality.

Cauchy Schwarz inequality: $|\langle u, v \rangle| \leq \|u\| \|v\|$.

Let us show that the triangle inequality follows from Cauchy Schwarz:

$$\|x + y\|^2 = \langle x + y, x + y \rangle$$

$$= \langle x, x \rangle + \langle x, y \rangle + \langle y, x \rangle + \langle y, y \rangle$$

$$= \|x\|^2 + \langle x, y \rangle + \overline{\langle x, y \rangle} + \|y\|^2$$

$$\leq \|x\|^2 + 2\operatorname{Re}|\langle x, y \rangle| + \|y\|^2$$

$$\leq \|x\|^2 + 2\|x\| \|y\| + \|y\|^2$$

$$= (\|x\| + \|y\|)^2.$$

Theorem: 2.2.4 (Manhattan Norm)

The Manhattan norm on \mathbb{R}^n is defined for $x \in \mathbb{R}^n$ as $\|x\| = \sum_{i=1}^n |x_i|$, Where

Fig. 2.1 is absolute value. The left panel of Fig. 1.1 shows all vectors $x \in \mathbb{R}^2$ with $\|x\|$

$= 1$. The Manhattan norm is also called l_1 norm.

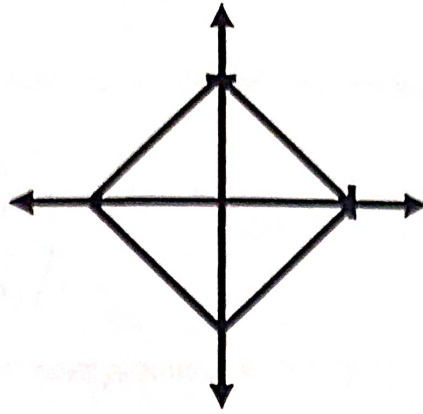


Figure:2.1

Theorem: 2.2.5 (Euclidean norm)

The Euclidean norm of $x \in \mathbb{R}^3$ is defined as $\|x\|_2 = \sqrt{\sum_{i=1}^n x_i^2}$ and computes the Euclidean distance of x from the origin. The right panel of Fig. 2.2 shows all vectors $x \in \mathbb{R}^2$ with $\|x\|_2 = 1$. The Euclidean norm is also called l_2 norm.

2.3 Inner Product

We know that even simple vector spaces like \mathbb{R}^2 or \mathbb{R}^3 have a richer structure. If we think of vectors in \mathbb{R}^2 as arrows, then we have angles. We can measure length, and even distance $d(v_1, v_2)$ is the length of $v_2 - v_1$.

If we admit an inner product, V is called an **inner product space**.

Definition: 2.3.1

Let V be a vector space over \mathbb{R} or \mathbb{C} , an inner product on V is an operation defined on pairs of vectors, which gives a scalar H is denoted by $\langle u, v \rangle$ and satisfies three axioms:

- $\langle u, v \rangle = \overline{\langle v, u \rangle}$ (over \mathbb{R} $\langle u, v \rangle = \langle v, u \rangle$). Conjugate Symmetry
- $\langle \alpha u, v \rangle = \alpha \langle u, v \rangle$
 $\langle u + w, v \rangle = \langle u, v \rangle + \langle w, v \rangle$. Linearity in first component.
- $\langle v, v \rangle \geq 0$ $\langle v, v \rangle = 0 \iff v = 0$. Positive definiteness

Example: 2.3.2

(1) $V = \mathbb{R}$ $\langle x, y \rangle = xy$ defines an inner product on \mathbb{R} .

(2) $V = \mathbb{R}^n$ for $x = \begin{pmatrix} x^1 \\ x^2 \\ \vdots \\ x_n \end{pmatrix}$; $y = \begin{pmatrix} y^1 \\ y^2 \\ \vdots \\ y_n \end{pmatrix}$ defines this is an inner product on \mathbb{R}^n

called the standard inner product. $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$

$$= (x_1 y_1 + x_2 y_2 + \dots + x_n y_n)$$

(3) $V =$ vector space of integrable real valued function on $[a, b]$ interval $\langle f, g \rangle =$

$\int_a^b f(x)g(x)dx$ is an inner product. $\langle u, v \rangle$ is an inner product. $\|v\| =$

$$\sqrt{\langle v, v \rangle} \text{ is a norm are } \langle u, v \rangle = \left\langle \begin{pmatrix} u^1 \\ u^2 \end{pmatrix}, \begin{pmatrix} v^1 \\ v^2 \end{pmatrix} \right\rangle = u_1 v_1 + u_2 v_2$$

$$\left\| \begin{pmatrix} v^1 \\ v^2 \end{pmatrix} \right\| = \sqrt{\left\langle \begin{pmatrix} v^1 \\ v^2 \end{pmatrix}, \begin{pmatrix} v^1 \\ v^2 \end{pmatrix} \right\rangle}$$

$$= \sqrt{v^{12} + v^{22}}$$

Remark: 2.3.3

There are many norms and matrices, even on \mathbb{R}^2 there are norms that can't be defined via inner product.

Definition: 2.3.4

Let V be a vector space and $\Omega: V \times V \rightarrow \mathbb{R}$ be a bilinear mapping that takes two vectors and map them onto a real number. Then

- A positive definite, symmetric bilinear mapping $\Omega: V \times V \rightarrow \mathbb{R}$ is called an **inner product** on V . We typically write $\langle x, y \rangle$ instead of $\Omega(x, y)$.
- The pair $(V, \langle \cdot, \cdot \rangle)$ is called an **inner product space** or **vector space with inner product**. If we use the dot product we call $(V, \langle \cdot, \cdot \rangle)$ a **Euclidean vector space**.

Example: 2.3.5 (Inner product that is Not the Dot product)

Consider $V = \mathbb{R}^2$. If we define $\langle x, y \rangle = (x_1 y_2 + x_2 y_1) + 2x_1 y_1$ then $\langle \cdot, \cdot \rangle$ is an inner product but different from the dot product.

2.4 Symmetric Positive Definite Matrices

The idea of symmetric positive semi definite matrices is key in the definition of kernels. Consider an n -dimensional vector space V with an inner product $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ and an ordered basis $B = (b_1, \dots, b_n)$ of V . Any vectors $x, y \in V$ can be written as linear combinations of the basis vector so that $x = \sum_{i=1}^n \psi_i b_i$ and $y = \sum_{j=1}^n \lambda_j b_j \in V$ for suitable $\psi_i, \lambda_j \in \mathbb{R}$. Due to the bilinearity of the inner product, it holds for all $x, y \in V$ that,

$$\begin{aligned} \langle x, y \rangle &= \left\langle \sum_{i=1}^n \psi_i b_i, \sum_{j=1}^n \lambda_j b_j \right\rangle \\ &= \sum_{i=1}^n \sum_{j=1}^n \psi_i \langle b_i, b_j \rangle \lambda_j = \hat{x}^T A \hat{y} \dots \dots (1) \end{aligned}$$

Where $A_{ij} := \langle b_i, b_j \rangle$ and \hat{x}, \hat{y} are the coordinates of x and y with respect to the basis B . This implies that the inner product $\langle \cdot, \cdot \rangle$ is uniquely determined through A . Therefore, A is symmetric, the positive definiteness of the inner product implies that

$$\forall x \in V \setminus \{0\} : x^T A x > 0 \dots \dots \dots (2)$$

Example: 2.4.1 (Symmetric, Positive Definite Matrices)

Consider the matrices

$$A_1 = \begin{bmatrix} 9 & 6 \\ 6 & 5 \end{bmatrix}, A_2 = \begin{bmatrix} 9 & 6 \\ 6 & 3 \end{bmatrix}$$

A_1 is positive definite because it is symmetric and

$$x^T A_1 x = [x_1 \ x_2] \begin{bmatrix} 9 & 6 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$\begin{aligned}
&= [9x_1 + 6x_2 \quad 6x_1 + 5x_2] \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\
&= 9x_1^2 + 6x_1x_2 + 6x_1x_2 + 5x_2^2 \\
&= (3x_1 + 2x_2)^2 - x_2^2 > 0
\end{aligned}$$

From (2) A is symmetric but not positive definite because $x^T A_2 x = 9x_1^2 + 12x_1x_2 + 3x_2^2 = (3x_1 + 2x_2)^2 - x_2^2$ can be less than 0.

Theorem: 2.4.2

For a real valued finite-dimensional vector space V and an ordered basis B of V , it holds that $\langle \cdot, \cdot \rangle : V \times V \rightarrow \mathbb{R}$ is an inner product if and only if there exists a symmetric, positive definite matrix $A \in \mathbb{R}^{n \times n}$ with $\langle x, y \rangle = \hat{x}^T A \hat{y}$.

Proof :

The properties will hold $A \in \mathbb{R}^{n \times n}$ if A is symmetric and positive definite.

- The null space (kernel) of A consists only of 0 because $x^T A x > 0$ for all $x \neq 0$.

This implies that $Ax \neq 0$ if $x \neq 0$.

- The diagonal elements a_{ii} of A are positive because $a_{ii} = e_i^T A e_i > 0$, where e_i is the i th vector of the standard basis in \mathbb{R}^n .

2.5 Length and distance

Norms that we can use to compute the length of a vector. Inner product and norms are closely related in the sense that any inner product induces a norm

$$\|x\| := \sqrt{\langle x, x \rangle}$$

Definition: 2.5.1

The length of V is $\sqrt{V_1^2 + V_2^2}$ by the standard inner product on \mathbb{R}^2 (or \mathbb{R}^3) gives the familiar length of a vector in Euclidean space.

Theorem: 2.5.2 (Cauchy-Schwarz Inequality).

For an inner product vector space $(V, \langle \cdot, \cdot \rangle)$ the induced norm $\|\cdot\|$ satisfies the Cauchy-Schwarz inequality $|\langle x, y \rangle| \leq \|x\| \|y\|$.

Definition: 2.5.3 (Distance)

Define $d(u, v) = \|u - v\|$

$$= \sqrt{\langle u - v, u - v \rangle}$$

this coincides with the regular distance in \mathbb{R}^2 . (also in \mathbb{R} : $d(x, y) = |x - y|$)

Theorem: 2.5.4

Let $d(u, v) = \|u - v\|$ is a metric on V defined by a metric satisfies four axioms.

(i) $d(u, v) \geq 0$

(ii) $d(u, v) = 0 \Leftrightarrow u = v$

(iii) $d(u, v) = d(v, u)$

(iv) $d(u, w) \leq d(u, v) + d(v, w)$ (the triangle inequality)

Proof:

$$\begin{aligned} \text{(iii)} \quad \sqrt{\langle u - v, u - v \rangle} &= (\langle u, v \rangle - \langle u, v \rangle - \langle v, u \rangle + \langle v, v \rangle)^{\frac{1}{2}} \\ &= (\langle v, v \rangle - \langle v, u \rangle - \langle u, v \rangle + \langle u, u \rangle)^{\frac{1}{2}} \\ &= \sqrt{\langle v - u, v - u \rangle} = d(v, u) \end{aligned}$$

(iv) $d(u, w) = \|u - w\| = \|u - v + v - w\|$

$$\leq \|u - v\| + \|v - w\|$$

$$= d(u, v) + d(v, w)$$

2.5.5 Angle in norm

We define $\cos \alpha = \frac{\langle u, v \rangle}{\|u\| \|v\|}$ and we get the regular notion of angles in \mathbb{R}^2 .

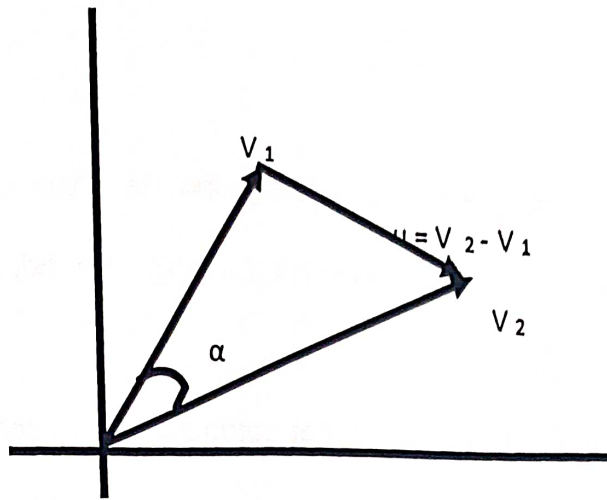


Figure: 2.2

Example: 2.5.6 (Angle between vectors)

Let us compute the angle between $x = [1,1]^T \in \mathbb{R}^2$ and $y = [1,2]^T \in \mathbb{R}^2$; where we use the dot product as the inner product. Then

$$\cos \omega = \frac{\langle x, y \rangle}{\sqrt{\langle x, y \rangle \langle y, y \rangle}} = \frac{x^T y}{\sqrt{x^T x y^T y}} = \frac{3}{\sqrt{10}}$$

and the angle between the two vectors is $\arccos(3/\sqrt{10}) \approx 0.32$ rad which corresponds to about 18° .

Theorem: 2.5.7

If we define in \mathbb{R}^2 $u \cdot v = \|u\| \|v\| \cos \alpha$ then we can show that $u \cdot v = u_1 v_1 + u_2 v_2 = \langle u, v \rangle$ therefore we define for $u, v \in V$ over \mathbb{R} in general.

$$\alpha = \arccos \frac{\langle u, v \rangle}{\|u\| \|v\|}$$

to be the angle between u and v ($\cos \alpha = \frac{\langle u, v \rangle}{\|u\| \|v\|}$) note that by Cauchy-Schwarz

inequality $|\langle u, v \rangle| \leq \|u\| \|v\|$ and therefore $|\cos \alpha| \leq 1$.

2.6 Orthogonality

Definition: 2.6.1

Two vectors x and y are orthogonal if and only if $(x, y) = 0$ and we write $x \perp y$. If additionally, $\|x\| = 1 = \|y\|$ i.e., the vectors are unit vectors, then x and y are orthogonal.

An implication of this definition is that the 0-vector is orthogonal to every vector in the vector space.

Definition: 2.6.2

Consider an n - dimensional vector space V and a basis $\{b_1, \dots, b_n\}$ of V . If

$$\langle b_i, b_j \rangle = 0 \text{ for } i \neq j \quad \dots \dots \dots (1)$$

$$\langle b_i, b_i \rangle = 1 \text{ for all } i, j = 1, 2, \dots, n \quad \dots \dots \dots (2)$$

then the basis is called an **orthonormal basis (ONB)**. If only (1) is satisfied, then the basis is

called the **orthogonal basis**.

Note: 2.6.3(2) implies that every basis vector has length/ norm 1.

Example: 2.6.4(Orthogonal basis)

The canonical / Standard basis for a Euclidean vector space R^n an orthonormal basis, where the inner product is the dot product of vectors.

In R^2 , the vector

$$b_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad b_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \text{ decomposed into}$$

$$\langle b_1, b_2 \rangle = b_1^T b_2 = \frac{1}{\sqrt{2}} [1, 1] \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

$$= \frac{1}{2} \times 0$$

$$= 0$$

$$\|b_1\| = b_1^T b_1$$

$$= 1\sqrt{2}[1 \ 1] \times 1\sqrt{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$= 1/2 \times 2$$

$$= 1$$

So, we can say b_1 and b_2 form an orthonormal basis. Since $\langle b_1, b_2 \rangle = 0$ and $\langle b_1, b_1 \rangle = \langle b_2, b_2 \rangle = 1$.

2.7 Orthogonal Complement

- The orthogonal complement of U is denoted as U^\perp .
- U^\perp is a $(D - M)$ dimensional subspace of V , and contains all vectors in V that are orthogonal to every vector in U .

$$\text{Therefore } U \cap U^\perp = \{0\}$$

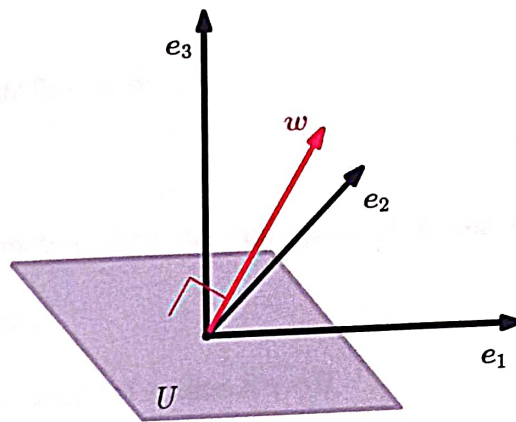


Figure : 2.3

Any vector $x \in V$ can be uniquely decomposed into

$$x = \sum_{m=1}^M \lambda_m b_m + \sum_{j=1}^{D-M} \psi_j b_j^\perp, \lambda_m, \psi_j \in \mathbb{R}$$

Where (b_1, b_2, \dots, b_M) is a basis of U and $(b_1^\perp, \dots, b_{D-M}^\perp)$ is a basis of U^\perp .

- The Orthogonal complement can also use to describe a plane U (2D subspace) in a 3D vector space

- The vector w with $\|w\|=1$ which is orthogonal to the plane U , is the basis vector of U^\perp . All vectors that are orthogonal to w must lie in the plane U .
- The vector w is called the normal vector of U .

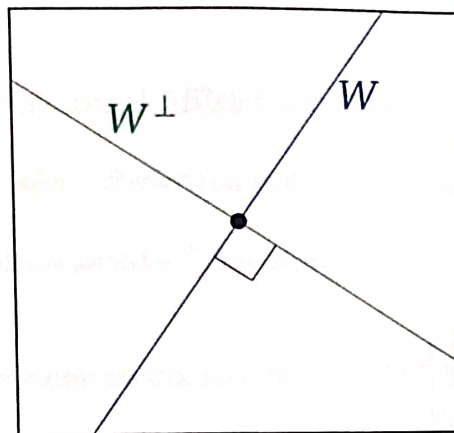


Figure : 2.4

The orthogonal complement of a line W through the origin in \mathbb{R}^2 is the perpendicular line of W .

Theorem: 2.7.1

If A is an $m \times n$ matrix, then the null space of A and the row space of A are orthogonal complements.

Proof: If \bar{x} is in the null space of A then $A\bar{x} = \mathbf{0}$

So, $\bar{r}_i \cdot \bar{x} = 0$ for each $i=1, \dots, m$

Let \bar{v} be any vector in the row space of A .

So $\bar{v} = K_1 \bar{r}_1 + \dots + K_m \bar{r}_m$

$\bar{v} \cdot \bar{x} = (K_1 \bar{r}_1 + \dots + K_m \bar{r}_m) \cdot \bar{x}$

$= K_1 \bar{r}_1 \cdot \bar{x} + \dots + K_m \bar{r}_m \cdot \bar{x} = 0.$

2.8 Affine Spaces

Definition: 2.8.1

A Affine space A in a set of vectors such that there exists a vector subspace V that every element of A can be written as $x_0 + v$ for $v \in V$.

Remark: 2.8.2

Any general two-dimensional Affine transformation can always be expressed as *Translation, Rotation, Scaling, Reflection* and *Shearing* of the object.

Remark: 2.8.3 (2D Transformation – Translation)

The general 2D Transformation matrix now become 3×3
$$\begin{bmatrix} a & c & l \\ b & d & m \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{i.e. } \begin{bmatrix} x' \\ y' \\ w \end{bmatrix} = \begin{bmatrix} a & c & l \\ b & d & m \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ l \end{bmatrix}$$

$$x' = ax + cy + l$$

$$y' = bx + dy + m$$

$$w = 1$$

Example: 2.8.5

Compute W where $W = \text{span} \left(\begin{pmatrix} 1 \\ 7 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix} \right)$

Solution:

According to the proposition, we need to compute the null space of the matrix

$$\begin{pmatrix} 1 & 7 & 2 \\ -2 & 3 & 2 \end{pmatrix} \xrightarrow{RREF} \begin{pmatrix} 1 & 0 & -\frac{1}{17} \\ 0 & 1 & \frac{5}{17} \end{pmatrix}$$

The free variable is x_3 , so the parametric form of the solution set is

$$x^1 = \frac{x^3}{17}, x^2 = -\frac{5x^3}{17} \text{ and the parametric vector}$$

$$\begin{pmatrix} x^1 \\ x^2 \\ x^3 \end{pmatrix} = x_3 \begin{pmatrix} \frac{1}{17} \\ -\frac{5}{17} \\ 1 \end{pmatrix}$$

Scaling by a factor of 17, we see that

$$W^\perp = \text{span} \begin{pmatrix} 1 \\ -5 \\ 7 \end{pmatrix}$$

We can check out work:

$$\begin{pmatrix} 1 \\ 7 \\ 2 \end{pmatrix} \begin{pmatrix} 1 \\ -5 \\ 17 \end{pmatrix} = 0 \quad \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ -5 \\ 17 \end{pmatrix} = 0$$

Chapter 3

Chapter 3

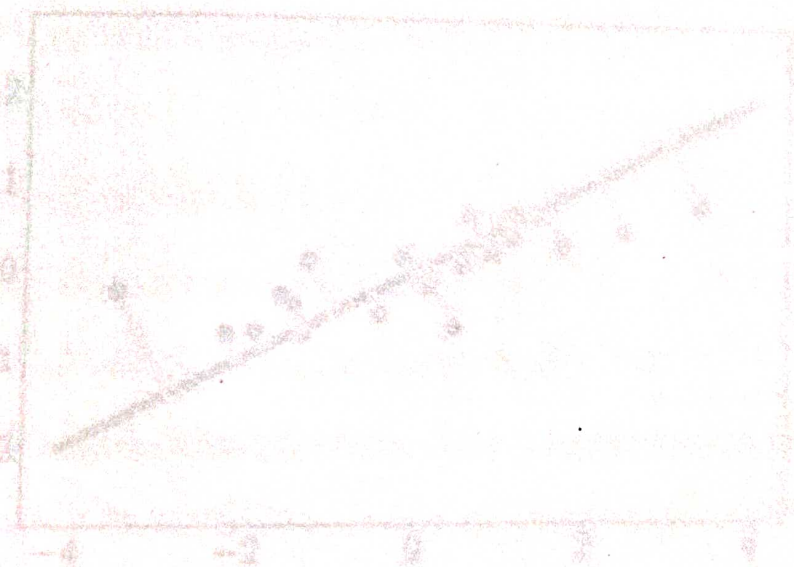


Figure 3.1

CHAPTER 3

ORTHOGONAL PROJECTION

3.1 Introduction

Projections are an important type of linear transformation (besides rotations and reflections) and play an important role in graphics, coding theory, statistics and machine learning. In machine learning, we often deal with data that is high-dimensional. High-dimensional data is often hard to analyze or visualize. However, high-dimensional data quite often possesses the property that only a few dimensions contain most information, and most other dimensions are not essential to describe key properties of the data. When we compress or visualize high-dimensional data, we will lose information. More, we can project the original high-dimensional data onto a lower-dimensional feature space and work in this lower-dimensional space.

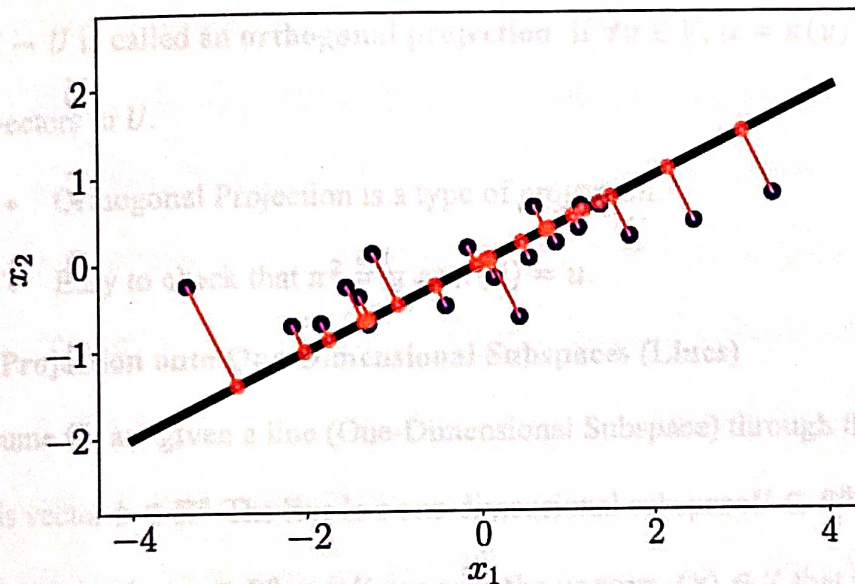


Figure: 3.1

3.2 Projection

Definition: 3.2.1

Let V be a vector space and $U \subseteq V$ a subspace of V . A linear mapping $\pi: V \rightarrow U$ is called a **projection** if $\pi^2 = \pi \circ \pi = \pi$.

Since linear mapping can be expressed by transformation matrices, the preceding definition applies equally to a special kind of transformation matrices, the projection matrices P_π , which exhibit the property that $P_\pi^2 = P_\pi$.

In the following, we will derive orthogonal projection of vectors in the inner product space $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ onto subspaces. We will start with one-dimensional subspaces, which are also called line. If not mentioned otherwise, we assume that the dot product $\langle x, y \rangle = x^T y$ as the inner product.

Definition: 3.2.2

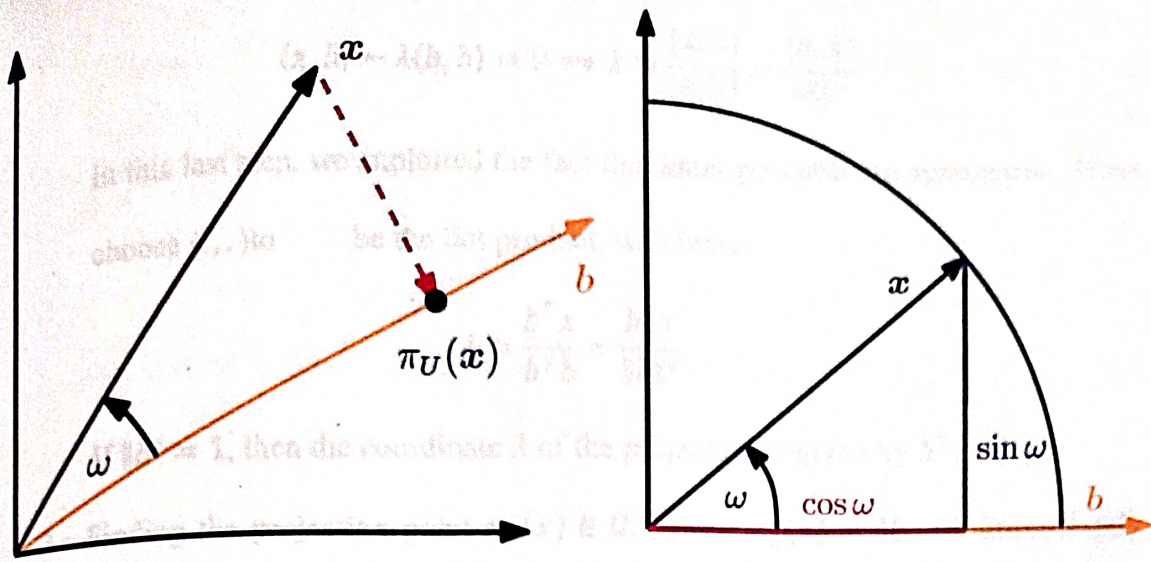
Let V be a vector space and $U \subseteq V$ a subspace of V . A linear mapping $\pi: V \rightarrow U$ is called an **orthogonal projection** if $\forall v \in V, u = \pi(v)$ is the closest v for all vectors in U .

- Orthogonal Projection is a type of projection.
- Easy to check that $\pi^2 = \pi$ as $\pi(u) = u$.

3.3 Projection onto One-Dimensional Subspaces (Lines)

Assume we are given a line (One-Dimensional Subspace) through the origin with basis vector $b \in \mathbb{R}^n$. The line is a one-dimensional subspace $U \subseteq \mathbb{R}^n$ spanned by b .

When we project $x \in \mathbb{R}^n$ onto U , we seek the vector $\pi_U(x) \in U$ that is closest to x .



a) Projection $x \in \mathbb{R}^2$ onto a Subspace U With basis vector b .

b) Projection of a two-dimensional vector x with $\|x\| = 1$ onto a one dimensional subspace spanned by b .

Figure: 3.2

Using geometric arguments, Let us characterize some properties of the projection $\pi_U(x)$

- The projection $\pi_U(x)$ is closest to x , where “closest” implies that the distance $\|x - \pi_U(x)\|$ is minimal. It follows that the segment $\pi_U(x) - x$ from $\pi_U(x)$ to x is orthogonal to U . The orthogonality condition yields $\langle \pi_U(x) - x, b \rangle = 0$. Since angles between vectors are defined via in the inner product.
- The projection $\pi_U(x)$ of x onto U and therefore, a multiple of the basis vector b that spans U . Hence, $\pi_U(x) = \lambda b$, for some $\lambda \in \mathbb{R}$. λ is the coordinates of $\pi_U(x)$ with respect to b .

In the following three steps, we determine the coordinate λ , the projection $\pi_U(x) \in U$, and the projection matrix P_π that maps any $x \in \mathbb{R}^n$ onto U .

1. Finding the coordinate λ . The orthogonality condition yields

$$\langle x - \pi_U(x), b \rangle = 0 \iff \langle x - \lambda b, b \rangle = 0$$

We can now exploit the bilinearity of the inner product and arrive at

$$\langle x, b \rangle - \lambda \langle b, b \rangle = 0 \Leftrightarrow \lambda = \frac{\langle x, b \rangle}{\langle b, b \rangle} = \frac{\langle b, x \rangle}{\|b\|^2}$$

In this last step, we exploited the fact that inner products are symmetric. If we choose $\langle \cdot, \cdot \rangle$ to be the dot product, we obtain

$$\lambda = \frac{b^T x}{b^T b} = \frac{b^T x}{\|b\|^2}$$

If $\|b\| = 1$, then the coordinate λ of the projection is given by $b^T x$.

