DESIGN SYNTHESIS AND PERFORMANCE EVALUATION OF CODES WITH GOOD RANK DISTANCE PROPERTIES FOR WIRELESS COMMUNICATIONS AND INFORMATION STORAGE SYSTEMS

Thesis

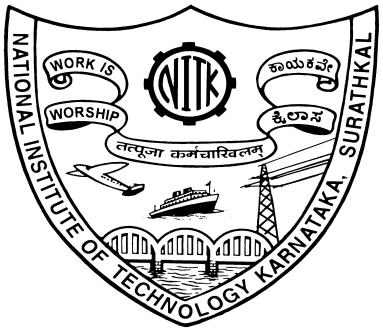
Submitted in partial fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

RAGHAVENDRA M.A.N.S

(135048EC13F04)



Department of Electronics and Communication Engineering

National Institute of Technology Karnataka

Surathkal, Mangalore - 575025, India

March, 2020

DECLARATION

I hereby ***declare*** that the Research Thesis entitled **Design Synthesis and Performance Evaluation of Codes with Good Rank Distance Properties for Wireless Communications and Information Storage Systems** which is being submitted to the ***National Institute of Technology Karnataka, Surathkal*** in partial fulfilment of the requirements for the award of the Degree of ***Doctor of Philosophy*** is a ***bonafide report of the research work carried out by me***. The material contained in this report has not been submitted to any University or Institution for the award of any degree.

Raghavendra M.A.N.S

Register No.: 135048EC13F04

Department of E & C Engineering

Place: NITK, Surathkal.

Date: 09 March 2020

CERTIFICATE

This is to ***certify*** that the Research Thesis entitled **Design Synthesis and Performance Evaluation of Codes with Good Rank Distance Properties for Wireless Communications and Information Storage Systems**, submitted by **Raghavendra M.A.N.S** (Register Number: 135048EC13F04) as the record of the research work carried out by him, is *accepted as the Research Thesis submission* in partial fulfillment of the requirements for the award of degree of ***Doctor of Philosophy***.

Prof. U Shripathi Acharya
Research Supervisor and Professor
Department of E & C Engineering
NITK Surathkal - 575025

Prof. Laximinidhi T
HoD and Chairman - DRPC
Department of E & C Engineering
NITK Surathkal - 575025

To My Beloved Parents, Teachers and Friends

Code Poem

In Galois Fields, full of flowers
primitive elements dance for hours
climbing sequentially through the trees
and shouting occasional parities.

The syndromes like ghosts in the misty damp
feed the smoldering fires of the Berlekamp
and high flying exponents sometimes are downed
on the jagged peaks of the Gilbert bound.

S.B. Weinstein

A message of content and clarity
Has gotten to be quite a rarity.
To avoid the terror
Of serious error,
Use bits of appropriate parity.

Solomon W. Golomb

ACKNOWLEDGEMENTS

It has been a long and wonderful stay at NITK. Ph.D is one of the few experiences that makes the one pursuing it rich in thoughts. Fortunately, I learned a lot both personally and professionally and enjoyed this journey at NITK very much. During this journey I had the opportunity to find lots of friends, collaborate with brilliant colleagues and learn many life development lessons. As a mark of gratitude I would like to express my sincere heartfelt appreciation to all the people who are part of my life.

First and foremost, I would like to express my sincere gratitude to Prof. U Shripathi Acharya, my Research Supervisor, Guide, Philosopher Well wisher and everything. I am really grateful to him for his trust on me and my abilities. I really could not achieve work satisfaction without his endless support, trust, patience and timely guidance. I am extremely grateful for him, for the freedom which he gave me always, to explore all different dimensions of research and personal life. I wholeheartedly thank you, Sir. Also, I express my sincere gratitude to his family for taking care of me during my Ph.D.

My life at NITK started in the year 2011, as a post graduate student. During my stay at NITK the entire staff of E & C department extended their support. Their contribution means a lot in my life. The inspiring lectures of all the teaching faculty motivated me and many of friends to understand every little aspect in its totality. This has driven most of us to pursue Ph.D. On this note, I would like to thank all the faculty of E & C department for helping us realize the beauty of technology and grow professionally.

In particular, I would like to extend my sincere gratitude to Prof. M Kulkarni, Professor (Dept. of E&C Engg.) and RPAC member, and Prof. M N Satyanarayan, Professor (Dept. of Physics) and RPAC member for their support throughout this research work. Their suggestions during my Ph.D helped me to shape my work in a

better way.

A special acknowledgment goes to all the faculty of E&C department for their valuable support and guidance in academic and research activities. I am extremely grateful to them. I am grateful present director Prof. Uma Maheshwar Rao, and past director Prof. Swapan Bhattacharya, for providing the necessary infrastructure and resources to accomplish my research work. Also, I would like to extend my sincere thanks to the entire staff of NITK (both teaching and non-teaching), who have helped me with my stay at NITK and without them this would not have been possible.

The financial support provided by Ministry of Human Resource and Development, Govt. of India for my research work was indispensable and I am grateful.

I am lucky to have many nice and kind people and friends around me. I would like to thank all ot them, all the M Tech (Research) and Ph.D scholars who were part of NITK, E & C department during 2013-2019. Everyone of them inspired me with their skills and work approach. A special thanks to all my lab colleagues for their support. Their support mattered a lot in continuation of my Ph.D and also grow personally.

Always the most important part, my deep gratitude goes to my father M Suryanarayana , mother M L S Kameshwari, and my beloved brother M Laksmi Narayana for their unconditional love, support and encouragement in my life. I would dedicate this work to my father mother and brother, who have spent their life for the betterment of my well being. I have nothing to give them till now, but I am sure this work would make them proud and help me build a career that every parent would dream about.

ABSTRACT

Rank-metric codes, a class of subspace codes, are error control codes that can be used to correct errors in applications that require two dimensional information transmission. In these applications, errors are confined to certain rows or columns or both. This is due to the nature of perturbations introduced by the channel. When errors are confined to a few columns (error bursts), error control codes possessing burst error correction capability can be employed. However, in scenarios where errors disturb the information transmission (all the columns), such that one or few rows are corrupted, burst error correcting codes by themselves fail to detect and correct all the errors. It has been shown that if error pattern is such that it has disturbed the information transmission uniformly (error matrix having rank less than certain value), then rank metric codes are the best choice for ensuring information integrity. The design and synthesis of rank error correcting codes started with the discovery of maximum rank distance (MRD) codes and maximum rank array codes (MRA) codes. These were mainly designed to overcome rank errors or crisscross errors. The search for codes with good rank distance properties continued and many low rate codes with good rank distance properties were identified within the class of Cyclic and Abelian codes. These were used to construct non-orthogonal Space Time Block codes (STBC). The application of the rank metric codes as Space-Time Block codes for MIMO systems has the potential to improve the performance of MIMO communication systems. In literature, Space- Time Block Code designs have been extracted from $(m, 1)$ MRD codes, MRA codes and Full rank cyclic codes over the Galois fields $\mathbb{F}_{q^m}$ with rate $1/n$. While these full rank codes had good rank-distance properties, they suffered from low spectral efficiencies and the lack of a suitable decoding algorithm. It was then felt that if high rate full rank codes could be synthesized from the family of Cyclic or Abelian codes, and an efficient decoding algorithm could be devised, it could lead to the design of highly efficient STBCs for wireless communication, codes for correcting crisscross errors in both storage media and power line communication. This motivated us to search for the existence of high rate full rank codes from within the families of Quasi-Cyclic, Cyclic and Abelian codes (polynomial codes). We have demonstrated that full rank high rate codes

can be found within the class of polynomial codes by specifying the procedure that can be used to construct (n, k) full rank codes over $\mathbb{F}_{q^m}$. Further, we have stated and proved theorems that allow the determination of the exact rank of these codes. A decoding algorithm based on the parity check matrix representation has been devised. It determines the unique solution if rank of the error vector $R_q(\mathbf{e}) \leq \lfloor \frac{m-1}{2} \rfloor$. The use of Galois Field Fourier Transform (GFFT) description of polynomial allows the specification of a direct relationship between the choice of k free transform components and rank of the corresponding codeword vector. Additionally, the use of GFFT provides an additional degree of freedom in the choice of $k-$ free transform components for a specified rank requirement. This freedom can be employed to construct an index key based communication scheme, which can provide an additional layer of physical layer security.

We have demonstrated that the bit error rate (BER) performance of the proposed codes as STBCs in wireless applications is superior to that of codes derived from MRD and MRA constructions. Rank preserving maps such as the Gaussian Integer map or Eisenstein-Jacobi integer map have been employed to synthesize STBC designs.

The BER performance of these codes has been determined in power line communication applications also. It is observed that the performance is identical to that of Low Rank Parity Check codes (derived from Gabidulin codes). In addition, the proposed constructions provide flexibility as a large number of full rank codes meeting various needs can be easily synthesized.

Thus, the focus of the research work reported in this thesis is the discovery of high rate full rank codes from the families of polynomial codes and assessment of their performance in a variety of applications. The performance of these codes is broadly superior to the state of the art in most cases and comparable in some instances. Hence, we believe that these codes can be gainfully used in many applications to strengthen the process of information transfer, storage and dissemination.

Keywords : Abelian, Crisscross Error, Galois Field Fourier Transform, Index Modulation, Multiple-Input Multiple-Output, Orthogonal Frequency Division Multiplexing, Quasi-Cyclic, Rank-Distance.

Contents

List of Figures

List of Tables

ABBREVIATIONS

AWGN	Additive White Gaussian noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
COD	Complex Orthogonal Design
CP	Cyclic Prefix
CSI	Channel State Information
DFT	Discrete Fourier Transform
FEC	Forward Error Correction
FRC	Full Rank Codes
gcd	greatest common divisor
GFFT	Galois Field Fourier Transform
IDFT	Inverse Discrete Fourier Transform
IM	Index Modulation
lcm	least common multiple
LOS	Line of Sight
LTO	Linear Tape Open
MIMO	Multiple-Input Multiple-Output
ML	Maximum Likelihood
MLC	Multi-level Cell
MMSE	Minimum Mean Square Error
mPLC	Multicarrier PLC
MRD	Maximum Rank Distance Codes
NSFBC	Non-orthogonal Space-Frequency Block Code
NSTBC	Non-orthogonal Space-Time Block Code
OFDM	Orthogonal Frequency Division Multiplexing
PEP	Pairwise Error Probability

PLC	Power Line Communication
QC	Quasi-Cyclic
QPSK	Quadrature Phase Shift Keying
RC	Rank Codes
RBER	Raw Bit Error Rate
SER	Symbol Error Rate
SM	Spatial Modulation
TLC	Triple Level cell
UAV	Unmanned Aerial Vehicle
WOM	Write Once Memory

SYMBOLS

$\mathbb{F}_q-$ finite field of characteristic q

$\mathfrak{e}$-exponent of the code.

N_T- Number of transmit antennas

e_j-Size of the $q-$cyclotomic coset.

$n-$ Length of the code (codewords)

$[]_n-$ q-cyclotomic coset modulo n.

N_R- Number of receive antennas

$()_{n,m}-$ residue class modulo n/m.

$m-$ smallest integer such that $n|q^m-1$

$\Psi-$ character of a group $\mathbf{G}$

$N-$ Number of orthogonal subcarriers per $\mathbf{X}_\rho$.

$\mathscr{R}-$ Symbol rate of the code.

$\mathbb{F}_{q^m}-$ m^{th} extension field of $\mathbb{F}_q$

α_i- Galois field element of order i

N_F- Total number OFDM carriers

$\alpha-$ Primitive $(q^m-1)^{th}$ root of unity in $\mathbb{F}_{q^m}$.

$\boldsymbol{Y}-$Received column vector corresponding to.

$\mathscr{C}-$ Represent cyclic code of length n.

NSFBC-IM codeword

$\mathbf{c}-$ $n-$length codeword vector $\in \mathscr{C}$

$\mathbf{Y}-$Received Matrix.

$\mathbf{C}-$ $m \times n$ matrix corresponding to $\mathbf{c}$

$\mathbf{H}-$Channel matrix.

$\mathbf{X}_\rho-$NSFBC codeword obtained from $\mathbf{C}$.

$\eta-$ Spectral efficiency

$\mathbf{X}_{\rho,IM}-$NSFBC-IM codeword.

$|||[\cdot]|||_F^2-$ Frobenius norm or L_2- norm.

$\mathcal{X}-$ NSFBC obtained from $\mathscr{C}$.

$[]_n-$ q-cyclotomic coset mod n.

$\mathbf{S}-$ NSFBC-MIMO-OFDM-IM block.

$\mathcal{L}$- Number of $q-$ cyclotomic cosets of size m

$R_q(\cdot)$−Rank of $[\cdot]$.

L− Length of the channel impulse response.

$\mathbf{L}$− Length of the index key.

$\mathscr{X}$ − Space-Time/Frequency Block Code.

Chapter 1

Introduction

When information is conveyed over a physical channel or stored in an optical, semiconductor or magnetic medium, there is always a finite probability of the stored data being distorted/ destroyed/ corrupted due to errors. The use of error control codes to overcome these errors has become ubiquitous in modern information based society. Algebraic coding theory is a discipline of Information Theory that is concerned with the design and analysis of codes that can be employed to detect and correct errors introduced by channels and/ or memory devices. The objective of this discipline (also known as channel coding) is to synthesize constructive techniques which allow the corrupted data to be recovered without errors as far as possible. The history of error correcting codes goes back to 1948 with the publication of a classic paper entitled "A Mathematical theory of Communication" by C.E. Shannon Shannon (1948). In his paper, Shannon proved that whenever the transmission rate required of a communication system is less than the capacity of the channel, it is possible to design an encoding/ decoding scheme, with the help of which, the probability of error in the reconstructed sequence can be made as small as desired. The power of modern algebra, especially Galois fields, has been harnessed to synthesize a large class of codes (known as block codes) which are capable of correcting errors in a received vector. Several metrics have been proposed for quantifying the error correction performance of error correcting codes. The Hamming metric was the first such metric to be proposed. Typical examples of Hamming metric based codes include Cyclic codes, Bose Chaudhury Hocquenghem (BCH) codes, Reed Solomon (RS) and the capacity approaching Low Density Parity Check (LDPC) codes. With the use

of suitable interleavers, these codes can be employed to correct large error bursts. However, While studying the error patterns induced in certain applications involving storage/ transmission of information in the form of 2D matrices and also the while studying the construction of error control codes as block codes for multiple-input multiple-output systems, several researchers realized that the Hamming metric based codes are not well suited. They proposed a new metric, called the Rank metric and devised code constructions based on rank metric Roth (1991), Gabidulin (1985), Plass et al. (2008). Rank-metric codes are also known as subspace codes. The class of subspace codes have been studied by Khalegi et.al Khaleghi et al. (2009). Following is the detailed discussion on few applications where rank-metric codes are suitable.

1.1 Rank Codes in Multicarrier communication systems

In case of multi-carrier transmission schemes, the symbols are transmitted in a frame structure which can be represented in matrix form. In hot spot scenarios the channel generates error patterns which are mainly limited to several sub-carriers due to time stationarity of the channel. The erroneous frame obtained at the receiver can be described as shown in Figure 1.1 (Plass et al. (2008)). In Figure 1.1, N represents the number of subcarriers and n

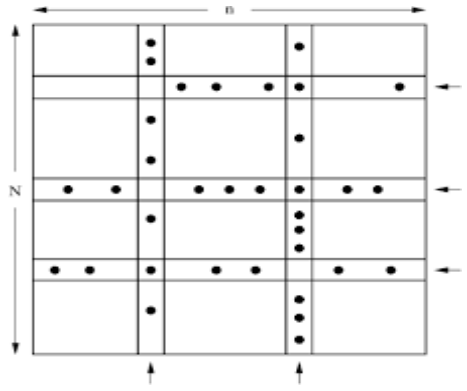


Figure 1.1: Error Patterns in Multicarrier communication systems

represents the length of the frame. The errors in the received matrix are observed to be confined to certain rows and or or columns. These matrix errors were termed as rank errors or

criss-cross errors. Since rank codes are capable of correcting a specified number of rows and columns (Gabidulin (1985); Plass et al. (2008); Roth (1991)), these codes are capable of correcting a greater number of errors when compared with competing burst error correcting codes. After Gabidulin (1985) proposed the first constructions of rank-metric codes , Roth (1991) proposed constructions of Maximum rank array codes. In these constructions the value of n is chosen such that $n \leq m$. The approach proposed by Roth (1991) is similar to that of Gabidulin codes but differ in the decoding strategy. The decoding strategy proposed by Gabidulin is based on Euclidean division algorithm while the decoding approach by Roth is similar to Peterson-Gorenstein-Zierler (PGZ) algorithm.

1.2 Rank codes in MIMO communications

Rank codes can also be used as space-time block codes (STBC) or space-frequency block codes (SFBC) in MIMO systems In general, the STBC/SFBC designed should satisfy the following design criteria (Tarokh et al. (1998)).

- Rank Criterion: Maximization of the diversity advantage, i.e the rank distance between two STBC/SFBC codewords should be as high as possible. Hence a rectangular code characterized by rank distance equal to the number of rows yields best performance.
- Product Distance Criterion: Maximization of the coding gain offered by the code or equivalently, the coding advantage over all pair of distinct codewords $\mathbf{X}, \mathbf{X}' \in \mathscr{X}$ should be made as large as possible.

The performance of MIMO based communication system can be further improved by the use of an (n, k) error control code in concatenation with the Alamouti code (Liew and Hanzo (2002)). However, this approach requires needs an additional error control encoder and decoder which further increases computational complexity. Hence, there is a need to improve error performance in STBC or SFBC based MIMO communications without using an external error control code. This can be achieved by designing an STBC or SFBC code with maximum distance (with internal (built in) error correcting structure). Several researchers

have proposed schemes (Lusina et al. (2003); Martin and Taylor (2004); Plass et al. (2008); Sripati et al. (2004a,b)) in which an error control code is embedded in the MIMO design. Some of these approaches are enumerated below:

1. STBCs with rank $r < N_T$, obtained from Bose-Chaudhury-Hocquenghem (BCH) and Reed-Solomon (RS) codes, were used in (Martin and Taylor (2004)) for $N_T \times 4$ MIMO communications (where, N_T represents the number of transmit antennas). Here, performance improvement is obtained by maximizing the minimum squared Euclidean distance between any two codewords. Hamming metric (not a rank metric) has been considered to design STBCs resulting in STBCs with rank $r < N_T$. Due to this, at least four receive antennas have to be employed to satisfy the condition $rN_R \geq 4$. This limits the usage of codes to MIMO systems employing $N_R \geq 4$ receive antennas. Hence, there is a need for synthesizing full rank STBCs for MIMO systems with $N_R < 4$ antennas as well as arbitrary N_T and N_R.

2. Gabidulin codes over $\mathbb{F}_{q^m}$ (along with rank preserving Gaussian integer map) have been used by Lusina et al. (2003) as STBCs for MIMO systems. The codewords of a Gabidulin code are viewed as $m \times n$ matrices over the base field $\mathbb{F}_q$. These constructions ensure that $n \leq m$. Further, these constructions are extended to a class of cyclic codes, also called $q-$ cyclic codes. Because of the maximum rank distance property and the code structure which ensures that $n \leq m$, Gabidulin codes can be used as STBCs (full rank) if $n = m$ and $d = m$, implying $k = 1$. Thus, $(n, 1)$ Gabidulin codes alone with $n = m$ are used as STBCs. This results in the synthesis of a STBC with q^m possible codewords.

3. Sripati et al. (2004b) designed $(n, 1)$ full rank codes by employing discrete Fourier transform (DFT) description were used to synthesize STBCs for MIMO systems. It was shown that the proposed STBCs outperformed STBCs obtained from Orthogonal designs in the case of propagation over quasi-static Rayleigh fading environment. The construction involves DFT description of cyclic codes over $\mathbb{F}_{q^m}$ proposed by Sripati and Rajan (2003). Unlike Gabidulin codes, the length n of the code was chosen to be a

divisor of $q^m - 1$, hence codewords of length $n \geq m$ were possible. Similar to Gabidulin codes, the codewords of these codes could be viewed as $m \times n$ matrices over the base field $\mathbb{F}_q$, with $n \geq m$. The separation (in terms of rank distance) between any two codewords was found to be at least d, with $d \leq m$. Full rank ($d = m$) code constructions were proposed. But the limitation was that full rank could be obtained only when $k = 1$. Full rank constructions for higher values of k were not proposed. This lacuna is addressed in this work and higher rate full rank ($d = m$) designs derived from cyclic, quasi-cyclic and Abelian codes are proposed. This is followed by a discussion of their applications in the domains of wireless communication, power line communication and storage systems.

1.3 Rank codes in storage system

Matrix codes (2D code) can also be used in applications like Linear Tape Open (LTO) and Flash drives.

1.3.1 Tape Drives

Tape drives are being considered as potential solutions to address the issue of storage of backup data in case of cloud systems. Table 1.1 shows the comparison of various tape drives that are being used today. In case of tape drives information is generally stored in 2D format.

Table 1.1: Various technologies and data transfer rates of tape drives

Drive technology	Data Transfer Rate (MB/s)	Capacity (TB)
LTO-6	160	2.5
TS1150	360	10
T10000D	252	8

It is observed that when read/write head is corrupted the information read from/written onto particular track of the tape drive is corrupted. Rank-metric codes are useful in recovering data from these scenarios (Roth (1991)).

1.3.2 Flash Drives

Cai et al. (2012) has designed and implemented a framework for fast and accurate characterization of MLC flash memory throughout its lifetime. In (Cai et al. (2012)) error patterns of TLC flash memory has been analyzed, over its lifetime (3,000 P/E cycles). The observed errors are classified into four different types from the controller's point of view (Cai et al. (2012)).

- Erase error- happens when an erase operation fails to reset the cells to the erased state. This is mainly due to manufacturing process variations or defects caused by trapped electrons in the tunnel oxide after stress due to repeated Program/Erase (P/E) cycles.
- Program Interference error- happens when the data stored in a page changes (unintentionally) while a neighboring page is being programmed due to parasitic capacitance-coupling.
- Retention error- happens when the data stored in a cell changes over time. The main reason is that the charge programmed in the floating gate may dissipate gradually through the leakage current.
- Read error-happens when the data stored in a cell changes as a neighbouring cell on the same string is read over and over.

Figure 1.2 is a plot of the Bit error rate as a function of the number of P/E cycles, in MLC NAND flash memories. It is observed that at the beginning of the flash's lifetime the error rate is relatively low and the raw bit error rate is below 10^{-6}, within the specified lifetime. As number of P/E cycles increase the retention errors are found to be most dominant. Table 1.2 shows the percentage of errors given current symbol stage. Table 1.3 shows the percentage of errors of various bits.

Table 1.3 shows that the probability of single bit being in error is more as compared to two or three bits of the cell, in case of TLC flash drive. As seen from table 1.2 the least significant bits of symbols have more probability of error as compared to most significant bits. This is due to progressive writing mechanism incorporated in flash drives, to avoid high Raw Bit

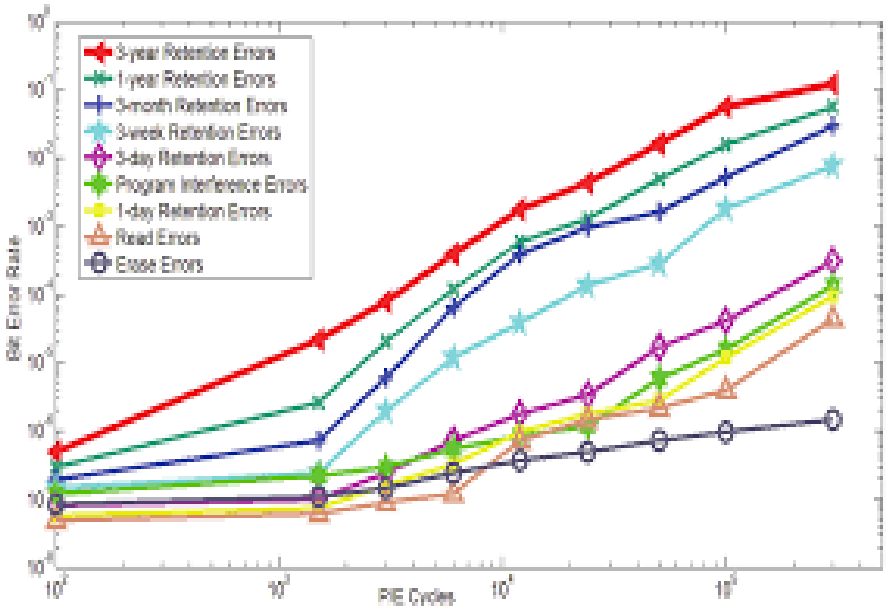


Figure 1.2: BER vs. Program/Erase Cycles in case of MLC NAND Flash memory

Error Rate (RBER). From the above table 1.2, it is important to note that the symbols can be arranged in the form of an array such that all the errors are associated with a specific column and row, as shown in Figure 1.3,

0	0	1	1	1	0	1	0	1	0
1	0	0	1	0	0	1	1	0	1
0	1	1	0	0	1	0	0	1	1

Figure 1.3: Crisscross error pattern in TLC flash drive

The BCH codes used in present day Single Level Cell (SLC) Flash memories cannot be employed directly to correct these types of errors (Cai et al. (2012)). Reed-Solomon (RS) codes can be employed if the errors are confined to columns. Product codes employing RS codes can correct certain matrix errors when errors are confined to few rows or columns. However, if the error matrix is such that all the rows and columns are in error but the rank of the error is less than the rank error correcting capability, then RS codes and product codes may not be able to correct these errors. In such scenario, rank codes can be used to decrease the BER of the MLC/TLC flash memory.Hence suitably designed rank-error correcting codes can be used to detect and correct these errors.

Table 1.2: Prominent error patterns observed in TLC Nand flash drive

Programmed state	Error state	Percentage of errors
000	010	0.2467
000	001	0.2444
111	101	0.0820
111	110	0.0807
000	100	0.0669
011	001	0.0556
100	110	0.0550
011	010	0.0547
100	101	0.0540
111	011	0.0217

Table 1.3: Flash cell error patterns

Number of bits in Flash cell that err	Percentage of errors
1	0.9617
2	0.0314
3	0.0069

1.4 Motivation

In recent years, a number of researchers have been engaged in the design of low complexity advanced data detection techniques for rank metric codes. For decoding Gabidulin codes, decoding approaches such as Welch-Berlekamp like algorithm (Loidreau (2006)) and List decoding of Gabidulin subcodes over finite fields have been proposed by Ding (2015); Guruswami and Xing (2013); Wachter-Zeh (2014). In case of Roth codes, a low complex decoder for constructions over larger fields has been proposed in (Roth (2018)). As seen from Sections 1.1,1.2, the other well known application of rank-metric codes in MIMO communication. In (Lusina et al. (2003)) $(n = m, 1)$ Gabidulin codes (Gabidulin (1985)) were synthesized and employed as STBCs for MIMO communications. To construct STBCs the Gabidulin constructions were restricted to $(n = m, k = 1)$ codes, since an increase in the value of k results in rank-deficient codes (rank distance $d < m$) (Lusina et al. (2003)-Asif

et al. (2017)). In (Sripati et al. (2004b)-Sripati et al. (2004a)) $(n, 1)$ codes over $GF(q^m)$ with rank=m and length $n \geq m$ have been used as STBCs for MIMO communication over block fading channels Sripati et al. (2004a). The STBC codes presented in (Lusina et al. (2003); Martin and Taylor (2004); Sripati and Rajan (2003); Sripati et al. (2004b)) are obtained from full rank $(n, 1)$ codes.

Full rank codes (full row rank) with rectangular structure (number of columns greater than number of rows) can improve the BER performance of MIMO and Multicarrier communications. Further, for the case of rank error correction, it will be interesting to find the existence of codes analogous to the Gabidulin codes and Roth codes. Additionally, full rank codes with $k > 1$ can result in more number of possible codewords and hence increase in code efficiency. The problem of synthesizing full rank codes for $k \geq 2$ has not been addressed in prior literature (Lusina et al. (2003); Martin and Taylor (2004); Sripati and Rajan (2003); Sripati et al. (2004b)). In this thesis, we have attempted to synthesize STBC codes for higher values of $(k > 1)$ and showed that these codes provide better performance without compromising the code rate. Additionally, we have obtained rank metric properties from various class of codes like quasi-cyclic and abelian codes. Realizing the importance and need for well designed, large rank distance codes, low complexity codes for error correction in this class of applications, we have designed, codes with good rank distance properties for wireless/ power line and storage systems. We have devised a low complexity decoding algorithms for these codes and have assessed their performance over various channel models.

Motivated by the requirement of (n, k) full rank codes with $k \geq 2$ for MIMO communications, power line communications and storage devices, we have demonstrated the existence of $(n = km, k)$ full rank codes over $\mathbb{F}_{q^m}$, with $k \geq 2$. To construct (n, k) full rank codes we have followed the Transform domain (GFFT) approach presented by Rajan and Siddiqi (1992); Sripati and Rajan (2003). The Galois field Fourier transform (GFFT) description of cyclic and Abelian codes has been employed in the synthesis of these codes. This has been done for the following reasons.

- The GFFT description enables us to determine a direct relationship between the size of a $q-$cyclotomic coset and the rank of the code constructed by employing certain elements of this coset as indices of free transform domain components.

- The GFFT description points to the fact that there is a certain freedom in choosing indices of free transform domain components from a $q-$ cyclotomic coset. The freedom provided by the choice of free transform components can be employed to design a an additional layer of security at the level of the physical layer.

We started our work by proving that (n, k) full rank cyclic codes exist for $k \geq 2$. We have evaluated their performance in MIMO systems and powerline communication systems. Later we have generalized the results to a more general class of cyclic codes called quasi cyclic codes. These results are then extended to a more general class of codes called Abelian codes. Below we present some mathematical preliminaries used throughout our work. Preliminaries that are required to understand only specific constructions are presented in corresponding chapters.

1.5 Mathematical preliminaries

This section describes the fundamental mathematical concepts that are employed in development of the theory of error control codes. Let S be a non-empty set. A map $* : S \times S \rightarrow S$, $(a, b) \rightarrow a * b$ is called a binary operation on S. So $*$ takes 2 inputs a, b from S and produces a single output $a * b \in S$. In this situation we may say that 'S is closed under $*$'. We say

- $*$ is commutative if, for all $a, b \in S$,

  $a * b = b * a$

- $*$ is associative if, for all $a, b, c \in S$,

  $a * (b * c) = (a * b) * c$

(note that binary operation (bop) ensures that each side of this equation makes sense). If $*$ is associative we can unambiguously write $a * b * c$ to denote either of the iterated products.

1. **Group**

   Let S be a non-empty set and let $*$ be a binary operation on S : $*$:$S \times S \rightarrow S$, $(a, b) \rightarrow a * b$. Then $(S; *)$ is a group G if the following axioms are satisfied:

   $(G1)$ Associativity: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$

   $(G2)$ Identity element: there exists $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.

   $(G3)$ Inverses: for any $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = a-1 * a = e$.

   If in addition the following holds

   $(G4)$ Commutativity: $a * b = b * a$ for all $a, b \in G$. then $(G; *)$ is called an Abelian group, or simply a commutative group. For a finite group G, the order of the group is defined to be the number of elements in it. The order is denoted by $|G|$. Otherwise we say that G has infinite order. If $(G; *)$ is a group then the identity e is unique and the inverse of any a in G is uniquely determined by a.

2. **Character of a group**

   A character is (most commonly) a special kind of function from a group to a field

   A character on a group G is a group homomorphism from G to the multiplicative group of contained within the field $\mathbb{F}_q$. If G is any group, then the set $Ch(G)$ of these morphisms forms an abelian group under point-wise multiplication. This group is referred to as the character group of G.Multiplicative characters are linearly independent, i.e. if $\chi_1, \ldots, \chi_n$ are different characters on a group G then from $a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$ it follows that $a_1 = a_2 = \cdots = a_n = 0$.

3. **Ring**

   A structure $(R, +, \cdot)$ is a ring if R is a non-empty set and + and $\cdot$ are binary operations: $+ : R \times R \rightarrow R$, $(a, b) \rightarrow a + b \cdot : R \times R \rightarrow R$, $(a, b) \rightarrow a \cdot b$ such that Addition: $(R, +)$ is an abelian group, that is,

   (A1) Associativity: for all $a, b, c \in R$ we have $a + (b + c) = (a + b) + c$

   (A2) Zero element: there exists $0 \in R$ such that for all $a \in R$ we have $a + 0 = 0 + a = a$

   (A3) Inverses: for any $a \in R$ there exists $-a \in R$ such that $a + (-a) = (-a) + a = 0$

   (A4) Commutativity: for all $a, b \in R$ we have $a + b = b + a$

Multiplication: (M1) Associativity: for all $a, b, c \in R$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Addition and multiplication together

(D) $\forall a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot b + b \cdot c$

We sometimes say $'R'$ is a ring, taken it as given that the ring operations are denoted + and $\cdot$. As in ordinary arithmetic we shall frequently suppress $\cdot$ and write ab instead of $a \cdot b$.

Assume $(R; +, \cdot)$ is a ring. We say R is a commutative ring if its multiplication $\cdot$ is commutative, that is,

(M4) Commutativity: $a \cdot b = b \cdot a$ for all $a, b \in R$. We say R is a ring with 1 (or ring with identity) if there exists an identity for multiplication, that is,

(M2) identity element: there exists $1 \in R$ such that for all $a \in R$ we have $a \cdot 1 = 1 \cdot a = a$.

There are many examples of rings. In this work we use polynomial rings. Polynomials, with real coefficients, form a commutative ring with identity under the usual addition and multiplication; we denote this by $R[x]$.

Ideals

An ideal is a subset I of elements in a ring R that forms an additive group and has the property that, whenever x belongs to R and y belongs to I, then xy and yx belong to I.

4. **Galois Field**

A structure $(R, +, \cdot)$, where + and $\cdot$ are binary operations on R is a field if $(A1) - (A4), (M1) - (M4)$, and (D) hold, and $0 \neq 1$. This can be expressed in a more modular way as follows $(R, +, \cdot)$ is a field if (A) $(R, +)$ is an abelian group; (M) $(R\ \{0\}, \cdot)$ is an abelian group; (D) the distributive laws hold. There are two family of fields: finite fields (Galois field) and infinite fields $(\mathcal{Q}, \mathcal{R}, C,)$. Finite fields find application in coding theory and applied algebra. In this work we have employed Galois fields and finite complex fields (Eisenstein-Jacobi integer field and Gaussian integer field).