2. Finding the projection point $\pi_U(x) \in U$. Since $\pi_U(x) = \lambda b$, we immediately obtain with that

$$\pi_U(x) = \lambda b = \frac{\langle x, b \rangle}{\|b\|^2} b = \frac{b^T x}{\|b\|^2} b$$

Where the last equality holds for the dot product only. We can also compute the length of $\pi_U(x)$

$$\|\pi_U(x)\| = \|\lambda b\| = |\lambda| \|b\|$$

Hence, our projection is of length $|\lambda|$ times the length of b . This is also adds the intuition that λ is the coordinate of $\pi_U(x)$ with respect to the basis vector b that spans our one-dimensional subspace U .

If we use the dot product as an inner product we get

$$\|\pi_U(x)\| = \frac{|b^T x|}{\|b\|^2} \|b\| = |\cos w| \|x\| \|b\| \frac{\|b\|}{\|b\|} = |\cos w| \|x\|$$

Here, w is the angle between x and b . This equation should be familiar from trigonometry. If $\|x\| = 1$, then x lies on the unit circle. It follows that the rejection onto the horizontal axis spanned by b is exactly $\cos w$, and the length of the corresponding vector $|\pi_U(x)| = |\cos w|$.

3. Finding the projection matrix P_π . We know that a projection is a linear mapping. Therefore, there exists a projection matrix P_π , such that $\pi_U(x) = P_\pi x$. With the dot product as inner product and

$$\pi_U(x) = \lambda b = b\lambda = b \frac{b^T x}{\|b\|^2} = \frac{bb^T}{\|b\|^2} x,$$

We immediately see that

$$P_\pi = \frac{bb^T}{\|b\|^2}.$$

Note that bb^T (and consequently, P_π) is a symmetric matrix (of rank 1), and

$$\|b\|^2 = \langle b, b \rangle \text{ is a scalar.}$$

Remark: 3.3.1

The projection matrix P_π projects any vector $x \in \mathbb{R}^n$ is still an n -dimensional vector not a scalar. However, we no longer require n coordinates to represent the projection, but only a single one if we want to express it with respect to the basis vector b that spans the subspace $U: \lambda$.

Example: 3.3.2 (Projection onto a line)

Find the projection matrix P_π onto the line through the origin spanned by $b = [1 \ 2 \ 2]^T$. b is a direction and a basis of the one-dimensional subspace (line through origin).

Solution:

We obtain,

$$P_\pi = \frac{bb^T}{b^T b} = \frac{1}{9} \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} [1 \ 2 \ 2] = \frac{1}{9} \begin{bmatrix} 1 & 2 & 2 \\ 2 & 4 & 4 \\ 2 & 4 & 4 \end{bmatrix}$$

Let us now choose a particular x and see whether it lies in the subspace spanned by

b . For $x = [1 \ 1 \ 1]^T$, the projection is

$$\pi_U(x) = P_\pi x = \frac{1}{9} \begin{bmatrix} 1 & 2 & 2 \\ 2 & 4 & 4 \\ 2 & 4 & 4 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{9} \begin{bmatrix} 5 \\ 10 \\ 10 \end{bmatrix} \in \text{span} \left[\begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \right].$$

Note that the application of P_π to $\pi_U(x)$ does not change anything, i.e., $P_\pi \pi_U(x) = \pi_U(x)$.

Example: 3.3.3 (Projection onto One-Dimensional subspaces in \mathbb{R}^2)

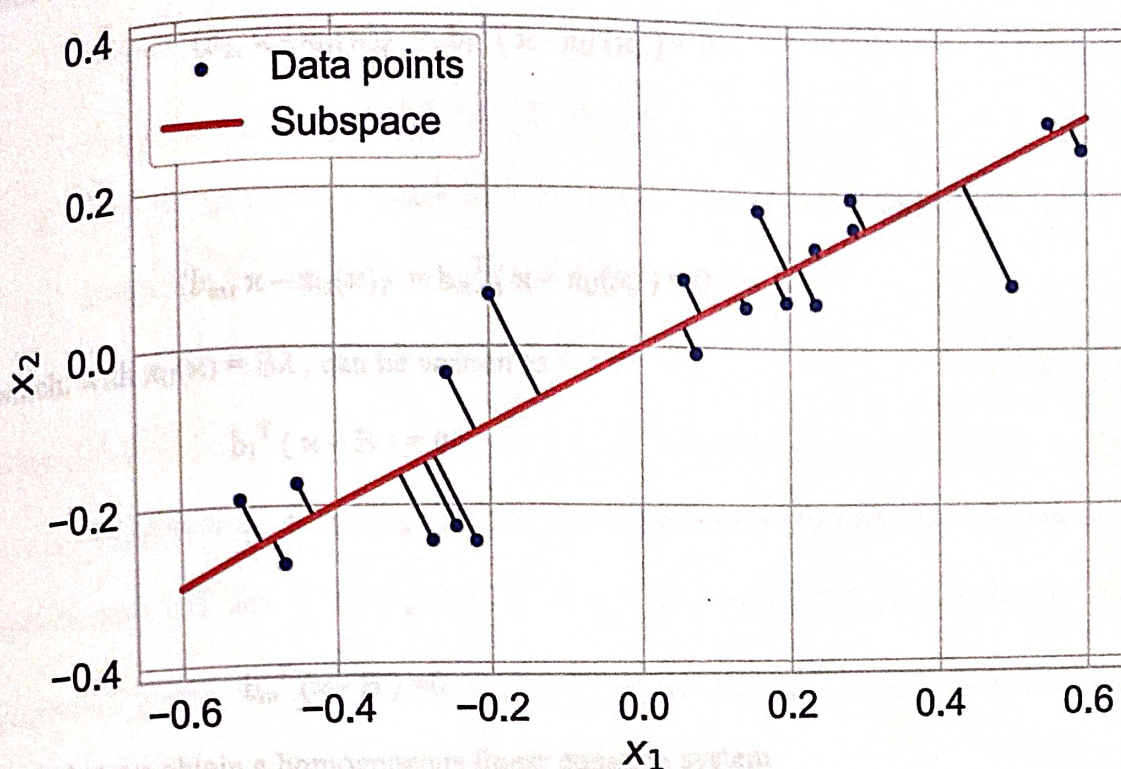


Figure: 3.3

Subspace U spanned by $\mathbf{b} = [1, 0.5]^T \in \mathbb{R}^2$, different data points are projected onto subspace U .

3.4 Projection onto a Two Dimensional Subspace

As in the 1D case, we follow a three-step procedure to find the projection $\pi_U(\mathbf{x})$ and the projection matrix P_π :

1. Find the coordinates $\lambda_1, \lambda_2, \dots, \lambda_m$ of the projection (with respect to the basis of U), such that the linear combination

$$\begin{aligned}\pi_U(\mathbf{x}) &= \sum_{i=1}^m \lambda_i \mathbf{b}_i \\ &= B\boldsymbol{\lambda}\end{aligned}$$

$$B = [\mathbf{b}_1, \dots, \mathbf{b}_m] \in \mathbb{R}^{m \times n}, \quad \boldsymbol{\lambda} = [\lambda_1, \lambda_2, \dots, \lambda_m]^T \in \mathbb{R}^m,$$

is closest to $\mathbf{x} \in \mathbb{R}^n$. As in the 1D case, "closest" means "minimum distance", which implies that the vector connecting $\pi_U(\mathbf{x}) \in U$ and $\mathbf{x} \in \mathbb{R}^n$ must be orthogonal to all

basis vectors of U . Therefore, we obtain m simultaneous conditions (assuming the dot product as the inner product)

$$\langle b_1, \kappa - \pi_U(\kappa) \rangle = b_1^T (\kappa - \pi_U(\kappa)) = 0$$

$$\langle b_m, \kappa - \pi_U(\kappa) \rangle = b_m^T (\kappa - \pi_U(\kappa)) = 0$$

which, with $\pi_U(\kappa) = B\lambda$, can be written as

$$b_1^T (\kappa - B) = 0$$

$$b_m^T (\kappa - B) = 0$$

such that we obtain a homogeneous linear equation system

$$\begin{bmatrix} b_1^T \\ \vdots \\ b_m^T \end{bmatrix} [\kappa - B\lambda] = 0 \Leftrightarrow B^T (\kappa - B\lambda) = 0$$

$$\Leftrightarrow B^T B \lambda = B^T \kappa.$$

The last expression is called **normal equation**. Since b_1, \dots, b_m are a basis of U and, therefore, linearly independent, $B^T B \in \mathbb{R}^{m \times m}$ is regular and can be inverted. This allows us to solve for the coefficients coordinates,

$$\lambda = (B^T B)^{-1} B^T \kappa$$

The matrix $(B^T B)^{-1} B^T$ is also called the **pseudo-inverse** of B , which can be computed for non-square matrices B .

It only requires that $B^T B$ is positive definite, which is the case if B is full rank. In practical applications (e.g., linear regression), we often add a "jitter term" ϵI to $B^T B$ to guarantee increased numerical stability and positive definiteness.

This "ridge" can be rigorously derived using Bayesian inference.

1. Find the projection $\pi_U(\kappa) \in U$. We already established that $\pi_U(\kappa) = B\lambda$.

Therefore,

$$\pi_U(\kappa) = B (B^T B)^{-1} B^T \kappa \quad \dots\dots\dots(1)$$

2. Find the projection matrix P_π . From (1), we can immediately see that the projection matrix that solves $P_\pi \kappa = \pi_U(\kappa)$ must be

$$P_\pi = B (B^T B)^{-1} B^T \quad \dots\dots\dots(2)$$

Note: 3.4.1

The solution for projecting onto general subspaces includes the 1D case as a special case. If $\dim(U) = 1$, then $B^T B \in \mathbb{R}$ is a scalar and we can rewrite the projection matrix in (2) $P_\pi = B (B^T B)^{-1} B^T$ as $P_\pi = \frac{B B^T}{B^T B}$, which is exactly the projection matrix.

Example: 3.4.2(Projection onto a Two-dimensional Subspace)

For a subspace $U = \text{span} \left[\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \right] \subseteq \mathbb{R}^3$ and $\kappa = \begin{bmatrix} 6 \\ 0 \\ 0 \end{bmatrix} \in \mathbb{R}^3$, find the coordinates λ of κ in terms of the subspace U , the projection point $\pi_U(\kappa)$ and the projection matrix P_π .

Solution: First, we see that the generating set of U is a basis (linear independence)

and write the basis vectors of U into a matrix $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 2 \end{bmatrix}$.

Second, we compute the matrix $B^T B$ and the vector $B^T \kappa$ as

$$\begin{aligned} B^T B &= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1+1+1 & 0+1+2 \\ 0+1+2 & 0+1+4 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 3 \\ 3 & 5 \end{bmatrix}. \end{aligned}$$

$$B^T \kappa = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 6 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix}.$$

Third, we solve the normal equation $B^T B (\lambda) = B^T \kappa$ to find λ :

$$\Rightarrow \begin{bmatrix} 3 & 3 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix}$$

$$\Rightarrow \lambda = \begin{bmatrix} 5 \\ -3 \end{bmatrix}$$

Fourth, the projection $\pi_U(\kappa)$ of κ onto U , i.e., into the column space of B , can be directly computed via, $\pi_U(\kappa) = B \lambda$

$$= \begin{bmatrix} 5 \\ 2 \\ -1 \end{bmatrix}$$

The corresponding **projection error** is the norm of the difference vector between the original vector and its projection onto U , i.e.,

$$\|\kappa - \pi_U(\kappa)\| = \|[1 \ 2 \ -1]^T\|$$

$$\Rightarrow \sqrt{6}$$

(The projection error is also called the **reconstruction error**.)

Fifth, the projection matrix (for any $\kappa \in \mathbb{R}^3$) is given by,

$$P_\pi = B (B^T B)^{-1} B^T$$

$$= \frac{1}{6} \begin{bmatrix} 5 & 2 & -1 \\ 2 & 2 & 2 \\ -1 & 2 & 5 \end{bmatrix}$$

$$P_\pi = \frac{1}{6} \begin{bmatrix} 5 & 2 & -1 \\ 2 & 2 & 2 \\ -1 & 2 & 5 \end{bmatrix}$$

Remark: 3.4.3

❖ The projections $\pi_U(\kappa)$ are still vectors in \mathbb{R}^n although they lie in an m -dimensional subspace $U \subseteq \mathbb{R}^n$. However, to represent a projected vector we only need the m coordinates $\lambda_1, \dots, \lambda_m$ with respect to the basis vectors b_1, \dots, b_m of U .

❖ In vector spaces with general inner products, we have to pay attention when computing angles and distances, which are defined by means of the inner product. (We can find approximate solutions to linear equation systems using projections)

Example: 3.4.4

Find the projection matrix onto the plane $x + y + z = 0$.

Soluton: A basis for this plane is $(1, 0, -1)$ and $(0, 1, -1)$. Putting these as the columns of a matrix. We get the following results:

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & -1 \end{bmatrix}$$

$$A^T = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}$$

$$A^T A = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & -1 \end{bmatrix}$$

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

$$= \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

$$(A^T A)^{-1} = \frac{1}{|A^T A|} (\text{adj } A)$$

$$|A| = \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix}$$

$$= 4-1$$

$$= 3$$

$$= \frac{1}{3} \begin{vmatrix} 2 & -1 \\ -1 & 2 \end{vmatrix}$$

$$(A^T A)^{-1} = \begin{bmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{bmatrix}$$

$$P = A (A^T A)^{-1} A$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \end{bmatrix}$$

The final projection matrix $P = \begin{bmatrix} 2/3 & -1/3 & -1/3 \\ -1/3 & 2/3 & -1/3 \\ -1/3 & -1/3 & 2/3 \end{bmatrix}$

Note: 3.4.5

- ❖ Projections allow us to look at situations where we have a linear system $Ax = b$ without a solution.
- ❖ Recall that this means that b does not lie in the span of A , i.e., the vector b does not lie in the subspace spanned by the columns of A . Given that the linear equation cannot be solved exactly, we can find an *approximate solution*.
- ❖ The idea is to find the vector in the subspace spanned by the columns of A that is closest to b , i.e., we compute the orthogonal projection of b onto the subspace spanned by the columns of A .

The obtained solution is called the *least-squares solution* (assuming the dot product as the inner product) of an overdetermined system.

Remark: 3.4.6

We just looked at projections of vectors x onto a subspace U with basis vectors $\{b_1, \dots, b_k\}$. The projection equation (1) simplifies greatly to

$$\pi_U(x) = B B^T x$$

since $B^T B = I$ with coordinates $\lambda = B^T x$. (This means that we no longer have to compute the inverse (1), which saves computation time.)

3.5 Projection onto General Subspace

Orthogonal projections of vectors $\mathbf{x} \in \mathbb{R}^n$ onto lower-dimensional subspaces $U \subseteq \mathbb{R}^n$ with $\dim(U) = m \geq 1$. Assume that (b_1, b_2, \dots, b_m) is an ordered basis of U . Any projection $\pi_U(\mathbf{x})$ onto U is necessarily an element of U . Therefore, they can be represented as the linear combinations of the basis vectors b_1, b_2, \dots, b_m of U , such that $\pi_U(\mathbf{x}) = \sum_{i=1}^m \lambda_i b_i$.

Theorem: 3.5.1

If the columns of A are independent, then $A^T A$ is invertible.

Proof:

Actually, this is iff; if the columns of A are not independent, then A has a nontrivial null vector, which is also a nontrivial null vector of $A^T A$, so the latter can't be invertible. On the other hand, if $A^T A$ is not invertible, it has a nontrivial null vector \mathbf{n} .

Then $A^T A \mathbf{n} = 0$. So $\mathbf{n}^T A^T A \mathbf{n} = 0$. Thus $(A \mathbf{n})^T (A \mathbf{n}) = 0$, so $\|A \mathbf{n}\| = 0$, and $A \mathbf{n} = 0$. Thus the columns of A weren't independent after all.

Theorem: 3.5.2

A matrix is a projection matrix if and only if $P = P^T = P^2$.

Proof:

Let $P = P^T = P^2$ (properties of projection) and let V be the column space of P . We show that P projects onto this space. Certainly for any vector \mathbf{x} , we have $\mathbf{x} = P\mathbf{x} + (\mathbf{x} - P\mathbf{x})$, and $P\mathbf{x}$ is certainly in the column space. We need to show that $\mathbf{x} - P\mathbf{x}$ is orthogonal to the column space. So let \mathbf{y} be any vector in V , so that $\mathbf{y} = P\mathbf{z}$ for some \mathbf{z} .

$$\text{Then } \mathbf{y} \cdot (\mathbf{x} - P\mathbf{x}) = \mathbf{y}^T \mathbf{x} - \mathbf{y}^T P\mathbf{x} = \mathbf{z}^T P^T \mathbf{x} - \mathbf{z}^T P^T P\mathbf{x} = \mathbf{z}^T P\mathbf{x} - \mathbf{z}^T P^2 \mathbf{x} = \mathbf{z}^T P\mathbf{x} - \mathbf{z}^T P\mathbf{x} = 0.$$

Corollary: 3.5.3

If P is the projection matrix onto a subspace V , then $I - P$ is the projection matrix onto its orthogonal complement.

Proof:

$(I - P)x = x - Px$, which is exactly what's left over when we split off the V part of x in the above proof.

3.6 Gram-Schmidt Orthogonalization

Projections are at the core of the Gram-Schmidt method that allows us to constructively transform any basis (b_1, \dots, b_n) of an n -dimensional vector space V into an orthogonal/orthonormal basis (u_1, \dots, u_n) of V . This basis always exists (Liesen and Mehrmann, 2015) and $\text{span}[b_1, \dots, b_n] = \text{span}[u_1, \dots, u_n]$.

The *Gram-Schmidt orthogonalization* method iteratively constructs an orthogonal basis (u_1, \dots, u_n) from any basis (b_1, \dots, b_n) of V as

$$u_1 = b_1$$

$$u_k := b_k - \pi_{\text{span}[u_1, \dots, u_{k-1}]}(b_k)$$

$$(k = 2, \dots, n) \dots \dots \dots (1)$$

In (1), the k th basis vector b_k is projected onto the subspace spanned by the first $k - 1$ constructed orthogonal vectors u_1, \dots, u_{k-1} . This projection is then subtracted from b_k and yields a vector u_k that is orthogonal to the $(k - 1)$ -dimensional subspace spanned by u_1, \dots, u_{k-1} .

Repeating this procedure for all n basis vectors b_1, \dots, b_n yields an orthogonal basis (u_1, \dots, u_n) of V . If we normalize the u_k , we obtain an **Orthonormal basis** (ONB) where $\|u_k\| = 1$ for $k = 1, \dots, n$.

3.6.1: Gram – Schmidt Process:

It is the Iterative method to build orthonormal basis. Assume the set $\{\tilde{b}_1, \dots, \dots, \tilde{b}_n\}$

1. Concentrate them to matrix B

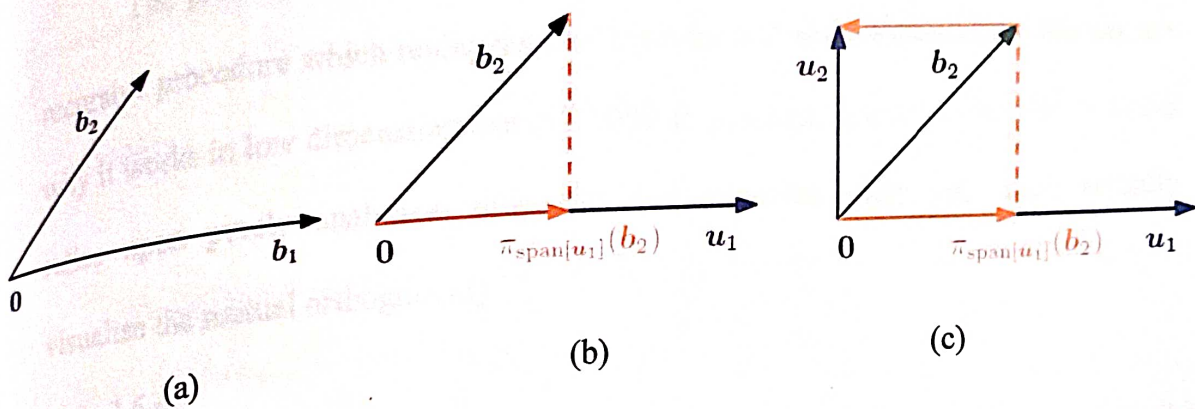
$$\tilde{B} = [\tilde{b}_1, \tilde{b}_2, \dots, \tilde{b}_n]$$

2. Apply Gaussian Elimination to the augmented matrix

$$[\tilde{B} \mid \tilde{B}^T \tilde{B}]$$

3. The result will be the orthonormal basis.

Example: 3.6.2 (Gram-Schmidt Orthogonalization)



(a) Original non-orthogonal basis vectors b_1, b_2 .

(b) First new basis vector $u_1 = b_1$ and projection of b_2 onto the subspace spanned by u_1

(c) Orthogonal basis vectors u_1 and $u_2 = b_2 - \pi_{\text{span}[u_1]}(b_2)$.

Consider a basis (b_1, b_2) of \mathbb{R}^2 , where $b_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$ and $b_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

Figure (a). Using the Gram-Schmidt method, we construct an orthogonal basis

(u_1, u_2) of \mathbb{R}^n as follows (assuming the dot product as the inner product):

$$u_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$b_1 = \begin{bmatrix} 2 \\ 0 \end{bmatrix},$$

$$u_2 = b_2 - \pi_{\text{span}[u_1]}(b_2)$$

$$= b_2 - \frac{u_1 u_1^T}{\|u_1\|^2} b_2$$

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

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

$$u_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

3.6.3: Why Gram-Schmidt orthogonalization works ?

The Gram-Schmidt orthogonalisation process is fundamental to linear algebra and its applications to machine learning for instance. In many courses it is presented as an algorithm that works without any real motivation.

The proof of the Gram-Schmidt (GS) orthogonalisation process relies upon a recursive procedure which replicates why it works in 2 and 3 dimensions. We can see why it works in low dimensions but in a 1000 dimensional space the fact that it works relies upon purely analytical properties and induction since you can't actually visualise the mutual orthogonality.

Note 3.6.4:

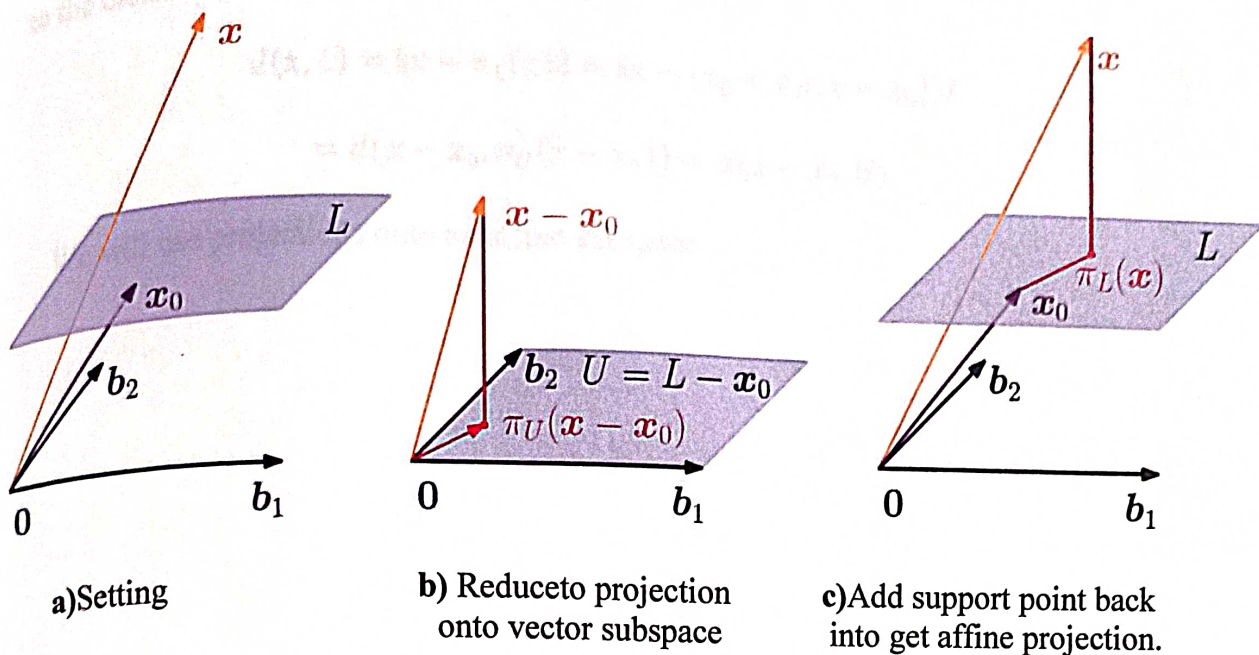
- To obtain an orthonormal basis, which is an orthogonal set in which each vector has norm 1, for an inner product space V , use the Gram-Schmidt algorithm to construct an orthogonal basis. Then simply normalize each vector in the basis.

- For \mathbb{R}_n with the Euclidean inner product dot product, we of course already know

the orthonormal $\{ (1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots \}$

For more abstract spaces, however the existence of an orthonormal basis is not obvious. The Gram-Schmidt algorithm is powerful in that it not only guarantees the existence of an orthonormal basis for any inner product space, but actually gives the construction of such a basis.

3.7: Projection Onto Affine Subspace:



We discussed how to projection a vector onto a lower – dimensional subspace U . In the following , we provid a solution to project a vector onto an affine subspace. Consider the setting in figure (a) . We are given an affine space $L = x_0 + U$, Where b_1, b_2 are basis vectors of U . To determine the orthogonal projection $\pi_L(x)$ of x onto L , we transform the problem into a problem that we know how to solve: the projection onto a vector subspace. In order to get there ,we subtract the support point x_0 from x and from L , so that $L - x_0 = U$ is exactly the vector subspace U . We can now use the orthogonal projection onto a subspace we discussed and obtain the projection $\pi_U(x - x_0)$, which is illustrated in figure (b) . this projection can now be translated back into L by adding x_0 , so that we obtain the orthogonal projection onto an affine space L as

$$\pi_L(x) = x_0 + \pi_U(x - x_0),$$

Where $\pi_U(.)$ is the orthogonal projection onto subspace U , i.e., the direction space of L ; see figure c.

From figure (b) it is also evident that distance of x from the affine space L is identical to the distance of $x - x_0$ from U , i.e. ,

$$d(x, L) = \|x - \pi_L(x)\| = \|x - (x_0 + \pi_U(x - x_0))\|$$

$$= d(x - x_0, \pi_U(x - x_0)) = d(x - x_0, U).$$

We will use projections onto an affine subspace .

Chapter 4

Chapter 4

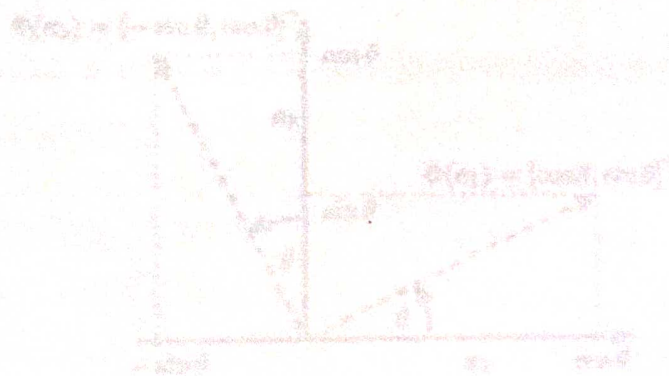


Figure: 4.1

CHAPTER 4

ROTATION

4.1 Introduction

In linear algebra, a **rotation matrix** is a transformation matrix that is used to perform a rotation in Euclidean space. For example, using the convention below, the

matrix $R = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$ rotates points in the xy plane counter clockwise through an angle θ with respect to the positive x axis about the origin of a two-dimensional Cartesian coordinate system. To perform the rotation on a plane point with standard

coordinates $\mathbf{v} = (x, y)$, it should be written as a column vector, and multiplied by the matrix R :

$$R\mathbf{v} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \cos \theta - y \sin \theta \\ x \sin \theta + y \cos \theta \end{bmatrix}$$

If x and y are the endpoint coordinates of a vector, where x is cosine and y is sine, then the above equations become the trigonometric summation angle formulae. Indeed, a rotation matrix can be seen as the trigonometric summation angle formulae

in matrix form. One way to understand this is say we have a vector at an angle 30° from the x axis, and we wish to rotate that angle by a further 45° . We simply need to compute the vector endpoint coordinates at 75° .

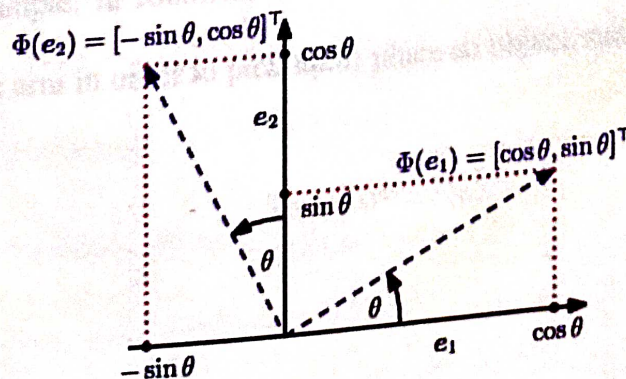


Figure: 4.1

A rotation is a linear mapping (more specifically, an automorphism of a Euclidean vector space) that rotates a plane by an angle θ about the origin, i.e., the origin is a fixed point. For a positive angle $\theta > 0$, by common convention, we rotate in a counter clockwise direction. An example is shown in the figure, where the transformation matrix is

$$R = \begin{bmatrix} -0.38 & -0.92 \\ 0.92 & -0.38 \end{bmatrix}$$

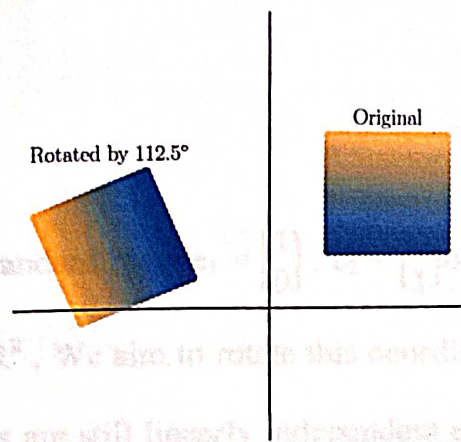


Figure: 4.2

A rotation rotates objects in a plane about the origin. If the rotation angle is positive, we rotate counter clockwise.