5. **Linear codes** -

A $q-$ary block code of size M is a set of M $q-$ary sequences of fixed length n over a finite set of symbols called the *alphabet*. The elements of a code are called the codewords. Under the component-wise vector addition and scalar multiplication, the set of $n-$ tuples over $\mathbb{F}_q$ forms a linear space denoted by $\mathbb{F}_q^n$. A linear code C is a subspace of $\mathbb{F}_q^n$. When the dimension of C is k ($k \leq n$), it is called linear $[n, k]$ code and is denoted by $C[n, k]$.

It can be noted that if $\mathscr{C}$ is designed over a Galois field $\mathbb{F}_{q^m}$ then the elements of codeword vectors in $\mathscr{C}$ belong to $\mathbb{F}_{q^m}$. From the theory of Galois field we know that the elements in $\mathbb{F}_{q^m}$ can be represented as $m-$tuple elements over $\mathbb{F}_q$. Thus the $n-$length codeword vectors can be expressed as $m \times n$ codeword matrices.

Rank metric Linear codes An (n, k, d) linear code $\mathscr{C}$ over the Galois field $\mathbb{F}_{q^m}$ can be thought of as a $k-$dimensional linear space of $m \times n$ matrices over $\mathbb{F}_q$ with d being the minimum weight of any non-zero matrix in $\mathscr{C}$. This can be denoted as an $(m \times n, k, d)$ array code over the field $\mathbb{F}_q$.

General properties of codes

A distance $d(x, y)$ between a $n-$length vectors x, y is a function satisfying conditions $d(x, y) \geq 0, \forall x, y$; (Non-negative). $d(x, y) = 0 \iff x = y$; (zero value) $d(x, y = d(y, x)$;(Symmetry). $d(x, y) \leq d(x, z) + d(z, y), \forall x, y, z$ (Triangle inequality). A norm function $N(x)$ is associated with the distance function. Similar to distance function, the norm function should satisfy the following axioms: $N(x) \geq 0, \forall x$;(Non-negative). $N(x) = 0 \iff 0 \iff x = 0$;(Zero value). $N(x + y) \leq N(x) + N(y), \forall x, y$ (Triangle inequality). The norm function allows to construct the distance function as follows: $d(x, y) := N(x - y)$. The distance between $n-$length vectors $x, y \in \mathscr{X}^n$ is defined as follows.

$$d(x, y) = \sum_{i=1}^{n} d(x_i, y_i)$$

Similarly, for the coordinate-wise norm, we have

$$N_n(x) = \sum_{i=1}^{n} N(x_i)$$

Norm functions are used to quantify the distance between two codewords in coordinate wise or non-coordinate wise manner. The hamming distance (Hamming norm) is defined coordinate-wise however the rank distance (Rank norm) cannot be defined coordinate wise.

Singleton Bound

In coding theory, the Singleton bound is an upper bound on the size of an arbitrary block code C with block length n, size M and minimum distance d. The minimum distance of a set C of codewords of length n is defined as

$$d = \min_{\{x,y \in C : x \neq y\}} d(x, y)$$

where $d(x, y)$ is the Hamming distance between x and y. The expression $A_q(n, d)$ represents the maximum number of possible codewords in a $q-$ary block code of length n and minimum distance d. Then the Singleton bound states that $A_q(n, d) \leq q^{n-d+1}$.
If C is a linear code with block length n, dimension k and minimum distance d over the finite field with $q$elements, then the maximum number of codewords is q^k and the Singleton bound implies: $q^k \leq q^{n-d+1}$,so that $k \leq n - d + 1$, which is usually written as $d \leq n - k + 1$. Codes that attain maximum distance i.e that is codes with satisfy singleton like bound with equality (called as Maximum Distance Separable) are preferred in communication theory. Since rank of a codeword matrix is less than the hamming distance of the corresponding codeword vector, the rank distance of a code $\mathscr{C}$ is upper bounded by its hamming distance d. Thus the codes satisfying maximum rank distance are called Maximum Rank Distance codes (MRD codes).

6. **Cyclic codes as ideals in polynomial rings**. The concept of an ideal contained within

a ring plays a fundamental role in the study of cyclic codes. We know that if V is a vector space under vector addition, it has no natural multiplicative structure. A useful way of introducing a multiplication is to identify the vectors $(a_0, a_1, \cdots, a_{n-1})$ in V with the polynomials

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$$

where $\mathbb{F}_q$ is a Galois field, and then use the multiplication in this ring as the multiplication of the corresponding vectors. Doing this clearly transforms vector space V into a ring isomorphic to the polynomial ring modulo $(x^n - 1)$. Since it is so easy to go back and forth between these two representations (i.e., vectors and polynomials) we will often blur the distinction between the two and just deal with the polynomials. Notice that the choice of $x^n - 1$ as $f(x)$ means that multiplying by x corresponds to a cyclic shift of a vector. Since $\mathscr{C}$ is a subspace and cyclic, if all the codeword vectors are cyclic shifts of other codeword vectors, the polynomial ring associated with $\mathscr{C}$ is an ideal. Thus cyclic codes are ideals in polynomial rings. This mathematical structure is employed in this work.

1.6 Contribution of the Thesis

The main contribution is as follows:

- Rank distance characterization of (n, k) QC codes over $\mathbb{F}_{q^m}$.

  In this, we have analyzed the rank distance properties of (n, k) QC codes designed by considering free transform component indices from different $q-$ cyclotomic coset integers. We have proved that (n, k) full row rank codes can be obtained by choosing free transform component indices such that they do not belong to same $q-$ cyclotomic coset.

- Rank distance characterization of (n, k) Abelian codes over $\mathbb{F}_{q^\tau}$.

  In this, we have analyzed the rank distance properties of (n, k) Abelian codes designed

by considering free transform component indices from different $q-$ cyclotomic coset integers. Abelian groups that were considered are obtained from direct product of cyclic groups. We have proved that (n,k) full row rank Abelian codes can be obtained by choosing free transform component indices such that they do not belong to same $q-$ cyclotomic coset modulo n.

- Design of STBC/SFBCs from (n,k) cyclic codes. The full rank codes derived in this work satisfy the Rank criterion and Determinant criterion. Thus we have used the full rank codes are Space-Time/Frequency Block Codes using two well known rank-preserving maps: Gaussian Integer map and Eisenstein-Jacobi Integer map.

- Performance evaluation of $(m,1)$ rank-metric codes derived from cyclic codes. Performance of the proposed rank-metric codes has been evaluated in multicarrier PLC (mPLC) system. It was found that the rank error performance of MRD codes obtained in this work, is same as the rank error performance of Gabidulin codes.

1.7 Organization of the thesis

This thesis is organized into six chapters as follows:

Chapter 2 presents the construction (synthesis) of (n,k) $\ell-$ Quasi Cyclic (QC) codes with desired rank distance properties. A systematic procedure for synthesizing $l-$ QC codes with good rank distance properties has been proposed.

Chapter 3 presents the construction (synthesis) of (n,k) Abelian codes with the desired rank distance properties. The theorems proposed in this chapter are proved using the definition of abelian code as direct product of cyclic codes. A systematic procedure for synthesizing Abelian codes with good rank distance properties has been proposed.

Chapter 4 discusses the application of the proposed codes as space-time block codes or space-time/frequency block codes (STBC/SFBC) for MIMO systems. This chapter discusses the details of MIMO system employing OFDM and IM strategies.An upper bound on the BER performance has been derived by invoking the Union bound.

Chapter 5 discusses the application of rank-metric cyclic codes for applications involving crisscross errors: namely power line communication and multi level storage/tape drives. Chapter 6 concludes the work and gives details of the future scope.

.

Chapter 2

Rank-metric Quasi-Cyclic codes

2.1 Introduction

In this chapter, we will consider the rank distance properties of $n-$length $\ell-$quasi-cyclic codes over the Galois field $\mathbb{F}_{q^m}$ with $m \leq n$, $n|q^m - 1$ and $\ell|n$. We have determined the exact rank of these codes by using the transform domain description of (n, k) Quasi-Cyclic (QC) codes given by Dey and Rajan (2003), Specifically, we have determined the exact rank of two classes of (n, k) QC codes namely arbitrary QC codes and minimal QC codes. We have shown that full rank QC codes can be obtained for any $k \geq 1$ only in case of arbitrary QC codes and have discussed the relation between rank distance of $(n, k \geq 1)$ QC codes and the free transform domain component indices. Further, we have shown that the arbitrary QC codes can be punctured to (e_j, k) codes without altering their rank with $e_j = km$. We have applied the analysis to the case of minimal QC codes and have determined the exact rank of (n, k) QC codes. In addition to this we have provided a simple technique to enable construction of parity check matrix. A decoding strategy making use of the parity check matrix has beeen derived.

In Section 2.2 we give the definitions and corresponding examples of concepts required to understand the design of QC codes. In section 2.3 we present the theorems on the rank-distance properties of QC codes. Section 2.4 provides a brief description of the technique that can be used to puncture QC codes without bringing about an alteration in the rank. In section 2.5 we give generator matrix representation of the proposed codes and their punctured

equivalents. Construction of parity check matrix is given in section 2.7. Using the check matrix, a general and low complex decoding strategy is given in section 2.7.1. In section 2.8 we discuss the rank distance properties of cyclic (1-QC) codes and provide details of MRD codes (analogous to Gabidulin codes).

2.2 Preliminaries

- **Residue class**: Consider the set $I = \{0, 1, \cdots, n-1\}$. For any $j \in [0, n-1]$ and for any ℓ such that $\ell | n$, the residue class modulo $\frac{n}{\ell}$ of j, denoted by $(j)_{n,\ell}$ is given as (Dey and Rajan (2003)),

$$(j)_{n,\ell} = \left\{ i \in [0, n-1] : j \equiv i \bmod \frac{n}{\ell} \right\} \tag{2.1}$$

***Example* 2.2.1** let us consider the set $I = \{0, 1, 2, \cdots, 14\}$ with $n = 15$. Since $2^4 - 1 = 15$, let us consider the field $\mathbb{F}_{2^4}$. Following are the residue classes modulo 5 and modulo 3 of the set I.

Table 2.1: Residue Classes modulo $\frac{n}{\ell}$ for $n = 15$ and $\ell = 3, 5$.

Residue class modulo 5	Residue class modulo 3
$(0)_{15,3} = \{0, 5, 10\}$	$(0)_{15,5} = \{0, 3, 6, 9, 12\}$
$(1)_{15,3} = \{1, 6, 11\}$	$(1)_{15,5} = \{1, 4, 7, 10, 13\}$
$(2)_{15,3} = \{1, 6, 11\}$	$(2)_{15,5} = \{2, 5, 8, 11, 14\}$
$(3)_{15,3} = \{3, 8, 13\}$	
$(4)_{15,3} = \{4, 9, 14\}$	

- **Cyclotomic Cosets**: Consider the set $I = \{0, 1, \cdots, n-1\}$. For any positive integer $j \in [0, n-1]$, the $q-$ cyclotomic coset of j modulo n is given as (Moon (2005)),

$$[j]_n = \left\{ j, jq, \cdots, jq^l, \cdots, jq^s, \cdots, jq^{l+s}, \cdots, jq^{r_j - 1} \right\} \tag{2.2}$$

The cardinality of the set $[j]_n$ is denoted as r_j.

***Example* 2.2.2**: Let us consider the set $I = \{0, 1, 2, \cdots, 14\}$. Let $n = 15$. Since $2^4 - 1 = 15$, let us consider the field $\mathbb{F}_{2^4}$. Following are the 2−cyclotomic cosets modulo 15 of the set I.

Table 2.2: 2^1−cyclotomic cosets of j modulo 15.

$[0]_{15} = \{0\}$	$[5]_{15} = \{5, 10\}$
$[1]_{15} = \{1, 2, 4, 8\}$	$[7]_{15} = \{7, 14, 13, 11\}$
$[3]_{15} = \{3, 6, 12, 9\}$	

- **Separation of $q-$ cyclotomic coset coefficients**: Let $[j]_n = \left\{j, jq, \cdots, jq^l, \cdots, jq^s, \cdots, jq^{l+s}, \cdots, jq^{r_j-1}\right\}$ be the $q-$ cyclotomic coset of integer j. We define the Separation between two elements jq^l and jq^{l+s} as the difference in powers of q associated with the elements i.e. separation between jq^l and jq^{l+s} is given as $l + s - l = s$.

  ***Example* 2.2.3** Consider the coset $[3]_{15} = \{3, 6, 12, 9\}$, the separation between elements $6 = 3.2$ and $9 = 3.2^3$ is $3 - 1 = 2$. Similarly the separation between 3 and 6 is 1, and the separation between 3 and 9 is 3.

- **Reciprocal Polynomial**: If $f(x)$ is a minimal polynomial (irreducible) given by $f(x) = a_{\mathrm{t}}x^{\mathrm{t}} + a_{\mathrm{t}-1}x^{\mathrm{t}-1} + \cdots + a_1x + a_0$, then the reciprocal polynomial $f(x)^*$ of $f(x)$ is given by

$$f(x)^* = x^{\mathrm{t}} * f(x^{-1}) = a_0x^{\mathrm{t}} + a_1x^{\mathrm{t}-1} + a_2x^{\mathrm{t}-2} + \cdots + a_{\mathrm{t}-1}x^1 + a_{\mathrm{t}};$$

  where t is some positive integer.

  [Note that the degree of $f(x)^*$ is same as the degree of $f(x)$ and the coefficients are positioned in reverse order. Also, if $f(x)$ is irreducible then $f(x)^*$ is also irreducible Roman (2005).]

  ***Example* 2.2.4** Consider the Galois field $\mathbb{F}_{2^4}$, the conjugacy classes of this field and their corresponding minimal polynomials and reciprocal polynomials are shown in the Table 2.3.

Table 2.3: Minimal and Reciprocal polynomials over $\mathbb{F}_{2^4}$

Conjugacy Class	**Minimal Polynomial**	**Reciprocal Polynomial**
$\{1\}$	$y+1$	$y+1$
$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$	y^4+y+1	y^4+y^3+1
$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$	$y^4+y^3+y^2+y+1$	$y^4+y^3+y^2+y+1$
$\{\alpha^5, \alpha^{10}\}$	y^2+y+1	y^2+y+1
$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$	y^4+y^3+1	y^4+y+1

- **Galois field Fourier transform (GFFT)**: In coding theory, Galois field Fourier transform (GFFT) is defined as the Discrete Fourier Transform (DFT) over Galois field $\mathbb{F}_{q^m}$ with a primitive element α. Following (Blahut (1983)), for the case $n|q^m-1$ the GFFT of a vector $\mathbf{u} = \{u_i,\ 0 \le i \le n-1\}, u_i \in \mathbb{F}_{q^m}$ is defined as,

$$U_j = \sum_{i=0}^{n-1} u_i \beta^{-ij}\ ; \qquad 0 \le j \le n-1 \tag{2.3}$$

Here, $\beta = \alpha^{\frac{q^m-1}{n}}$ is the n^{th} root of unity in F_{q^m}. If $n = q^m-1$ then $\beta = \alpha$. The inverse GFFT (IGFFT) of $\mathbf{U} = \left\{U_j,\ 0 \le j \le n-1\right\}$ is given by,

$$u_i = (n\ mod\ q)^{-1} \sum_{j=0}^{n-1} U_j \beta^{-ij}\ ; \qquad 0 \le i \le n-1 \tag{2.4}$$

Following usual terminology, $\mathbf{u} = (u_0, u_1, \cdots, u_{n-1})$ is called the time domain vector and $\mathbf{U} = (U_0, U_1, \cdots, U_{n-1})$ is called the transform domain vector of $\mathbf{u}$.

***Example* 2.2.5**: Let us consider the Galois field $\mathbb{F}_{2^4}$ obtained using primitive polynomial X^4+X+1. The elements of the Galois field are

$\mathbb{F}_{2^4} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha+1, \alpha^2+\alpha, \alpha^3+\alpha^2, \alpha^3+\alpha+1, \alpha^2+1, \alpha^3+\alpha, \alpha^2+\alpha+1, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1, \alpha^3+\alpha^2+1, \alpha^3+1\}$.