Important application areas of rotations include computer graphics and robotics. For example, in robotics, it is often important to know how to rotate the joints of a robotic arm in order to pick up or place an object, see the figure 4.3.

$$R(\theta) = [\Phi(e_1) \quad \Phi(e_2)] = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

For Example: This rotates column vectors by means of the following matrix multiplication

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

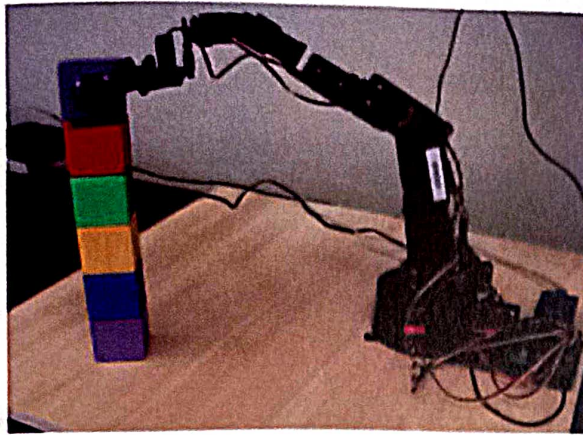


Figure: 4.3

The robotic arm needs to rotate its joints in order to pick up objects or to place them correctly.

4.2 Rotation in \mathbb{R}^2

Consider the standard basis $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ of \mathbb{R}^2 , which defines the standard coordinate system in \mathbb{R}^2 . We aim to rotate this coordinate system by an angle θ . Note that the rotated vectors are still linearly independent and, therefore, are a basis of \mathbb{R}^2 . This means that the rotation performs a basis change.

Rotations Φ are linear mappings so that we can express them by a rotation matrix $R(\theta)$. Trigonometry allows us to determine the coordinates of the rotated axes (the image of Φ) with respect to the standard basis in \mathbb{R}^2 . We obtain

$$\Phi(e_1) = \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix} \quad \Phi(e_2) = \begin{bmatrix} -\sin \theta \\ \cos \theta \end{bmatrix}$$

Therefore, the rotation matrix that performs the basis change into the rotated coordinates $R(\theta)$ is given as:

$$R(\theta) = [\Phi(e_1) \quad \Phi(e_2)] = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

For Example: This rotates column vectors by means of the following matrix multiplication

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Thus, the new coordinates (x', y') of a point (x, y) after rotation are:

$$x' = x \cos \theta - y \sin \theta$$

$$y' = x \sin \theta + y \cos \theta$$

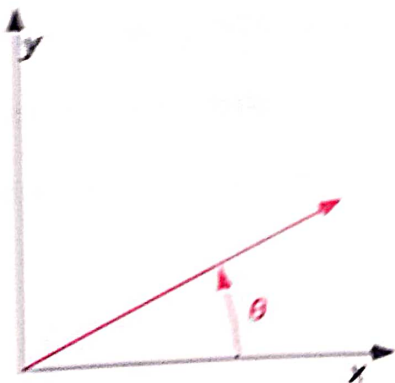


Figure: 4.4

a counter clockwise rotation of a vector through angle θ . The vector is initially aligned with the x -axis.

4.2.1: Direction

The direction of vector rotation is counter clockwise if θ is positive (e.g., 90°), and clockwise if θ is negative (e.g., -90°). Thus, the clockwise rotation matrix is found as

$$R = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}$$

The two-dimensional case is the only non-trivial (i.e., not one-dimensional) case where the rotation matrices group is commutative, so that it does not matter in which order multiple rotations are performed. An alternative convention uses rotating axes and the above matrices also represent a rotation of the axes clockwise through an angle θ .

4.2.2 Non-standard orientation of the coordinate system

If a standard **right-handed Cartesian coordinate system** is used, with the x -axis to the right and the y -axis up, the rotation $R(\theta)$ is counter clockwise. If a left-handed Cartesian coordinate system is used, with x directed to the right but y directed down, $R(\theta)$ is clockwise. Such non-standard orientations are rarely used in mathematics but are common in **2D computer graphics**, which often have the origin in the top left corner and the y -axis down the screen or page.

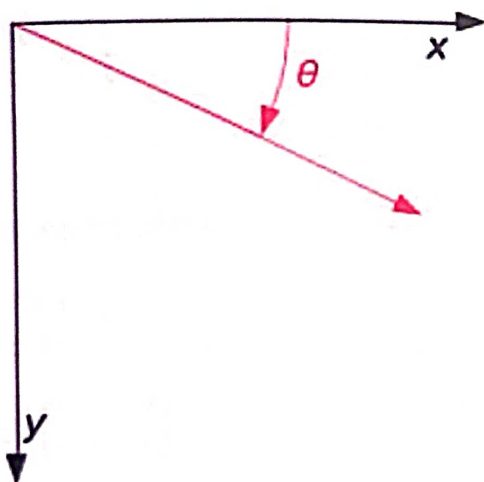


Figure: 4.5

4.2.3 Common Rotation

A 180° rotation (middle) followed by a positive 90° rotation (left) is equivalent to a single negative 90° (positive 270°) rotation (right). Each of these figures depicts the result of a rotation relative to an upright starting position (bottom left) and includes the matrix representation of the permutation applied by the rotation (centre right), as well as other related diagrams

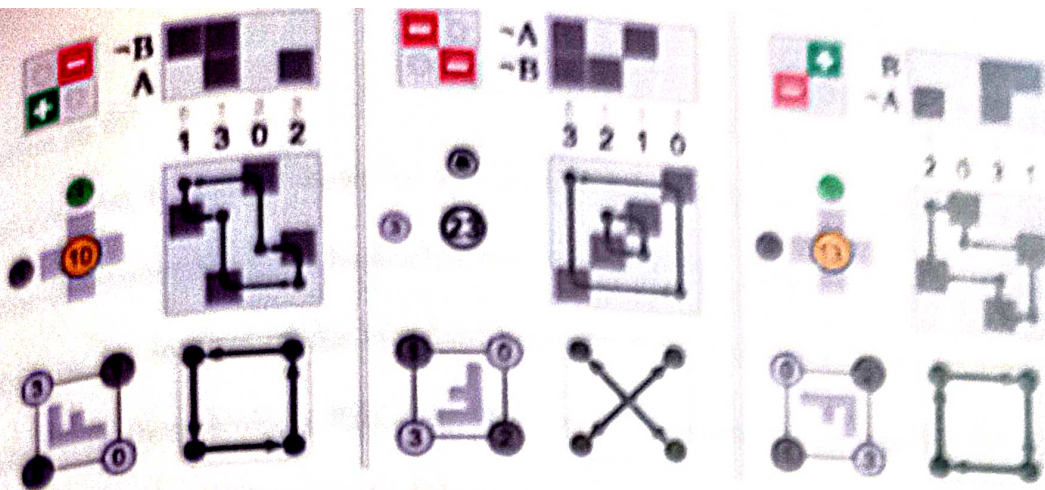


Figure: 4.6

For 90° , 180° , and 270° counter-clockwise rotations:

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

4.2.4 Relationship with complex plane

Since $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$

The matrix is of the shape: $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$

form a ring isomorphic to the field of the complex numbers \mathbb{C} . Under this isomorphism, the rotation matrices correspond to circle of the unit complex numbers, the complex numbers of modulus 1.

If one identify \mathbb{R}^2 with \mathbb{C} through the linear isomorphism $(a, b) \rightarrow a + ib$ the action of a matrix of the above form on vectors of \mathbb{R}^2 corresponds to the multiplication by the complex number $x + iy$, and rotations correspond to multiplication by complex numbers of modulus 1.

As every rotation matrix can be written as $\begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix}$, the above correspondence associates such a matrix with the complex number

$$\cos t + i \sin t = e^{it}$$

4.3 Rotation in \mathbb{R}^3

In contrast to the \mathbb{R}^2 case, in \mathbb{R}^3 we can rotate any two-dimensional plane about a one-dimensional axis. The easiest way to specify the general rotation matrix is to specify how the images of the standard basis e_1, e_2, e_3 are supposed to be rotated, and making sure these images Re_1, Re_2, Re_3 are orthonormal to each other. We can then obtain a general rotation matrix R by combining the images of the standard basis. To have a meaningful rotation angle, we have to define what "counter-clockwise" means when we operate in more than two dimensions. We use the convention that a "counter-clockwise" (planar) rotation about an axis refers to a rotation about an axis when we look at the axis "head on, from the end toward the origin". In \mathbb{R}^3 , there are therefore three (planar) rotations about the three standard basis vectors.

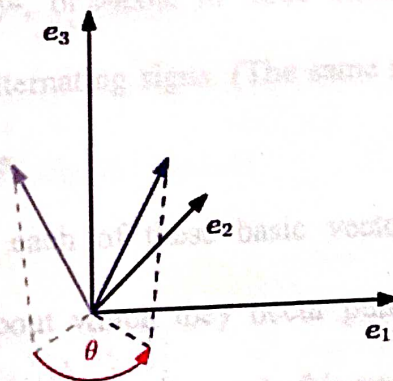


Figure: 4.7

- Rotation about the e_1 -axis

$$R_1(\theta) = [\Phi(e_1) \quad \Phi(e_2) \quad \Phi(e_3)] = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

Here, the e_1 coordinate is fixed, and the counter clockwise rotation is performed in the e_2e_3 plane.

- Rotation about the e_2 -axis

$$R_2(\theta) = \begin{bmatrix} \cos \theta & 0 & \sin \theta \\ 0 & 1 & 0 \\ -\sin \theta & 0 & \cos \theta \end{bmatrix}$$

If we rotate the e_1e_3 plane about the e_2 axis, we need to look at the e_2 axis from its "tip" toward the origin.

- Rotation about the e_3 -axis

$$R_3(\theta) = \begin{bmatrix} \cos \theta & \sin \theta & 0 \\ -\sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

4.3.1 Basic rotations

A basic rotation (also called elemental rotation) is a rotation about one of the axes of a coordinate system. The following three basic rotation matrices rotate vectors by an angle θ about the x -, y -, or z -axis, in three dimensions, using the right-hand rule—which codifies their alternating signs. (The same matrices can also represent a clockwise rotation of the axes.

For column vectors, each of these basic vector rotations appears counter clockwise when the axis about which they occur points toward the observer, the coordinate system is right-handed, and the angle θ is positive. R_z , for instance, would rotate toward the y -axis a vector aligned with the x -axis, as can easily be checked by operating with R_z on the vector $(1,0,0)$:

$$R_z(90) \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos 90 & \sin 90 & 0 \\ -\sin 90 & \cos 90 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

This is similar to the rotation produced by the above-mentioned two-dimensional rotation matrix. See below for alternative conventions which may apparently or actually invert the sense of the rotation produced by these matrices.

4.4 General Rotation

Other rotation matrices can be obtained from these three using matrix multiplication. For example, the product

$$R = R_z(\alpha) R_y(\beta) R_x(\nu)$$

$$= \begin{bmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \cos\beta & 0 & \sin\beta \\ 0 & 1 & 0 \\ -\sin\beta & 0 & \cos\beta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\nu & -\sin\nu \\ 0 & \sin\nu & \cos\nu \end{bmatrix}$$

$$= \begin{bmatrix} \cos\alpha\cos\beta & \cos\alpha\sin\beta\sin\nu - \sin\alpha\cos\nu & \cos\alpha\sin\beta\cos\nu + \sin\alpha\sin\nu \\ \sin\alpha\cos\beta & \sin\alpha\sin\beta\sin\nu + \cos\alpha\cos\nu & \sin\alpha\sin\beta\cos\nu - \cos\alpha\sin\nu \\ -\sin\beta & \cos\beta\sin\nu & \cos\beta\cos\nu \end{bmatrix}$$

represents a rotation whose yaw, pitch, and roll angles are α , β and γ , respectively.

More formally, it is an intrinsic rotation whose Tait-Bryan angles are α , β , γ , about axes z , y , x , respectively. Similarly, the product

$$R = R_z(\nu) R_y(\beta) R_x(\alpha)$$

$$= \begin{bmatrix} \cos\nu & -\sin\nu & 0 \\ \sin\nu & \cos\nu & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \cos\beta & 0 & \sin\beta \\ 0 & 1 & 0 \\ -\sin\beta & 0 & \cos\beta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{bmatrix}$$

$$= \begin{bmatrix} \cos\nu\cos\beta & \cos\nu\sin\beta\sin\alpha - \sin\nu\cos\alpha & \cos\nu\sin\beta\cos\alpha + \sin\nu\sin\alpha \\ \sin\nu\cos\beta & \sin\nu\sin\beta\sin\alpha + \cos\nu\cos\alpha & \sin\nu\sin\beta\cos\alpha - \cos\nu\sin\alpha \\ -\sin\beta & \cos\beta\sin\alpha & \cos\beta\cos\alpha \end{bmatrix}$$

represents an extrinsic rotation whose (improper) Euler angles are α , β , γ , about axes x , y , z .

These matrices produce the desired effect only if they are used to remultiply column vectors, and (since in general matrix multiplication is

not commutative) only if they are applied in the specified order. The order of rotation operations is from right to left; the matrix adjacent to the column vector is the first to be applied, and then the one to the left.

4.5 Rotation in n-Dimensions

The generalization of rotations from 2D and 3D to n-dimensional Euclidean vector spaces can be intuitively described as fixing $n - 2$ dimensions and restrict the rotation to a two-dimensional plane in the n-dimensional space. As in the three-dimensional case, we can rotate any plane (two-dimensional subspace of \mathbb{R}^n).

Definition: 4.5.1 (Givens Rotation).

Let V be an n-dimensional Euclidean vector space and $\Phi : V \rightarrow V$ an automorphism with transformation matrix.

$$R_{ij}(\theta) = \begin{bmatrix} I(i-1) & 0 & \dots & \dots & 0 \\ 0 & \cos \theta & 0 & -\sin \theta & 0 \\ 0 & 0 & I(j-i-1) & 0 & 0 \\ 0 & \sin \theta & 0 & \cos \theta & 0 \\ 0 & \dots & \dots & 0 & I(n-j) \end{bmatrix}$$

for $1 \leq i \leq j$ and $\theta \in \mathbb{R}$. Then $R_{ij}(\theta)$ is called a *Givens rotation*. Essentially, $R_{ij}(\theta)$ is the identity matrix I_n with

$$r_{ii} = \cos \theta, r_{ij} = -\sin \theta, r_{ji} = \sin \theta, r_{jj} = \cos \theta.$$

4.6 Properties of Rotation

Rotations exhibit a number of useful properties, which can be derived by considering them as orthogonal matrices

- Rotations preserve distances, i.e., $\|x-y\| = \|R\theta(x)-R\theta(y)\|$. In other words, rotations leave the distance between any two points unchanged after the transformation.

- Rotations preserve angles, i.e., the angle between $R\theta x$ and $R\theta y$ equals the angle between x and y .
- Rotations in three (or more) dimensions are generally not commutative. Therefore, the order in which rotations are applied is important, even if they rotate about the same point. Only in two dimensions vector rotations are commutative, such that $R(\varphi)R(\theta) = R(\theta)R(\varphi)$ for all $\varphi, \theta \in [0, 2\pi)$. They form an Abelian group (with multiplication) only if they rotate about the same point.

CONCLUSION

This project brings the mathematical foundations of basic machine learning concepts to the fore and collects the information in a single place so that this skills gap is narrowed or even closed. We have deeply discussed the concepts of the analytic geometry used in machine learning along with the orthogonal projection and their rotation. It has applications in nearly every other field of study and is already being implemented commercially because machine learning can solve problems which are too difficult or time consuming for humans to solve.

REFERENCE

1. Marc Peter Deisenroth, A. Aldo Faisal, Cheng Soon Ong, "MATHEMATICS FOR MACHINE LEARNING"
2. Sheldon Axler, "LINEAR AGEBRA DONE RIGHT"
3. Wikipedia https://en.wikipedia.org/wiki/Rotation_matrix

**MATHEMATICAL FOUNDATION FOR
CYBERSECURITY AND CODING THEORY**

A project submitted to

ST. MARY'S COLLEGE (Autonomous), THOOTHUKUDI.

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NO
S. ESTHER	19SUMT09
S. JENISHLIN OIDA	19SUMT14
T. MALATHI	19SUMT18
K. NISHA	19SUMT25
S. VARSHINI	19SUMT38
S. VIJAYA ISWARYA	19SUMT40

Under the guidance of

Dr. R. MARIA IRUDHAYA ASPIN CHITRA M.Sc., M.Phil., Ph.D.,



DEPARTMENT OF MATHEMATICS

St. Mary's College (Autonomous), Thoothukudi.

May- 2022

CERTIFICATE

This is to certify that this project work entitled "MATHEMATICAL FOUNDATION FOR CYBERSECURITY AND CODING THEORY" is submitted to St. Mary's College (Autonomous), Thoothukudi affiliated to Manonmaniam Sundaranar University, Tirunelveli in partial fulfilment for the award of degree of Bachelor of Science in Mathematics and is the work done during the year 2021-2022 by the following students.

NAME	REGISTER NO
S. ESTHER	19SUMT09
S. JENISHLIN OIDA	19SUMT14
T. MALATHI	19SUMT18
K. NISHA	19SUMT25
S. VARSHINI	19SUMT38
S. VIJAYA ISWARYA	19SUMT40



Signature of the Guide



Signature of the Coordinator



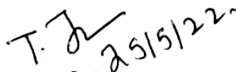
Signature of the Director
Director

Self Supporting Courses
St. Mary's College (Autonomous)
Thoothukudi - 628 001.



Signature of the Principal

Principal
St. Mary's College (Autonomous)
Thoothukudi - 628 001.



Signature of the Examiner

DECLARATION

We hereby declare that the project entitled "MATHEMATICAL FOUNDATION FOR CYBERSECURITY AND CODING THEORY" submitted for the degree of Bachelor of Science is my work carried out under the guidance of guide Dr. R. Maria Irudhaya Aspin Chitra M.Sc., M.Phil., Ph.D., Assistant Professor, Department of Mathematics (SSC), St.Mary's College(AUTONOMOUS), Thoothukudi.

S. Esther
(ESTHER .S)

S. Jenishlin Oida
(JENISHLIN OIDA .S)

T. Malathi
(MALATHI.T)

K. Nisha
(NISHA .K)

S. Varshini
(VARSHINI .S)

S. vijaya Iswarya
(VIJAYA ISWARYA .S)

ACKNOWLEDGEMENT

First of all, we thank the Almighty for showering his blessings to undergo this project. We express our sincere gratitude and heartfelt thanks to our Principal **Rev. Dr. Sr. A . S. J. Lucia Rose M.Sc., PGDCA., M.Phil., Ph.D.**, and to our Director **Rev. Sr. Josephine Jeyarani M.Sc.,B.Ed.**, for kindly permitting us to do this project.

We express our gratitude to **Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D.**, Coordinator, Department of Mathematics (SSC) for her inspirational ideas and encouragement.

We are very thankful to our guide **Dr. R. Maria Irudhaya Aspin Chitra M.Sc.,M.Phil.,Ph.D.**, Assistant Professor, Department of Mathematics (SSC) for her efficient and effective guidance. She played a key role in the preparation of this project.

We also thank our staff members for their encouragement in all our efforts. Finally, we thank all those who extended their help regarding this project.

Place: Thoothukudi

Date: 17-05-2022

CONTENT

CHAPTER	TOPIC	PAGE NO.
	Introduction	
1	Preliminaries	1
2	Abstract Algebra	4
3	Probability Theory	15
4	Coding Theory	25
5	Cyber security and	35
	Pseudo Random Generation	
	Applications	42
	Conclusion	
	References	

INTRODUCTION

The field of mathematics plays a vital role in various fields . One of important field in mathematics is **Cyber security and Coding Theory** . They are still a young subject . Cyber security originated in later 1970s and coding thory in later 1940s repectively. Cyber security has began with the project called **The Advanced Research Projects Agency Network (ARPANET)** . This was the connectivity developed prior itself .Cyber security is the applications of technologies , process and controls to protect systems , networks , programs , devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the systems and technologies . On the otherhand **Coding Theory** is the study of properties of codes and their respective fitness for specific applications.It is worthwhile nothing that all communications channels have errors , and thus codes are widely used . In addition to practical application **Cyber security and Coding Theory** has many applications in the theory of computer science .

The Project consists of five chapters.

In chapter 1 , we have dicussed **Preliminaries** and results thst are needed for the subsequent chapters.

In chapter 2 , we have discussed about the **Abstract Algebra** and its principle of well ordering.

In chapter 3 , we have discussed about the **Probability Theory** and its main concepts.

In chapter 4 , we have discussed about the **Coding Theory** and types of codes.

In chapter 5 , we have discussed about the **Cyber security and Pseudo Random Number Generation**.

Chapter 1

CHAPTER-1

PRELIMINARIES

Definition:1.1

A **code** is a set X such that for all $x \in X$, x is a codeword .

Definition:1.2

An **error correcting code** is an algorithm for expressing a sequence of numbers such that any errors which are introduced can be detected and corrected based on the remaining numbers .

Definition:1.3

The **Möbius inversion** formula μ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is the product} \\ & \text{of } k \text{ distinct prime factors} \\ 0 & \text{otherwise.} \end{cases}$$

Definition:1.4

An ideal S is called a **prime ideal** if $ab \in S$ implies $a \in S$ or $b \in S$. An ideal S in a ring R is called **maximal** if for every ideal I with $S \subset I \subset R$, I or $I = R$ ($S \neq R$) . If a ring has a unique maximal ideal , it is called a **local ring**.

Definition:1.5

Let $p(x), q(x)$ be open statements defined for a given universe.

The open statements $p(x)$ and $q(x)$ are called **(logically) equivalent**, and we write for all x [$p(x) \leftrightarrow q(x)$] when the biconditional $p(a) \leftrightarrow q(a)$ is true for each replacement a from the universe (that is, $p(a) \leftrightarrow q(a)$ for each a in the universe). If the implication $p(a) \Rightarrow q(a)$ for each a in the universe), then we write for all x [$p(x) \Rightarrow q(x)$] and say that $p(x)$ logically implies $q(x)$.

Definition:1.6

For open statements $p(x), q(x)$ defined for prescribed universe and the universally quantified statement for all $x [p(x) \rightarrow q(x)]$, we define

- 1) The **contrapositive** of for all $x [p(x) \rightarrow q(x)]$ to be for all $x [\neg q(x) \rightarrow \neg p(x)]$.
- 2) The **converse** of for all $x [p(x) \rightarrow q(x)]$ to be for all $x [q(x) \rightarrow p(x)]$.
- 3) The **inverse** of for all $x [p(x) \rightarrow q(x)]$ to be for all $x [\neg p(x) \rightarrow \neg q(x)]$.

Definition:1.7

For any nonempty set A, B , any function $f: A \times A \rightarrow B$ is called a **binary operation** on A . If $B \subseteq A$, then the binary operation is said to be closed. (When $B \subseteq A$ we may also say that A is closed under f).

Definition:1.8

For sets A and B , if $D \subseteq A \times B$, then $\pi_A : D \rightarrow A$ defined by $\pi_A (a, b) = a$, is called the **projection on the first coordinate**. The function $\pi_A : D \rightarrow B$, defined by $\pi_B (a, b) = b$, is called the **projection on the second coordinate**.

Definition:1.9

If $f: A \rightarrow B$, then f is said to be **invertible** if there is a function $g: B \rightarrow A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

Definition:1.10

If $f: A \rightarrow B$ and $B_1 \subseteq B$, then $f^{-1}(B_1) = \{x \in A \mid f(x) \in B_1\}$. The set $f^{-1}(B_1)$ is called the **preimage** of B_1 under f .

Definition:1.11

Let $f, g: \mathbb{Z}^+ \rightarrow \mathbb{R}$. We say that g **dominates** f (or f is dominated by g) if there exist constants $m \in \mathbb{R}^+$ and $k \in \mathbb{Z}^+$ such that $|f(n)| \leq m|g(n)|$ for all $n \in \mathbb{Z}^+$, where $n \geq k$.

Definition:1.12

If Σ is an alphabet and $n \in \mathbb{Z}^+$, we define the powers of Σ recursively as follows:

$$1) \Sigma^1 = \Sigma; \text{ and}$$

$$2) \Sigma^{n+1} = \{xy \mid x \in \Sigma, y \in \Sigma^n\}, \text{ where } xy \text{ denotes the juxtaposition of } x \text{ and } y.$$

Definiton:1.13

For an alphabet Σ we define $\Sigma^0 = \{\lambda\}$, where λ denotes the **empty string** - that is, the string consisting of no symbols taken from Σ .

Definition:1.14

$$\text{If } \Sigma \text{ is an alphabet, then a) } \Sigma^+ = \bigcup_{n=1}^{\infty} \Sigma^n = \bigcup_{n \in \mathbb{Z}^+} \Sigma^n$$

$$\text{and b) } \Sigma^* = \bigcup_{n=0}^{\infty} \Sigma^n.$$

Definition:1.15

If $w_1, w_2 \in \Sigma^+$ then we may write $w_1 = x_1 x_2 \dots x_m$ and $w_2 = y_1 y_2 \dots y_n$, form, $n \in \mathbb{Z}^+$, and $x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n \in \Sigma$. We say that the strings w_1 and w_2 are equal, and we write $w_1 = w_2$, if $m = n$, and $x_i = y_i$ for all $1 \leq i \leq m$.

Definition:1.16

Let $w = x_1 x_2 \dots x_n \in \Sigma^+$ where $x_i \in \Sigma$ for each $1 \leq i \leq n$. We define the length of w , which is denoted by $|w|$, as the value n . For the case of λ , we have $|\lambda| = 0$.

Definition:1.17

Let $x, y \in \Sigma^+$ with $x = x_1 x_2 \dots x_m$ and $y = y_1 y_2 \dots y_n$, so that each x_i , for $1 \leq i \leq m$, and each y_j , for $1 \leq j \leq n$, is in Σ . The concatenation of x and y , which we write as xy , is the string $x_1 x_2 \dots x_m y_1 y_2 \dots y_n$.

The concatenation of x and λ is $x\lambda = x_1 x_2 \dots \lambda x_m = x_1 x_2 \dots x_m = x$ and the concatenation of λ and x is $\lambda x = \lambda x_1 x_2 \dots x_m = x_1 x_2 \dots x_m = x$. finally, the concatenation of λ is $\lambda\lambda = \lambda$.

Chapter 2

CHAPTER – 2

ABSTRACT ALGEBRA

2.1 Integers

Definition:2.1.1

Throughout abstract algebra, the set of integers provides a source of examples.

In fact, many algebraic abstractions came from the integers.

For Example, If n and m are Integers with $n < m$ then there exists a positive integer $t \in \mathbb{Z}$ such that $m = n + t$.

Definition:2.1.2

Let S be a subset of \mathbb{Z}^* . Suppose that S has a following Properties:

- 1) $n_0 \in s$, i.e there exists an element $n_0 \in s$
- 2) for all $n \geq n_0$ $n \in \mathbb{Z}^*$ if $n \in s$ then $n+1 \in s$

Theorem:2.1.3

Let $x, y \in \mathbb{Z}$ with $y \neq 0$. Then there exist unique integers q and r such that $x = qy + r$, $0 \leq r < |y|$.

Proof:

Let us first assume $y \geq 0$ Then $y \geq 1$. Consider the set

$S = \{x - uy \mid u \in \mathbb{Z}, x - uy \geq 0\}$ Since $y \geq 1$ we have $x - (-|x|)y \in s$. Thus, S is a nonempty set of nonnegative integers. Hence by the principle of well ordering, S must have a smallest element, say r . Since $r \in S$ we have $r \geq 0$ and $r = x - qy$ for some $q \in \mathbb{Z}$ Then $x = qy + r$. we must show that $r < |y|$. Suppose on the contrary that $r \geq |y| = y$ Then $x - (q+1)y = (x - qy) - y = r - y \geq 0$ so that $r - y \in s$ a contradiction since r is the smallest non negative Integer in s and $r - y < r$. Hence it must be the case that $r < |y|$. This proves the theorem in case $y > 0$.

Suppose now that $y < 0$. Then $|y| > 0$. Thus there exists integers q', r such that $x = q' |y| + r$, $0 \leq r < |y|$ by the above argument. Since $y < 0$, $|y| = -y$. Hence $x = -q' y + r$. Let $q = -q'$.

Then $x = q y + r$, $0 \leq r < |y|$ the desired conclusion. The uniqueness of q and r remains to be shown. Suppose there are integers q', r such that

$$x = q y + r = q' y + r'$$

$$0 \leq r' < |y|, 0 \leq r < |y| \text{ then } r' - r = (q - q') y$$

Thus, $|r' - r| = |q - q'| |y|$. Now $-|y| < r' - r \leq 0$ and $0 \leq r' < |y|$. Therefore if we add these inequalities $-|y| < r' - r < |y|$. Since $q - q'$ is an integer we must have

$0 = |q - q'|$. It now also follows that $|r - r'| = 0$. Thus $q - q' = 0$ and $r - r' = 0$ or $q = q'$ and $r = r'$. Consequently q and r are unique.

2.2 Relatively Prime

Definition:2.2.1

Let $x, y \in \mathbb{Z}$. A nonzero integer c is called a common divisor of x and y if $c \mid x$ and $c \mid y$.

Definition:2.2.2

A nonzero integer d is called a greatest common divisor (\gcd) of the integers x and y if

- i. $d \mid x$ and $d \mid y$
- ii. for all $c \in \mathbb{Z}$ if $c \mid x$ and $c \mid y$ then $c \mid d$.