Let us assume the transform domain vector $\mathbf{U}$ is $\mathbf{U} = \{0, \alpha^2+\alpha, 0, \alpha^3+\alpha^2+1, 0, 0, 0, \alpha^2, 0, 0, 0, 0, 0, 0, 1\}$. Using 2.4 the time domain vector $\mathbf{u}$ is given by, $\mathbf{u} = \{\alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1, 0, 1, 1, \alpha^2, 0, 0, \alpha^2+1, \alpha^3+\alpha, \alpha^3+\alpha^2, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha, \alpha^3+\alpha^2+1, 0\}$

- **Rank**: Let $\mathbf{u} = (u_0, u_1, u_2, \cdots u_{n-1})$ be a $n-$length vector with $u_i \in \mathbb{F}_{q^m}$, $0 \le i \le n-1$. From the Galois theory we know that each $u_i \in \mathbb{F}_{q^m}$ can be expressed as $m-$ tuple

vector over the base field $\mathbb{F}_q$. Following this, the vector $\mathbf{u}$ can be written as $m \times n$ matrix that is obtained by expanding each element of $\mathbf{u}$ as an $m-$tuple over $\mathbb{F}_q$. Such a matrix is shown in (2.5).

$$\mathbf{u} = (u_0, u_1, u_2, \cdots u_{n-1}) = \begin{bmatrix} u_{0,0} & u_{0,1} & u_{0,2} & \cdots & u_{0,n-1} \\ u_{1,0} & u_{1,1} & u_{1,2} & \cdots & u_{1,n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ u_{m-1,0} & u_{m-1,1} & u_{m-1,2} & \cdots & u_{m-1,n-1} \end{bmatrix} \tag{2.5}$$

The rank of vector $\mathbf{u}$ (denoted as $R_q(\mathbf{u})$) is now defined as the rank of the above matrix over $\mathbb{F}_q$.If $R_q(\mathbf{u}) = m$ (full row rank), then we call the above matrix and equivalently vector $\mathbf{u}$ as full rank. For example, for the vector $\mathbf{u} = \{\alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1, 0, 1, 1, \alpha^2, 0, 0, \alpha^2+1, \alpha^3+\alpha, \alpha^3+\alpha^2, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha, \alpha^3+\alpha^2+1, 0\}$ with element in $\mathbb{F}_{2^4}$, the corresponding matrix over $\mathbb{F}_2$ is given by

$$\mathbf{u} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{2.6}$$

The rank of this matrix is considered as the rank of the vector $\mathbf{u}$.

2.3 Rank distance properties of QC codes

Dey and Rajan (2003) have given a GFFT domain description of Quasi-Cyclic (QC) codes. It was shown that for any $\ell | n$, $\ell-$QC codes are obtained by restricting the free transform components to β^ℓ invariant subspaces over the field $\mathbb{F}_{q^m}$. The class of arbitrary QC codes can be obtained using the IDFT equation and by choosing the free transform components $C_{j_1}, C_{j_2}, \cdots, C_{j_k}$ with indices $j_1, j_2, \cdots j_k$ from only one residue class modulo n/ℓ or from different residue classes related with conjugacy constraints. Furthermore, it was shown that for any $j \in [0, \frac{n}{m-1}]$, $C_{j_{n,m}}$ assume values from $\beta^{r_{m_j}}-$ invariant subspace.

For the class of minimal QC codes, it was shown that for any $j_1, j_2, \cdots, j_k \in [0, n-1]$, $A_{j_1}, A_{j_2}, \cdots, A_{j_{n-1}}$ should take values from minimal $\beta^{\ell}-$ invariant subspace and that $A_{j_1}, \cdots, A_{j_{n-1}}$ are related using linear invertible maps. Alternately this implies that the indices $j_1, \cdots, j_k$ should belong to the same cyclotomic coset modulo $\frac{n}{\ell}$.

The IDFT equation with $k-$ non-zero free transform components $\{C_{j_1}, C_{j_2}, \cdots C_{j_k}\}$, (and rest of the components are constrained to zero) is be given by,

$$c_i = (C_{j_1}\beta^{-ij_1} + \cdots + C_{j_k}\beta^{-ij_k}),\ i \in [0, n-1] \tag{2.7}$$

Let $\beta^{-j_1}, \cdots, \beta^{-j_k}$ be roots of polynomial $y(x)$ specified as,

$$y(x) = b_{e_j}x^{e_j} + b_{e_j-1}x^{e_j-1} + b_{e_j-2}x^{e_j-2} + \cdots + b_1 x + b_0 \tag{2.8}$$

Here $b_{\mathscr{I}} \in \mathbb{F}_q$ for all $0 \leq \mathscr{I} \leq e_j - 1$. Since for $1 \leq \mathscr{W} \leq k$, $\beta^{-j_{\mathscr{W}}}$ are roots of $y(x)$, from (2.8) we have

$$\beta^{-e_j j_{\mathscr{W}}} = -\tfrac{1}{b_{e_j}} \textstyle\sum_{i=0}^{e_j-1} b_i \beta^{-ij_{\mathscr{W}}} \quad 1 \leq \mathscr{W} \leq k \tag{2.9}$$

For $i = e_j + \mathfrak{v}$ with $0 \leq \mathfrak{v} \leq n - e_j - 1$, from (2.7) we have

$$c_{e_j+\mathfrak{v}} = (n \bmod q)^{-1}(C_{j_1}\beta^{-(e_j+\mathfrak{v})j_1} + \cdots + C_{j_k}\beta^{-(e_j+\mathfrak{v})j_k}) \tag{2.10}$$

Substituting for $\beta^{-e_j j_1}, \cdots, \beta^{-e_j j_{\mathscr{W}}}$ in (2.10) we get

$$c_{e_j+\mathfrak{v}} = \frac{C_{j_1}\beta^{-\mathfrak{v}j_1}\sum_{i=0}^{e_j-1} b_i'\beta^{-ij_1} + \cdots + C_{j_k}\beta^{-\mathfrak{v}j_k}\sum_{i=0}^{e_j-1} b_i'\beta^{-ij_k}}{(n \bmod q)} \tag{2.11}$$

Here $b_i' = b_i/b_{e_j}$. The above (2.11) can be simplified to

$$c_{e_j+\mathfrak{v}} = \frac{\sum_{i=0}^{e_j} b_i'(C_{j_1}\beta^{-(\mathfrak{v}+i)j_1} + \cdots + C_{j_k}\beta^{-\mathfrak{v}j_k}\beta^{-ij_k})}{(n \bmod q)} \tag{2.12}$$

From (2.7), the term in the brackets on the RHS of (2.12) is equal to c_i. Thus, (2.12) can be written as

$$c_{e_j+\mathfrak{v}} - \frac{1}{(n \bmod q)}\sum_{i=0}^{e_j-1} b_i' c_{i+\mathfrak{v}} = \frac{1}{(n \bmod q)}\sum_{i=0}^{e_j} b_i' c_{i+\mathfrak{v}} = 0 \tag{2.13}$$

Here $b'_{e_j} = (n \ mod \ q)$. From (2.13) we can infer that the codeword elements starting from index e_j can be expressed as linear combination of previous e_j elements. Thus, the rank of any codeword vector can be decided by the number of linearly independent elements in the set $\{c_0, c_1, \cdots, c_{e_j-1}\}$.

Lemma 2.3.1: Let $\mathbb{F}_{q^g} \subseteq \mathbb{F}_{q^m}$. If $\mathscr{X} = \{x_o, x_1, \cdots, x_{g-1}\}$ forms the trivial basis of $\mathbb{F}_{q^g}$ then there exists $\delta_1, \neq \delta_2 \neq \cdots \neq \delta_{m/g} \in \mathbb{F}_{q^m}$ and not in $\mathbb{F}_{q^g}$ such that $\{\delta_1 x_o, \delta_1 x_1, \cdots, \delta_1 x_{g-1}, \cdots, \delta_{m/g} x_o, \delta_{m/g} x_1, \cdots, \delta_{m/g} x_{g-1}\}$ forms the set of m linearly independent elements in $\mathbb{F}_{q^m}$.

Lemma 2.3.2: If β_1 is root of a minimal polynomial y_1 of degree r_1 and β_2 is a root of minimal polynomial y_2 of degree r_2, then the degree e_j of the minimal polynomial for which both β_1 and β_2 are roots is $e_j = r_1$; if $y_1 = y_2$ or $e_j = r_1 + r_2$; if $y_1 \neq y_2$.

2.3.1 Arbitrary (non-minimal) QC codes

We have employed the DFT description of $\ell-$QC codes described by Dey and Rajan (2003), to analyze the rank distance properties of (n, k) QC codes. The main result of this correspondence is that the rank of arbitrary QC code does not depend on the residue classes from which the indices are chosen and depends on the $q-$cyclotomic-coset modulo n to which the indices belong. This implies that irrespective of the residue classes or irrespective of the $q-$cyclotomic cosets modulo $\frac{n}{m}$ from which the indices are drawn, the rank distance properties depend on size of the cyclotomic coset to which these indices belong to. The rank distance properties of $\ell-$QC codes are described in the following Theorems.

Theorem 2.3.1: Let $\mathscr{C}$ be an arbitrary $\ell-$ QC code over $\mathbb{F}_{q^m}$ obtained using free transform components $\{C_{j_1}, C_{j_2}, \cdots, C_{j_k}\}$ with indices $j_1 \neq j_2 \neq j_3 \neq \cdots \neq j_{k-1}$ and other transform components constrained to zero.

1. If $j_1, j_2, \cdots j_k \in [j]_n$ then there exists $\mathscr{C}$ with $R_q(\mathscr{C}) = r_{j_1} - (k-1)g$. Here $g|S$ where

S is the separation between elements of $[j]_n$.

2. If $j_1 \in [j_1]_n, j_2 \in [j_2]_n, \cdots j_k \in [j_k]_n$, then $R_q(\mathscr{C}) = min(r_{j_1}, r_{j_2}, \cdots, r_{j_k})$.

Proof: **Case 1:** Without loss of generality let us consider the transform component indices $j_1, j_2 = j_1 q^{s_1}, \cdots, j_k = j_1 q^{s_{k-1}}$, that are chosen from the cyclotomic coset $[j_1]_n$ of size $_{j_1}$. The reciprocal polynomial $y_{j_1}(x)$ associated with $\beta^{[j_1]_n}$ will have representation as given in (2.8) with degree $e_j = r_{j_1}$ (Roman (2005)). Also, from (2.7) we have

$$c_i = (C_{j_1}\beta^{-ij_1} + \cdots + C_{j_1 q^{s_{k-1}}}\beta^{-ij_1 q^{s_{k-1}}}) \tag{2.14}$$

Since the first $e_j = r_{j_1}$ codeword elements determine the rank of the codeword, for $\mathfrak{v} = 0$ in 2.13 we have

$$\sum_{i=0}^{r_{j_1}} b_i^{'}(C_{j_1}\beta^{-ij_1} + \cdots + C_{j_1 q^{s_{k-1}}}\beta^{-ij_1 q^{s_{k-1}}}) = 0 \tag{2.15}$$

We are interested in determining codeword $\mathbf{c}$ that has $r_u < e_j$ number of linearly independent elements. To this extent let us consider a subfield $\mathbb{F}_{q^g}$ such that $g = gcd(r_{j_1}, S_1, \cdots, S_{k-1}, m)$. Here S_u represents the separation between j_1 and j_{1+u} for $0 \leq u \leq k-1$. From the definition of QC codes we see that $\mathscr{C}$ is QC if the free transform component assumes values from $\beta^{\ell}-$ invariant subspaces. From the definition of $\beta^{\ell}-$ invariant subspace we know that there exists a subspace with at least one element in the field $\mathbb{F}_{q^g}$ with $g|m$. Since C_{j_1} takes values from any $\beta^{\ell_{j_1}}-$ invariant subspace, let us consider $\mathbf{c}$ obtained from ${C_{j_1}}^{-1} = x \in \mathbb{F}_{q^g}$, then from (2.15) we have

$$\sum_{i=0}^{r_u} b_i^{'}\beta^{-ij_1} + \cdots + xC_{j_1 q^{s_{k-1}}}\left(\sum_{i=0}^{r_u} b_i^{'}\beta^{-ij_1}\right)^{q^{s_{k-1}}} = 0 \tag{2.16}$$

Since $x \in \mathbb{F}_{q^g}$, the element x can be expressed as $\sum_{i=0}^{g-1} d_i x_i$, with $d_i \in \mathbb{F}_q$. (2.16) can now be written as

$$\sum_{i=0}^{r_u} v_i\beta^{-ij_1} + \cdots + \left(\sum_{i=0}^{g-1} d_i x_i\right) C_{j_1 q^{s_{k-1}}}\left(\sum_{i=0}^{r_u} v_i\beta^{-ij_1}\right)^{q^{s_{k-1}}} = 0 \tag{2.17}$$

Let us define $\delta_w = C_{j_1 q^{s_w}}\left(\sum_{i=0}^{r_a} v_i\beta^{-ij_1}\right)^{q^{s_w}}$ for $w \in [1, k-1]$. (2.17) can now be written as

$$\sum_{i=0}^{r_u} v_i\beta^{-ij_1} + (\delta_1 + \cdots + \delta_{k-1})\sum_{i=0}^{g-1} d_i x_i = 0 \tag{2.18}$$

Following the definition of the QC code $C_{j_1}, C_{j_2}, \cdots, C_{j_k}$ take values independently from any $\beta^{ljz}-$ invariant subspace for $1 \leq \mathcal{Z} \leq k$, there exist a codeword $\mathbf{c}$ for $C_{j_1}, C_{j_2}, \cdots, C_{j_k}$ such

that $\delta_1 \neq \delta_2 \neq \cdots \neq \delta_k$ then the set $\{\delta_1 x_0, \cdots, \delta_1 x_{g-1}, \cdots, \delta_k x_0, \cdots, \delta_k x_{g-1},\}$ can form the set of kg linearly independent elements in the field $\mathbb{F}_{q^m}$ From the theory of Galois fields we know that if $\beta^{-j_1} \in \mathbb{F}_{q^{r_{j_1}}}$ then $\{\beta^{-j_1}, \beta^{-2j_1}, \cdots \beta^{-r_{j_1} j_1}\}$ forms the set of linearly independent elements in $\mathbb{F}_{q^{r_{j_1}}}$ and also in $\mathbb{F}_{q^m}$ since $r_{j_1}|m$. However according to (2.15) the summation should contain r_{j_1} terms, thus $r_u = r_{j_1} - kg = r_{j_1} - (k-1)g$. Since $r_{j_1|m}$ we have $r_{j_1} - (k-1)g < m$ linearly independent columns. Thus $R_q(\mathscr{C}) = r_{j_1} - (k-1)g$. If $r_{j_1} = m$ then $R_q(\mathscr{C}) = m - (k-1)g$.

Case 2: Since $j_1 \in [j_1]_n \neq j_2 \in [j_2]_n \neq \cdots, \neq j_k \in [j_k]_n$ the polynomial $y_j(x)$ that has representation as given in (2.8) has degree $e_j = r_{j_1} + r_{j_2} + \cdots + r_{j_k}$. From (2.7) we have

$$c_i = (C_{j_1}\beta^{-ij_1} + \cdots + C_{j_k}\beta^{-ij_k}),\ i \in [0, n-1] \tag{2.19}$$

Since the first e_j codeword elements determine the rank of the codeword, for $\mathfrak{v} = 0$ in (2.13) we have

$$\sum_{i=0}^{e_j} b_i^{'}(C_{j_1}\beta^{-ij_1} + \cdots + C_{j_1 q^{s_{k-1}}}\beta^{-ij_1 q^{s_{k-1}}}) = 0 \tag{2.20}$$

Similar to analysis given in case 1, we are interested in determining the existence of a codeword $\mathbf{c}$ that has $r_u < e_j$ number of linearly independent elements. In this case since $j_1, j_2, \cdots, j_k$ are all chosen from different $q-$cyclotomic cosets modulo n, we consider g such that $g|r_{j_1}, g|r_{j_2}, \cdots, g|r_{j_k}$. Let us consider $\mathbf{c}$ obtained from ${C_{j_1}}^{-1} = x \in \mathbb{F}_{q^g}$, then from (2.20) we have.

$$\sum_{i=0}^{r_u} b_i^{'}\beta^{-ij_1} + \cdots + xC_{j_k}\sum_{i=0}^{r_u} b_i^{'}\beta^{-ij_k} = 0 \tag{2.21}$$

Similar to the analysis given in case 1, let us define $\Delta_W = C_{j_W}\sum_{i=0}^{r_u} b_i^{'}\beta^{-ij_W}$ for $2 \leq W \leq k$. From the theory of cyclotomic cosets we know that the number of $q-$cyclotomic cosets modulo n are upper bounded by $\lfloor n/m \rfloor$. Since free transform component indices are chosen from k different $q-$ cyclotomic cosets modulo n, this implies that $k \leq n/m$. Following the analysis given in case 1, we see that $C_{j_1}, C_{j_2}, \cdots, C_{j_k}$ can take values independently from any $\beta^{lj_1}-$ invariant subspace, such that $\delta_1 \neq \cdots \neq \delta_k$ then the set $\left\{\delta_1 x_0, \cdots, \delta_1 x_{g-1}, \cdots, \delta_k x_0, \cdots, \delta_k x_{g-1}\right\}$ forms the set of kg linearly independent elements in the field $\mathbb{F}_{q^m}$. This set of linearly inde-

pendent elements can by extended to form the non-trivial basis of $\mathbb{F}_{q^m}$ by choosing the remaining $m - kg$ linearly independent elements in $\mathbb{F}_{q^m}$. Since $\beta^{-j_1} \in \mathbb{F}_{q^{r_{j_1}}} \subseteq \mathbb{F}_{q^m}$, the elements $\{\beta^{-j_1}, \cdots, \beta^{-(m-g)j_1}, \delta_1 x_0, \cdots, \delta_1 x_{g-1}, \cdots, \delta_k x_0, \cdots, \delta_k x_{g-1}\}$ can form the set of m linearly independent elements. According to (2.15) the summation should contain e_j terms, thus $r_u = e_j - (k-1)g = e_j - (m-1)g$. This implies that the codeword elements starting from location e_j can be expressed as linear combination of previous e_j elements. If $e_j < m$ then the rank of this codeword is e_j. This is indeed the minimum rank because for any other values of $C_{j_1}, C_{j_2}, \cdots, C_{j_k}$ the rank will be greater than e_j. Also, if $e_j \geq m$ then rank of $\mathbf{c}$ is m. Since $C_{j_1}, C_{j_2}, \cdots, C_{j_k}$ take values independently, there exists codewords with only one non-zero free transform domain component, in which case the rank of the corresponding codeword is given by r_{j_W} for $1 \leq W \leq k$. Thus in general $R_q(\mathscr{C}) = min(r_{j_1}, r_{j_2}, \cdots, r_{j_k}, m)$ At this point it can be noted that the above theorems are true for the case of cyclic codes which are $1-$ QC codes.