Example:2.2.3

Consider the integers 45 and 126

$$126 = 2 \cdot 45 + 36$$

$$45 = 1 \cdot 36 + 9$$

$$36 = 4 \cdot 9 + 0$$

Thus $9 = \gcd(45, 126)$ Also

$$9 = 45 - 1.36$$

$$= 45 - 1 \cdot [126 - 2.45]$$

$$= 3.45 + (-1) \cdot 126.$$

Here $s = 3$ $t = -1$

Theorem:2.2.4

Let x and y be nonzero Integers. Then x and y are relatively prime if and only if there exist $s, t \in \mathbb{Z}$ such that $1 = sx + ty$

Proof:

Let x and y be nonzero Integers. Then $\gcd(x, y) = 1$ there exist integers s and t such that $1 = sx + ty$

Conversely suppose $1 = sx + ty$ for some pairs of Integers s, t . Let $d = \gcd(x, y)$. Then $d \mid x$ and $d \mid y$ and so $d \mid (sx + ty)$. Since d is a positive integer and $d \mid 1$, $d = 1$. Thus $\gcd(x, y) = 1$ and so x and y are relatively prime.

Theorem:2.2.5

Let $x, y, z \in \mathbb{Z}$ with $x \neq 0$ if $x \mid yz$ and x, y are relatively prime then $x \mid z$.

Proof:

Since x and y are relatively prime there exist $s, t \in \mathbb{Z}$ such that $1 = sx + ty$. Let x, y be a nonzero integers. Then x, y are relatively prime if and only if there exist $s, t \in \mathbb{Z}$ such that $1 = sx + ty$. Thus $z = sxz + tyz$. Now $x \mid x$ and hypothesis $x \mid yz$. Thus $x \mid (sxz + tyz)$ and so $x \mid z$.

Corollary:2.2.6

Let $x, y, p \in \mathbb{Z}$ with p a prime. If $p \mid xy$ then either $p \mid x$ or $p \mid y$.

2.3 Correspondence Theorem

Definition:2.3.1

Let n be a positive Integer. Let $\varphi(n)$ denote the number of positive Integers m such that $m \leq n$ and $\gcd(m, n) = 1$ $\varphi(n) = |\{m \in \mathbb{N} \mid m \leq n \text{ and } \gcd(m, n) = 1\}|$ $\varphi(n)$ is called the Euler φ - function.

Example:2.3.2

Let a and b be Integers such that $\gcd(b, 4) = 2$ prove that $\gcd(a + b, 4) = 4$

Solution:

Since $\gcd(a, 4) = 2$, $2 \mid a$ but 4 does not divide a . Therefore $a = 2x$ for some Integer x such that $\gcd(2, x) = 1$ Similarly $b = 2y$ for some Integer y such that $\gcd(2, y) = 1$ thus x and y are both odd integers. This implies that $x + y$ is an even integer and so $x + y = 2n$ for some Integer n . Now $a + b = 2(x + y) = 4n$ hence ,
 $\gcd(a + b, 4) = \gcd(4n, 4) = 4$.

Example:2.3.3

Find Integers x and y such that $512x + 320y = 64$

Solution

$$512 = 320 \cdot 1 + 192$$

$$320 = 192 \cdot 1 + 128$$

$$192 = 128 \cdot 1 + 64$$

$$128 = 64 \cdot 2 + 0$$

$$\text{Thus } 64 = 192 - 128 = 192 - (320 - 192)$$

$$= 192 \cdot 2 + 320 \cdot (-1)$$

$$= (512 - 320) \cdot 2 + 320 \cdot (-1)$$

$$= 512 \cdot 2 + 320 \cdot (-3)$$

$$\text{Hence } x = 2 \text{ and } y = -3$$

Theorem:2.3.4

Let f be a homomorphism of a group G onto a group G_1 . The f induces a one – one inclusion preserving correspondence between the subgroups of G_1 . In fact if H and K are corresponding subgroups of G and G_1 respectively then H is a normal subgroup of G_1 .

Proof:

Let $\mu = \{H | H \text{ is a subgroup of } G \text{ such that } \ker f \subseteq H\}$

And $K = \{k | k \text{ is a subgroup of } G_1\}$.

Define $f^*: H \rightarrow K$ by for all $H \in \mu$, $f^*(H) = \{f(h) | h \in H\}$ Then $f^*(H) \in K$. Hence f^* is a function since f is a function. Let $a \in \ker f$ then $f(a) = e_1 \in k$ and so $a \in f^{-1}(k) = H$. Thus $\ker f \subseteq H$ let $a, b \in H$ Then $f(a), f(b) \in k$ and so $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b^{-1}) \in k$. Therefore $a b^{-1} \in H$ and so H is a subgroup of G containing $\ker f$. Hence $f^*(H_1) = f^*(H_2)$. Let $h_1 \in H_1$. Then there exists $h_2 \in H_2$ such that $f(h_1) = f(h_2)$. This implies that $f(h_1 h_2^{-1}) = e_1$ and so $h_1 h_2^{-1} \in \ker f \subseteq H_2$ if Hence $h_1 = (h_1 h_2^{-1}) h_2 \in H_2$. Clearly Therefore $H_1 \subseteq H_2$ if and only if similarly $H_2 \subseteq H_1$ Thus $H_1 = H_2$ and so f^* is one - one clearly $H_1 \subseteq H_2$ if and only if $f^*(H_1) \subseteq f^*(H_2)$. In fact f^* is one – one $H_1 \subset H_2$ if and only if $f^*(H_1) \subset f^*(H_2)$.

Suppose H is a normal subgroup of G such that $\ker f \subseteq H$ let $k = f^*(H)$ we show that k is a normal subgroup of G_1 let $f(a) \in G$, $f(b) \in k$ Now $a h a^{-1} \in H$ since H is a normal subgroup of G and so $f(a) f(h) f(a^{-1}) = f(a h a^{-1}) \in k$ Hence k is a normal subgroup of G_1 let J be a normal subgroup of G_1 and $L \in \mu$ be such that $f^*(L) = J$ let $a \in G$ and $h \in L$ Then $f(a h a^{-1}) = f(a) f(h) f(a^{-1})$ and so $a h a^{-1} \in L$ This proves that L is a normal subgroup of G .

Example:2.3.5

Show that $4\mathbb{Z} \mid (2\mathbb{Z} \simeq \mathbb{Z}_3)$

Solution:

Define $f: 4\mathbb{Z} \rightarrow \mathbb{Z}_3$ by $f(4n) = [n]$ for all $4n \in 4\mathbb{Z}$ one can show that f is an epimorphism Then from the first Isomorphism Theorem $4\mathbb{Z} / \ker f \simeq \mathbb{Z}_3$ Now

$$\ker f = \{4n \in 4\mathbb{Z} \mid f(4n) = [0]\} = \{4n \in 4\mathbb{Z} \mid [n] = [0]\} = 12\mathbb{Z}$$

2.4 The Groups of D_4 and Q_8

Definition:2.4.1

A group G is called a dihedral group of degree 4 if G is generated by two elements a and b satisfying the relations $o(a) = 4$ $o(b) = 2$ and $ba = a^3b$.

Example:2.4.2

Let T be a group of all 2×2 invertible matrices over \mathbb{R} under usual matrix multiplication Let G be the subgroup of T generated by the matrices.

Definition:2.4.3

A group G is called a quaternion group if G is generated by two elements a, b satisfying the relation $o(a) = 4$ $a^2 = b^2$ and $ba = a^3b$.

Example:2.4.4

Let T be the group of all 2×2 invertible matrices over \mathbb{C} under usual matrix multiplication let G be the subgroup of T generated by the matrices

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Then $o(A) = 4$ and

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = B^2$$

$$BA = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$$

Thus $BA = A^3B$ Hence G is quaternion group.

Theorem:2.4.5

There exist only two noncommutative non isomorphic groups of order 8

Proof:

Let G be a noncommutative group of order 8 since $|G|$ is even there exist an element $u \in G$ $u \neq e$ such that $u^2 = e$ if $x^2 = e$ for all $x \in G$ then G is commutative. A contradiction. Thus there exists $a \in G$ such that $a^2 \neq e$. Since $o(a) \mid 8$, $o(a) = 4$ or 8 . If $o(a) = 8$ then G is cyclic and hence commutative contradiction, Thus $o(a) = 4$ let $H = \{e, a, a^2, a^3\}$. Then H is a subgroup of G of index 2 and so H is a normal subgroup of G . Let $b \in G$ be such that $b \notin H$. Then $G = H \cup Hb$ and $H \cap Hb = \emptyset$ This implies that $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\} = \langle a, b \rangle$. Now $ba b^{-1} \in H$. If $ba b^{-1} = e$ then $a = e$ a contradiction. Thus $ba b^{-1} \neq e$ if $ba b^{-1} = a$ then $ab = ba$ and hence G is commutative a contradiction. If $ba b^{-1} = a^2$ then $ba^2 b^{-1} = (ba b^{-1})^2 = a^4 = e$ and so $a^2 = e$ a contradiction. Therefore $ba b^{-1} = a^3$ and so $ba = a^3b$. Since $[G:H] = 2$ and $b \notin H$, $o(Hb) = 2$ Hence $b^2 = a$ or a^3 then $o(b) = 8$ and so G is commutative a contradiction. Therefore either $b^2 = e$ or $b^2 = a^2$. It now follows that if G is a noncommutative group of order 8 then either $G = \langle a, b \rangle$ such that $o(b) = 2$ and $ba = a^3b$. In the first case $G \cong D_4$ and in the second case $G \cong Q_8$.

Example:2.4.6

Find $z(D_4)$

Solution:

It is known that $z(D_4)$ is a normal subgroup of D_4 . Now D_4 has five normal subgroups. D_4 , $\{e\}$, $T_1 = \{e, a^2\}$, $T_2 = \{e, a, a^2, a^3\}$, $T_3 = \{e, a^2b, a^3b\}$, $T_4 = \{e, ab, a^3b\}$. Since $ab \neq ba$ in D_4 , T_1 and T_2 cannot be $z(D_4)$. If $(ab)b = b(ab)$ then $a = (ba)b = a^3b^2 = a^3$ and so $a^2 = e$ a contradiction hence $T_3 \neq z(D_4)$ and $T_4 \neq z(D_4)$. Thus $z(D_4) = \{e, a^2\} = T_1$.

2.5 Group Actions

Definition:2.5.1

Let G be a group and s a nonempty set. A (left) action of G on S is a function :
 $G \times S \rightarrow S$ such that

- i. $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ and
- ii. $E \cdot x = x$ where e is the Identity of G for all $x \in S$ $g_1, g_2 \in G$

Example:2.5.2

Let G be a permutation group on a set S . Define a left action of G on S by

$$\sigma_x = \sigma(x)$$

For all $\sigma \in G$, $x \in s$ let $x \in s$ Now $e \cdot x = e(x) = x$ where e is the identity permutation on s . Let $\sigma_1, \sigma_2 \in G$. Then:

$$(\sigma_1 \circ \sigma_2) \cdot x = (\sigma_1 \circ \sigma_2)(x) = \sigma_1(\sigma_2(x)) = \sigma_1 \cdot (\sigma_2(x)) = \sigma_1 \cdot (\sigma_2 \cdot x). \text{ Hence } S \text{ is a } G\text{-set.}$$

Theorem:2.5.3

Let s be a finite nonempty set and G be a finite group. If s is a G -set then the number of orbits of G is $\frac{1}{|G|} \sum_{g \in G} f(g)$ where $f(g)$ is the number of elements of s fixed by g .

Proof:

Let $T = \{ (g, a) \in G \times S \mid g \cdot a = a \}$ since $f(g)$ is the number of elements $a \in s$ such that $(g, a) \in T$. it follows that $|T| = \sum_{g \in G} f(g)$. Also $|G \cdot a|$ is the number of elements $g \in G$ Such that $(g, a) \in T$ Hence $|T| = \sum_{a \in s} |G \cdot a|$. Let $s = [a_1] \cup [a_2] \cup \dots \cup [a_k]$ is the set of all distinct orbits of G on s Then

$$\sum_{g \in G} f(g) = \sum_{a \in [a_1]} |G \cdot a| + \sum_{a \in [a_2]} |G \cdot a| + \dots + \sum_{a \in [a_k]} |G \cdot a|$$

Suppose a, b are in same orbit. Then $[a] = [b]$ and $[G : G_a] = |[a]| = |[b]| = [G : G_b]$

This implies:

$$\frac{|G|}{|Ga|} = \frac{|G|}{|Gb|}$$

And also $|Ga| = |Gb|$ Thus

$$\begin{aligned}\sum_{g \in G} f(g) &= |[a_1]| |Ga_1| + |[a_2]| |Ga_2| + \dots + |[a_k]| |Ga_k| \\ &= \frac{|G|}{|Ga_1|} |Ga_1| + \frac{|G|}{|Ga_2|} |Ga_2| + \dots + \frac{|G|}{|Ga_k|} |Ga_k|\end{aligned}$$

Where k is the number of distinct orbits consequently

$$K = \frac{1}{|G|} \sum_{g \in G} f(g).$$

Example:2.5.4

Let s be a finite G -set where G is a group of order p^n let

$$s_0 = \{a \in s \mid ga = a \text{ for all } g \in G\} \text{ Show that } |s| \equiv p^{|s_0|}$$

Solution:

$$|s| = \sum_{a \in A} |Ga| \quad \text{where } A \text{ is a subset of } s \text{ containing exactly one element}$$

from each orbit $[a]$ of G Now $a \in s_0$ if and only if $ga = a$ for all $g \in G$

$$|s| = |s_0| + \sum_{a \in A} \frac{|G|}{|Ga|} \text{ since } |Ga| \neq |G| \text{ for all } a \in A \setminus s_0 \text{ Thus } \frac{|G|}{|Ga|} \text{ is divisible by } p$$

proving that $|s| \equiv p^{|s_0|}$

2.6 Sylow Theorem

Definition:2.6.1

Let H be a subgroup of a group G and $a \in G$ if $aha^{-1} = H$ then H is called invariant under a .

Example:2.6.2

Let G be a finite group and $a \in G$ be such that a has only two conjugates proves that $c(a)$ is a normal subgroup of G .

Solution:

$|G : c(a)| = |c_i(a)|$ Now $|c_i(a)|=2$ Hence $|G : c(a)| = 2$ proving that $c(a)$ is a normal subgroup of G .

Theorem:2.6.3

Let G be a finite group of order $p^r m$ where p is a prime r and m are positive Integers p and m are relatively prime Then G has a subgroup of order p^k for all $k, 0 \leq k \leq r$.

Definition:2.6.4

Let G be a finite group and p a prime. A subgroup P of G is called a SYLOW p subgroup of G if P is a p subgroup and is not properly contained in any other p subgroup of G .

Theorem:2.6.5

Let G be a finite group of order $p^r m$ where p is a prime r and m are positive Integers and p and m are relatively prime. Then any two SYLOW P - subgroups of G are conjugate and therefore isomorphic.

Theorem:2.6.6

Let G be a finite group of order $p^r m$ where P is a prime r and m are positive Integers and p and m are relatively prime Then the number n_p of SYLOW P -subgroups of G is $1 \neq k_p$ for some nonnegative integer k and $n_p \mid p^r m$.

Example:2.6.7

The Symmetric group S_2 has three SYLOW 2 subgroups namely.

Solution:

$$\left\{ H_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} - \left\{ H_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

$$\left\{ H_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix} \right\}$$

Thus a SYLOW p-subgroup of a given group need not be unique.

Chapter 3

CHAPTER 3

PROBABILITY THEORY

3.1 Probability

Definition:3.1.1

A **probability model** is a Mathematical description of an uncertain situation . It must be in accordance with a fundamental framework.

Definition:3.1.2

1. **(Nonnegative)** $P(A) \geq 0$, for every event A.
2. **(Additivity)** If A and B are two disjoint events , then the probability of their union satisfies.

$$P(A \cup B) = P(A) + P(B).$$

3. **(Normalization)** The probability of the entire sample space Ω is equal to 1, that is $P(\Omega) = 1$.

Example:3.1.3

Consider an experiment involving a single coin toss. There are two possible outcomes , heads (H) and tail (T). The sample space is $\Omega = \{H, T\}$, and the events are

$$\{H, T\} , \{H\} , \{T\} , \phi$$

If the coin is fair , if we believe that heads and tails are “equally likely” we should assign equal probabilities to the two possible outcomes and specific that $P(\{H\}) = P(\{T\}) = 0.5$. The additivity axiom implies that

$$\begin{aligned} P(\{H, T\}) &= P(\{H\}) + P(\{T\}) \\ &= 1, \end{aligned}$$

Which is consistent with the normalization axiom . Thus, the probability law is given by

$P(\{H,T\}) = 1$, $P(\{H\}) = 0.5$, $P(\{T\}) = 0.5$, $P(\phi) = 0$, and satisfies all three axiom.

Consider another experiment in three coin tosses . The outcomes will now be 3 – long string of heads or tails .The sample space is

$$\Omega = \{ HHH , HHT , HTH , HTT , THH , THT , TTH , TTT \}$$

We assume that each possible of $1/8$. Let us construct a probability law that satisfies the three axioms . Consider , as an example the event .

$$\begin{aligned} A &= \{ \text{exactly 2 heads occur} \} \\ &= \{ HHT , HTH , THH \}. \end{aligned}$$

Using additivity the probability of A is the sum of the probability of its element:

$$\begin{aligned} P(\{HHT , HTH , THH\}) &= P(\{HHT\}) + P(\{HTH\}) + P(\{THH\}) \\ &= 1/8 + 1/8 + 1/8 \\ &= 3/8. \end{aligned}$$

Similarly, The probability of any event is equal to $1/8$ times the number of possible outcomes contained in the event . This defines a probability law satisfies the three axioms .

Remark:3.1.4

Consider a probability law and let A,B and C be event .

- a) If $A \subset B$, then $P(A) < P(B)$.
- b) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.
- c) $P(A \cup B) < P(A) + P(B)$.

$$P(A \cup B \cup C) = P(A) + P(A^c \cap B) + P(A^c \cap B^c \cap C)$$

3.2 Conditional Probability

Definition:3.2.1

Conditional probability provides us with a way to reason about the outcome of an experience based on **partial information**.

Remark:3.2.2

- The conditional probability of an event A , given an event B with $P(B) > 0$, is defined by

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \text{ and specific a new conditional probability.}$$

- If the possible outcomes are finitely many and equally likely, then

$$P(A/B) = \frac{\text{Number of elements of } A \cap B}{\text{Number of elements of } B}$$

Example:3.2.3

We toss a fair coin three successive times. We wish to find the conditional probability $P(A/B)$ when A and B are events.

$$A = \{ \text{more heads than tails come up} \},$$

$$B = \{ 1^{\text{st}} \text{ toss is a head} \}.$$

The sample consists of eight sequence

$$\Omega = \{ HHH, HHT, HTH, HTT, THH, THT, TTH, TTT \}$$

Which we assume to be equally likely. The event B consists of the four elements HHH, HHT, HTH, HTT , so its probability is

$$P(B) = 4/8.$$

The event $A \cap B$ consists of the three elements HHH, HHT, HTH , so its probability is

$$P(A \cap B) = 3/8.$$

Thus, the conditional probability $P(A/B)$ is

$$P(A/B) = \frac{P(A \cap B)}{P(B)} = \frac{3/8}{4/8} = 3/4.$$

Because all possible outcomes are equally likely here, we can also compute $P(A/B)$ using a shortcut .we can bypass the calculation of $P(B)$ and $P(A \cap B)$ and simply divide the number of elements shared by A and B (which is 3) with the number of elements of B (which is 4).

Theorem:3.2.4

Let A_1, \dots, A_n be disjoint events that form a partition of the sample space each possible outcome is included in exactly one of the A_1, \dots, A_n and assume that $P(A_i) > 0$, for all i . Then for any events B , we have

$$\begin{aligned} P(B) &= P(A_1 \cap B) + \dots + P(A_n \cap B) \\ &= P(A_1) P(B/A_1) + \dots + P(A_n) P(B/A_n). \end{aligned}$$

Example:3.2.5

You enter a chess tournament where your probability of winning a game is 0.3 against half the players (call them type 1), 0.4 against a quarter of the players and 0.5 against the remaining quarter of the players you play a game against a randomly chosen opponent. What is the probability of winning?

Solution:

Let A_i be the event of playing with an opponent of type i , we have

$$P(A_1) = 0.5, P(A_2) = 0.25, P(A_3) = 0.25.$$

Thus, by the total probability of winning is

$$\begin{aligned} P(B) &= P(A_1) P(B/A_1) + P(A_2) P(B/A_2) + P(A_3) P(B/A_3) \\ &= 0.5 \cdot 0.3 + 0.25 \cdot 0.4 + 0.25 \cdot 0.5 = 0.375. \end{aligned}$$

Definition:3.3.1

Let A_1, A_2, \dots, A_n be disjoint events that form a partition of the sample space, and assume that $P(A_i) > 0$, for all i . Then, for any event B such that $P(B) > 0$, we have

$$\begin{aligned} P(A_i|B) &= \frac{P(A_i) P(B|A_i)}{P(B)} \\ &= \frac{P(A_i) P(B|A_i)}{P(A)P(B|A_1) + \dots + P(A_n)P(B|A_n)} \end{aligned}$$

Example:3.3.2

Let us return to the radar detection problem of

$A = \{\text{an aircraft is present}\}$

$B = \{\text{The radar generates an alarm}\}$

We are given that

$$P(A) = 0.05, P(B|A) = 0.99, P(B|A^c) = 0.1.$$

Applying Nate's rule with $A_1 = A$ and $A_2 = A^c$,

$$\begin{aligned} P(\text{aircraft present} / \text{alarm}) &= P(A/B) \\ &= P(A) P(B|A) / P(B) \\ &= \frac{P(A) P(B|A)}{P(A) P(B|A) + P(A^c) P(B|A^c)} \\ &= \frac{0.05 \cdot 0.99}{0.05 \cdot 0.99 + 0.95 \cdot 0.1} \approx 0.3426. \end{aligned}$$

Example:3.3.3

Let us return to the class problem here A_i is the event of getting an opponent of type i , and

$$P(A_1) = 0.5, P(A_2) = 0.25, P(A_3) = 0.25$$

Also, B is the event of winning and

$$P(B/A_1) = 0.3, P(B/A_2) = 0.4, P(B/A_3) = 0.5$$

Suppose that you win what is probability $P(A_1/B)$ that you had an opponent of types.

Using Baye's rule, we have

$$\begin{aligned} P(A_1 | B) &= \frac{P(A_1)P(B|A_1)}{P(A_1)P(B|A_1) + P(A_2)P(B|A_2) + P(A_3)P(B|A_3)} \\ &= \frac{0.5 \cdot 0.3}{0.5 \cdot 0.3 + 0.25 \cdot 0.4 + 0.25 \cdot 0.5} = 0.4 \end{aligned}$$

3.4 Independence

Definition:3.4.1

- Two events A and B are said that be **Independent** if

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

If in addition, $P(B) > 0$, Independent is equivalent to the condition

$$P(A/B) = P(A).$$

- If A and B are independent so are A and B^c
- Two events A and B are said to be **conditional independent**, given another event C with $P(C) > 0$, if

$$P(A \cap B) = P(A/C) P(B/C)$$

If in addition, $P(B \cap C) > 0$, conditional independent is equivalent to be equivalent to the condition

$$P(A/B \cap C) = P(A/C).$$

- Independent does not imply conditional independence and vice versa.

Example:3.4.2

Let A and B be independent events use the definition of independence to

prove the following

- (a) The events A and B^c are independent.

- (b) The events A^c and B^c are independent.
- (a) The event A is the union of the disjoint events $A \cap B^c$ and $A \cap B$ additivity axioms and the independent of A and B

$$P(A) = P(A \cap B) + P(A \cap B^c) = P(A)P(B) + P(A \cap B^c).$$

$$P(A \cap B^c) = P(A)(1 - P(B)) = P(A)P(B^c) \text{ so } A \text{ and } B \text{ are independent.}$$

- (b) Apply the result to part (a) twice : first on A and B . then on B^c and A .

3.5 Random Variables

Main Concepts Related to Random Variable:

Starting with a probabilities model of an experiment:

- A **random variable** is a real valued function of the outcome of the experiment.
- A **function of a random variable** defines another random variables.
- We can associate with each random variable certain average of interest such as the **mean** and the **variance**.
- A random variable can be **conditioned** on an event or on another random variable.
- There is a notion of **independence** of a random variable from an event or from another random variable.

Example:3.5.1

Consider two independent coin tosses ,each with a $\frac{1}{2}$ probability of a head and let x be the number of heads obtained .

Solution:

This a binomial random variable with parameters $n = 2$ and $p = \frac{1}{2}$ its PMF is

$$P_X(k) = \begin{cases} \left(\frac{1}{4}\right)^2 & \text{if } k = 0 \\ 2 \cdot \left(\frac{1}{4}\right) \cdot \left(\frac{3}{4}\right) & \text{if } k = 1 \\ \left(\frac{3}{4}\right)^2 & \text{if } k = 2 \end{cases}$$

So the mean is

$$\begin{aligned} E[X] &= 0 \cdot (1/4)^2 \\ &= 1 \cdot (2 \cdot \frac{1}{4} \cdot \frac{3}{4}) \\ &= 2 \left(\frac{3}{4}\right)^2 \\ &= 24/16 \\ &= 3/2 \end{aligned}$$

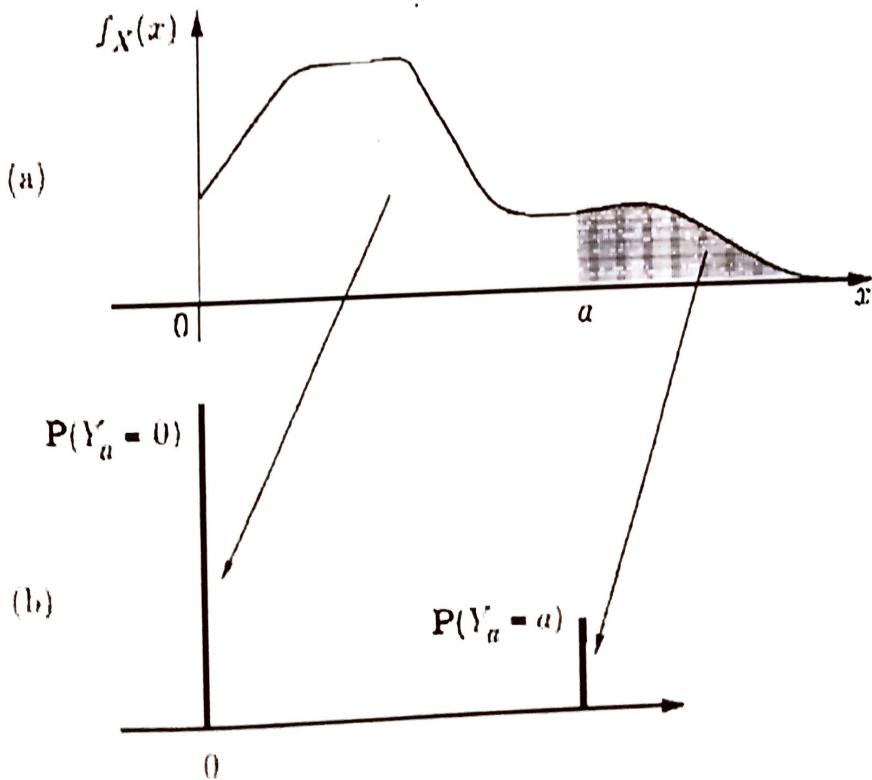
3.5 Markov Inequality

Definition:3.5.1

If a random variable X can only take nonnegative values, then ;

$$P(X \geq a) \leq E(X) / a, \text{ for all } a > 0.$$

Example:3.5.2



Let X be uniformly distributed in the interval $[0,4]$ and note that $E(X) = 2$. Then the **Markov Inequality** assert that :

$$P(X \geq 2) \leq \frac{2}{2} = 1 ,$$

$$P(X \geq 3) \leq \frac{2}{3} = 0.67 ,$$

$$P(X \geq 4) \leq \frac{2}{4} = 0.5 .$$

By comparing with the exact probabilities :

$$P(X \geq 2) = 0.5 ,$$

$$P(X \geq 3) = 0.25 ,$$

$P(X \geq 4) = 0$. We see that the bounds provided by the *Markov inequality* can be quite loose .

3.6 Chebyshev Inequality

Definition:3.6.1

If X is a random variable with mean μ and variance σ^2 , then

$$P((X - \mu) \geq c) \leq \sigma^2 / c^2 , \text{ for all } c > 0 .$$

Example:3.6.2

When X is known to take values in a range $[a, b]$, we claim that

$\sigma^2 \leq (b-a)^2 / 4$. Thus , if σ^2 is unknown , we may use the bound $(b-a)^2 / 4$ in place of σ^2 in the **Chebyshev Inequality** , and obtain

$$P(|X - \mu| \geq c) \leq (b-a)^2 / 4 c^2 , \text{ for all } c > 0 .$$

To verify our claim, note that for any constant γ , we have

$$E[(X - \gamma)^2] = E[X^2] - 2E[X]\gamma + \gamma^2 ,$$

and the above quadratic is minimized when $\gamma = E[X]$. It follows that

$$\sigma^2 = E[(X - E[X])^2] \leq E[(X - \gamma)^2] , \text{ for all } \gamma . \text{ By letting}$$

$$\gamma = (a + b) / 2 , \text{ we obtain}$$

$$\sigma^2 \leq E[(X - (a+b)/2)]^2 = E[(X-a)(X-b)] + (b-a)^2 / 4 \leq (b-a)^2 / 4 ,$$

where the equality above is verified by straightforward calculation , and the last inequality follows from the fact $(x-a)(x-b) \leq 0$ for all x in range $[a,b]$. The bound $\sigma^2 (b - a)^2/4$ may be quite conservative, but in the absence of further information about X , it cannot be improved.

Chapter 4

CHAPTER - 4

CODING THEORY

4.1 Coding

Definition:4.1.1

If x and y are two n -tuples of 0s and 1s, then we shall say that their Hamming-distance (usually just distance) is $d(x, y) = |\{i\} 1 \leq i \leq n, x_i \neq y_i|$.

Definition:4.1.2

The code C with eight words of length 6 which we treated above has the property that any two distinct code words have distance at least 3. That is why any error-pattern with one error could be corrected. The code is **single-error-correcting code**.

Definition: 4.1.3

This means that if y is received we try to find a code word x such that $d(x, y)$ is minimal. This principle is called **maximum-likelihood-decoding**.

4.2 Shannon Theorem

If $0 < R < 1 + p \log p + q \log q$ and $M_n := 2^{\lfloor Rn \rfloor}$ then $p^*(M_n, n, p) \rightarrow 0$ if $n \rightarrow \infty$.
 $P = 0.001$, i.e. $1 + p \log p + q \log q$ is nearly 1. The requirement in the experiment was that the rate should be at least $\frac{1}{2}$. We see that for $\epsilon > 0$ and n sufficiently large there is a code C of length n , with rate nearly 1 and such that $p_e < \epsilon$.

Theorem:4.2.1

In the proof of Shannon's we shall pick the code word x_1, x_2, \dots, x_m at random (independently). we decode as follows. If y is received and if there is exactly one codeword x_i such that $d(x_i, y) \leq \rho$, then decode y as x_i , Otherwise we declare an error

(or if we must decode, then we always decode as x_i). Let p_i be as defined above. We have

$$p_i = \sum_{y \in \{0,1\}^n} p(y|x_i) g_i(y)$$

$$= \sum_y p(y|x_i) \{1 - f(y, x_i)\} + \sum_y \sum_{j \neq i} p(y|x_i) f(y, x_j).$$

here the first term on the right-hand side is the probability that the received word y is not in $B_p(x_i)$. By $p(w > n p + b) \leq \frac{1}{2}\epsilon$ this probability is at most $\frac{1}{2}\epsilon$. Hence we have

$$p_C \leq \frac{1}{2}\epsilon + M^{-1} \sum_{i=1}^M \sum_y \sum_{j \neq i} p(y|x_i) f(y, x_j).$$

The main principle of the proof is the fact that $p^*(M, n, p)$ is less than the expected value of p_C over all possible codes C picked at random. Therefore we have

$$p^*(M, n, p) \leq \frac{1}{2}\epsilon + M^{-1} \sum_{i=1}^M \sum_y \sum_{j \neq i} \epsilon (p(y|x_i) \epsilon (f(y, x_j))).$$

$$= \frac{1}{2}\epsilon + M^{-1} \sum_{i=1}^M \sum_y \sum_{j \neq i} \epsilon (p(y|x_i) \cdot |B_p| / 2n) = \frac{1}{2}\epsilon + (M-1)2^{-n} |B_p|$$

we now take logarithms apply

$$|B_p(x)| = \sum_{i \leq p} \binom{n}{i} < \frac{1}{2} n \binom{n}{p} \leq \frac{1}{2} n \cdot n^n / p^p (n-p)^{n-p} \text{ and}$$

$$\rho/n \log \rho/n = 1/n [n p + b]/n = p \log p + o(n^{-1/2}). \text{ and then we divide by } n.$$

The result is $n^{-1} \log (p^*(M, n, p) - \frac{1}{2}\epsilon) \leq n^{-1} \log M - (1+p \log p + q \log q) + o(n^{-1/2})$ substituting

$M=M_n$ on the right-hand side we find, using the restriction on R ,

$$n^{-1} \log (p^*(M_n, n, p) - \frac{1}{2}\epsilon) < -\beta < 0, \text{ for}$$

$$n > n_0, \text{ i.e. } p^*(M, n, p) < \frac{1}{2}\epsilon + 2^{-\beta n} \text{ This proves the theorem.}$$

4.3 Coding Gain

Definition: 4.3.1

The ratio between SNR(un code) and NSR' (coded) for equal error probability

after decoding is called the **coding gain**.

$$P_e = \int_{\sqrt{E}}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-y^2/2\sigma^2) dy = Q(\sqrt{E} b/\sigma^2). a$$

Where,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-y^2/2} dy = \frac{1}{2} \operatorname{erfc}(x/\sqrt{2}).$$

The ratio E_b/σ^2 is called the signal to noise

Ratio(SNR).

Example:4.3.2

Consider the example of the mariner code. Suppose that for a useful picture, each 6-tuple may be wrong with probability p_e at most 10^{-4} . In case of no coding we need $E_b/\sigma^2 \approx 17.22$ to achieve this, since $p_e = Q(\sqrt{17.22}) \approx 10^{-4}/6$, and $PE = 1 - (1 - p_e)^6 \approx 10^{-4}$.

Next suppose that we use [32,6] code, Correcting at most seven errors, at the same SNR of 17.22. Since $R = 6/32$, we obtain ' p_e ' ≈ 0.036 (note that this error probability is 2000 times as large as before 1) After decoding, we obtain erroneous 6-tuples with probability

$$p'_e = \sum_{i>7} \binom{32}{i} (p_e)^i (1 - p_e)^{32-i} \approx 1.4 \cdot 10^{-5} \text{ which is almost order of magnitude better than } p_e$$

Example:4.3.3

A binary channel has a probability $q = 0.9$ that Q transmitted symbol is received correctly and a probability $p = 0.1$ that an erasure occurs (i.e. we received). On this channel we wish to use a code with rate $1/2$. Does the probability of correct interpretation increase if we repeat each transmitted symbol? Is it possible to construct a code with eight words of length 6 such that two erasures can do no harm? Compare the probabilities of correct interpretation for these two codes. (Assume that the receiver does not change the erasures by guessing symbol).

Solution:

For the code using repetition of symbols the probability of correct reception of a repeated symbol is $1 - p^2$. Therefore the code of length 6 with code words $(a_1, a_2, a_3, a_1, a_2, a_3)$ has probability $(1 - p^2)^3 = 0.97$ of correct reception. The code of $(s_1, s_2, s_3) = (1, 1, 0)$. This

can be caused by the error $(101011), (011101), (110000), (010011), (100101), (000110), (111110)$ and ofcourse by (001000) which is the most likely one. Has the property that any two code – words differ in three places and therefore two erasures can do no harm. In fact an analysis of all possible erasure patterns with three erasures show that 16 of these do no harm either. This leads to a probability $(1-p)^3(1+3p+6p^2+6p^3) = 0.996$ of Correct of reception. This is a remarkable improvement considering the fact that the two codes are very similar.

Definition:4.3.4

A generator matrix G for a linear code C is a k by n matrix for which the rows are a basis of C .

Theorem:4.3.5

For a linear code C the minimum distance is equal to the minimum weight.

Proof:

$d(x, y) = d(x - y, 0) = W(x - y)$ and if $x \in C, y \in C$ then $x - y \in C$.

4.4 Self Dual Code

Definition:4.4.1

If C is an $[n, k]$ code we define the dual code C^\perp by

$$C^\perp = \{y \in R^n \mid \langle x, y \rangle = 0 \text{ for all } x \in C\}.$$

Definition:4.4.2

The subspaces C and C^\perp can Have an intersection larger than $\{0\}$ and in fact they can even be equal. If $C = C^\perp$ then C is called self-dual code.

Definition:4.4.3

If C is a code of length n over the alphabet F_q we define the extended

$$\text{Code } C \text{ by } \bar{C} = \{(c_1, c_2, \dots, c_n, c_{n+1}) \mid (c_1, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}$$

Definition:4.4.4

Let $n = (q^k - 1)/(q - 1)$. The $[n, n-k]$ Hamming code over F_q is a code for which the parity check matrix has columns that are pairwise linearly independent (over F_q), i.e. the columns are a maximal set of pairwise linearly independent vectors.

Theorem:4.4.5

Hamming codes are perfect codes.

Proof:

Let C be the $[n, n-k]$ Hamming code over F_q , where $n = (q^k - 1)/(q - 1)$. If $x \in C$ then $|B(x)| = 1 + n(q - 1) = q^k$. Therefore the q^{n-k} disjoint sphere of radius 1 around the codewords of C constant $|C|q^k = q^n$ words i.e, all possible words, Hence is perfect C a code $C \subset Q^n$ with minimum distance $2e+1$ is called a perfect code if every $x \in Q^n$ has distance $\leq e$ to exactly one code-word. The fact the minimum distance is $2e+1$ means that the code is e -error- correcting. The following is obvious. Sphere-packing condition. If $C \subset Q^n$ is perfect e -error- correcting code, then

$$|C| \sum_{i=0}^e \binom{n}{i} (q-1)^i = q^n.$$

Example:4.4.6

Suppose that we use an extended Hamming code of length $n=2^m$ on a B.S.C, with bit error probability p ; ($q=1-p$). The expected number of errors per block before decoding is np . If one error occurs, it is corrected. If two errors occur, then we have error detection but no correction. So, the two errors remain. Otherwise, it is possible that the decoder introduces an extra error by changing a received word with ≥ 3 errors into the closed codeword. Therefore, the expected number of errors per block after decoding is at most

$$2 \binom{n}{2} p^2 q^{n-2} + \left(\sum_{i=3}^n (i+1) \right) \binom{n}{i} p^i q^{n-i}$$

$$\begin{aligned}
&= 2 \binom{n}{2} p^2 \{q^{n-2} + (\sum_{i=3}^n (i+1)) \binom{n}{i} / 2 \binom{n}{2} p^{i-2} q^{n-i}\} \\
&\leq 2 \binom{n}{2} p^2 \{q^{n-2} + (\sum_{i=3}^n \binom{n-2}{i-2}) p^{i-2} q^{n-i}\} \\
&= n(n-1) p^2 < (np)^2.
\end{aligned}$$

If p is small enough, this is a considerable.

4.5 Lee Weight

Definition:4.5.1

Consider Z_m as alphabet. The Lee weight of an integer i ($0 \leq i < m$) is defined by

$$w_i = \min\{i, m-i\}. \text{ This Lee metric on } Z_m^n \text{ is defined by } w_L(a) = \sum_{i=1}^n u_L(a_i),$$

where the sum is defined in N_0 , we defined Lee distance by $d_L(x, y) = w_L(x-y)$.

Definition:4.5.2

The Lee weight enumerator of a code $C \subseteq Z_4^n$ is defined by

$$Lee_C(x, y) = \sum_{c \in C} x^{2n-WL(c)} y^{WL(c)}. \text{ Note that } Lee_C(x, y) = Sw_C(x^2, xy, y^2)$$

Example:4.5.3

1) Let C be a $[2k+1, k]$ binary code such that $C \subset C^\perp$. Describe $C^\perp \setminus C$

Solution:

Since $C \subset C^\perp$ every $c \in C$ has the Property $\langle c, c \rangle$, i.e. $w(c)$ is even and hence

$\langle c, 1 \rangle = 0$. However, $\langle 1, 1 \rangle = 1$ Since the word length is odd. Therefore $C^\perp \setminus C$ is obtained by

adding 1 to all the words C .

2) Let p be a prime. Is there an $[8, 4]$ self dual code over F_p ?

Solution:

i) If $p \equiv 1 \pmod{4}$ then there is an $a \in F_p$ such that $a^2 = -1$. Then $G(14, a14)$ is the

generator matrix of the required code.

ii) If $p \equiv 1 \pmod{4}$ we use the fact that not all the elements of F_p are squares and hence there is an α which is a square, say $\alpha = \beta^2$, such that $\alpha + 1 = -\gamma^2$. Hence $\beta^2 + \gamma^2 = -1$. Then

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & \beta & \gamma & 0 & 0 \\ 0 & 1 & 0 & 0 & -\gamma & \beta & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \beta & \gamma \\ 0 & 0 & 0 & 1 & 0 & 0 & -\gamma & \beta \end{bmatrix}$$

3) Let C be a binary code with generator matrix

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

decode the following received words.

a) $(1\ 1\ 0\ 1\ 0\ 1\ 1)$;

b) $(0\ 1\ 1\ 0\ 1\ 1\ 1)$;

c) $(0\ 1\ 1\ 1\ 0\ 0\ 0)$;

From the generator matrix we find for $c \in C$. $c_1 + c_2 + c_5 = c_3 + c_4 + c_6 = c_1 + c_2 + c_3 + c_4 + c_7 = 0$

Hence the syndromes $(s_1, s_2, s_3) = (e_1 + e_2 + e_5, e_3 + e_4 + e_6, e_1 + e_2 + e_3 + e_4 + e_7)$,

For the three received words are respectively $(0, 0, 0), (0, 0, 1), (1, 0, 1)$, Hence (a) is a code word;

by maximum likelihood decoding (b) has an error in position 7; (c) has an error in position 1

or an error in position 2, so here we have a choice.

3) Let C be the binary $[10, 5]$ code with generator matrix.

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

Show that C is uniquely decodable in the following sense: For every received word x there is

a unique code word C such that $d(x, c)$ is minimal.

Solution:

The subcode on positions 1,9 and 10 is the repetition code which is perfect and single-error correcting. The subcode on the remaining seven positions is the [7,4] Hamming code which is also perfect. So we have a unique way of correcting at most one error on each of these two subsets of positions. C has minimum distance 3 and covering radius 2.

4.6 The Gilbert bound:

Definition:4.6.1

$$A(n,d) = \text{Max } \{M \mid \text{an } (n, M, d) \text{ code exists} \}.$$

A code C such that $|C| = A(n,d)$ is called optimal.

Definition:4.6.2

$d = n-k+1$. Such codes are optimal in the sense of $|C| = A(n, d)$. Usually $[n,k,n-k+1]$ codes are called maximum distance separable codes (MDS codes).

Theorem:4.6.3

For binary codes we have $A(n, 2t-1) = A(n+1, 2t)$. We remind the reader of the definition of a sphere $B_r(x)$, given in according to Block codes and we define;

$$V_q(n,r) = |B_r(x)| = \sum_{i=0}^r \binom{n}{i} (q-1)^i \text{ sphere-packing condition.}$$

In order to study the function α , we need a generalization of the entropy function defined in

the binary entropy function H is defined by $H(0) = 0, H(x) = -x \log x - (1-x) \log(1-x)$,

$(0 < x \leq 1/2)$. We define the entropy function H_q on $[0, \theta]$, where

$$Q := (q-1)/q, \text{ by}$$

$$H_q(0) = 0,$$

$$H_q(x) = x \log_q (q-1) - x \log_q x - (1-x) \log_q (1-x) \text{ for } 0 < x \leq \theta.$$

Note that $H_q(x)$ increases from 0 to 1 as x runs from 0 to θ .

Lemma:4.6.4

Lemma $0 \leq \lambda \leq \theta, q \geq 2$. Then $\lim_{n \rightarrow \infty} n^{-1} \log_q V_q(n, [\lambda n]) = H_q(\lambda)$.

Theorem:4.6.5

If $0 \leq \delta \leq \theta$ then $\alpha(\delta) \geq 1 - H_q(\delta)$.

Proof:

By $A(n,d) \geq q^n / v_q(n,d-1)$ and $\lim_{n \rightarrow \infty} n^{-1} \log_q v_q(n, [\lambda n]) = H_q(\lambda)$, we have

$$\alpha(\delta) = \lim_{n \rightarrow \infty} n^{-1} \log_q A(n, \delta_n) \geq \lim_{n \rightarrow \infty} \{1 - n^{-1} \log_q v_q(n, \delta_n)\} = 1 - H_q(\delta).$$

Example:4.6.6

Consider a generator matrix for the $[31,5]$ dual binary Hamming code. Show that it is possible to leave out a number of columns of this matrix in such a way that the resulting code has $d=10$ and meets the Gilbert bound.

Solution:

The columns of generator matrix are the points $(x_1, x_2, x_3, x_4, x_5)$ of $PG(4,2)$. We know that all the non zero codewords of the $[31,5]$ code have weight 16. By the same result the positions corresponding to $x_1=x_2=0$ yield a subcode of length 7 with all non zero weights equal to 4 and the positions with $x_3-x_4=x_5=0$ give a subcode of length 3 with all non zero weights equal to 2. If we puncture by these ten positions the remaining $[21,5]$ code therefore

has $d = 16 - 4 \cdot 2 = 8$. From Griesmer Bound $n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$ we find

$n \geq 10 + 5 + 3 + 2 + 1 = 21$, i.e. the punctured code meets the Griesmer bound.

Lemma:4.6.7

If A and C are subsets of Q^n then there is an $x \in Q^n$ such that

$$|(x+A) \cap C| / |A| \geq |C| / q^n.$$

4.7 Elias Bound**Theorem:4.7.1**

Let $q, n, d, r \in \mathbb{N}$, $q \geq 2$, $0 \leq r \leq n$ and $r^2 - 2\theta n r + \theta n d > 0$. Then

$$A(n, d) \leq (\theta n d / r^2 - 2\theta n r + \theta n d) \cdot (q^n / v_q(n, r))$$

Proof:

If A and C are subset of Q^n then there is an $x \in Q^n$ such that $|(x + A) \cap C| / |A| \geq |C|/q^n$
 we know that an (n, M, d) code has a subcode with $k \geq M v_q(n, r) / q^n$ words which are in
 some $B_r(x)$. So we may apply lemma,

$$d \leq k r / r - 1(2 - r/\theta n)$$

This yields $q^n M v_q(n, r) \leq k \leq \theta n d / r^2 - 2 \theta n r + \theta n d$

Note that $r = \theta n, d > \theta n$ yields the plotting bound.

Definition: 4.7.2

We denote by (n, d, w) the maximal number of code-words in a binary code of length n
 and minimum distance $\geq d$ for which all codewords have weight w .

Definition: 4.7.3

Let $C \in Q^n$ be a code with M words. We define

$$A_i = M^{-1} |\{(x, y) \mid x \in C, y \in C, d(x, y) = i\}|.$$

The sequence $(A_i)_{i=0}^n$ is called the distance distribution or inner distribution is the
 weight distribution.

Chapter 5

5.1 Metrices

Definition:5.1.1

We may wish to measure the distance of elements in a set. If X is the set of objects we wish to measure, then we can define a distance function on the cross product of set with itself mapped to the set of positive real no. In other words

$$d : X \times X \rightarrow \mathbb{R}$$

- (Nonnegativity) $d(x,y) \geq 0$
- (Coincidence) $d(x,y) = 0$ if $x=y$
- (Symmetry) $d(x,y) = d(y,x)$
- (Triangle inequality) $d(x,y) + d(y,z) \geq d(x,z)$

Definition:5.1.2

A pseudometric is a distance function, that possibly fails the coincidence requirement. That requires that if $d(x,y)=0$ then $x=y$. In the pseudometric, it is possible that $x \neq y$. In other words means that the distance may fail to distinguish to objects in the original set.

Definition:5.1.3

If a function satisfies all of the requirements of the distance function except for symmetry, then it is a quasimetric. In this case, $d(x,y)$ might not be the same as $d(y,x)$. A simple illustration of this metric is a city that only has one way streets. The distance between home and the office may not be the same as the distance between the office and home depending on the streets.

5.2 Kernel and Index

Definition:5.2.1

Machine learning provides us with another similarity that is based on the Euclidean metric, so it defined on elements of R^n . Let $d(x, y)$ denote the Euclidean metric between two vectors x and y . The similarity is called the **Gaussian kernel**

$$K(x, y) = e^{-d(x, y)}$$

If $x=y$, then $d(x, y)=0$, so $k(x, y)=1$ from the negative sign on the exponent, we know that the values of $k(x, y)$ are between 0 and 1, and are only if the two values are equal.

Definition:5.2.2

We will take the ratio of that with the number of objects that are in the two sets and this will given as the similarity called the **jaccard index** or the jaccard coefficient. In precise terms the jaccard index $J(A, B) = \frac{|A \cap B|}{|A \cup B|}$.

Let $(0,0,0,0)$ and $(0.1,0.1,0.1,0.1)$ be elements of the set R^4 . Then the Euclidean distance of the two elements is 0.2. However, if we consider the Jaccard index, the similarity is 0, as the two vector have no elements in common. So the fact that the Euclidean distance is small means that they are closed together by using that metric but the similarity given by the Jaccard index implies that they are very different.

Remark:5.2.3

1.If an open statement becomes true for all replacements by the 2 members in a given universe, then that open statement is true for each specific individual member in that universe. (A bit more symbolically – if $p(x)$ is an open statement for a given universe, and if The following solution of an algebraic equation parallels the valid argument.

1) If $3x - 7 = 20$, then $3x = 27$.

2) If $3x = 27$, then $x = 9$.

3) Therefore, if $3x - 7 = 20$, then $x = 9$.

2. When we dealt with the universe of all quadrilaterals in plane geometry, we may have found ourselves relating something like this:

"Since every square is a rectangle, and every rectangle is a parallelogram, it follows that every square is a parallelogram."

In this case we are using the argument.

$p(x)$: x is a square $q(x)$: x is a rectangle $r(x)$: x is a parallelogram.

Definition:5.2.4

Let n be an integer. We call n even if n is divisible by 2 – that is, if there exists an integer r so that $n = 2r$. If n is not even, then we call n odd and find this case that there exists an integer s where $n = 2s + 1$.

5.3 The pigeonhole principle

Definition:5.3.1

In mathematics one sometimes finds that an almost obvious idea, when applied in a In mathematics one sometimes finds that an almost obvious idea, when applied in a rather , subtle manner , is the key needed to solve a troublesome problem . On the list of such obvious ideas many would undoubtedly place the following rule, known as the **pigeonhole principle**.

If m pigeons occupy n pigeonholes and $m > n$, then atleast one pigeonhole has two or more pigeon roosting in it.

Example:5.3.2

Any subset of size 6 from the set $S = \{1, 2, 3, \dots, 9\}$ must contain two elements whose sum is 10. Here the pigeons constitute a six-element subset of $\{1, 2, 3, \dots, 9\}$, and the **pigeonholes** are the subsets: $\{1, 9\}$, $\{2, 8\}$, $\{3, 7\}$, $\{4, 6\}$, $\{5\}$. When the six pigeons go to their respective pigeonholes, they must fill at least one of the two-element subsets whose members sum to 10.

Definition:5.3.3

For sets A and B , if D is a $\subseteq A \times B$, then $\pi_A: D \rightarrow A$ defined by $\pi_A(a, b) = a$, is called the **projection of the first coordinate**. The function $\pi_B: D \rightarrow B$, defined by $\pi_B(a, b)$, is called the **projection of the second coordinate**.

Example:5.3.4

If $A = \{w, x, y\}$ and $B = \{1, 2, 3, 4\}$, let $D = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 4)\}$. Then the projection $\pi_A: D \rightarrow A$ satisfies $\pi_A(x, 1) = \pi_A(x, 2) = \pi_A(x, 3) = x$, and $\pi_A(y, 1) = \pi_A(y, 4) = y$. Since $\pi_A(D) = \{x, y\} \subset A$, this function is not onto. For $\pi_B: D \rightarrow B$ we find that $\pi_B(x, 1) = \pi_B(y, 1) = 1$, $\pi_B(x, 2) = 2$, $\pi_B(x, 3) = 3$, and $\pi_B(y, 4) = 4$, so $\pi_B(D) = B$ and this **projection** is an onto function.

5.4 Pseudo random generation :

Definition:5.4.1

The typical structure of a random number generator is as follows. There is a finite set S of states, and a function $f: S \rightarrow S$. There is an output space U , and an output function $g: S \rightarrow U$. We will always take the output space to be $(0, 1)$. The generator is given an initial value S_0 for the state, called the **seed**. The seed is typically provided by the user. Then a sequence of random numbers is generated by defining: $S_n = f(S_{n-1})$, $n = 1, 2, 3, \dots$ $U_n = g(S_n)$

Definition:5.4.2

A **Pseudo - Random Bit Generator (PRBG)** is a deterministic algorithm which, given a truly random binary sequence :

of length n , output a binary sequence of length $l(n) > n$ Which appears to be random, with $l(n)$ being a polynomial. The input to the PRBG is called the **seed**, and the output is called a **pseudo random bit sequence**.

Definition:5.4.3

Let $g : \{0,1\}^n \rightarrow \{0,1\}^{l(n)}$ be an efficient (Computable in polynomial time) function ensemble, with $l(n)$ being a polynomial with $l(n) > n$. Let X and I be random variable uniformly distributed respectively on $\{0,1\}^n$ and on $\{1, \dots, l(n)\}$. Then g is a **next bit unpredictable PRBG**, if for all adversaries. A running in polynomial time the success probability (Prediction Probability) of A for g

$$P[A(I, g(x)\{1, \dots, I-1\}) = g(x)I] \frac{1}{p(n)} < \text{for all } p$$

Where p is a polynomial.

5.5 The Blum - Blum Shub Generator

Definition :5.5.1

Let $n \in \mathbb{N}$ Then $a \in \mathbb{Z}_n^*$ called a **quadratic residue modulo n** if there exists $b \in \mathbb{Z}_n^*$ such that $a \equiv b^2 \pmod{n}$

The set of quadratic residues modulo n is denoted by QR_n . Furthermore, $Q \cap R_n = \mathbb{Z}_n^* \setminus QR_n$ is called the **set of quadratic non residues**.

Example:5.5.2

For \mathbb{Z}_{23}^* , We have $QR_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$

and

$$QNR_{23} = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$$

Definition :5.5.3

Let p be an odd prime. For $a \in \mathbb{Z}_p^*$, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p/a \\ 1 & a \in QR_p \\ -1 & a \notin QR_p \end{cases}$$

The following theorem shows how to compute the Legendre symbol of an element $a \in \mathbb{Z}_p^*$.

Theorem: 5.5.4

Let p be an odd prime and Let $a \in \mathbb{Z}_p^*$. Then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Proof:

Let $a \in QR_p$, i.e., $a = b^2$ in \mathbb{Z}_p^* for some $b \in \mathbb{Z}_p^*$

Then $a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod{p}$ because of Fermat's little theorem. Let $a \in QNP_p$. Let g be a generator of \mathbb{Z}_p^* (a cyclic group of order $p-1$). Then $a = g^t$ for some odd $t = 2s+1$ (otherwise, $a = g^t = g^{2s} = (g^s)^2$), and $a^{p-1/2} \equiv (g^t)^{p-1/2} \equiv (g^{2s})^{p-1/2} \cdot g^{p-1/2} \equiv g^{p-1/2} \pmod{p}$. Now $(g^{p-1/2})^2 = 1$, hence $g^{p-1/2} \in \{-1, 1\}$. Because g is a generator of \mathbb{Z}_p^* , the order of g is equal to $p-1$ and $g^{p-1/2} = -1$.

Example: 5.5.5

Let $n = p \cdot q = 7 \cdot 19 = 133$ and $s = 100$. Then we have $x_0 = 1002 \pmod{133} = 25$.

The sequence $x_1 = 25^2 \pmod{133} = 93$, $x_2 = 93^2 \pmod{133} = 4$, $x_3 = 4^2 \pmod{133} = 16$, $x_4 = 16^2 \pmod{133} = 123$ produces the output 1,0,0,1.

Properties: 5.5.6

Pseudo-Random Numbers:

- Problems when generating pseudo-random numbers.
- The generated numbers might not be uniformly distributed.
- The generated numbers might be discrete-valued instead of continuous-valued.
- The mean of the generated numbers might be too high or too low.

• The variance of the generated numbers might be too high or too low.

• There might be dependence.

• Autocorrelation between numbers

• Numbers successively higher or lower than adjacent numbers.

• To achieve maximum density and avoid cycling.

• Most digital computers use a binary representation of numbers.

• Speed and efficiency are aided by a modulus, m , to be (or close) a power of 2.

• The LCG has full period if and only if the following three conditions hold (Hull and

Dobell, 1962):

1. The only positive integer that (exactly) divides both m and c is 1

2. If q is a prime number that divides m , then q divides $a-1$.

3. If 4 divides m , then 4 divides $a-1$.

APPLICATIONS OF CYBER SECURITY AND CODING THEORY

Introduction

Cyber security is defined as technologies and processes constructed to protect computers, computer hardware, software, networks and data from unauthorized access, vulnerabilities supplied through Internet by cyber criminals, terrorists groups and hackers . As internet offers on the one hand huge number of benefits and on the other hand it also provides equal opportunities for cyber-terrorists and hackers. Error control coding has been used extensively in digital communication systems because of its cost-effectiveness in achieving efficient, reliable digital transmission. Coding now plays an important role in the design of modern communication systems.

Cyber security Applications

Nature of Cyberspace

Cyberspace is virtual space that use electronics and electromagnetic spectrum to store, modify and exchange information through the use of networked system and concerned physical structure . It is intangible where communications and internet related activities take place. Cyberspace is imaginary where contained objects are neither exist nor representation of physical world.

Salami Attack

In this cyber criminals and attackers steal money in very little amount from several bank accounts to make a huge amount. The alteration becomes so insignificant that in a single case it would be difficult to notice. It is general perception that no customer will probably notice this unauthorized deduction, but it will be beneficial to cyber criminals that make large money.

Spoofing

It refers to a technique to have unauthorized access to computers, whereby perpetrator sends messages to a networked computer with an IP address. At the recipient end it seems that messages are being transmitted from a trustworthy source. To conduct IP spoofing, a hacker first makes attempt to find an trusted host IP address and then modification and alteration of packets are done to show that the packets are being generated from original host.

Coding Theory Applications:

In Satellite Communications

Two of the most treasured resources in satellite communications are power and bandwidth. Error control coding often used to improve the transmission quality, which is otherwise compromised by interference and power limitations. FEC techniques tends to be more widely used than ARQ techniques, which require data retransmission. In satellite communication systems, convolutional codes with constraint length 7 are widely used. Block codes are also applied in some satellite systems .

Examples of using block codes include a (31, 15) RS code for the joint tactical information distribution system (mDS), a (127, 112) BCH code for the INTELSAT V system, and a (7, 2) RS code for the air force satellite communications (AFSATCOM) wideband channel.

In Mobile Applications

In the mobile environment, it burst errors due to multipath fading are dominant. Since the bandwidth available to each channel is strictly limited , the code rate must be high. Furthermore, since each mobile terminal must obviously include a decoder, codes requiring a complex decoder cannot be used. Therefore, burst-error-correcting

codes with simple decoding algorithms are preferable for mobile communications. In some systems, BCH codes are used in conjunction with ARQ.