***Example* 2.3.1**: Let us consider the design of $3-$ QC code $\mathscr{C}$ over $\mathbb{F}_{2^4}$ obtained using free transform components C_1, C_4. The component indices $\{1,4\} \in (1)_{15,3}$ & $\in [1]_{15}$, and the separation between 1,4 is $S = 2$. If $\mathscr{C}$ is obtained from some β^3 invariant subspace with elements from field $\mathbb{F}_{2^g}$ for some $g = gcd(S, r_1, m) = 2$, we have $R_q(\mathscr{C}) = min(r_1, r_1 - (k-1)g) = min(4, 4 - (2-1).2) = 2$.

For $C_1 = 1$ and $C_4 \in \{1, \beta^3, \beta^6, \beta^9\beta^{12}\}$ we have rank 2 codewords listed below. By exhaustive computation it has been confirmed that no non-zero codeword exists having rank less than 2. Thus $R_q(\mathscr{C}) = 2$.

Example 2.3.2 Consider $(15, 2)$ $5-$QC odes over $\mathbb{F}_{2^4}$ obtained for free transform components C_1, C_6 taking values independently from β^5- invariant subspace-$\{0, 1, \beta^5, \beta^{10}\}$. Table 2.5 fives the list of all possible 15 non-zero codewords each having rank 4.

Example 2.3.3: Let us consider the design of $3-$ QC code $\mathscr{C}$ over $\mathbb{F}_{2^4}$ obtained using free transform components C_1, C_7. The component indices $\{1,7\} \in [1]_{15/3}$ & $\{1\} \in [1]_{15}$, $\{7\} \in [7]_{15}$. Here $r_1 = r_7 = 4$. If $\mathscr{C}$ is obtained from some β^3 invariant subspace we have $R_q(\mathscr{C}) = min(r_1, r_7, m) = 4$. Table 2.6 gives the list of all 36 codewords obtained by con-

Table 2.4: A few selected codewords of rank 2 in $\mathscr{C}$ corresponding to Example 2.3.1

$\begin{bmatrix} 0101100100011111 \\ 0111101011001000 \\ 0111101011001000 \\ 0000000000000000 \end{bmatrix}$	$\begin{bmatrix} 1001000111101010 \\ 0011110101100100 \\ 0000000000000000 \\ 1010110010001111 \end{bmatrix}$	$\begin{bmatrix} 1101011001000110 \\ 0000000000000000 \\ 1101011001000110 \\ 1100100011110100 \end{bmatrix}$
$\begin{bmatrix} 1110101100100010 \\ 1110101100100010 \\ 0110010001111010 \\ 1110101100100010 \end{bmatrix}$	$\begin{bmatrix} 0000000000000000 \\ 1011001000111101 \\ 1111010110010001 \\ 1111010110010001 \end{bmatrix}$	-

sidering the β^3- invariant subspace $\{0, 1, \beta^3, \beta^6, \beta^9\beta^{12}\}$. It can be seen that All non-zero codewords have rank 4.

2.3.2 Minimal QC codes

Dey and Rajan (2003) have shown that $(n, 1)$ $\ell-$ minimal QC code $\mathscr{C}$ can be obtained by restricting the free transform component C_j to minimal β^{ℓ_j} invariant subspace. For the case of $k > 1$ minimal QC codes are obtained by choosing the k transform components such that their indices belong to only one cyclotomic-coset modulo $\frac{n}{m}$. Further, it was shown that the free transform components with indices belonging to same q-cyclotomic coset modulo $\frac{n}{m}$ but different $q-$cyclotomic coset modulo n are related Dey and Rajan (2003).

Theorem 2.3.2: Let $\mathscr{C}$ be an $(n, 1)$ minimal $\ell-$ QC code over $\mathbb{F}_{q^m}$ obtained using C_j with $j \in [j]_n$ of size r_j, then $R_q(\mathscr{C}) = r_j$.

Proof: C_j takes value from β^{ℓ_j} invariant subspace. Since $j \in [j]_n$ of size r_j , the polynomial $y(x)$ associated with β^{-j} has representation as given in (2.8) with $e_j = r_j$. If $r_j < m$, then for $k = 1$ following the analysis given in Theorem 2.3.1, we have $R_q(\mathscr{C}) = r_j$. If $r_j > m$ then $R_q(\mathscr{C}) = m$.

Example 2.3.4: Consider $5-$ quasi-cyclic code of length $n = 15$ over $\mathbb{F}_{2^4}$. The transform component with indices from cyclotomic cosets $\{1, 2, 4, 8\}, \{5, 10\}, \{7, 11, 13, 14\}$ are related such that $C_5 = \alpha^{11}C_1^2$, $C_7 = \alpha^3 A_1$. Also $C_2 = C_1^2, C_4 = C_1^4, C_8, C_1^8, C_{10} = C_5^2, C_{14} = C_7^2, C_{13} =$

Table 2.5: List of codewords of rank 4 in $\mathscr{C}$ corresponding to Example 2.3.2

$\begin{bmatrix} 010001011000000 \\ 000010001011000 \\ 000010011010011 \\ 011010001001001 \end{bmatrix}$	$\begin{bmatrix} 100101001010010 \\ 010100101001010 \\ 000110001100011 \\ 011110111101111 \end{bmatrix}$	$\begin{bmatrix} 011000110001100 \\ 100011000110001 \\ 101111011110111 \\ 010010100101001 \end{bmatrix}$
$\begin{bmatrix} 111101111011110 \\ 110111101111011 \\ 101001010010100 \\ 001100011000110 \end{bmatrix}$	$\begin{bmatrix} 111101011001000 \\ 000111101011001 \\ 001111010110010 \\ 011110101100100 \end{bmatrix}$	$\begin{bmatrix} 011000010011010 \\ 010011000010011 \\ 001001011010001 \\ 000000010001011 \end{bmatrix}$
$\begin{bmatrix} 100101101000100 \\ 100100101101000 \\ 100000001000101 \\ 001100001001101 \end{bmatrix}$	$\begin{bmatrix} 000000100010110 \\ 110000000100010 \\ 100110000100110 \\ 010010110100010 \end{bmatrix}$	$\begin{bmatrix} 010001111010110 \\ 110010001111010 \\ 100100011110101 \\ 001000111101011 \end{bmatrix}$
$\begin{bmatrix} 110100110000100 \\ 100110100110000 \\ 100010010010110 \\ 010110000000100 \end{bmatrix}$	$\begin{bmatrix} 001001001011010 \\ 010001001001011 \\ 001011000000010 \\ 011010011000010 \end{bmatrix}$	$\begin{bmatrix} 101100000001000 \\ 000101100000001 \\ 001101001100001 \\ 000100100101101 \end{bmatrix}$
$\begin{bmatrix} 101100100011110 \\ 110101100100011 \\ 101011001000111 \\ 010110010001111 \end{bmatrix}$	$\begin{bmatrix} 001001101001100 \\ 100001001101001 \\ 101101000100100 \\ 001000101100000 \end{bmatrix}$	$\begin{bmatrix} 110100010010010 \\ 010110100010010 \\ 000100010110000 \\ 000100110100110 \end{bmatrix}$

$C_7^4, C_{11} = C_7^8$. Thus there is only one degree of freedom in terms of C_{j_1}. Also C_1 takes value from any α^5 invariant subspace. Let us consider the subspace $\{0, \alpha, \alpha^6, \alpha^{11}\}$. The codeword matrices obtained for different values of C_1 are shown in Table 2.7.

Theorem 2.3.3: Let $\mathscr{C}$ be an (n, k) minimal $\ell-$ QC code over $\mathbb{F}_{q^m}$ obtained using k free transform components with indices $\{j_1, j_2, \cdots, j_k\} \in [j_1]_{\frac{n}{m}}$, then $R_q(\mathscr{C}) = 1$.

Proof: Following the definition of minimal QC code, the elements of $[j_1]_{\frac{n}{m}}$ belonging to same cyclotomic coset modulo n are related with conjugacy constraints and the elements belonging to different $q-$ cyclotomic cosets are related appropriately. Since all the elements

Table 2.6: List of codewords in $\mathscr{C}$ corresponding to Example 2.3.3

$\begin{bmatrix} 000000000000000 \\ 000000000000000 \\ 000000000000000 \\ 000000000000000 \end{bmatrix}$	$\begin{bmatrix} 110001001101011 \\ 001101011110001 \\ 010011010111100 \\ 000100110101111 \end{bmatrix}$	$\begin{bmatrix} 000000111001110 \\ 001100010100011 \\ 000110100001011 \\ 011010100000101 \end{bmatrix}$
$\begin{bmatrix} 110001001101011 \\ 001101011110001 \\ 010011010111100 \\ 000100110101111 \end{bmatrix}$	$\begin{bmatrix} 001101011110001 \\ 011110001001101 \\ 010111100010011 \\ 110101111000100 \end{bmatrix}$	$\begin{bmatrix} 011110001001101 \\ 001001101011110 \\ 100010011010111 \\ 111000100110101 \end{bmatrix}$
$\begin{bmatrix} 001001101011110 \\ 101011110001001 \\ 011010111100010 \\ 100110101111000 \end{bmatrix}$	$\begin{bmatrix} 101011110001001 \\ 110001001101011 \\ 111100010011010 \\ 101111000100110 \end{bmatrix}$	$\begin{bmatrix} 111101011001000 \\ 000111101011001 \\ 001111010110010 \\ 011110101100100 \end{bmatrix}$
$\begin{bmatrix} 001100010100011 \\ 001010110101000 \\ 011100000001110 \\ 011010011001011 \end{bmatrix}$	$\begin{bmatrix} 110000000111001 \\ 011001100010100 \\ 011000110100001 \\ 101011010100000 \end{bmatrix}$	$\begin{bmatrix} 100011010000101 \\ 001110000000111 \\ 101101001100101 \\ 100110001010001 \end{bmatrix}$
$\begin{bmatrix} 110100110010110 \\ 101100011010000 \\ 010101101010000 \\ 111000000011100 \end{bmatrix}$	$\begin{bmatrix} 010110101000001 \\ 110110100110010 \\ 110011000101000 \\ 110001101000010 \end{bmatrix}$	$\begin{bmatrix} 000111101011001 \\ 001000111101011 \\ 010001111010110 \\ 100011110101100 \end{bmatrix}$
$\begin{bmatrix} 110110100110010 \\ 000101100011010 \\ 000010101101010 \\ 100111000000011 \end{bmatrix}$	$\begin{bmatrix} 001010110101000 \\ 010110110100110 \\ 000110011000101 \\ 010110001101000 \end{bmatrix}$	$\begin{bmatrix} 011001100010100 \\ 000001010110101 \\ 110011100000001 \\ 011011010011001 \end{bmatrix}$
$\begin{bmatrix} 001110000000111 \\ 100011001100010 \\ 001011000110100 \\ 000101011010100 \end{bmatrix}$	$\begin{bmatrix} 101100011010000 \\ 111001110000000 \\ 101101101001100 \\ 001100110001010 \end{bmatrix}$	$\begin{bmatrix} 001000111101011 \\ 011001000111101 \\ 110010001111010 \\ 100100011110101 \end{bmatrix}$
$\begin{bmatrix} 111001110000000 \\ 010100011001100 \\ 100001011000110 \\ 100000101011010 \end{bmatrix}$	$\begin{bmatrix} 000101100011010 \\ 000111001110000 \\ 100101101101001 \\ 010001100110001 \end{bmatrix}$	$\begin{bmatrix} 010110110100110 \\ 010000101100011 \\ 010000010101101 \\ 011100111000000 \end{bmatrix}$
$\begin{bmatrix} 000001010110101 \\ 110010110110100 \\ 101000110011000 \\ 000010110001101 \end{bmatrix}$	$\begin{bmatrix} 100011001100010 \\ 101000001010110 \\ 001110011100000 \\ 001011011010011 \end{bmatrix}$	$\begin{bmatrix} 011001000111101 \\ 101011001000111 \\ 010110010001111 \\ 101100100011110 \end{bmatrix}$
$\begin{bmatrix} 101000001010110 \\ 100110010110110 \\ 000101000110011 \\ 101000010110001 \end{bmatrix}$	$\begin{bmatrix} 010100011001100 \\ 110101000001010 \\ 000001110011100 \\ 011001011011010 \end{bmatrix}$	$\begin{bmatrix} 000111001110000 \\ 100010100011001 \\ 110100001011000 \\ 010100000101011 \end{bmatrix}$

$\begin{bmatrix} 010000101100011 \\ 000000111001110 \\ 001100101101101 \\ 001010001100110 \end{bmatrix}$	$\begin{bmatrix} 110010110110100 \\ 011010000101100 \\ 101010000010101 \\ 000011100111000 \end{bmatrix}$	$\begin{bmatrix} 101011001000111 \\ 111101011001000 \\ 111010110010001 \\ 110101100100011 \end{bmatrix}$
$\begin{bmatrix} 011010000101100 \\ 110000000111001 \\ 101001100101101 \\ 110001010001100 \end{bmatrix}$	$\begin{bmatrix} 100110010110110 \\ 100011010000101 \\ 101101010000010 \\ 000000011100111 \end{bmatrix}$	$\begin{bmatrix} 110101000001010 \\ 110100110010110 \\ 011000101000110 \\ 001101000010110 \end{bmatrix}$
$\begin{bmatrix} 100010100011001 \\ 010110101000001 \\ 100000001110011 \\ 010011001011011 \end{bmatrix}$		

Table 2.7: List of codewords of minimal 5−QC code $\mathscr{C}$corresponding to Example 2.3.4

$\begin{bmatrix} 000000000000000 \\ 000000000000000 \\ 000000000000000 \\ 000000000000000 \end{bmatrix}$	$\begin{bmatrix} 011110011101000 \\ 000000000000000 \\ 000000000000000 \\ 000000000000000 \end{bmatrix}$	$\begin{bmatrix} 010000111100111 \\ 000000000000000 \\ 000000000000000 \\ 000000000000000 \end{bmatrix}$
$\begin{bmatrix} 001110100000111 \\ 000000000000000 \\ 000000000000000 \\ 000000000000000 \end{bmatrix}$		

with indices belonging the same $q-$ cyclotomic coset modulo n are non-zero, from case 1 of Theorem 2.3.1 we see that $R_q(\mathscr{C}) = 1$.

Example 2.3.5: Consider (15, 1), minimal 5− quasi-cyclic code over $\mathbb{F}_{2^4}$. Let the free transform component be C_5 that take values from α^5 invariant subspace $\{0, \alpha, \alpha^6, \alpha^{11}\}$. The 3 non-zero codewords of rank 4 obtained for different values of C_5 are shown in Table 2.8.

Example 2.3.6: Consider length 24, 6−QC code over $\mathbb{F}_{5^2}$. The codewords are obtained with only one non-zero free transform component C_1 taking values from α^6- invariant subspace $\{0, 1, \alpha^6, \alpha^{12}, \alpha^{18}\}$. The non-zero codewords listed in Table 2.9 are observed to have rank 2.

Theorem 2.3.4: Let $\mathscr{C}$ be a QC code of length $n|q^m - 1$ over $\mathbb{F}_{q^m}$ such that the transform domain component $C_{jq^s} \in C_{[j]}$ is free and all other transform components are constrained to zero. Let $|[j]| = e_j$. Consider any non zero codeword $\mathbf{c} \in \mathscr{C}$

Table 2.8: List of codewords of code $\mathscr{C}$ corresponding to Example 2.3.5

$\begin{bmatrix} 000000000000000 \\ 000000000000000 \\ 000000000000000 \\ 000000000000000 \end{bmatrix}$	$\begin{bmatrix} 011110101100100 \\ 100011110101100 \\ 000111101011001 \\ 001111010110010 \end{bmatrix}$	$\begin{bmatrix} 001000111101011 \\ 011001000111101 \\ 110010001111010 \\ 100100011110101 \end{bmatrix}$
$\begin{bmatrix} 010110010001111 \\ 111010110010001 \\ 110101100100011 \\ 101011001000111 \end{bmatrix}$		

Table 2.9: List of 4 non-zero codewords of rank 2 corresponding to Example 2.3.6

$\begin{bmatrix} 1211403133204344102422 30 \\ 0242230121140313320434 41 \end{bmatrix}$	$\begin{bmatrix} 2422301211403133204344 10 \\ 0434410242230121140313 32 \end{bmatrix}$
$\begin{bmatrix} 4344102422301211403133 20 \\ 0313320434410242230121 14 \end{bmatrix}$	$\begin{bmatrix} 3133204344102422301211 40 \\ 0121140313320434410242 23 \end{bmatrix}$

$\mathbf{c} = \{c_0, c_1, \cdots c_{e_j-1}, \cdots, c_{ke_j}, \cdots, c_{(k+1)e_j-1} \cdots c_{n-1}\}$.

There are two cases:

(i). $e_j|n$: If $e_j|n$, then $\frac{n}{e_j}$ sets $\{\{c_0, c_1, \cdots, c_{e_j-1}\}, \{c_{e_j}, \cdots, c_{2e_j-1}\} \cdots, \{c_{n-e_j}, \cdots, c_{n-1}\}\}$ are linearly independent sets over $\mathbb{F}_q$. If these sets are viewed as $m \times e_j$ matrices over $\mathbb{F}_q$, then each matrix has $\mathbb{F}_q$ rank equal to e_j.

(ii). e_j does not divide n: If e_j does not divide n, then $\lfloor \frac{n}{e_j} \rfloor$ sets $\{\{c_0, c_1, \cdots, c_{e_j-1}\}, \{c_{e_j}, \cdots, c_{2e_j-1}\} \cdots, \{c_{n-\lfloor \frac{e_j}{n} \rfloor - e_j}, \cdots, c_{n-\lfloor \frac{e_j}{n} \rfloor - 1}\}\}$ are linearly independent sets over $\mathbb{F}_q$ and have rank e_j if these sets are viewed as $m \times e_j$ matrices over $\mathbb{F}_q$. The last set $\{c_{n-\lfloor \frac{e_j}{n} \rfloor}, \cdots, c_{n-1}\}\}$ consisting of $n - \lfloor \frac{e_j}{n} \rfloor$ terms is also linearly independent and has $\mathbb{F}_q$ rank equal to $n - \lfloor \frac{e_j}{n} \rfloor$ when viewed as $m \times n - \lfloor \frac{e_j}{n} \rfloor$ matrix over $\mathbb{F}_q$.

2.4 Puncturing of QC codes

In section 2.3 we have seen that for any codeword $\mathbf{c}$ the codeword elements from index e_j are a linear combination of first e_j elements. Hence the $(1 \times n)$ codeword vectors of an $\ell-$QC code $\mathscr{C}$ can be punctured to $(1 \times e_j)$ codeword vectors without altering their rank and struc-

tural relation .

Theorem 2.3.5: If $\mathscr{C}_p$ is rank$-m$ $(m, 1)$ punctured code obtained from $(n, 1)$ arbitrary QC code $\mathscr{C}$, then $\mathscr{C}_p$ is maximum distance separable (MDS) with $d = m$.

Proof: The transform domain description of $(n, 1)$ QC codes can be given by

$$c_i = C_{j_k}\beta^{-ij_k},\ i \in [0, n-1] \tag{2.22}$$

From Theorem 2.3.2, for $(n, 1)$ QC code $\mathscr{C}$ of rank m, the value of e_j is m resulting in punctured code $\mathscr{C}_p$ with $m \times m$ codeword matrices. Since rank is m, any two codewords in $\mathscr{C}_p$ will differ in m elements. In other words, the hamming distance d of $\mathscr{C}_p$ is equal to m. Also according to singleton bound $d \leq n - k + 1 = m - 1 + 1 = m$. Thus $\mathscr{C}_p$ is MDS.

2.5 Generator Matrix of rank-metric QC codes

From the transform domain description of cyclic codes, the codewords of QC codes are obtained using (2.3) can be expressed in vector form as

$$\{c_0, c_1, c_2, \cdots c_{n-1}\} = \left\{\sum_j C_j, \sum_j C_j\beta^{-1j}, \sum_j C_j\beta^{-2j}, \cdots, \sum_j C_j\beta^{-(n-1)j}\right\}, \tag{2.23}$$

Here $j \in \{j_1, j_2, \ldots, j_k\}$. Expressing (2.23) in the matrix form we have,

$$\{c_0, c_1, \cdots c_{n-1}\} = (C_{j_1}, C_{j_2}, \cdots C_{j_k})\begin{bmatrix} 1 & \beta^{-j_1} & \beta^{-2j_1} & \ldots & \beta^{-(n-1)j_1} \\ 1 & \beta^{-j_2} & \beta^{-2j_2} & \ldots & \beta^{-(n-1)j_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{-j_k} & \beta^{-2j_k} & \ldots & \beta^{-(n-1)j_k} \end{bmatrix} \tag{2.24}$$

The generator matrix of the code $\mathscr{C}$ is given by

$$\mathbf{G} = \begin{bmatrix} 1 & \beta^{-j_1} & \beta^{-2j_1} & \dots & \beta^{-(n-1)j_1} \\ 1 & \beta^{-j_2} & \beta^{-2j_2} & \dots & \beta^{-(n-1)j_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{-j_k} & \beta^{-2j_k} & \dots & \beta^{-(n-1)j_k} \end{bmatrix} \tag{2.25}$$

The codewords of $\mathscr{C}$ are now obtained by the multiplying the generator matrix with corresponding transform vector, represented as $\mathbf{c} = C \times \mathbf{G}$.

With $C = DFT(\mathbf{c}) = \{C_0, C_1, \cdots, C_{m-1}\}$ with $C_i \in \mathbb{F}_{q^m}$. Since punctured code $\mathscr{C}_p$ is obtained by deleting last $n - e_j$ columns from the codeword vectors, the generator matrix of the punctured code $\mathscr{C}_p$ is given by,

$$\mathbf{G}_p = \begin{bmatrix} 1 & \beta^{-j_1} & \beta^{-2j_1} & \dots & \beta^{-(e_j-1)j_1} \\ 1 & \beta^{-j_2} & \beta^{-2j_2} & \dots & \beta^{-(e_j-1)j_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{-j_k} & \beta^{-2j_k} & \dots & \beta^{-(e_j-1)j_k} \end{bmatrix} \tag{2.26}$$

2.6 Maximum Rank distance (MRD) codes

Following Theorems 2.3.1 and 2.3.2 we see that for full rank codes with transform domain indices chosen from different q-cyclotomic cosets of size m, the value of $e_j = km$. Since rank error correctability of code depends on its rank distance, full rank codes that are maximum rank distance separable are desirable for communication over channels inducing *crisscross* errors. According to Theorem 2.3.2, if k free transform components are chosen from same $q-$cyclotomic coset mod n then the codeword matrices are of dimension $e_j \times m$. If $e_j = m$, we obtain an (m, k) MRD codes with $m \times m$ codeword matrices with rank at least d_R. These codes are analogous to the Gabidulin codes (as is evident from the generator matrix description).

The generator matrix of a MRD code with $m \times m$ codewords is specified as

$$\mathbf{G}_p = \begin{bmatrix} 1 & \beta^{-j_1} & \beta^{-2j_1} & \dots & \beta^{-(m-1)j_1} \\ 1 & \beta^{-j_2} & \beta^{-2j_2} & \dots & \beta^{-(m-1)j_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{-j_k} & \beta^{-2j_k} & \dots & \beta^{-(m-1)j_k} \end{bmatrix} \tag{2.27}$$

2.7 Construction of parity check matrix

From Theorem 2.3.2 we see that if $\mathscr{C}$ and hence $\mathscr{C}_p$ is obtained using only one free transform component C_{jq^s} with $jq^s \in (j)_{n,m} \& jq^s \in [j]_n$ we have

$$\mathbf{c} = \frac{1}{n \bmod q} C_{jq^s} \left(1, \beta^{-jq^s}, \cdots, \beta^{-(n-1)jq^s}\right) \tag{2.28}$$

From (2.28), we see that $\forall\ C_{jq^s} \in \beta^{\ell j}-$invariant subspace of F_{q^m}, the term $\left(1, \beta^{-jq^s}, \beta^{-2jq^s}, \cdots, \beta^{-(n-1)jq^s}\right)$ on the RHS remain same and the ratio between two successive elements is β^{-jq^s}. Thus, if $\mathbf{c} \in \mathscr{C}$ is a codeword vector then

$$\begin{pmatrix} \beta^{-jq^s} & -1 & 0 & \cdots & 0 & 0 \\ 0 & \beta^{-jq^s} & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & \beta^{-jq^s} & -1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{2.29}$$

The codewords of (e_j, k) code $\mathscr{C}_p$ can be obtained by puncturing (n, k) code $\mathscr{C}$. Thus the above analysis holds good for codewords of $\mathscr{C}_p$. Since IDFT is a linear transform $\mathscr{C}$ can be obtained by linear combination of codewords of different $(n, 1)$ codes $\mathscr{C}^1, \mathscr{C}^2, \cdots, \mathscr{C}^k$ obtained using different free-transform domain components. For example let $\mathscr{C}^1$ be the $(n, 1)$ code obtained using only C_{j_1}. The codeword vectors can be written as $c_i = C_{j_1}\beta^{-ij_1}$. Similarly, let $\mathscr{C}^2$ be another $(n, 1)$ code obtained using only C_{j_2}, then $c_i = C_{j_2}\beta^{-2j}$. The code $\mathscr{C}$ obtained using free transform components C_{j_1} and C_{j_2} with $c_i = C_{j_1}\beta^{-1j} + C_{j_2}\beta^{-ij_2}$ $(0 \le i \le n-1)$ will have codewords that are linear combinations of codewords of $\mathscr{C}^1$ and $\mathscr{C}^2$.

$$c_i = C_{j_1}\beta^{-ij_1} + C_{j_1}\beta^{-ij_2} \quad \forall\ 0 \le i \le n-1 \tag{2.30}$$

Let $c_i^{'} = \beta^{-j_1} c_i - c_{i+1}, 0 \leq i \leq n-2;$. Substituting for c_i and c_{i+1} we get,

$$c_i^{'} = \beta^{-j_1}\left(C_{j_1}\beta^{-ij_1} + C_{j_2}\beta^{-ij_2}\right) - C_{j_1}\beta^{-(i+1)j_1} - C_2\beta^{-(i+1)j_2} \quad 0 \leq i \leq n-2; \tag{2.31}$$

Simplifying we get

$$c_i^{'} = C_{j_2}\beta^{-j_1-ij_2} - C_{j_2}\beta^{-(i+1)j_2}, 0 \leq i \leq n-2; \tag{2.32}$$

$$c_i^{'} = C_{j_2}\beta^{-ij_2}\left(\beta^{-j_1} - \beta^{-j_2}\right), 0 \leq i \leq n-2; \tag{2.33}$$

From equation 2.33 we infer that

$$\beta^{-j_2} c_i^{'} - c_{i+1}^{'} = 0, 0 \leq i \leq n-2; \tag{2.34}$$

Substituting for $c_i^{'} = \beta^{-j_1} c_i - c_{i+1}$ and $c_{i+1}^{'} = \beta^{-j_1} c_{i+1} - c_{i+2}$, we get

$$\beta^{-j_2}\left(\beta^{-j_1} c_i - c_{i+1}\right) - \left(\beta^{-j_1} c_i + 1 - c_{i+2}\right) = 0 \quad 0 \leq i \leq n-2; \tag{2.35}$$

$$\beta^{-j_2}\beta^{-j_1} c_i - \left(\beta^{-j_2} + \beta^{-j_1}\right) c_{i+1} + c_{i+2} = 0 \quad 0 \leq i \leq n-2; \tag{2.36}$$

Formulating in terms of matrix we get

$$\begin{bmatrix} \beta^{-j_2} & -1 & 0 & \cdots & 0 & 0 \\ 0 & \beta^{-j_2} & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0\cdots & \beta^{-j_2} & -1 \end{bmatrix} \begin{bmatrix} \beta^{-j_1} & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \beta^{-j_1} & -1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \beta^{-j_1} & -1 & 0 \\ 0 & 0 & 0 & 0\cdots & 0 & \beta^{-j_1} & -1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-2} \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{2.37}$$

The product of $n-2 \times n-1$ and $n-1 \times n$ matrix is given by equation 2.38 The $n-2 \times n$ matrix on the LHS can be considered as check matrix of code $\mathscr{C}_p$. In the above matrix it can

$$\begin{bmatrix} \beta^{-j_2-j_1} & -(\beta^{-j_2}+\beta^{-j_1}) & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & \beta^{-j_2-j_1} & -(\beta^{-j_2}+\beta^{-j_1}) & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \beta^{-j_2-j_1} & -(\beta^{-j_2}+\beta^{-j_1}) & 1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-2} \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{2.38}$$

be observed that the consecutive non-zero entries in each row are convolution of $\left\{\beta^{-2}, -1\right\}$ and $\left\{\beta^{-1}, -1\right\}$. In general, if quasi-cyclic code is designed by using k free transform components $\{j_1, j_2, j_3, \cdots, j_k\}$, then by mathematical induction, for k-free transform components 2.38 is given by,

$$\begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_k & 0 & \cdots & 0 & 0 \\ 0 & h_0 & h_1 & \cdots & h_{k-1} & h_k & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & h_{k-1} & h_k \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{2.39}$$

Where $\{h_0, h_1, \cdots, j_k\}$ are obtained from the convolution of $\left\{\beta^{-j_1}, -1\right\}, \left\{\beta^{-j_2}, -1\right\}, \left\{\beta^{-j_3}, -1\right\}, \cdots, \left\{\beta^{-j_k}, -1\right\}$. Thus any codeword $\{c_0, c_1, \cdots, c_{n-1}\} \in \mathscr{C}$ satisfies equation 2.39. From 2.39 the $n-k \times n$ check matrix is now given by

$$\begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_k & 0 & \cdots & 0 & 0 \\ 0 & h_0 & h_1 & \cdots & h_{k-1} & h_k & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & h_{k-1} & h_k \end{bmatrix} \tag{2.40}$$

As seen from 2.40 the check matrix is a band matrix with bandwidth $k+1$. For the case of punctured code $\mathscr{C}_p$ the structure of the check matrix remains same but the dimensions are reduced to $e_j - k \times e_j$.

2.7.1 Decoding in Rank metric

Let $\mathbf{R_x} = \mathbf{C} + \mathbf{E}$ be the received matrix with elements over $\mathbb{F}_q$. Equivalently, let $\mathbf{r} = \mathbf{c} + \mathbf{e}$ be the received vector with elements over $\mathbb{F}_{q^m}$. Decoding is realized by solving $\mathbf{H}r = \mathscr{S}$,

where $\mathscr{S}$ is $e_j \times 1$ syndrome vector. Since the check matrix is of dimension $n-k \times n$, there exists q^{km} solutions for the same syndrome. Solutions can be obtained using numerical methods or computer program based interative simulations. The decoder selects the solution with minimum rank as an estimate of the error vector. This estimated error vector is then used to obtain an estimate of the transmitted vector. It can be noted that the decoder gives correct solution only if it has the knowledge of the transform component indices used at the transmitter. The solution of the decoding algorithm is unique if $R_q(\mathbf{e}) \leq \lfloor \frac{m-1}{2} \rfloor$: Without loss of generality let $\boldsymbol{x_1}$, $\boldsymbol{x_2}$ be two solutions of rank $\leq \lfloor \frac{m-1}{2} \rfloor$ such that $\mathbf{H} \cdot (\boldsymbol{x_1}) = \mathbf{H} \cdot (\boldsymbol{x_2}) \implies \mathbf{H} \cdot (\boldsymbol{x_1} - \boldsymbol{x_2}) = \mathbf{H} \cdot \mathbf{d}_x = 0$. Since $\mathbf{H}$ is orthogonal to $\mathscr{C}$, this is true only if $\mathbf{d}_x = 0$ or $\mathbf{d}_x \in \mathscr{C}$ which means $R_q(\mathbf{d}_x) = m$. However, according to the rank inequality we have $R_q(\mathbf{d}_x) \leq R_q(\boldsymbol{x_1}) + R_q(\boldsymbol{x_2})$. Since $R_q(\boldsymbol{x_1}) = R_q(\boldsymbol{x_2}) \leq \lfloor \frac{m-1}{2} \rfloor$, $R_q(\mathbf{d}_x) \leq 2\lfloor \frac{m-1}{2} \rfloor < m$ contradicting the condition $R_q(\mathbf{d}_x) = m$. Thus, $\boldsymbol{x_1} = \boldsymbol{x_2}$, indicating that the proposed decoding algorithm gives unique solution if $R_q(\mathbf{e}) \leq \lfloor \frac{\mathbf{m-1}}{\mathbf{2}} \rfloor$. To illustrate the rank error correction ability of the proposed codes, let us consider a code designed over $\mathbb{F}_{2^3}$. Consider $(3, 1)$ punctured $1-$QC code over $\mathbb{F}_{2^3}$. Let the free transform component be C_1. Since $1 \in [1]_7$ with $r_1 = 3$, the codeword matrices will be of rank 3 over $\mathbb{F}_2$. Thus this code is rank $\lfloor \frac{3-1}{2} \rfloor = 1$ error correcting code. Let the Error matrix be

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

The above matrix corrupts all the codeword elements. However, since the rank of the error matrix is 1, the proposed decoder will uniquely find the error pattern. Table 2.10 gives the list of $q^{km} = 2^3$ solutions for error matrices and corresponding ranks. It can be observed that out of these 8 solutions, there is one unique solution of rank 1 which is the desired solution.