A recent example is the coding standard for digital mobile radio proposed by the North American railroads for advanced train control systems (ATCS). The (16,12) RS code adopted for ATCS provides the best trade-off between throughput, delay, and implementation complexity. The RS code will be used in a hybrid FEC/ARQ system, ensuring a probability of undetected error of less than 10^{-10}

CONCLUSION

In this project , we have learned about the basics of **Mathematical Foundation for Cyber Security and Coding Theory** . We have proved many theorems using the concepts of abstract algebra , probability theory and pseudo random number generation. Also the development of basic coding theory and the state of art coding techniques have been reviewed . The need, nature of cyber security and the coding in communication systems and future trends have also been discussed in the applications section . The mentioned definitions and theorems can be extended to other fields of mathematics .

REFERENCES

- [1] Bersekas D. P , Introduction to Probability , Athena Scientific, 2008.
- [2] Chuck Easttom ,Modern Cryptography: Applied Mathematics
for Encryption and Information Security.
- [3] Douglas Stinson, Cryptography – Theory and Practice, CRC Press, 2006.
- [4] Ivan M . Niven , Montgomery . H.L and Zuckerman.H S , An Introduction
to the Theory of Numbers, John Wiley and Sons, 2004.
- [5] Leigh Metcalf, William Casey, Cyber security and Applied Mathematics,
Syngress Publisher(s): Released in June 2016.
- [6] Liu .C.L , Elements of Discrete Mathematics ,McGraw Hill, 2008.
- [7] Malik,. D. S, Mordeson.J , Sen . M . K , Fundamentals of Abstract
Algebra, Tata McGraw Hill.
- [8] Saikia P . K , Linear Algebra, Pearson Education, 2009.
- [9] Sheldon M Ross, Introduction to Probability Models, Academic Press,
2003.

AN INTRODUCTION TO FUZZY MATHEMATICS

A project submitted to

ST.MARY'S COLLEGE (Autonomous), THOOTHUKUDI.

affiliated to

Manonmaniam Sundaranar University, Tirunelveli

in partial fulfilment for the award of the degree of

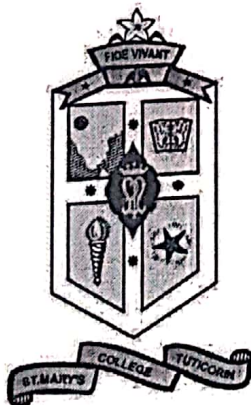
BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

NAME	REGISTER NO
P. ESTHER ANGEL	19SUMT10
M. MANJULA	19SUMT19
N. PADMASHRI	19SUMT27
P. SHANMUGA PRIYA	19SUMT37
V. VINOOTHINI	19SUMT41

Under the guidance of

Ms. J. JENIT AJITHA M.Sc., M.Phil.,



DEPARTMENT OF MATHEMATICS

St. Mary's College (Autonomous), Thoothukudi.

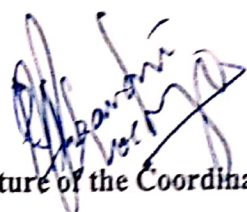
May-2022

CERTIFICATE

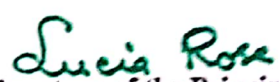
This is to certify that this project work entitled "AN INTRODUCTION TO FUZZY MATHEMATICS" is submitted to St.Mary's College (Autonomous), Thoothukudi affiliated to Manonmaniam Sundaranar University, Tirunelveli in partial fulfilment for the award of degree of Bachelor of Science in Mathematics and is the work done during the year 2021-2022 by the following students.

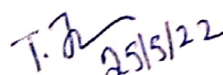
NAME	REGISTER NO
P. ESTHER ANGEL	19SUMT10
M. MANJULA	19SUMT19
N. PADMASHRI	19SUMT27
P. SHANMUGA PRIYA	19SUMT37
V. VINOOTHINI	19SUMT41


Signature of the Guide


Signature of the Coordinator


Signature of the Director
Director
Self Supporting Courses
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Principal
Principal
St. Mary's College (Autonomous)
Thoothukudi - 628 001.


Signature of the Examiner

DECLARATION

We hereby declare that the project entitled "AN INTRODUCTION TO FUZZY MATHEMATICS" submitted for the degree of Bachelor of Science is our work carried out under the guidance of Ms. J. Jenit Ajitha M.Sc., M.Phil., Department of Mathematics (SSC), St.Mary's College(Autonomous), Thoothukudi.

P. Esther angel.
(ESTHER ANGEL. P)

M. Manjula
(MANJULA. M)

N. Padmashri.
(PADMASHRI. N)

P. Shan muga Priya
(SHANMUGA PRIYA. P)

V. Vin^othini
(VINO^THINI.V)

ACKNOWLEDGEMENT

First of all, we thank the Almighty for showering his blessings to undergo this project.

We express our sincere gratitude and heartfelt thanks to our Principal Rev. Dr. Sr. A. S. J. Lusia Rose M.Sc., PGDCA., M.Phil., Ph.D., and to our Director Rev. Sr. Josephine Jeyarani M.Sc., B.Ed., for kindly permitting us to do this project.

We express our gratitude to Dr. P. Anbarasi Rodrigo M.Sc., B.Ed., Ph.D., Coordinator, Department of Mathematics (SSC) for her inspirational ideas and Encouragement.

We are very thankful to our guide Ms. J. Jenit Ajitha, M.Sc., M.Phil., Assistant Professor, Department of Mathematics (SSC) for her efficient and effective guidance. She played a key role in the preparation of this project.

We also thank our staff members for their encouragement in all our efforts. Finally, we thank all those who extended their help regarding this project.

Place: Thoothukudi

Date: 17.05.2022.

CONTENT		
CHAPTER	TOPIC	PAGE NO.
	Introduction	
1	Preliminaries	1
2	Fuzzy Matrices	5
3	Fuzzy relations and Compositions	23
4	Fuzzy Graphs and Relations	36
5	Applications of Fuzzy Graphs	47
	Conclusion	
	References	

INTRODUCTION

Fuzzy sets are sets whose elements have degrees of membership. Fuzzy sets were introduced independently as an extension of the classical notion of set. Fuzzy relations, which are now used throughout fuzzy mathematics and have applications in areas such as linguistics decision making and clustering. The fuzzy set theory can be used in a wide range of domains in which information is incomplete or imprecise, such as bioinformatics.

Applications of fuzzy logic and fuzzy set theory in Decision – making, Pattern recognition, Image processing, Control systems, Neural networks, Genetic algorithm and in many other areas have given significant results. The Project consists of five chapters.

In chapter 1, we have discussed the basic concepts of concepts of Crisp Sets and to introduce notation and terminology useful for our discussion of fuzzy sets.

In chapter 2, we have discussed about properties of fuzzy matrices.

In chapter 3, we have discussed about Fuzzy Relations and Compositions, the concept of relations in the same manner as fuzzy sets generalize the fundamental idea of sets.

In chapter 4, we have discussed about Fuzzy Graphs and Relations, the usual convention between binary relations and Boolean matrices

In chapter 5, we have discussed about the Applications of Fuzzy Graphs in numerous applications in diverse parts of Science and Engineering like

Broadcast communications, producing, Social Network, man-made reasoning,
data hypothesis, neural systems and arranging and so forth.



CHAPTER 1

CHAPTER 1

PRELIMINARIES

1.1 DEFINITION OF FUZZY SETS

1.1.1 EXPRESSION FOR FUZZY SETS

Membership function μ_A in crisp set maps whole members in universal set X to set $\{0,1\}$

$$\mu_A: X \Rightarrow \{0, 1\}$$

Definition: 1.1.2

In fuzzy sets, each element is mapped to $[0, 1]$ by membership function.

$$\mu_A: X \rightarrow [0, 1]$$

Where $[0, 1]$ means real numbers between 0 and 1 (including 0, 1)

1.2 EXPANSION OF SETS

Definition: 1.2.1

The value of membership degree might include uncertainty. If the value of membership function is given by a fuzzy set, it is Type-2 fuzzy set. This concept can be extended up to Type-n fuzzy sets

Definition: 1.2.2

The term "Level-2 set" indicates fuzzy sets whose elements are fuzzy sets. The term "Level-1 set" is applicable to fuzzy sets whose elements are no fuzzy sets ordinary elements. In the same way, we can derive up to level-k fuzzy sets

1.3 α -CUT SET

Definition: 1.3.1

The α -cut set A_α is made up of members whose membership is not less than α .

$$A_\alpha = \{x \in X / \mu_A(x) \geq \alpha\}$$

Note that α is arbitrary. This α -cut set is a crisp set.

Definition: 1.3.2

The value α which explicitly shows the value of the membership function, is in the range of $[0, 1]$. The “level set” is obtained by the α 's.

$$\text{i.e. } \Lambda_A = \{\alpha / \mu_A(x) = \alpha, \alpha \geq 0, x \in X\}$$

1.4 CONVEX SETS

Definition: 1.4.1

Let the universal set X be defined in n -dimensional Euclidean vector space R^n . If all the α -cut sets are convex then the fuzzy sets with these α -cuts are also convex. In other words, if a relation,

$$\mu_A(t) \geq \text{Min} [\mu_A(r), \mu_A(s)]$$

Where $t = \lambda r + (1 - \lambda)s$, $r, s \in R^n$, $\lambda \in [0, 1]$ holds, the fuzzy set A is convex.

1.5 FUZZY NUMBER

Definition: 1.5.1

If a fuzzy set is convex and normalized, and its membership function is defined in \mathbb{R} and piecewise continuous, it is called as "Fuzzy Number".

1.6 FUZZY CARDINALITY

Definition: 1.6.1

The possibility for number of elements in A to be $|A_\alpha|$ is α . Then the membership degree of fuzzy cardinality $|A|$ is defined as,

$$\mu_{|A|}(|A_\alpha|) = \alpha, \alpha \in \Lambda_A$$

Where A_α is a α -cut set and μ_A is a level set.

1.6.2 SUBSET OF FUZZY SET

If there are two fuzzy sets A and B . When their degrees of membership are same, we say " A and B are equivalent". i.e.

$$A=B \text{ iff } \mu_A(x) = \mu_B(x), \forall x \in X.$$

1.7 STANDARD OPERATION OF FUZZY SETS

1.7.1 COMPLEMENT

We can find complement set of fuzzy set A in crisp set. We denote the complement set of A as \bar{A} . Membership degree can be calculated as following,

$$\mu_{\bar{A}}(x) = 1 - \mu_A(x), \forall x \in X.$$

1.7.2 UNION

Membership value of member x in the union takes the greater value of membership between A and B.

$$\mu_{A \cup B}(x) = \text{Max} [\mu_A(x), \mu_B(x)], \forall x \in X.$$

1.7.3 INTERSECTION

Intersection of fuzzy sets A and B takes smaller value of membership function between A and B.

$$\mu_{A \cap B}(x) = \text{Min} [\mu_A(x), \mu_B(x)], \forall x \in X$$

CHAPTER 2

CHAPTER 2

FUZZY MATRICES

Definition: 2.1

Let A be a $n \times m$ matrix defined by

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

The matrix A is called Fuzzy matrix if and only if $a_{ij} \in [0, 1]$ for $1 \leq i \leq n$ and $1 \leq j \leq m$.

In other words, any $n \times m$ matrix A is a fuzzy matrix if the elements of A are in the interval $[0, 1]$.

Definition: 2.2

We define fuzzy addition $+$, fuzzy multiplication \cdot , and fuzzy subtraction $-$, as follows:

$$a + b = \max(a, b),$$

$$a \cdot b = \min(a, b), \text{ and}$$

$$a - b = \begin{cases} a & \text{if } a > b \\ 0 & \text{if } a \leq b. \end{cases}$$

Proposition: 2.3

Let A, B, C be three $n \times n$ fuzzy matrices. With the fuzzy addition defined in

Definition 2.1, we have the following:

(1) $A + B = B + A$ (Commutativity),

(2) $(A + B) + C = A + (B + C)$ (Associativity),

(3) $A + 0 = 0 + A = A$ (Additive Identity).

Proof:

$$\text{Let } A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}, B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix}$$

$$\text{and } C = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$$

(1) Observe the following:

$$\begin{aligned} A + B &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} \\ &= \begin{bmatrix} \max(a_{11}, b_{11}) & \max(a_{12}, b_{12}) & \dots & \max(a_{1n}, b_{1n}) \\ \max(a_{21}, b_{21}) & \max(a_{22}, b_{22}) & \dots & \max(a_{2n}, b_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(a_{n1}, b_{n1}) & \max(a_{n2}, b_{n2}) & \dots & \max(a_{nn}, b_{nn}) \end{bmatrix} \end{aligned}$$

On the other hand,

$$\begin{aligned} B + A &= \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \\ &= \begin{bmatrix} \max(b_{11}, a_{11}) & \max(b_{12}, a_{12}) & \dots & \max(b_{1n}, a_{1n}) \\ \max(b_{21}, a_{21}) & \max(b_{22}, a_{22}) & \dots & \max(b_{2n}, a_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(b_{n1}, a_{n1}) & \max(b_{n2}, a_{n2}) & \dots & \max(b_{nn}, a_{nn}) \end{bmatrix} \end{aligned}$$

Thus $A + B = B + A$. It follows that the addition of fuzzy matrices is commutative.

(2) Observe the following:

$$(A+B) + C = \left(\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} \right) + \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \max(a_{11}, b_{11}) & \max(a_{12}, b_{12}) & \dots & \max(a_{1n}, b_{1n}) \\ \max(a_{21}, b_{21}) & \max(a_{22}, b_{22}) & \dots & \max(a_{2n}, b_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(a_{n1}, b_{n1}) & \max(a_{n2}, b_{n2}) & \dots & \max(a_{nn}, b_{nn}) \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$$

$$\begin{bmatrix} \max(\max(a_{11}, b_{11}), c_{11}) & \max(\max(a_{12}, b_{12}), c_{12}) & \dots & \max(\max(a_{1n}, b_{1n}), c_{1n}) \\ \max(\max(a_{21}, b_{21}), c_{21}) & \max(\max(a_{22}, b_{22}), c_{22}) & \dots & \max(\max(a_{2n}, b_{2n}), c_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(\max(a_{n1}, b_{n1}), c_{n1}) & \max(\max(a_{n2}, b_{n2}), c_{n2}) & \dots & \max(\max(a_{nn}, b_{nn}), c_{nn}) \end{bmatrix}$$

$$= \begin{bmatrix} \max(a_{11}, b_{11}, c_{11}) & \max(a_{12}, b_{12}, c_{12}) & \dots & \max(a_{1n}, b_{1n}, c_{1n}) \\ \max(a_{21}, b_{21}, c_{21}) & \max(a_{22}, b_{22}, c_{22}) & \dots & \max(a_{2n}, b_{2n}, c_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(a_{n1}, b_{n1}, c_{n1}) & \max(a_{n2}, b_{n2}, c_{n2}) & \dots & \max(a_{nn}, b_{nn}, c_{nn}) \end{bmatrix}$$

$$A + (B+C) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} +$$

$$\left(\begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix} \right)$$

$$\begin{aligned}
&= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} + \\
&\quad \begin{bmatrix} \max(b_{11}, c_{11}) & \max(b_{12}, c_{12}) & \dots & \max(b_{1n}, c_{1n}) \\ \max(b_{21}, c_{21}) & \max(b_{22}, c_{22}) & \dots & \max(b_{2n}, c_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(b_{n1}, c_{n1}) & \max(b_{n2}, c_{n2}) & \dots & \max(b_{nn}, c_{nn}) \end{bmatrix} \\
&= \begin{bmatrix} \max(a_{11}, \max(b_{11}, c_{11})) & \max(a_{12}, \max(b_{12}, c_{12})) & \dots & \max(a_{1n}, \max(b_{1n}, c_{1n})) \\ \max(a_{21}, \max(b_{21}, c_{21})) & \max(a_{22}, \max(b_{22}, c_{22})) & \dots & \max(a_{2n}, \max(b_{2n}, c_{2n})) \\ \vdots & \vdots & \ddots & \vdots \\ \max(a_{n1}, \max(b_{n1}, c_{n1})) & \max(a_{n2}, \max(b_{n2}, c_{n2})) & \dots & \max(a_{nn}, \max(b_{nn}, c_{nn})) \end{bmatrix} \\
&= \begin{bmatrix} \max(a_{11}, b_{11}, c_{11}) & \max(a_{12}, b_{12}, c_{12}) & \dots & \max(a_{1n}, b_{1n}, c_{1n}) \\ \max(a_{21}, b_{21}, c_{21}) & \max(a_{22}, b_{22}, c_{22}) & \dots & \max(a_{2n}, b_{2n}, c_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(a_{n1}, b_{n1}, c_{n1}) & \max(a_{n2}, b_{n2}, c_{n2}) & \dots & \max(a_{nn}, b_{nn}, c_{nn}) \end{bmatrix}
\end{aligned}$$

Thus $(A + B) + C = A + (B + C)$. It follows that addition of fuzzy matrices is

associative.

(3) Observe the following:

$$\begin{aligned}
A + 0 &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} + \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \\
&= \begin{bmatrix} \max(a_{11}, 0) & \max(a_{12}, 0) & \dots & \max(a_{1n}, 0) \\ \max(a_{21}, 0) & \max(a_{22}, 0) & \dots & \max(a_{2n}, 0) \\ \vdots & \vdots & \ddots & \vdots \\ \max(a_{n1}, 0) & \max(a_{n2}, 0) & \dots & \max(a_{nn}, 0) \end{bmatrix} \\
&= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}
\end{aligned}$$

Thus $A + 0 = A$. Since fuzzy matrix addition is commutative (Property 1), it follows

that $A + 0 = 0 + A = A$.

Proposition 2.4:

Let A be an $n \times n$ fuzzy matrix. With the **fuzzy subtraction** defined in

Definition 2.1, we have the following:

$$(1) 0 - A = 0,$$

$$(2) A - A = 0,$$

$$(3) A - 0 = A,$$

Proof:

$$\text{Let } A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

(1) Observe the following:

$$\begin{aligned} 0 - A &= \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} - \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \\ &= \begin{bmatrix} 0 - a_{11} & 0 - a_{12} & \dots & 0 - a_{1n} \\ 0 - a_{21} & 0 - a_{22} & \dots & 0 - a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 - a_{n1} & 0 - a_{n2} & \dots & 0 - a_{nn} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \\ &= 0. \end{aligned}$$

Thus $0 - A = 0$.

(2) Observe the following:

$$\begin{aligned}
 A - A &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} - \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \\
 &= \begin{bmatrix} a_{11} - a_{11} & a_{12} - a_{12} & \dots & a_{1n} - a_{1n} \\ a_{21} - a_{21} & a_{22} - a_{22} & \dots & a_{2n} - a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} - a_{n1} & a_{n2} - a_{n2} & \dots & a_{nn} - a_{nn} \end{bmatrix} \\
 &= \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \\
 &= 0.
 \end{aligned}$$

Thus $A - A = 0$.

(3) Let $i, j \in \mathbb{Z}^+$. Note that for any $1 \leq i, j \leq n$, $a_{ij} \geq 0$. Suppose $a_{ij} > 0$. Observe the following:

$$\begin{aligned}
 A - 0 &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} - \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \\
 &= \begin{bmatrix} a_{11} - 0 & a_{12} - 0 & \dots & a_{1n} - 0 \\ a_{21} - 0 & a_{22} - 0 & \dots & a_{2n} - 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} - 0 & a_{n2} - 0 & \dots & a_{nn} - 0 \end{bmatrix} \\
 &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \\
 &= A.
 \end{aligned}$$

In other words, $a_{ij} - 0 = a_{ij}$ since $a_{ij} > 0$. Suppose $a_{ij} = 0$. Then $a_{ij} - 0 = 0 = a_{ij}$.

Since $a_{ij} \leq 0$. Thus $A - 0 = 0$.

Lemma 2.5:

The fuzzy multiplication is distributive with respect to the fuzzy addition. In other words, if $a, b, c \in [0, 1]$, then $a(b + c) = ab + ac$;

That is , $\min(a, \max(b,c)) = \max(\min(a,b), \min(a,c))$.

Proof:

Let $a, b, c \in [0, 1]$. It suffices to consider the following six cases:

$$(1) a \leq b \leq c,$$

$$(2) a \leq c \leq b,$$

$$(3) b \leq a \leq c,$$

$$(4) b \leq c \leq a,$$

$$(5) c \leq a \leq b,$$

$$(6) c \leq b \leq a.$$

For Example, for case (1), we have:

$$a(b+c) = \min(a, \max(b,c))$$

$$= \min(a,c)$$

$$= a.$$

On the other hand,

$$ab + ac = \max(\min(a,b), \min(a,c))$$

$$= \max(a,a)$$

$$= a.$$

Thus case (1) is proved. The proofs of the other five cases are similar to case (1).

Proposition 2.6:

Let A, B, C be $n \times n$ fuzzy matrices. Then with the fuzzy operations

We have:

- (1) $A \cdot 0 = 0 \cdot A = 0$,
- (2) $A(B+C) = AB + AC$, (Distributive)
- (3) $A \cdot I = I \cdot A = A$ (Multiplicative Identity)
- (4) $(AB)C = A(BC)$ (Associativity).

Proof: Let $A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix}$

and $C = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$ be fuzzy matrices, and Let $i, j \in \mathbb{Z}^+$.

(1) Observe the following:

$$\begin{aligned} A \cdot 0 &= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \\ &= \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix}, \end{aligned}$$

where for each $1 \leq i, j \leq n$, $x_{ij} = \max\{\min(a_{ik}, 0), 1 \leq k \leq n\}$. Note that $a_{ik} \geq 0$,

and therefore, $\min(a_{ik}, 0) = 0$. It follows that $x_{ij} = 0$.

On the other hand, we have :

$$0.A = \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix},$$

where for each $1 \leq i, j \leq n$, $x_{ij} = \max\{\min(0, a_{kj}), 1 \leq k \leq n\}$. Note that $a_{kj} \geq 0$, and therefore, $\min(0, a_{kj}) = 0$. It follows that $x_{ij} = 0$.

Thus, we have that $A.0 = 0.A = 0$.

$$(2) \text{ Let } 1 \leq i, j \leq n. \text{ Note } B + C = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \dots & v_{nn} \end{bmatrix},$$

where $v_{ij} = \max\{b_{ij}, c_{ij}\}$.

$$\text{Then } A(B+C) = \begin{bmatrix} w_{11} & w_{12} & \dots & w_{1n} \\ w_{21} & w_{22} & \dots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n1} & w_{n2} & \dots & w_{nn} \end{bmatrix}, \text{ where } w_{ij} = \max\{\min(a_{ik}, v_{kj}), 1 \leq k \leq n\}.$$

$$\text{Now note that } AB = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix},$$

where $x_{ij} = \max\{\min(a_{ik}, b_{kj}), 1 \leq k \leq n\}$,

$$\text{And } AC = \begin{bmatrix} y_{11} & y_{12} & \dots & y_{1n} \\ y_{21} & y_{22} & \dots & y_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n1} & y_{n2} & \dots & y_{nn} \end{bmatrix}, \text{ where } y_{ij} = \max\{\min(a_{ik}, c_{kj}), 1 \leq k \leq n\}. \text{ It}$$

$$\text{follows that } AB + AC = \begin{bmatrix} z_{11} & z_{12} & \dots & z_{1n} \\ z_{21} & z_{22} & \dots & z_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1} & z_{n2} & \dots & z_{nn} \end{bmatrix}, \text{ where}$$

$z_{ij} = \max\{\min(x_{ij}, y_{ij}), 1 \leq k \leq n\}$. In other words, for any $1 \leq k \leq n$, we have :

$$z_{ij} = \max \{ \max(\min(a_{ik}, b_{kj})), \max(\min(a_{ik}, c_{kj})) \}.$$

Note that $w_{ij} = \max \{ (a_{ik}, v_{kj}) \} = \max \{ \min(a_{ik}, \max(b_{kj}, c_{kj})), 1 \leq k \leq n \}$. It suffices to show that $w_{ij} = z_{ij}$; that is,

$$\max \{ \min(x_{ij}, y_{ij}), 1 \leq k \leq n \} = \max \{ \min(a_{ik}, \max(b_{kj}, c_{kj})), 1 \leq k \leq n \}.$$

Observe the following:

$$\begin{aligned} z_{ij} &= \max \{ \max(\min(a_{ik}, b_{kj})), \max(\min(a_{ik}, c_{kj})) \} \\ &= (a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{ik}) + \\ &\quad (a_{i1}c_{1j} + a_{i2}c_{2j} + \dots + a_{ik}c_{kj}) \\ &= (a_{i1}b_{1j} + a_{i1}c_{1j}) + (a_{i2}b_{2j} + a_{i2}c_{2j}) + \dots + (a_{ik}b_{ik} + a_{ik}c_{kj}) \\ &= \max \{ (\min(a_{ik}, b_{kj}), \min(a_{ik}, c_{kj})) \} \end{aligned}$$

By Lemma 2.5, we have that $\max \{ (\min(a_{ik}, b_{kj}), \min(a_{ik}, c_{kj})) \} = \min \{ a_{ik}, \max(b_{kj}, c_{kj}) \}$

Now observe the following:

$$\begin{aligned} z_{ij} &= \min \{ a_{ik}, \max(b_{kj}, c_{kj}) \} \\ &= \min(a_{ik}, v_{kj}) \\ &= w_{ij}. \end{aligned}$$

Thus $z_{ij} = w_{ij}$. It follows that $A(B+C) = AB + AC$.

$$(3) \text{ Let } I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Observe the following:

$$A \cdot I = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

$$= \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix},$$

Where for each $1 \leq j \leq n$, $x_{ij} = \max\{\min(a_{ij}, 1), \min(a_{pq}, 0), 1 \leq p \leq n, 1 \leq q \leq n, p \neq i, q \neq j\}$. It follows that $x_{ij} = \max(a_{ij}, 0) = a_{ij}$. Therefore $A \cdot I = A$.

On the other hand,

$$I \cdot A = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{bmatrix},$$

Where for each $1 \leq i \leq n$ and $1 \leq j \leq n$, $x_{ij} = \max\{\min(1, a_{ij}), \min(0, a_{pq}), 1 \leq p \leq n, 1 \leq q \leq n, p \neq i, q \neq j\}$. It follows that $x_{ij} = \max(0, a_{ij}) = a_{ij}$. Therefore $A \cdot I = I \cdot A = A$.

(4) Observe the following:

$$(AB) C = \sum_{k=1}^n (AB)_{ik} C_{kj}$$

$$= \sum_{k=1}^n a_{ik} \left(\sum_{m=1}^n b_{km} c_{mj} \right)$$

$$= \sum_{k,m=1}^n a_{ik} b_{km} c_{mj}$$

$$= \sum_{k,m=1}^n \min(a_{ik}, b_{km}, c_{mj})$$

$$= \sum_{k,m=1}^n \min(a_{im}, b_{mk}, c_{kj})$$

$$= (AB)C.$$

Thus $(AB)C = A(BC)$.