Table 2.10: List of all solutions corresponding to Example 2.7.1

$\begin{bmatrix} 000 \\ 110 \\ 100 \end{bmatrix}$	$\begin{bmatrix} 100 \\ 011 \\ 110 \end{bmatrix}$	$\begin{bmatrix} 010 \\ 000 \\ 001 \end{bmatrix}$	$\begin{bmatrix} 101 \\ 001 \\ 010 \end{bmatrix}$	$\begin{bmatrix} 110 \\ 101 \\ 011 \end{bmatrix}$	$\begin{bmatrix} 111 \\ 111 \\ 111 \end{bmatrix}$	$\begin{bmatrix} 011 \\ 010 \\ 101 \end{bmatrix}$	$\begin{bmatrix} 001 \\ 100 \\ 000 \end{bmatrix}$
2	3	2	3	2	1	3	2

2.8 Rank Distance Properties of (n, k) Cyclic Codes

Cyclic codes are a special class of arbitrary $\ell-$ QC codes with $\ell = 1$. The theorems presented for arbitrary QC codes hold good for cyclic codes. The only difference is that since, $\ell = 1$ the subspace from which the free transform domain components assume values will be β^1 invariant subspce which is the extension field $\mathbb{F}_{q^m}$ itself. Further, the transform components of different $q-$ cyclotomic cosets are unrelated. This implies that unlike QC codes (minimal) full rank (n, k) cyclic codes over $\mathbb{F}_{q^m}$ can be obtained if the indices are chosen form different $q-$ cyclotomic cosets. In Theorem 2.3.4 we the fundamental results pertaining to rank distance of cyclic codes.

Theorem 2.8.1: Let $\mathscr{C}$ be a Cyclic code obtained using free transform components $\{C_{j_1}, C_{j_2}, \cdots, C_{j_k}\}$ with indices $j_1 \neq j_2 \neq j_3 \neq \cdots \neq j_{k-1} \in [0, n-1]$ and other transform components constrained to zero.

1. If $j_1, j_2, \cdots j_k \in [j]_n$ then there exists $\mathscr{C}$ with $R_q(\mathscr{C}) = r_{j_1} - (k-1)g)$. Here $g|S$ where S is the separation between elements of $[j]_n$.

2. If $j_1 \in [j_1]_n, j_2 \in [j_2]_n, \cdots j_k \in [j_k]_n$, then $R_q(\mathscr{C}) = min(r_{j_1}, r_{j_2}, \cdots, r_{j_k})$.

The proof is similar to the one given in Theorem 2.3.1. However, the free transform components will assume values from the field $\mathbb{F}_{q^m}$. Also it can be noted that in case of arbitrary QC codes there can exist one QC code that is full rank despite chosing coefficients from same $q-$ cyclotomic coset. This is because the free transform components assume values from $\beta^\ell-$ invariant subspace. However, in case of cyclic codes the rank degrades.

Case1: Example 2.8.1: Let us consider the design of Cyclic code $\mathscr{C}$ over $\mathbb{F}_{3^2}$. The $3-$ cyclotomic cosets modulo 7 are given below: Let us consider $\mathscr{C}$ obtained using free transform

$[0] = \{0\}$	$[1] = \{1, 3\}$	$[2] = \{2, 6\}$	$[4] = \{4\}$	$[5] = \{5, 7\}$

components C_1, C_3. Following is the list of all 32 non-zero codewords of rank-1 obtained by considering the IDFT equation 2.28.

Table 2.11: Non-zero codewords of rank 1 in $\mathscr{C}$. corresponding to Example 2.8.1

$\begin{bmatrix} 0000000 \\ 22021101 \end{bmatrix}$	$\begin{bmatrix} 12202110 \\ 00000000 \end{bmatrix}$	$\begin{bmatrix} 02110122 \\ 01220211 \end{bmatrix}$	$\begin{bmatrix} 20211012 \\ 20211012 \end{bmatrix}$	$\begin{bmatrix} 22021101 \\ 22021101 \end{bmatrix}$	$\begin{bmatrix} 00000000 \\ 12202110 \end{bmatrix}$
$\begin{bmatrix} 01220211 \\ 00000000 \end{bmatrix}$	$\begin{bmatrix} 20211012 \\ 10122021 \end{bmatrix}$	$\begin{bmatrix} 10122021 \\ 00000000 \end{bmatrix}$	$\begin{bmatrix} 22021101 \\ 11012202 \end{bmatrix}$	$\begin{bmatrix} 12202110 \\ 12202110 \end{bmatrix}$	$\begin{bmatrix} 00000000 \\ 01220211 \end{bmatrix}$
$\begin{bmatrix} 00000000 \\ 10122021 \end{bmatrix}$	$\begin{bmatrix} 11012202 \\ 00000000 \end{bmatrix}$	$\begin{bmatrix} 12202110 \\ 21101220 \end{bmatrix}$	$\begin{bmatrix} 01220211 \\ 01220211 \end{bmatrix}$	$\begin{bmatrix} 01220211 \\ 02110122 \end{bmatrix}$	$\begin{bmatrix} 10122021 \\ 10122021 \end{bmatrix}$
$\begin{bmatrix} 00000000 \\ 11012202 \end{bmatrix}$	$\begin{bmatrix} 21101220 \\ 00000000 \end{bmatrix}$	$\begin{bmatrix} 02110122 \\ 00000000 \end{bmatrix}$	$\begin{bmatrix} 10122021 \\ 20211012 \end{bmatrix}$	$\begin{bmatrix} 11012202 \\ 11012202 \end{bmatrix}$	$\begin{bmatrix} 00000000 \\ 21101220 \end{bmatrix}$
$\begin{bmatrix} 21101220 \\ 21101220 \end{bmatrix}$	$\begin{bmatrix} 00000000 \\ 02110122 \end{bmatrix}$	$\begin{bmatrix} 20211012 \\ 00000000 \end{bmatrix}$	$\begin{bmatrix} 11012202 \\ 22021101 \end{bmatrix}$	$\begin{bmatrix} 21101220 \\ 12202110 \end{bmatrix}$	$\begin{bmatrix} 02110122 \\ 02110122 \end{bmatrix}$
$\begin{bmatrix} 00000000 \\ 20211012 \end{bmatrix}$	$\begin{bmatrix} 22021101 \\ 00000000 \end{bmatrix}$				

Case2: Example 2.8.2: Let us consider the design of length 8 Cyclic code $\mathscr{C}$ over $\mathbb{F}_{3^2}$. Let us consider $\mathscr{C}$ obtained using free transform components C_1, C_7. Table 2.12 gives the list of all 80 non-zero codewords obtained by making use of the IDFT equation (2.28) to define the time-domain components.

2.9 Conclusion

In this chapter, we have analyzed the rank distance properties of Quasi-Cyclic (QC) codes. The important class of cyclic codes are a sub-class of the class of QC codes. We have demonstrated that (n,k) full rank QC codes can be obtained for any value of $k \geq 1$. Further, we have shown that full rank QC codes can be obtained only in the case of arbitrary QC codes and that minimal QC codes are rank deficient. Additionally, we have stated and proved theorems that allow the determination of the exact rank of (n,k) QC codes. Using the underlying geometric progression property of $(n,1)$ codes we have constructed a parity check matrix for (n,k) QC codes (Arbitrary and Minimal). A check matrix based decoding strategy has been derived to correct rank errors. We have derived a class of rank distance codes called MRD-QC codes and provided generator matrix representation of these codes. These codes are observed to be analogous to MRD Gabidulin codes. In the concluding section of the chapter, we have pro-

Table 2.12: List of all non-zero codewords of rank 2 in $\mathscr{C}$. corresponding Example 2.8.2

$\begin{bmatrix}01120221\\11202210\end{bmatrix}$	$\begin{bmatrix}11202210\\12022101\end{bmatrix}$	$\begin{bmatrix}12022101\\20221011\end{bmatrix}$	$\begin{bmatrix}20221011\\02210112\end{bmatrix}$	$\begin{bmatrix}02210112\\22101120\end{bmatrix}$	$\begin{bmatrix}22101120\\21011202\end{bmatrix}$
$\begin{bmatrix}21011202\\10112022\end{bmatrix}$	$\begin{bmatrix}10112022\\01120221\end{bmatrix}$	$\begin{bmatrix}01220211\\10122021\end{bmatrix}$	$\begin{bmatrix}02010102\\21021201\end{bmatrix}$	$\begin{bmatrix}12122121\\22111122\end{bmatrix}$	$\begin{bmatrix}10212012\\00010002\end{bmatrix}$
$\begin{bmatrix}21111222\\12002100\end{bmatrix}$	$\begin{bmatrix}00100020\\02220111\end{bmatrix}$	$\begin{bmatrix}20021001\\01100220\end{bmatrix}$	$\begin{bmatrix}22201110\\20201010\end{bmatrix}$	$\begin{bmatrix}11002200\\11212212\end{bmatrix}$	$\begin{bmatrix}10122021\\11012202\end{bmatrix}$
$\begin{bmatrix}11212212\\22211112\end{bmatrix}$	$\begin{bmatrix}21021201\\20001000\end{bmatrix}$	$\begin{bmatrix}22111122\\01200210\end{bmatrix}$	$\begin{bmatrix}00010002\\10222011\end{bmatrix}$	$\begin{bmatrix}12002100\\00110022\end{bmatrix}$	$\begin{bmatrix}02220111\\02020101\end{bmatrix}$
$\begin{bmatrix}01100220\\21121221\end{bmatrix}$	$\begin{bmatrix}20201010\\12102120\end{bmatrix}$	$\begin{bmatrix}11012202\\21101220\end{bmatrix}$	$\begin{bmatrix}12102120\\02000100\end{bmatrix}$	$\begin{bmatrix}22211112\\00120021\end{bmatrix}$	$\begin{bmatrix}20001000\\11022201\end{bmatrix}$
$\begin{bmatrix}01200210\\20011002\end{bmatrix}$	$\begin{bmatrix}10222011\\10202010\end{bmatrix}$	$\begin{bmatrix}00110022\\12112122\end{bmatrix}$	$\begin{bmatrix}02020101\\01210212\end{bmatrix}$	$\begin{bmatrix}21121221\\22221111\end{bmatrix}$	$\begin{bmatrix}21101220\\02110122\end{bmatrix}$
$\begin{bmatrix}22221111\\10012002\end{bmatrix}$	$\begin{bmatrix}02000100\\11102220\end{bmatrix}$	$\begin{bmatrix}00120021\\22001100\end{bmatrix}$	$\begin{bmatrix}11022201\\01020201\end{bmatrix}$	$\begin{bmatrix}20011002\\21211212\end{bmatrix}$	$\begin{bmatrix}10202010\\20121021\end{bmatrix}$
$\begin{bmatrix}12112122\\12222111\end{bmatrix}$	$\begin{bmatrix}01210212\\00200010\end{bmatrix}$	$\begin{bmatrix}02110122\\20211012\end{bmatrix}$	$\begin{bmatrix}00200010\\01110222\end{bmatrix}$	$\begin{bmatrix}10012002\\02200110\end{bmatrix}$	$\begin{bmatrix}11102220\\10102020\end{bmatrix}$
$\begin{bmatrix}22001100\\22121121\end{bmatrix}$	$\begin{bmatrix}01020201\\12012102\end{bmatrix}$	$\begin{bmatrix}21211212\\11222211\end{bmatrix}$	$\begin{bmatrix}20121021\\00020001\end{bmatrix}$	$\begin{bmatrix}12222111\\21001200\end{bmatrix}$	$\begin{bmatrix}20211012\\22021101\end{bmatrix}$
$\begin{bmatrix}21001200\\00220011\end{bmatrix}$	$\begin{bmatrix}01110222\\01010202\end{bmatrix}$	$\begin{bmatrix}02200110\\12212112\end{bmatrix}$	$\begin{bmatrix}10102020\\21201210\end{bmatrix}$	$\begin{bmatrix}22121121\\11122221\end{bmatrix}$	$\begin{bmatrix}12012102\\10002000\end{bmatrix}$
$\begin{bmatrix}11222211\\02100120\end{bmatrix}$	$\begin{bmatrix}00020001\\20111022\end{bmatrix}$	$\begin{bmatrix}22021101\\12202110\end{bmatrix}$	$\begin{bmatrix}20111022\\20101020\end{bmatrix}$	$\begin{bmatrix}00220011\\21221211\end{bmatrix}$	$\begin{bmatrix}01010202\\02120121\end{bmatrix}$
$\begin{bmatrix}12212112\\11112222\end{bmatrix}$	$\begin{bmatrix}21201210\\01000200\end{bmatrix}$	$\begin{bmatrix}11122221\\00210012\end{bmatrix}$	$\begin{bmatrix}10002000\\22011102\end{bmatrix}$	$\begin{bmatrix}02100120\\10022001\end{bmatrix}$	$\begin{bmatrix}12202110\\01220211\end{bmatrix}$
$\begin{bmatrix}10022001\\12122121\end{bmatrix}$	$\begin{bmatrix}20101020\\10212012\end{bmatrix}$	$\begin{bmatrix}21221211\\21111222\end{bmatrix}$	$\begin{bmatrix}02120121\\00100020\end{bmatrix}$	$\begin{bmatrix}11112222\\20021001\end{bmatrix}$	$\begin{bmatrix}01000200\\22201110\end{bmatrix}$
$\begin{bmatrix}00210012\\11002200\end{bmatrix}$	$\begin{bmatrix}22011102\\02010102\end{bmatrix}$				

vided a description of rank distance properties of cyclic codes which follow from the more general results specified for Arbitrary QC codes. Applications of rank distance codes synthesized in this chapter for STBC designs, channel codes for storage systems and powerline communications have been discussed in chapters 4 and 5.

Chapter 3

Rank-metric Abelian codes

In chapter 2 we have provided construction of $n-$length rank metric codes from Quasi-Cyclic. The Galois field $\mathbb{F}_{q^m}$ over which the codes are designed is chosen such that the length n of the code is a divisor of $q^m - 1$. In this chapter we will consider rank distance properties of codes with length n such that n may or may not be a divisor of $q^m - 1$. Following Rajan and Siddiqi (1992), we have considered codes which are direct product of codes over cyclic groups. These are termed as Abelian codes i.e. codes constructed over finite Abelian groups. Any finite Abelian group G of order n can be expressed as a direct product of it's r cyclic subgroups, $C_0, C_1, \cdots C_{r-1}$ having orders $m_0, m_1, \cdots, m_{r-1}$ respectively. Then any element $g \in G$ can be represented as $g = (g_0)^{i_0}(g_1)^{i_1} \cdots (g_{r-1})^{i_{r-1}}$, where g_k is a generator of C_k, $k = 0, 1, \cdots, (r-1)$. Alternately, Abelian codes are considered as linear $q-$ ary codes of length n that are ideals in the Abelian group algebra of a finite Abelian group of order n Rajan and Siddiqi (1992). Cyclic codes are special class of Abelian codes, in that a cyclic code is an ideal over cyclic group, which is a special case of an Abelian group. Berman (1967) has shown that under certain conditions the general class of Abelian codes have better error correcting capabilities than the class of cyclic codes. Unlike cyclic and QC codes where the length n is constrained to satisfy the condition $n|q^{m-1}$, the length of Abelian codes is defined as $n = m_0 m_1 m_2 \cdots m_{r-1}$, where m_i is the order of the i^{th} cyclic groups C_i constituting the Abelian group and i varies from 0 to $r-1$. Additionally, the Galois field over Abelian codes are constructed can be subfield of the fields considered in the case of QC codes. This is because the field over which Abelian codes are constructed is decided by the exponent (e)

of the Abelian group. The exponent of the group is defined as the least common multiple of the orders of constituent cyclic groups (i.e, $\mathfrak{e} = lcm(m_0, m_1, \cdots, m_{r-1})$). The field $\mathbb{F}_{q^\tau}$ is considered such that $\mathfrak{e}|q^\tau - 1$. This can be illustrated by considering construction of length 9 rank metric code. For a length 9 rank metric code, construction from QC codes demand the Galois field to be $2^6 - 1$, as $9|2^6 - 1$. However, in case of Abelian codes the Galois field over which rank metric codes can be constructed is $\mathbb{F}_{2^2}$. This is because $9 = 3{\times}3$, $\mathfrak{e} = lcm(3, 3) = 3$ and $3|2^2 - 1$. Thus, by suitable choice of $m_0, m_1, \cdots, m_{r-1}$ greater flexibility in the codeword length n can be attained. A transform domain description of Abelian codes considering them as direct product of codes over cyclic groups has been provided in Rajan and Siddiqi (1992).

In Section 3.1 the transform domain description of Abelian codes and the preliminaries required to understand the construction of has been discussed. In Section 3.2 the construction of rank metric based Abelian codes has been discussed with relevant examples. In Section 3.4 we give the generator matrix representation of Abelian codes. Puncturing of Abelian codes without altering their rank has been discussed in Section 3.3. In section 3.5 we gave the details of parity check matrix construction for the rank metric Abelian codes and derive a check matrix based decoding algorithm. This discussion has been concluded with a summary of the obtained results and their significance. 3.6.

3.1 Abelian Codes in the Transform Domain

Let $m_0, \cdots, m_{r-1}$ be specified positive integers called mixed radixes and let $n = m_0 m_1 \cdots m_{r-1}$. According to the definition, any integer $i, 0 \leq i \leq (n-1)$ can be uniquely expressed as, (Rajan and Siddiqi (1992))

$$i = i_{r-1}(m_0 m_1 \cdots m_{r-2}) + i_{r-2}(m_0 m_1 \cdots m_{r-3}) \cdots i_2(m_0 m_1) + i_1 m_0 + i_0 \tag{3.1}$$

where $0 \leq i_k \leq m_k, k = 0, 1, 2, (r-1)$. If G is an Abelian group, then any element $g \in G$ can now be denoted by $g_{<i_{r-1} i_1, i_0>}$ or simply by g_i where $i =< i_{r-1} \cdots i_1, i_0 >$ in mixed radix representation. Throughout our discussion on Abelian Codes we assume that the length n of

the code is such that $gcd(n, q) = 1$.