2.7 DEFINITION OF SQUARE MATRIX

Definition:2.7.1

The determinant $|A|$ of $n \times n$ fuzzy matrix A is defined as

$|A| = \det(A) = \sum_{\sigma \in S_n} a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$, where S_n denotes the symmetric group of all permutations of the indices $(1, 2, \dots, n)$. [2]

Example: 2.7.2

$$\text{Let } A = \begin{bmatrix} 0.7 & 0.1 & 0.9 \\ 0 & 0.4 & 1 \\ 0.2 & 0.3 & 0.5 \end{bmatrix}$$

Then,

$$\det(A) = 0.7 \begin{vmatrix} 0.4 & 1 \\ 0.3 & 0.5 \end{vmatrix} + 0.1 \begin{vmatrix} 0 & 1 \\ 0.2 & 0.5 \end{vmatrix} + 0.9 \begin{vmatrix} 0 & 0.4 \\ 0.2 & 0.3 \end{vmatrix}$$

$$= 0.7 (\min(0.4, 0.5) + \min(1, 0.3)) + 0.1 (\min(0, 0.5) + \min(1, 0.2)) + 0.9$$

$$(\min(0, 0.3) + \min(0.4, 0.2))$$

$$= 0.7 (0.4 + 0.3) + 0.1 (0 + 0.2) + 0.9 (0 + 0.2)$$

$$= 0.7 (0.4) + 0.1(0.2) + 0.9 (0.2)$$

$$= 0.4 + 0.1 + 0.2$$

$$= 0.4.$$

Remark : 2.7.3

- (1) Recall it in the case of classical matrices, we alternate between addition and subtraction when calculating the determinant, but in the case of fuzzy matrices, we only use **fuzzy addition**.
- (2) We have that $\det(A) \det(B) = \det(AB)$. But this is not always true for fuzzy matrices. For instance, consider the following examples:

Example: 2.7.4

$$\text{Let } A = \begin{bmatrix} 0.7 & 0.1 & 0.9 \\ 0 & 0.4 & 1 \\ 0.2 & 0.3 & 0.5 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0.2 & 0.1 & 0 \\ 0.8 & 1 & 0.3 \\ 0.4 & 0.9 & 0.4 \end{bmatrix} \text{ be two fuzzy}$$

matrices. Then

$$\begin{aligned} \det(A) &= 0.7 \begin{vmatrix} 0.4 & 1 \\ 0.3 & 0.5 \end{vmatrix} + 0.1 \begin{vmatrix} 0 & 1 \\ 0.2 & 0.5 \end{vmatrix} + 0.9 \begin{vmatrix} 0 & 0.4 \\ 0.2 & 0.3 \end{vmatrix} \\ &= 0.7 (\min(0.4, 0.5) + \min(1, 0.3)) + 0.1 (\min(0, 0.5) + \min(1, 0.2)) + 0.9 \\ &\quad (\min(0, 0.3) + \min(0.4, 0.2)) \\ &= 0.7 (0.4 + 0.3) + 0.1 (0 + 0.2) + 0.9 (0 + 0.2) \\ &= 0.7 (0.4) + 0.1(0.2) + 0.9 (0.2) \\ &= 0.4 + 0.1 + 0.2 \\ &= 0.4. \end{aligned}$$

Now observe that

$$\det(B) = 0.2 \begin{vmatrix} 1 & 3 \\ 0.9 & 0.4 \end{vmatrix} + 0.1 \begin{vmatrix} 0.8 & 0.3 \\ 0.4 & 0.4 \end{vmatrix} + 0 \begin{vmatrix} 0.8 & 1 \\ 0.4 & 0.9 \end{vmatrix}$$

$$\begin{aligned}
&= 0.2 (\min(1,0.4) + \min(0.3,9)) + 0.1 (\min(0.8,0.4) + \min(0.3,0.4)) + 0 \\
&\quad (\min(0.8,0.9) + \min(1,0.4)) \\
&= 0.2 (0.4 + 0.3) + 0.1 (0.4 + 0.3) + 0 (0.8 + 0.4) \\
&= 0.2 (0.4) + 0.1(0.4) + 0 (0.8) \\
&= 0.2 + 0.1 + 0 \\
&= 0.4.
\end{aligned}$$

It follows that $\det(A) \cdot \det(B) = \min(0.4,0.2) = 0.2$. On the other hand,

$$\begin{aligned}
AB &= \begin{bmatrix} 0.7 & 0.1 & 0.9 \\ 0 & 0.4 & 1 \\ 0.2 & 0.3 & 0.5 \end{bmatrix} \cdot \begin{bmatrix} 0.2 & 0.1 & 0 \\ 0.8 & 1 & 0.3 \\ 0.4 & 0.9 & 0.4 \end{bmatrix} \\
&= \begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \\
&= \begin{bmatrix} \max(0.2, 0.1, 0.4) & \max(0.1, 0.1, 0.9) & \max(0, 0.1, 0.4) \\ \max(0, 0.4, 0.4) & \max(0, 0.4, 0.9) & \max(0, 0.3, 0.4) \\ \max(0.2, 0.3, 0.5) & \max(0.1, 0.3, 0.5) & \max(0, 0.3, 0.4) \end{bmatrix} \\
&= \begin{bmatrix} 0.4 & 0.9 & 0.4 \\ 0.4 & 0.9 & 0.4 \\ 0.4 & 0.5 & 0.4 \end{bmatrix}
\end{aligned}$$

where

$$x_{11} = \max (\min (0.7, 0.2), \min (0.1, 0.8), \min (0.9, 0.4)) ,$$

$$x_{12} = \max (\min (0.7, 0.1), \min (0.1, 1), \min (0.9, 0.9)),$$

$$x_{13} = \max (\min (0.7, 0), \min (0.1, 0.3), \min (0.9, 0.4)),$$

$$x_{21} = \max (\min (0, 0.2), \min (0.4, 0.8), \min (1, 0.4)),$$

$$x_{22} = \max (\min (0, 0.1), \min (0.4, 1), \min (1, 0.9)),$$

$$x_{23} = \max (\min (0, 0), \min (0.4, 0.3), \min (1, 0.4)),$$

$$x_{31} = \max (\min (0.2, 0.2), \min (0.3, 0.8), \min (0.5, 0.4)),$$

$$x_{32} = \max (\min (0.2, 0.1), \min (0.3, 1), \min (0.5, 0.9)),$$

$$x_{33} = \max (\min (0.2, 0), \min (0.3, 0.3), \min (0.5, 0.4)).$$

$$\det(AB) = 0.4 \begin{vmatrix} 0.9 & 0.4 \\ 0.5 & 0.4 \end{vmatrix} + 0.9 \begin{vmatrix} 0.4 & 0.4 \\ 0.4 & 0.4 \end{vmatrix} + 0.4 \begin{vmatrix} 0.4 & 0.9 \\ 0.4 & 0.5 \end{vmatrix}$$

$$= 0.4(\min(0.9,0.4) + \min(0.4,0.5)) + 0.9(\min(0.4,0.4) + \min(0.4,0.4)) + 0.4$$

$$(\min(0.4,0.5) + \min(0.9,0.4))$$

$$= 0.4 (0.4 + 0.4) + 0.9 (0.4 + 0.4) + 0.4 (0.4 + 0.4)$$

$$= 0.4 (0.4) + 0.9(0.4) + 0.4 (0.4)$$

$$= 0.4 + 0.4 + 0.4$$

$$= 0.4.$$

Therefore $\det(A) \det(B) = 0.2 \neq 0.4 = \det(AB)$. Also, note that $\det(A) + \det(B) = 0.4$.

Now observe the following:

$$A + B = \begin{bmatrix} 0.7 & 0.1 & 0.9 \\ 0 & 0.4 & 1 \\ 0.2 & 0.3 & 0.5 \end{bmatrix} + \begin{bmatrix} 0.2 & 0.1 & 0 \\ 0.8 & 1 & 0.3 \\ 0.4 & 0.9 & 0.4 \end{bmatrix}$$

$$= \begin{bmatrix} \max(0.7,0.2) & \max(0.1,0.1) & \max(0.9,0) \\ \max(0,0.8) & \max(0.4,1) & \max(1,0.3) \\ \max(0.2,0.4) & \max(0.3,0.9) & \max(0.5,0.4) \end{bmatrix}$$

$$= \begin{bmatrix} 0.7 & 0.1 & 0.9 \\ 0.8 & 1 & 1 \\ 0.4 & 0.9 & 0.5 \end{bmatrix}$$

$$\begin{aligned} \det(A+B) &= 0.7 \begin{vmatrix} 1 & 1 \\ 0.9 & 0.5 \end{vmatrix} + 0.1 \begin{vmatrix} 0.8 & 0.1 \\ 0.4 & 0.5 \end{vmatrix} + 0.9 \begin{vmatrix} 0.8 & 1 \\ 0.4 & 0.9 \end{vmatrix} \\ &= 0.7 (\min(1,0.5) + \min(1,0.9)) + 0.1 (\min(0.8,0.5) + \min(1,0.4)) \\ &\quad + 0.9 (\min(0.8,0.9) + \min(1,0.4)) \\ &= 0.7 (0.5 + 0.9) + 0.1(0.5 + 0.4) + 0.9(0.8 + 0.4) \\ &= 0.7 (0.9) + 0.1 (0.5) + 0.9 (0.8) \\ &= 0.7 + 0.1 + 0.8 \\ &= 0.8. \end{aligned}$$

Therefore $\det(A) + \det(B) = 0.4 \neq 0.8 = \det(A+B)$. Thus

$$\det(A) + \det(B) \neq \det(A+B).$$

Proposition 2.7.5:

$$\text{Let } A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \text{ be an } n \times n \text{ fuzzy matrix. Then } \det(A) =$$

$$\det(A^T).$$

Proof:

$$\text{Let } A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}. \text{ It follows that } \det(A) = \max(\min(a_{11} a_{22}), \min(a_{12} a_{21})).$$

$$\text{Now note that } A^T = \begin{bmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{bmatrix}.$$

$$\text{Then } \det(A) = \max(\min(a_{11} a_{22}), \min(a_{12} a_{21})) = \det(A).$$

$$\text{Let } B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}. \text{ Then } B^T = \begin{bmatrix} b_{11} & b_{21} & b_{31} \\ b_{12} & b_{22} & b_{32} \\ b_{13} & b_{23} & b_{33} \end{bmatrix}.$$

Observe the following:

$$\det(A) = b_{11} \begin{vmatrix} b_{22} & b_{23} \\ b_{32} & b_{33} \end{vmatrix} + b_{21} \begin{vmatrix} b_{12} & b_{13} \\ b_{32} & b_{33} \end{vmatrix} + b_{31} \begin{vmatrix} b_{12} & b_{13} \\ b_{22} & b_{23} \end{vmatrix}$$

$$= b_{11} \begin{vmatrix} b_{22} & b_{32} \\ b_{23} & b_{33} \end{vmatrix} + b_{21} \begin{vmatrix} b_{12} & b_{32} \\ b_{13} & b_{33} \end{vmatrix} + b_{31} \begin{vmatrix} b_{12} & b_{22} \\ b_{13} & b_{23} \end{vmatrix}$$

$$= \begin{vmatrix} b_{11} & b_{21} & b_{31} \\ b_{12} & b_{22} & b_{32} \\ b_{13} & b_{23} & b_{33} \end{vmatrix}$$

$$= \det(B^T).$$

2.8 TRACES OF FUZZY MATRIX

Proposition: 2.8.1

Let A and B be two $n \times n$ fuzzy matrices, and let λ be a real number such that

$\lambda \in [0,1]$. Then we have the following:

$$(1) \text{Tr}(A) + \text{Tr}(B) = \text{Tr}(A + B),$$

$$(2) \text{Tr}(A) = \text{Tr}(A^T),$$

$$(3) \text{Tr}(\lambda A) = \lambda \text{Tr}(A).$$

Proof:

$$\text{Let } A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \text{ and } B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} \text{ be two fuzzy}$$

matrices.

(1) Note that $\text{Tr}(A) = a_{11} + a_{22} + \dots + a_{nn} = \max(a_{11}, a_{22}, \dots, a_{nn})$ and $\text{Tr}(B) = b_{11} + b_{22} + \dots + b_{nn} = \max(b_{11}, b_{22}, \dots, b_{nn})$.

Then we obtain:

$$\text{Tr}(A) + \text{Tr}(B) = \max(\max(a_{11}, a_{22}, \dots, a_{nn}), \max(b_{11}, b_{22}, \dots, b_{nn}))$$

$$= \max(a_{11}, a_{22}, \dots, a_{nn}, b_{11}, b_{22}, \dots, b_{nn}).$$

$$A+B = \begin{bmatrix} \max(a_{11}, b_{11}) & \max(a_{12}, b_{12}) & \dots & \max(a_{1n}, b_{1n}) \\ \max(a_{21}, b_{21}) & \max(a_{22}, b_{22}) & \dots & \max(a_{2n}, b_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ \max(a_{n1}, b_{n1}) & \max(a_{n2}, b_{n2}) & \dots & \max(a_{nn}, b_{nn}) \end{bmatrix}$$

It follows that

$$\text{Tr}(A+B) = \max(\max(a_{11}, b_{11}), \max(a_{22}, b_{22}), \dots, \max(a_{nn}, b_{nn}))$$

$$= \max(a_{11}, b_{11}, a_{22}, b_{22}, \dots, a_{nn}, b_{nn})$$

$$= \max(a_{11}, a_{22}, \dots, a_{nn}, b_{11}, b_{22}, \dots, b_{nn}).$$

$$\text{Therefore } \text{Tr}(A) + \text{Tr}(B) = \text{Tr}(A+B).$$

$$(2) \text{ Note that } A^T = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

$$\text{Thus } \text{Tr}(A^T) = \max(a_{11}, a_{22}, \dots, a_{nn}) = \text{Tr}(A).$$

(2) Let A be an $n \times n$ fuzzy matrix, and let λ be a real number in the interval $[0, 1]$.

Then $\lambda A = \{\min(\lambda, a_{ij}) : 1 \leq i \leq n, 1 \leq j \leq n\}$. It follows that,

$$\text{Tr}(\lambda A) = \max\{\min(\lambda, a_{ii})\}.$$

Note that $\text{Tr}(A) = \max\{a_{ii}\}$. Then $\lambda \text{Tr}(A) = \min\{\lambda, \max\{a_{ii}\}\}$. Then by Lemma 2.5,

$$\text{Tr}(\lambda A) = \lambda \text{Tr}(A).$$

CHAPTER 3

CHAPTER 3

FUZZY RELATION AND COMPOSITION

Definition: 3.1

Fuzzy relation has degree of membership whose value is $[0, 1]$

$$\mu_R: A \times B \rightarrow [0, 1]$$

$$R = \{[(x, y), \mu_R(x, y)] \mid \mu_R(x, y) \geq 0, x \in A, y \in B\}$$

Here,

$\mu_R(x, y)$ is interpreted as strength of relation between x and y .

Fuzzy binary relation can be extended to n -ary relation. If we assume X_1, X_2, \dots, X_n to be fuzzy sets, fuzzy relation $R \subseteq X_1 \times X_2 \times \dots \times X_n$ can be said to be a fuzzy set of tuple elements (x_1, x_2, \dots, x_n) where $x_1 \in X_1, x_2 \in X_2, \dots, x_n \in X_n$

Example: 3.1.1

For instance, Crisp relation R in the following figure (a) reflects a relation in $A \times A$. Expressing this by membership function $\mu_R(a, c) = 1, \mu_R(b, a) = 1, \mu_R(c, b) = 1$ and $\mu_R(c, d) = 1$

If this relation is given as the value between 0 and 1 as in figure (b), this relation becomes a fuzzy relation.

Expressing this fuzzy relation by membership function yields,

$$\mu_R(a, c) = 0.8 \quad \mu_R(b, a) = 1.0 \quad \mu_R(c, b) = 0.9 \quad \mu_R(c, d) = 1.0$$

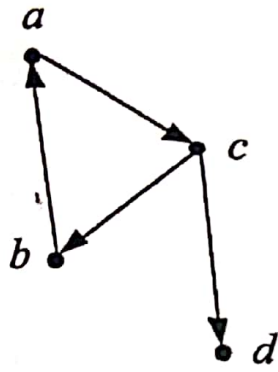


Figure 3.1

(a) Crisp relation

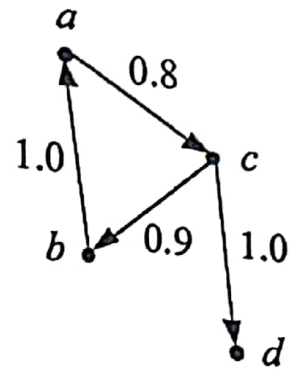


Figure 3.2

(b) Fuzzy relation

Its Corresponding matrix is as follows:

A	a	b	c	d
a	0.0	0.0	0.8	0.0
b	1.0	0.0	0.0	0.0
c	0.0	0.0	0.0	0.0
d	0.0	0.0	0.0	0.0

3.1.2 DOMAIN AND RANGE OF FUZZY RELATION

When a fuzzy relation R is defined in crisp sets A and B , the domain range of this relation are defined as:

$$\mu_{\text{dom}(R)}(x) = \max \mu_R(x, y)$$

$$\mu_{\text{dom}(R)}(y) = \max \mu_R(x, y)$$

COMPARISON OF RELATIONS

Property Relation	Reflexive	Anti Reflexive	Symmetric	Anti Symmetric	Transitive
Equivalence	✓		✓		✓
Compatibility	✓		✓		
Pre-Order	✓				✓
Order	✓			✓	✓
Strict order		✓		✓	✓

Table 3.1

3.2 FUZZY MATRIX

Given a certain vector, if an element of this vector has its value between 0 and 1, we call this vector a fuzzy vector. Fuzzy matrix is a gathering of such vectors. Given a fuzzy matrix $A=(a_{ij})$ and $B=(b_{ij})$, we can perform operation on these fuzzy matrices.

(1) SUM

$$A + B = \text{Max} [a_{ij}, b_{ij}]$$

(2) MAX PRODUCT

$$A.B = AB = \text{Max}_k [\text{Min} (a_{ik}, b_{kj})]$$

(3) SCALAR PRODUCT

λA where $0 \leq \lambda \leq 1$

Example: 3.2.1

The following are examples of sum and max product on fuzzy sets A and B.

	a	b	c
a	0.2	0.5	0.0
b	0.4	1.0	0.1
c	0.0	1.0	0.0

A =

	a	b	c
a	1.0	0.1	0.0
b	0.0	0.0	0.5
c	0.0	1.0	0.1

B =

	a	b	c
a	1.0	0.5	0.0
b	0.4	1.0	0.5
c	0.0	1.0	0.1

A + B =

	a	b	c
a	0.2	0.1	0.5
b	0.4	0.1	0.5
c	0.0	0.0	0.5

A.B =

Here let's have a closer look at the product $A \cdot B$ of A and B . For instance, in the first row and second column of the matrix $C=A \cdot B$, the value 0.1 ($c_{12}=0.1$) is calculated by applying the Max-Min operation to the values of the first row (0.2, 0.5 and 0.0)

$$\begin{array}{ccc}
 0.2 & 0.5 & 0.0 \\
 0.1 & 0.0 & 1.0 \\
 \text{Min} \Downarrow & \hline
 0.1 & 0.0 & 0.0 \Rightarrow \text{Max}
 \end{array}$$

In the same number $c_{13}=0.5$ is obtained by applying the same procedure of Calculation to the first row (0.2, 0.5, 0.0) of A and the third column of $B(0.0, 0.5, 0.1)$

$$\begin{array}{ccc}
 0.2 & 0.5 & 0.0 \\
 0.0 & 0.5 & 0.1 \\
 \hline
 0.0 & 0.5 & 0.0
 \end{array}$$

And for all i and j , if $a_{ij} \leq b_{ij}$ holds, matrix B is bigger than A .

$$a_{ij} \leq b_{ij} \Leftrightarrow A \leq B$$

Also when $A \leq B$ for arbitrary fuzzy matrices S and T , the following relation holds from the Max-product operation

$$A \leq B \Leftrightarrow SA \leq SB, AT \leq BT$$

Definition: 3.2.2

If a fuzzy relation R is given in the form of fuzzy matrix, its element represents the membership values of this relation.

That is, if the matrix is denoted by $\mu_R(i,j)$, then $M(R) = (\mu_R(i,j))$

3.3 OPERATION OF FUZZY RELATION

We know now a relation is one kind of sets. Therefore we can apply operations for fuzzy set to the relation. We assume $R \subseteq A \times B$ and $S \subseteq A \times B$.

(1) Union Relation

Union of two relations R and S is defined as follows:

$$\forall (x, y) \in A \times B$$

$$\mu_{R \cup S}(x, y) = \text{Max} [\mu_R(x, y), \mu_S(x, y)]$$

$$= \mu_R(x, y) \vee \mu_S(x, y)$$

We generally use the sign \vee for Max operation. For n relations, we extend it to the following.

$$\mu_{R_1 \cup R_2 \cup R_3 \cup \dots \cup R_n}(x, y) = \bigvee_{R_i} \mu_{R_i}(x, y)$$

If expressing the fuzzy relation by fuzzy matrices, i.e., M_R and M_S , matrix $M_{R \cup S}$ concerning the union is obtained from the sum of two matrices $M_R + M_S$

$$M_{R \cup S} = M_R + M_S$$

(2) Intersection relation

The intersection relation $R \cap S$ of set A and B is defined by the following membership function.

$$\begin{aligned}\mu_{R \cap S}(X) &= \text{Min}[\mu_R(X, Y), \mu_S(x, y)] \\ &= \mu_R(x, y) \wedge \mu_S(x, y)\end{aligned}$$

The symbol \wedge is for the Min operation. In the same manner, the intersection relation for n relations is defined by

$$\mu_{R_1 \cap R_2 \cap R_3 \cap \dots \cap R_n}(x, y) = \bigwedge_{R_i} \mu_{R_i}(x, y)$$

(3) Complement Relation

Complement relation \bar{R} for fuzzy relation R shall be defined by the following number ship function

$$\forall (x, y) \in A \times B \quad \mu_{\bar{R}}(x, y) = 1 - \mu_R(x, y)$$

Example: 3.3.1

Two fuzzy relation matrices M_R and M_S are given

M_R	a	b	c
1	0.3	0.2	1.0
2	0.8	1.0	1.0
3	0.0	1.0	0.0

M_S	a	b	c
1	0.3	0.0	0.1
2	0.1	0.8	1.0
3	0.6	0.9	0.3

Fuzzy relation matrices $M_{R \cup S}$ and $M_{R \cap S}$ corresponding $R \cup S$ and $R \cap S$ yield the followings

$M_{R \cup S}$	a	b	c
1	0.3	0.2	1.0
2	0.8	1.0	1.0
3	0.6	1.0	0.3

$M_{R \cap S}$	a	b	c
1	0.3	0.0	0.1
2	0.1	0.8	1.0
3	0.6	0.9	0.3

Also complement relation of fuzzy relation R shall be

$M_{\bar{R}}$	a	b	c
1	0.7	0.8	0.0
2	0.2	0.0	0.0
3	1.0	0.0	1.0

Inverse Relation

When a fuzzy relation $R \subseteq A \times B$ is given, the inverse relation of R^{-1} is defined by the following membership function.

For $a_k(x, y) \subseteq A \times B$

$$\mu_{R^{-1}}(y, x) = \mu_R(x, y)$$

3.4 COMPOSITION OF FUZZY RELATION

Definition: 3.4.1

Two fuzzy relation R and S are defined on sets A, B and C. That is,

$$R \subseteq A \times B, S \subseteq B \times C.$$

The composition $S.R=SR$ of two relations R and S is expressed by the relation from A to C , and this composition is defined by the following.

For $(x,y) \in A \times B$, $(y,z) \in B \times C$

$$\mu_{S.R}(x,z)=\text{Max}_y [\text{Min}[\mu_R(x,y),\mu_S(y,z)]]$$

$$=\bigvee_y \mu_R(x,y) \wedge \mu_S(y,z)$$

$S.R$ from this elaboration is a subset of $A \times C$. That is $S.R \subseteq A \times C$.

If the relations R and S are represented by matrices and M_S , the matrix corresponding to $S.R$ is obtained from the product of M_R and M_S

$$M_{S.R}=M_R \cdot M_S$$

Example: 3.4.2

Consider fuzzy relations $R \subseteq A \times B, S \subseteq B \times C$. The sets A, B and C shall be the sets of events. By the relation R , we can see the possibility of occurrence of B after A , and by S that of C after B . For example, by M_R , the possibility of occurrence of $a \in B$ after $1 \in A$ is 0.1. By M_S , the possibility of occurrence of α after a is 0.9

R	a	b	c	d
1	0.1	0.2	0.0	1.0
2	0.3	0.3	0.0	0.2
3	0.8	0.9	1.0	0.4

S	α	β	γ
a	0.9	0.0	0.3
b	0.2	1.0	0.8
c	0.8	0.0	0.7
d	0.4	0.2	0.3

Here, we cannot guess the possibility of C when A is occurred. So our main job now will be the obtaining the composition $S.R \subseteq A \times C$. The following matrix $M_{S.R}$ represents this composition and it is also given in following figure.

Now we see the possibility of occurrence of $\alpha \in C$ after event $1 \in A$ is 0.4, and that for $\beta \in C$ after event $2 \in A$ is 0.3 etc...

Presuming that there relations R and S are the expressions of rules that guide the occurrence of event or fact. Then the possibility of occurrence of event B when event A is happened is guided by the rule R and rule R indicates the possibility of C when B is existing. For further cases, the possibility of when A has occurred can be induced from the composition rule S.R. This manner is named as an "Influence" which is a process producing new information.

S.R	α	β	γ
1	0.4	0.2	0.3
2	0.3	0.3	0.3
3	0.8	0.9	0.8

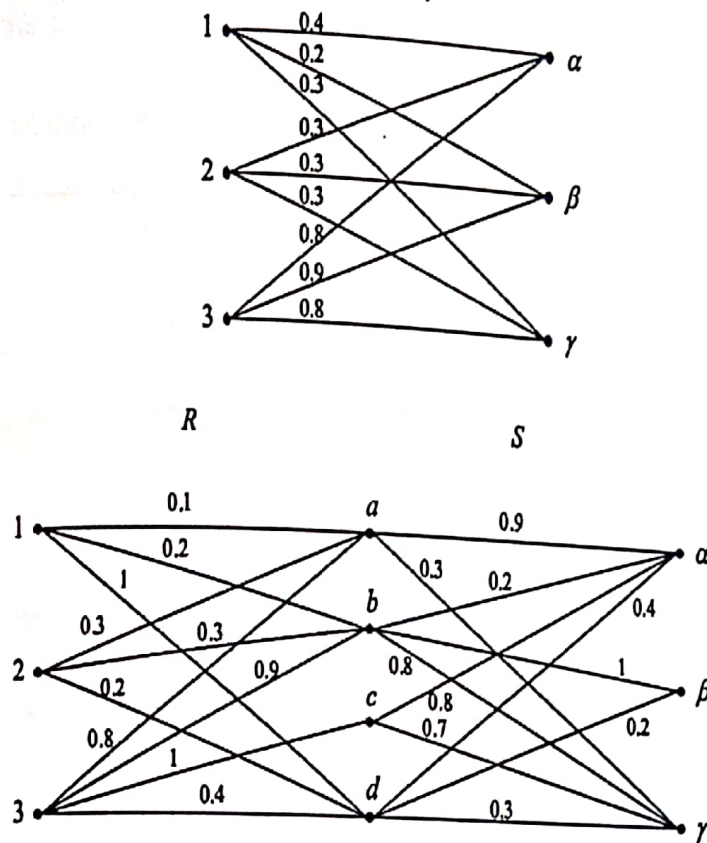


Figure: 3.3 Composition of fuzzy relation

3.5 α -CUT OF FUZZY RELATION

We have learned about α -cut for fuzzy sets, and we know a fuzzy relation is one kind of fuzzy sets. Therefore, we can apply the α -cut to the fuzzy relation.

Definition: 3.5.1

We can obtain α -cut relation from a fuzzy relation by taking the pairs which have membership degrees no less than α . Assume $R \subseteq A \times B$ and R_α is a α -cut relation. Then

$$R_\alpha = \{(x, y) | \mu_R(x, y) \geq \alpha, x \in A, y \in B\}$$

Note that R_α is a crisp relation.

Example: 3.5.2

For example, we have a fuzzy relation R

$$M_{R0.4} =$$

	0.9	0.4	0.0
0.2	0.2	1.0	0.4
0.0	0.0	0.7	1.0
0.4	0.4	0.2	0.0

Now the level set with degrees of membership function is,

$$A = \{0, 0.2, 0.4, 0.7, 0.9, 1.0\}$$

then we can have some α -cut relations in the following

$$M_{R0.4} =$$

	1	1	0
0	0	1	1
0	0	1	1
1	1	0	0

$$M_{R0.7} =$$

	1	0	0
0	0	1	0
0	0	1	1
0	0	0	0

$M_{R0.9} =$

1	0	0
0	1	0
0	0	1
0	0	0

$M_{R1.0} =$

0	0	0
0	1	0
0	0	1
0	0	0

CHAPTER 4



CHAPTER 4

FUZZY GRAPHS AND RELATIONS

Definition: 4.1

Let $\tilde{G} = (\tilde{V}, \tilde{E})$

\tilde{E} : fuzzy set of edges between vertices

The graph represents fuzzy relation of fuzzy nodes, and can be defined as follows

$$\tilde{G} = (\tilde{V}, \tilde{E})$$

We replace $\tilde{G} = (\tilde{V}, \tilde{E})$ with $G = (V, E)$ for convenience. This is called fuzzy graphs.

Example: 4.2

M_G	b_1	b_2
a_1	0.8	0.2
a_2	0.3	0.0
a_3	0.7	0.4

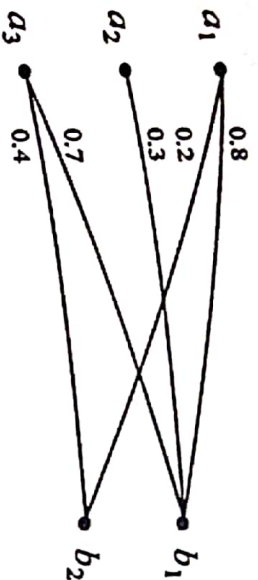


Figure 4.1 Fuzzy Graph

Definition: 4.3

A fuzzy graph structure $G = (\sigma_1, \mu_1, \mu_2, \dots, \mu_n)$ is μ_i -strong if

$$\mu_i(v_1, v_2) = \sigma(v_1) \wedge \sigma(v_2), \text{ for all } v_1, v_2 \in R_i, i \in \{1, 2, 3, \dots, n\}$$

If G is μ_i -strong $\forall i \in \{1, 2, 3, \dots, n\}$, then G is called fuzzy - graph structure.

Theorem: 4.4

Maximal product of two strong fuzzy - graph structure is also a strong fuzzy - graph structure.

Proof:

Let $G_1 = (\sigma_1, \mu_1', \mu_2', \dots, \mu_n')$ and $G_2 = (\sigma_2, \mu_1'', \mu_2'', \dots, \mu_n'')$ be two strong fuzzy graph structures.

Then $\mu_i'(v_1, v_2) = \sigma_1(v_1) \wedge \sigma_1(v_2)$ for any $v_1, v_2 \in R_i'$ and $\mu_i''(u_1, u_2) = \sigma_2(u_1) \wedge \sigma_2(u_2)$ for any $u_1, u_2 \in R_i''$, $i = 1, 2, 3, \dots, n$. Then proceeding according to the definition of maximal product.

Case I:

$u_1 = u_2$ and $v_1, v_2 \in R_i''$, Then,

$$\begin{aligned}\mu_i((u_1, v_1)(u_2, v_2)) &= \sigma_1(u_1) \vee \mu_i''(v_1, v_2) \\ &= \sigma_1(u_1) \vee [\sigma_2(v_1) \wedge \sigma_2(v_2)] \\ &= [\sigma_1(u_1) \vee \sigma_2(v_1)] \wedge [\sigma_1(u_1) \vee \sigma_2(v_2)] \\ &= [\sigma(u_1, v_1) \wedge \sigma(u_2, v_2)]\end{aligned}$$

Case 2:

$v_1 = v_2$ and $u_1, u_2 \in R_i$, Then,

$$\begin{aligned}\mu_i((u_1, v_1)(u_2, v_2)) &= \sigma_2(v_1) \vee \mu_i'(u_1, u_2) \\ &= \sigma_2(v_1) \vee [\sigma_1(u_1) \wedge \sigma_1(u_2)] \\ &= [\sigma_1(u_1) \vee \sigma_2(v_1)] \wedge [\sigma_1(u_2) \vee \sigma_2(v_1)] \\ &= [\sigma(u_1, v_1) \wedge \sigma(u_2, v_2)]\end{aligned}$$

Thus $\mu_i((u_1, v_1)(u_2, v_2)) = \sigma(u_1, v_1) \wedge \sigma(u_2, v_2)$ for all edges of maximal product.

Hence $G = G_1 * G_2 = (\sigma, \mu_1, \mu_2, \dots, \mu_n)$ is a strong fuzzy graph structure.

Remark: 4.4.1

Converse of the above theorem may not be true. That is, maximal product $G =$

$G_1 * G_2$ may be a Strong Fuzzy – graph structure, when G_1 and G_2 are not strong fuzzy

– graph structures.

Definition: 4.5

A fuzzy set A defined on X and any number $\alpha \in [0,1]$, the set α -cut α_A is the crisp set that contains all the elements of the universal set x whose membership grades in A are greater than or equal to the specified value of α

$$\alpha_A = \{ x \mid A(x) \geq \alpha \}$$

Example: 4.5.1

For $A = \{a, b, c\}$, $R \subseteq A \times A$ is defined as follows

	a	b	c
a	1.0	0.8	0.4
b	0.0	0.4	0.0
c	0.8	1.0	0.0

For level set $\{0, 0.4, 0.8, 1\}$, if we apply the α -cut operation, we also get crisp relations and corresponding graphs in the figure.

If we denote the graph from α -cut as G_α , the following relation between α and G_α holds.

$$\alpha_1 \geq \alpha_2 \Rightarrow R_{\alpha_1} \subseteq R_{\alpha_2}$$

$$G_{\alpha_1} \subseteq G_{\alpha_2}$$

$M_R =$

	a	b	c
a	1.0	0.8	0.4
b	0.0	0.4	0.0
c	0.8	1.0	0.0

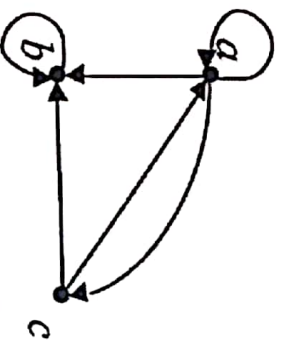


Figure 4.2

$M_{R0.4} =$

	a	b	c
a	1.0	1.0	1.0
b	0.0	1.0	0.0
c	1.0	1.0	0.0

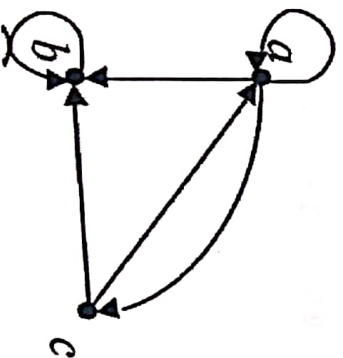


Figure 4.3

$$M_{R0,8} =$$

	a	b	c
a	1.0	1.0	0.0
b	0.0	0.0	0.0
c	1.0	1.0	0.0

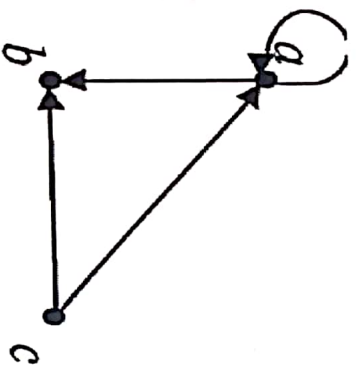


Figure 4.4

$$M_{R1,0} =$$

	a	b	c
a	1.0	0.0	0.0
b	0.0	0.0	0.0
c	0.0	1.0	0.0

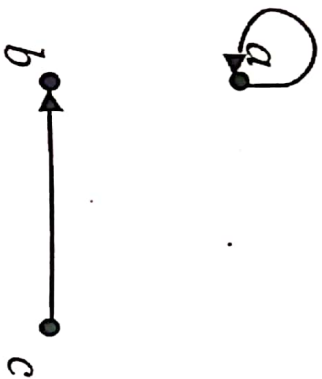


Figure 4.5

a cut of fuzzy graph

4.6 FUZZY EQUIVALENCE RELATION

Definition: 4.6.1

If a fuzzy relation R on $A \times A$ satisfies the following conditions, we call it a "fuzzy equivalence relation" or "similarity relation".

1. REFLEXIVE RELATION

$$\forall x \in A \Rightarrow \mu_R(x, x) = 1$$

2. SYMMETRIC RELATION

$$\forall (x, y) \in A \times A, \mu_R(x, y) = \mu \Rightarrow \mu_R(y, x) = \mu$$

3. TRANSITIVE RELATION

$$\forall (x, y), (y, z), (x, z) \in A \times A$$

$$\mu_R(x, z) \geq \text{Max} [\text{Min} [\mu_R(x, y), \mu_R(y, z)]]$$

Example: 4.6.2

Let's consider a fuzzy relation expressed in the following matrix. Since this relation is reflexive, symmetric and transitive, we see that it is a fuzzy equivalence relation.

	a	b	c	d
a	1.0	0.8	0.7	1.0
b	0.8	1.0	0.7	0.8
c	0.7	0.7	1.0	0.7
d	1.0	0.8	0.7	1.0

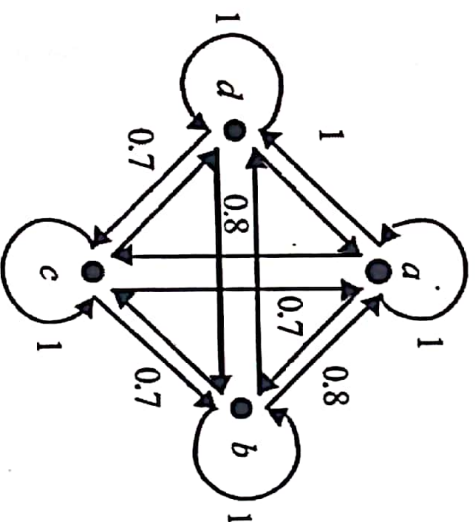


Figure 4.6

GRAPH OF FUZZY EQUIVALENCE RELATION

4.7 FUZZY COMPATIBILITY RELATION

Definition: 4.7.1

If fuzzy relation R in $\mathcal{S} A$ satisfies the following conditions, we call it "fuzzy compatibility relation" or "resemblance relation".

1. REFLEXIVE RELATION

$$\forall x \in A \Rightarrow \mu_R(x, x) = 1$$

2. SYMMETRIC RELATION

$$\forall (x, y) \in A \times A$$

$$\mu_R(x, y) = \mu \Rightarrow \mu_R(y, x) = \mu$$

Example: 4.7.2

In the figure $\alpha = 0.7$ cut we get compatibility class $\{a, b\}$, $\{c, d, e\}$, $\{d, e, f\}$ and these compatibility classes cover the set A . Note that elements d and e are far from partition since these appear in dual subsets.

	a	b	c	d	e	f
a	1.0	0.8	0.0	0.0	0.0	0.0
b	0.8	1.0	0.0	0.0	0.0	0.0
c	0.0	0.0	1.0	1.0	0.8	0.0
d	0.0	0.0	1.0	1.0	0.8	0.7
e	0.0	0.0	0.8	0.8	1.0	0.7
f	0.0	0.0	0.0	0.7	0.7	1.0

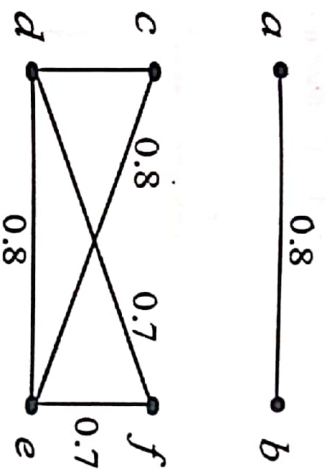


Figure 4.7

4.8 FUZZY PRE-ORDER RELATION

Definition: 4.8.1

Given fuzzy relation R in set A , if the followings are well kept for all $x, y, z \in A$, this relation is called Pre-Order relation.

1. REFLEXIVE RELATION

$$\forall x \in A \Rightarrow \mu_R(x, x) = 1$$

2. TRANSITIVE RELATION

$$\forall (x, y), (y, z), (x, z) \in A \times A$$

$$\mu_R(x, z) \geq \text{Max} [\text{Min} (\mu_R(x, y), \mu_R(y, z))]$$

Also if certain relation is transitive but not reflexive, this relation is called "Semi Pre-Order" or "non reflexive fuzzy pre-order".

Example: 4.8.2

Here goes a Semi Pre-Order relation

	a	b	c
a	0.2	1.0	0.4
b	0.0	0.6	0.3
c	0.0	1.0	0.3

If the membership function follows the relation $\mu_R(x,x) = 0$ for all x , we use the term "anti-reflexive fuzzy pre-order".

4.9 FUZZY ORDER RELATION

Definition: 4.9.1

If relation R satisfies the followings for all $x,y,z \in A$, it is called fuzzy order relation.

1. REFLEXIVE RELATION:

$$\forall x \in A \Rightarrow \mu_R(x,x) = 1$$

2. ANTI SYMMETRIC RELATION

$$\forall (x,y) \in A \times A$$

$$\mu_R(x,y) \neq \mu_R(y,x) \text{ or } \mu_R(x,y) = \mu_R(y,x) = 0$$

3. TRANSITIVE RELATION

$$\forall (x,y), (y,z), (x,z) \forall \in A \times A$$

$$\mu_R(x,z) \geq \text{Max}[\text{Min}(\mu_R(x,y), \mu_R(y,z))]$$

Example: 4.9.2

The figure shows a fuzzy order relation

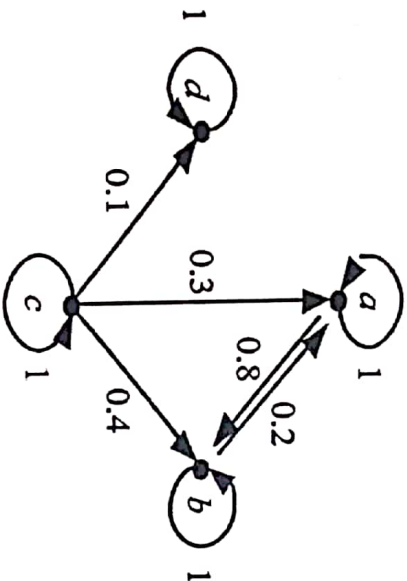


Figure 4.8

- (i) If $\mu_R(x, y) \geq \mu_R(y, x)$ then $\mu_{R1}(x, y) = 1$ $\mu_R(y, x) = 0$
- (ii) If $\mu_R(x, y) = \mu_R(y, x)$ then $\mu_{R1}(x, y) = \mu_R(y, x) = 0$

CHAPTER 5



CHAPTER 5

AN APPLICATION OF FUZZY GRAPH IN TRAFFIC CONGESTION

Definition: 5.1

Let $G: (\sigma, \mu)$ be a fuzzy graph. The strength of connectedness between two nodes x and y is defined as the maximum of the strengths of all paths between x and y and is denoted by $\text{CONN}_G(x, y)$.

x - y path P is called a strongest x - y path if its strength equals $\text{CONN}_G(x, y)$.

A fuzzy graph $G: (\sigma, \mu)$ is connected if for every x, y in σ^* , $\text{CONN}_G(x, y) > 0$.

Example: 5.2

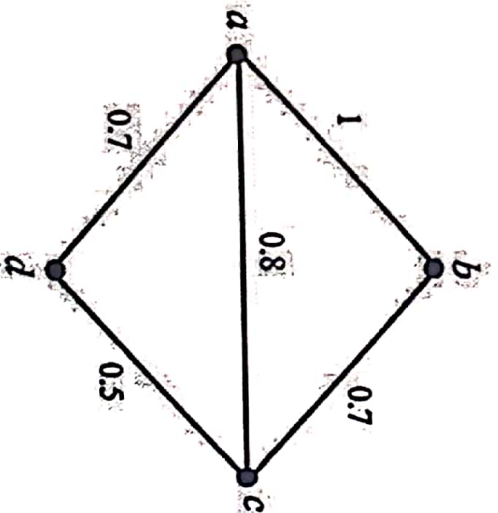


Figure 5.1. Strength of connectedness

Let $G: (\sigma, \mu)$ be a fuzzy graph with $\sigma^* = \{a, b, c, d\}$.

In this fuzzy graph, $\mu(a, b) = 1$, $\mu(b, c) = 0.7$, $\mu(d, a) = 0.7$, $\mu(a, c) = 0.8$,

$\mu(c, d) = 0.5$.

There are three different paths from a and c namely,

$$P_1 = a-b-c \quad P_2 = a-d-c \quad P_3 = \text{arc}(a,c)$$

Now,

$$\text{Strength of } P_1 = \min\{1, 0.7\} = 0.7$$

$$\text{Strength of } P_2 = \min\{0.7, 0.5\} = 0.5$$

$$\text{Strength of } P_3 = 0.8$$

Therefore, the strongest path joining a to c is the arc(a,c) with strength

$$0.8$$

Hence,

$$\text{CONN}_G(a,c) = 0.8$$

Similarly,

$$\text{CONN}_G(a,b) = 1$$

$$\text{CONN}_G(b,c) = 0.8$$

$$\text{CONN}_G(a,c) = 0.8$$

$$\text{CONN}_G(d,a) = 0.7$$

$$\text{CONN}_G(c,d) = 0.7$$

Definition: 5.3

An arc (x,y) in G is called α -strong, if $\mu(x,y) > \text{CONN}_{G-(x,y)}(x,y)$.

An arc (x,y) in G is called β -strong, if $\mu(x,y) = \text{CONN}_{G-(x,y)}(x,y)$.

An arc (x,y) in G is called δ -strong, if $\mu(x,y) < \text{CONN}_{G-(x,y)}(x,y)$.

A δ -arc (x,y) is called δ^* -arc, if $\mu(x,y) > \mu(u,v)$ where (u,v) is the weakest arc of G .

Example: 5.4

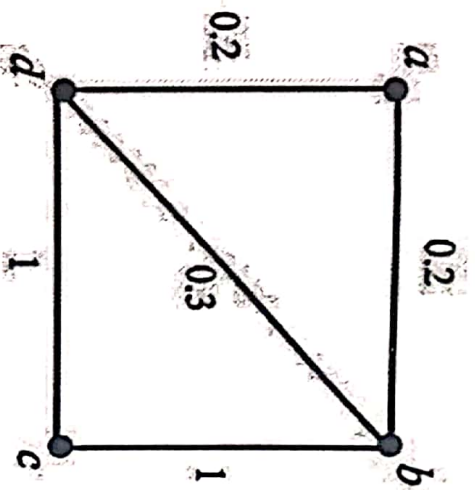


Figure 5.2. Strong arc in fuzzy graph

Let $G: (\sigma, \mu)$ be with $\sigma^* = \{a,b,c,d\}$, $\mu(a,b) = 0.2$, $\mu(b,c) = 1$, $\mu(c,d) = 1$, $\mu(d,a) = 0.2$, $\mu(b,d) = 0.3$.

$$\mu(a,b) = 0.2, \text{CONN}_G(a,b) = 0.2, \text{CONN}_G(a,b)(a,b) = 0.2$$

$$\mu(b,c) = 1, \text{CONN}_G(b,c) = 1, \text{CONN}_G(b,c)(b,c) = 0.3$$

$$\mu(c,d) = 1, \text{CONN}_G(c,d) = 1, \text{CONN}_G(c,d)(c,d) = 0.3$$

$$\mu(d,a) = 0.2, \text{CONN}_G(d,a) = 0.2, \text{CONN}_G(d,a)(d,a) = 0.2$$

$$\mu(b,d) = 0.3, \text{CONN}_G(b,d) = 1, \text{CONN}_G(b,d)(b,d) = 1$$

Therefore, (b,c) and (c,d) are α -strong arcs. (a,b) and (d,a) are β -strong arcs. (b,d) is a δ -arc.

Also, (b,d) is a δ^* -arc, since $\mu(b,d) > \mu(a,b)$, where (a,b) is a weakest arc of G .

5.5 A GRAPHICAL MODEL OF TRAFFIC PROBLEM AT THE CROSS ROADS

Consider a complete fuzzy graph that consists of 9 vertices and 27 edges respectively. We have seen 9 directional flows which are labeled by,

$$\sigma(V_1), \sigma(V_2), \sigma(V_3), \sigma(V_4), \sigma(V_5), \sigma(V_6), \sigma(V_7), \sigma(V_8), \sigma(V_9)$$

The following figure shows the direction of traffic flows,

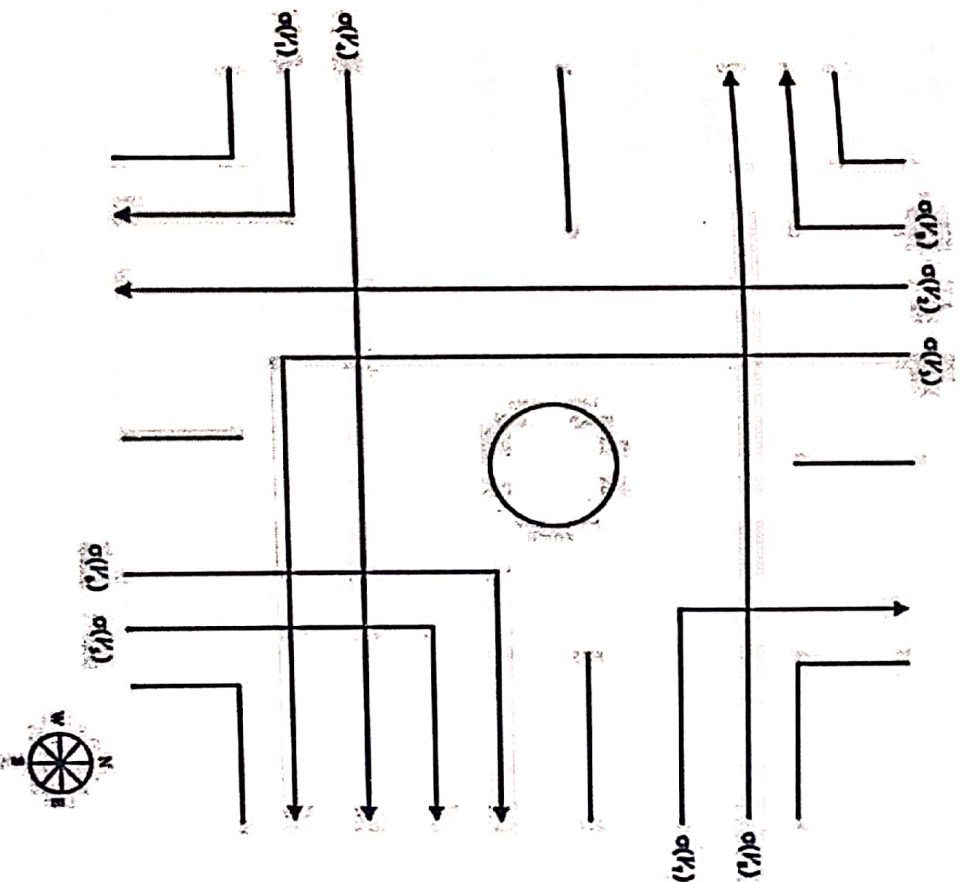


Figure 5.3.

The main street of Keene city road and the direction of movements

The fuzzy graph problem has represented below is a traffic flows which is considering in the figure 5.3. Each arrow shows the path of vehicles take from one direction to another.

The flows are compatible which can be seen in the following:

1. $\sigma(V_1)$ movement is compatible with the flows
 $\sigma(V_2), \sigma(V_3), \sigma(V_4), \sigma(V_5), \sigma(V_6), \sigma(V_7), \sigma(V_8), \sigma(V_9)$
2. $\sigma(V_2)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_3), \sigma(V_5), \sigma(V_6), \sigma(V_7), \sigma(V_9)$
3. $\sigma(V_3)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_2), \sigma(V_7), \sigma(V_9)$
4. $\sigma(V_4)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_7), \sigma(V_8), \sigma(V_9)$
5. $\sigma(V_5)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_2), \sigma(V_6), \sigma(V_7), \sigma(V_8), \sigma(V_9)$
6. $\sigma(V_6)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_2), \sigma(V_5), \sigma(V_7), \sigma(V_8), \sigma(V_9)$
7. $\sigma(V_7)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_2), \sigma(V_3), \sigma(V_4), \sigma(V_5), \sigma(V_6), \sigma(V_9)$
8. $\sigma(V_8)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_4), \sigma(V_5), \sigma(V_6), \sigma(V_9)$
9. $\sigma(V_9)$ movement is compatible with the flows
 $\sigma(V_1), \sigma(V_2), \sigma(V_3), \sigma(V_4), \sigma(V_5), \sigma(V_6), \sigma(V_7), \sigma(V_8)$

	V ₁	V ₂	V ₃	V ₄	V ₅	V ₆	V ₇	V ₈	V ₉
-	(0.22)	(0.05)	(0.21)	(0.35)	(0.28)	(0.41)	(0.39)	(0.02)	(0.24)
V ₁	-	0.22	0.27	0.40	0.28	0.31	0.41	0.29	0.28
(0.22)									
V ₂	0.22	-	0.27	-	0.14	0.47	0.39	-	0.19
(0.05)									
V ₃	0.27	0.27	-	-	-	-	0.39	-	0.41
(0.21)									
V ₄	0.40	-	-	-	-	-	0.46	0.35	0.41
(0.35)									
V ₅	0.28	0.14	-	-	-	0.04	0.39	0.29	0.33
(0.28)									
V ₆	0.31	0.47	-	-	0.04	-	0.44	0.41	0.42
(0.41)									
V ₇	0.41	0.39	0.39	0.46	0.39	0.44	-	-	0.48
(0.39)									

V_8 (0.02)	0.29	—	—	0.35	0.29	0.41	—	—	0.41
V_9 (0.24)	0.28	0.19	0.41	0.41	0.33	0.42	0.48	0.41	—

Table 5.1. Volume data

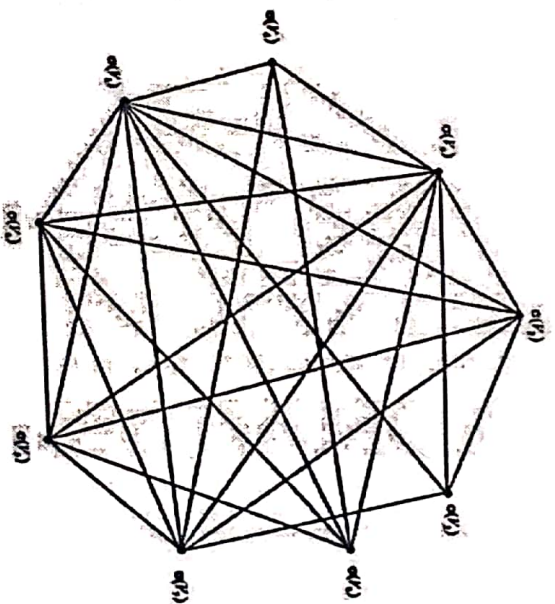


Figure 5.4. Complete graph

S.No	Origin to Destination	Weight of the edge of the path	Strength of the vertex of the path	Strong arc
1.	$\sigma(V_1) - \sigma(V_2)$	0.22	0.22	β -strong
	$\sigma(V_1) - \sigma(V_3)$	0.27	0.22	α -strong
	$\sigma(V_1) - \sigma(V_4)$	0.40	0.35	α -strong
	$\sigma(V_1) - \sigma(V_5)$	0.28	0.28	β -strong
	$\sigma(V_1) - \sigma(V_6)$	0.31	0.41	δ -strong
	$\sigma(V_1) - \sigma(V_7)$	0.41	0.39	α -strong
2.	$\sigma(V_1) - \sigma(V_8)$	0.29	0.22	α -strong
	$\sigma(V_1) - \sigma(V_9)$	0.28	0.24	α -strong
	$\sigma(V_2) - \sigma(V_3)$	0.27	0.22	α -strong
	$\sigma(V_2) - \sigma(V_5)$	0.14	0.28	δ -strong
	$\sigma(V_2) - \sigma(V_6)$	0.47	0.41	α -strong
	$\sigma(V_2) - \sigma(V_7)$	0.39	0.39	β -strong
3.	$\sigma(V_2) - \sigma(V_9)$	0.19	0.11	α -strong
	$\sigma(V_3) - \sigma(V_7)$	0.39	0.39	β -strong
	$\sigma(V_3) - \sigma(V_9)$	0.41	0.21	α -strong

4.	$\sigma(V_4) - \sigma(V_7)$	0.46	0.39	α -strong
	$\sigma(V_4) - \sigma(V_8)$	0.35	0.35	β -strong
	$\sigma(V_4) - \sigma(V_9)$	0.41	0.35	α -strong
5.	$\sigma(V_5) - \sigma(V_6)$	0.04	0.41	α -strong
	$\sigma(V_5) - \sigma(V_7)$	0.39	0.39	β -strong
	$\sigma(V_5) - \sigma(V_8)$	0.29	0.28	α -strong
	$\sigma(V_5) - \sigma(V_9)$	0.33	0.28	α -strong
6.	$\sigma(V_6) - \sigma(V_7)$	0.44	0.41	α -strong
	$\sigma(V_6) - \sigma(V_8)$	0.41	0.41	β -strong
	$\sigma(V_6) - \sigma(V_9)$	0.42	0.41	α -strong
7.	$\sigma(V_7) - \sigma(V_9)$	0.48	0.39	α -strong
8.	$\sigma(V_8) - \sigma(V_9)$	0.41	0.24	α -strong

Table 5.2

An observation of the crossroads forms are assumptions, as follows.

- The flows does not follow the light when turning to the left $\sigma(V_1)$, indicating that the flow can increase at any time under the waiting time of 0 (zero).
- The flow of the main street turning left from north $\sigma(V_2)$ is not directly related to the intersection of the left-turn lane before the intersection.

- For other flows, move the current to the left $\sigma(V_4)$, $\sigma(V_5)$, $\sigma(V_6)$ to follow the light.
- There is just one flow turn left $\sigma(V_3)$.
The number of vehicles are passing through each crossroad on the Krif road (in percentage)

Arc	α -strong	
	$\sigma(V_1) - \sigma(V_3)$	$\text{CONN}(V_1, V_3) = 0.22$
	$\sigma(V_1) - \sigma(V_4)$	$\text{CONN}(V_1, V_4) = 0.35$
	$\sigma(V_1) - \sigma(V_7)$	$\text{CONN}(V_1, V_7) = 0.39$
	$\sigma(V_1) - \sigma(V_8)$	$\text{CONN}(V_1, V_8) = 0.22$
	$\sigma(V_1) - \sigma(V_9)$	$\text{CONN}(V_1, V_9) = 0.24$
	$\sigma(V_2) - \sigma(V_3)$	$\text{CONN}(V_2, V_3) = 0.22$
	$\sigma(V_2) - \sigma(V_6)$	$\text{CONN}(V_2, V_6) = 0.41$
	$\sigma(V_2) - \sigma(V_9)$	$\text{CONN}(V_2, V_9) = 0.11$
	$\sigma(V_3) - \sigma(V_9)$	$\text{CONN}(V_3, V_9) = 0.21$
	$\sigma(V_4) - \sigma(V_7)$	$\text{CONN}(V_4, V_7) = 0.39$
	$\sigma(V_4) - \sigma(V_9)$	$\text{CONN}(V_4, V_9) = 0.35$
	$\sigma(V_5) - \sigma(V_8)$	$\text{CONN}(V_5, V_8) = 0.28$
	$\sigma(V_5) - \sigma(V_9)$	$\text{CONN}(V_5, V_9) = 0.28$
	$\sigma(V_6) - \sigma(V_7)$	$\text{CONN}(V_6, V_7) = 0.41$
	$\sigma(V_6) - \sigma(V_9)$	$\text{CONN}(V_6, V_9) = 0.41$
	$\sigma(V_7) - \sigma(V_9)$	$\text{CONN}(V_7, V_9) = 0.39$
	$\sigma(V_8) - \sigma(V_9)$	$\text{CONN}(V_8, V_9) = 0.24$

Arc	β -strong	$\sigma(V_1) - \sigma(V_2)$ $\sigma(V_1) - \sigma(V_5)$ $\sigma(V_2) - \sigma(V_7)$ $\sigma(V_3) - \sigma(V_7)$ $\sigma(V_4) - \sigma(V_8)$ $\sigma(V_5) - \sigma(V_7)$ $\sigma(V_6) - \sigma(V_8)$	$CONN(V_1, V_2) = 0.22$ $CONN(V_1, V_5) = 0.28$ $CONN(V_2, V_7) = 0.39$ $CONN(V_3, V_7) = 0.39$ $CONN(V_4, V_8) = 0.35$ $CONN(V_5, V_7) = 0.39$ $CONN(V_6, V_8) = 0.41$
	δ -strong	$\sigma(V_1) - \sigma(V_6)$ $\sigma(V_2) - \sigma(V_5)$ $\sigma(V_5) - \sigma(V_6)$	$CONN(V_1, V_6) = 0.41$ $CONN(V_2, V_5) = 0.28$ $CONN(V_5, V_6) = 0.41$

Table 5.3. Result

The rules of strong arc are classified as each link of the nodes. The classification shows a heavy congestion with an α -strong arcs, a medium flow in β -strong arcs and a normal flow in δ -arc.

The lanes with high traffic are represented by α -strong arcs. More number of vehicles will pass through the same lanes represented by α -strong arcs. Traffic congestion could be reduced in the roundabouts by diverting these lanes to other lanes, that is, β -strong, δ -arc with normal or medium flow.

The traffic jam of a road will be reduced an accidents minimized by this method. A better solution for roundabout traffic problem has been studied with the concept of strong arcs using fuzzy graph.

Long weights of junctions and congestion can be avoided more efficiently. The knowledge of strong arcs in fuzzy graph is very important in any real time

application. The rate of traffic flow in peak time is moderate and congestions have avoided in roundabouts by the application of strong arcs in traffic flow problems.

CONCLUSION

In this project, we have learned about the basics of Fuzzy Theory and its Applications. We have discussed many theorems using the concepts of fuzzy graphs, fuzzy matrix and fuzzy relations and compositions. The needs of the fuzzy graphs have also been examined in the applications section. The mentioned definitions and theorems can be extended to other fields of mathematics.

REFERENCES

- [1] George J. Klir and Tina A. Folger “Fuzzy Sets, Uncertainty, and Information”, Pearson Education, 2015.
- [2] Nanda .S and Das.N.R “Fuzzy Mathematical Concepts”, Narosa Publishing House, 2010.
- [3] Zadeh, Lotfi A., “Fuzzy Sets, Information and Control”, University of Granada, Spain, 1965.
- [4] Zemankova. M – Leech “Fuzzy Relational Data Bases – A key to Expert Systems”, Verlag and TUV Rheinland, Koln.
- [5] Zimmermann.H.J “Fuzzy Set Theory and its applications”, Kluwer Academic Publishers, 1976.