3.1.1 Preliminaries

- **Cyclotomic Cosets**

  Consider the set $I = 0, 1, \cdots, n-1$. For any $j \in I$ and for any divisor d of $m\tau$, the q^d - cyclotomic coset of $j =< j_{r-1}, j_{r-2}, \cdots, j_0 >$ can now be written as.

  $[j] = \{< j_{r-1}q^t \ mod \ m_{r-1}, \cdots, j_1 q^t \ mod \ m_1, j_0 q^t \ mod \ m_0 >, t \geq 0\}$

  Example 3.1.1: Let us consider an example to illustrate these concepts. Consider an Abelian group G of length $n = 21$ expressed as $G = C_0 \times C_1$ with cardinality of $|C_0| = m_0 = 3$ and cardinality of $|C_1| = m_1 = 7$. The exponent of the Abelian group is $e = lcm(3, 7) = 21$. Let us consider $q = 2$. The smallest integer ψ such that $21|2^\psi - 1$ is $\psi = 6$. We will express $2^6 - 1$ as $2^{3\times 2} - 1$ and set $m = 3, \tau = 2$.The $2-$ cyclotomic cosets modulo 21 are listed in Table 3.1 below.

Table 3.1: List of $2-$ cyclotomic cosets modulo 21 corresponding to Example 3.1.1

{<0,0>}	{<1,0>,<2,0>,<4,0>}
{<3,0>,<6,0>,<5,0>}	{<1,1>,<2,2>,<4,1>}
{<1,2>,<2,1>,<4,2>}	{<3,1>,<6,2>,<5,1>}
{<3,3>,<6,1>,<5,2>}	{<0,1>,<0,2>}

  Example 3.1.2: Let us consider an Abelian group G of length $n = 9$ expressed as $G = C_0 \times C_1$ with cardinality of $|C_0| = m_0 = 3$ and cardinality of $|C_1| = m_1 = 3$. The exponent of the Abelian group is $e = lcm(3, 3) = 3$. Let us consider $q = 2$. The smallest integer ψ such that $3|2^\psi - 1$ is $\psi = 2$. We will express $2^2 - 1$ as $2^{2\times 1} - 1$ and set $m = 2, \tau = 1$.The $2-$ cyclotomic cosets modulo 9 are listed in Table 3.2 below.

Table 3.2: List of $2-$ cyclotomic cosets modulo 9 corresponding to Example 3.1.2

{<0,0>}	{<1,0>,<2,0>}
{<0,1>,<0,2>}	{<1,1>,<2,2>}
{<1,2>,<2,1>}	

- **Separation of $q-$ Cyclotomic Coset Coefficients**

  Let $[j]_n = \left\{j, jq, \cdots, jq^l, \cdots, jq^s, \cdots, jq^{l+s}, \cdots, jq^{r_j-1}\right\}$ be the $q-$ cyclotomic coset of integer j. We define the Separation between two elements

  $\left\{< j_{r-1}q^l \ mod \ m_{r-1}, \cdots, j_1 q^l \ mod \ m_1, j_0 q^l \ mod \ m_0 >\right\}$ and

  $\left\{< j_{r-1}q^{l+s} \ mod \ m_{r-1}, \cdots, j_1 q^{l+s} \ mod \ m_1, j_0 q^{l+s} \ mod \ m_0 >\right\}$ as the difference in powers of q associated with the elements i.e. Separation is $l + s - l = s$.

  For example consider the coset $[< 0, 1 >] = \{< 0, 1 >, < 0, 2 >\}$, the separation between elements $< 0, 2 >=< 0.2^1, 1.2^1 >$ and $< 0.2^0, 1.2^0 >$ is $1 - 0 = 1$.

- **Conjugacy classes and Miminal Polynomials**

  Since each integer $0 \leq i \leq n-1$ can be represented using mixed radices, and since $n = m_0 m_1 \cdots m_{r-1}$, any Galois field element can be uniquely decomposed into the product of elements with orders $m_0, m_1, \cdots, m_{r-1}$. This results in a one to one and onto mapping, that allows us to extend the definition of conjugacy class and minimal polynomials to the definition involving mixed radix representation. An example representation of $\mathbb{F}_{2^4}$ is given in Table 3.3. Here $n = q = 2^m = 4 - 1 = 3 \times 5$. Thus $m_0 = 3, m_1 = 5$. We have $\alpha_{m_0} = \alpha^5$ as the element in $\mathbb{F}_{2^4}$ with order 3 and $\alpha_{m_1} = \alpha^3$ as the elements in $\mathbb{F}_{2^4}$ with order 5. Table 3.4 below gives the $\mathbb{F}_{2^4}$ field elements and their corresponding decomposition. Thus the conjugacy class, associated minimal polynomial and corresponding reciprocal polynomials are given in Table 3.4 . Here z is variable whose roots are of the form $\alpha_{m_0}^{i_0} \alpha_{m_1}^{i_1}$.

- **DFT domain description of Abelian codes**

  The DFT over G with mixed radix number system as indexing scheme suitable for length n Abelian codes over $\mathbb{F}_{q^m}$ is obtained as follows. Let G be expressible as the direct product of r cyclic subgroups $C_0, C_1, \cdots, C_{r-1}$ having orders respectively $m_0, m_1, \cdots m_{r-1}$. Let e be the exponent of G. Let τ be the smallest integer such that $e|q^{m\tau} - 1$, where q is a power of a prime p. Let $\alpha_{m_0}, \alpha_{m_1}, \cdots, \alpha_{m_r-1}$ denote respectively primitive elements of order $m_0, m_1, \cdots, m_{r-1}$ in $\mathbb{F}_{q^{m\tau}}$. Then for a vector $\mathbf{c} = (c_0, c_1, \cdots c_{n-1}) \in \mathbf{F}_q^{n_m}$, where $gcd(n, q) = 1$ (i.e n and q are relatively prime),

Table 3.3: Galois field elements representation in terms of mixed radix notation

Representation in terms of α	Representation in terms of $\alpha_{m_0}, \alpha_{m_1}$
α^0	$(\alpha_{m_1})^0(\alpha_{m_0})^0$
α^1	$(\alpha_{m_1})^2(\alpha_{m_0})^2$
α^2	$(\alpha_{m_1})^4(\alpha_{m_0})^1$
α^3	$(\alpha_{m_1})^1(\alpha_{m_0})^0$
α^4	$(\alpha_{m_1})^3(\alpha_{m_0})^2$
α^5	$(\alpha_{m_1})^0(\alpha_{m_0})^1$
α^6	$(\alpha_{m_1})^2(\alpha_{m_0})^0$
α^7	$(\alpha_{m_1})^4(\alpha_{m_0})^2$
α^8	$(\alpha_{m_1})^1(\alpha_{m_0})^1$
α^9	$(\alpha_{m_1})^3(\alpha_{m_0})^0$
α^{10}	$(\alpha_{m_1})^0(\alpha_{m_0})^2$
α^{11}	$(\alpha_{m_1})^2(\alpha_{m_0})^1$
α^{12}	$(\alpha_{m_1})^4(\alpha_{m_0})^0$
α^{13}	$(\alpha_{m_1})^1(\alpha_{m_0})^2$
α^{14}	$(\alpha_{m_1})^3(\alpha_{m_0})^1$

Table 3.4: Conjugacy class and Minimal Polynomials over $\mathbb{F}_{2^4}$

Conjugacy Class	**Minimal Polynomial**	**Reciprocal Polynomial**
$\{(\alpha_{m_1})^0(\alpha_{m_0})^0\}$	$z+1$	$z+1$
$\left\{\begin{matrix}(\alpha_{m_1})^0(\alpha_{m_0})^0, (\alpha_{m_1})^4(\alpha_{m_0})^1, \\ (\alpha_{m_1})^3(\alpha_{m_0})^2, (\alpha_{m_1})^1(\alpha_{m_0})^1\end{matrix}\right\}$	z^4+z+1	z^4+z^3+1
$\left\{\begin{matrix}(\alpha_{m_1})^1(\alpha_{m_0})^0, (\alpha_{m_1})^2(\alpha_{m_0})^0, \\ (\alpha_{m_1})^4(\alpha_{m_0})^0, (\alpha_{m_1})^3(\alpha_{m_0})^0\end{matrix}\right\}$	$z^4+z^3+z^2+z+1$	$z^4+z^3+z^2+z+1$
$\{(\alpha_{m_1})^1(\alpha_{m_0})^1, (\alpha_{m_1})^1(\alpha_{m_0})^2\}$	y^2+y+1	y^2+y+1
$\left\{\begin{matrix}(\alpha_{m_1})^4(\alpha_{m_0})^2, \alpha_{m_1})^3(\alpha_{m_0})^1, \\ (\alpha_{m_1})^1(\alpha_{m_0})^2, (\alpha_{m_1})^2(\alpha_{m_0})^1\end{matrix}\right\}$	z^4+z^3+1	z^4+z+1

using the mixed radix representation the DFT domain description of Abelian codes is given as Rajan and Siddiqi (1992).

$$C_j = c_i \sum_{i_{r-1}=0}^{m_{r-1}-1} \cdots \sum_{i_1=0}^{m_1-1} \sum_{i_0=0}^{m_0-1} (\alpha_{m_0})^{i_0 j_0} (\alpha_{m_1})^{i_1 j_1} \cdots (\alpha_{m_{r-1}})^{i_{r-1} j_{r-1}} ; 0 \le i \le n-1 \qquad (3.2)$$

In the above equation α_{m_k} $0 \leq k \leq n-1$ represents the element of $\mathbb{F}_{q^{m\tau}}$ of order m_k^{th}..

In similar manner, the inverse DFT can be defined by

$$c_i = \frac{1}{n \; mod \; p} C_j \sum_{j_{r-1}=0}^{m_{r-1}-1} \cdots \sum_{j_1=0}^{m_1-1} \sum_{j_0=0}^{m_0-1} (\alpha_{m_0})^{-i_0 j_0} (\alpha_{m_1})^{-i_1 j_1} \cdots (\alpha_{m_{r-1}})^{-i_{r-1} j_{r-1}} ; 0 \leq j \leq n-1 \tag{3.3}$$

- **Character representation** An $\mathbb{F}_{q^m}$ character Ψ of Abelian group G is an homomorphism of G into the group of e^{th} roots of unity in $\mathbb{F}_{q^m}$. The group $G^{'}$ of all $\mathbb{F}_{q^m}$ characters is isomorphic to G. In this work we will denote $\Psi_x(y)$ as $\Psi(x, y)$ and consider it as a map $\Psi : G \times G \rightarrow \mathbb{F}_{q^m}$. With this consideration let $\Psi : G \times G \rightarrow \mathbb{F}_{q^m}$ be defined as

$$\Psi(x, y) = \Psi(< i_{r-1,\cdots,i_1,i_0} >, < j_{r-1}, \cdots, j_1, j_0 >) = (\alpha_{m_r-1})^{i_r-1 j_r-1} \cdots (\alpha_{m_0})^{i_0 j_0} \rightarrow \mathbb{F}_{q^m} \tag{3.4}$$

- **Discrete Fourier transform using character representation (DFT)**

  Using the character representation Eq. 3.2 can be rewritten as

$$C_{<j_{r-1}q^s,\cdots,j_1 q^s, j_0 q^s>} = \frac{1}{|G|} \sum_{y \in G} \Psi\left(< i_{r-1}, \cdots, i_1, i_0 >, < j_{r-1}, \cdots, j_1, j_0 >\right) c_{<i_{r-1},\cdots,i_1,i_0>} \tag{3.5}$$

  Similarly, IGFFT is given by 3.6.

$$c_{<i_{r-1},\cdots,i_1,i_0>} = \frac{1}{|G|} \sum_{y \in G} \Psi\left(< i_{r-1}, \cdots, i_1, i_0 >, < j_{r-1}, \cdots, j_1, j_0 >\right)^{-1} C_{<j_{r-1}q^s,\cdots,j_1 q^s, j_0 q^s>} \tag{3.6}$$

In our study, we consider Abelian codes over $\mathbb{F}_{q^m}$ such that $e|q^m - 1$. The condition $e|q^m - 1$ ensures that $A_j \in \mathbb{F}_{q^m}$ and that every q^m -cyclotomic coset modulo e is a singleton set.

3.2 Rank distance properties of Abelian codes

The IDFT equation with $k-$ non-zero free transform components $\{C_{j_1}, C_{j_2}, \cdots C_{j_k}\}$,(and rest of the components constrained to zero) is be given by,

$$c_i = C_{<j_{11}, j_{12}, \cdots, j_{1r}>}\Psi(i, j_1)^{-1} + \cdots + C_{<j_{k1}, j_{k2}, \cdots, j_{kr}>}\Psi(i, j_k)^{-1} \tag{3.7}$$

Let $\Psi(i, j_1)^{-1}, \cdots, \Psi(i, j_k)^{-1}$ be roots of polynomial $y(x)$ specified as

$$y(x) = b_{e_j}x^{e_j} + b_{e_j-1}x^{e_j-1} + b_{e_j-2}x^{e_j-2} + \cdots + b_1x + b_0 \tag{3.8}$$

Here $b_{\mathscr{I}} \in \mathbb{F}_q$ for all $0 \leq \mathscr{I} \leq e_j - 1$. Since for $1 \leq \mathscr{W} \leq k$, , $\Psi(i, j_{\mathscr{W}})^{-1}$ are roots of $y(x)$, from Eq. (3.8) we have

$$\Psi(i, j_{\mathscr{W}})^{-1} = -\frac{1}{b_{e_j}} \sum_{i=0}^{e_j-1} b_i\Psi(i, j_{\mathscr{W}})^{-1} \quad 1 \leq \mathscr{W} \leq k \tag{3.9}$$

For $i = e_j + \mathfrak{v}$ with $0 \leq \mathfrak{v} \leq n - e_j - 1$, from Eq. (2.7) we have

$$c_{e_j+\mathfrak{v}} = (n \bmod q)^{-1}(C_{j_1}\Psi(e_j + \mathfrak{v}, j_1)^{-1} + \cdots + C_{j_k}\Psi(e_j + \mathfrak{v}, j_k)^{-1}) \tag{3.10}$$

Substituting for $\alpha^{-e_j j_1}, \cdots, \alpha^{-e_j j_{\mathscr{W}}}$ in Eq. (3.10) and considering $b_i^{'} = b_i/b_{e_j}$. The above Eq. (3.10) can be simplified to

$$c_{e_j+\mathfrak{v}} = \frac{\sum_{i=0}^{e_j} b_i^{'}(C_{j_1}\Psi(i + \mathfrak{v}, j_1)^{-1} + \cdots + C_{j_k}\Psi(i + \mathfrak{v}, j_k)^{-1})}{(n \bmod q)} \tag{3.11}$$

From Eq. (3.7), the term in the brackets on the RHS of Eq. (3.11) is equal to c_i. Thus, Eq. (3.11) can be written as

$$c_{e_j+\mathfrak{v}} - \frac{1}{(n \bmod q)} \sum_{i=0}^{e_j-1} b_i^{'}c_{i+\mathfrak{v}} = \frac{1}{(n \bmod q)} \sum_{i=0}^{e_j} b_i^{'}c_{i+\mathfrak{v}} = 0 \tag{3.12}$$

Here $b_{e_j}^{'} = (n \bmod q)$. From Eq. (3.12) we can infer that the codeword elements starting from

index e_j can be expressed as linear combination of previous e_j elements. Thus, the rank of any codeword vector can be decided by the number of linearly independent elements in the set $\{c_0, c_1, \cdots, c_{e_j-1}\}$.

Theorem 3.2.1: Let $\mathscr{C}$ be an Abelian code obtained using free transform components $\{C_{<j_{11},j_{12},\cdots,j_{1r}>}, \cdots, C_{<j_{21},j_{22},\cdots,j_{2r}>}, \cdots, C_{<j_{k1},j_{k2},\cdots,j_{kr}>}\}$ with indices $< j_{11}, j_{12}, \cdots, j_{1r} >, < j_{21}, j_{22}, \cdots, j_{2r} >, \cdots, < j_{k1}, j_{k2}, \cdots, j_{kr} >$ set free and other transform components constrained to zero.

1. If $< j_{11}, j_{12}, \cdots, j_{1r} >, < j_{21}, j_{22}, \cdots, j_{2r} >, \cdots < j_{k1}, j_{k2}, \cdots, j_{kr} > \in [j_1]_n$ then $R_q(\mathscr{C}) = r_{<j_{11},j_{12},\cdots,j_{1r}>} - (k-1)g$. Here $g|S$ where S is the separation between elements of $[j]_n$.

2. If $< j_{11}, j_{12}, \cdots, j_{1r} > \in [< j_{11}, j_{12}, \cdots, j_{1r} >]_n, < j_{21}, \cdots, j_{2r} > \in [< j_{21}, j_{22}, \cdots, j_{2r} >]_n, \cdots < j_{k1}, j_{k2}, \cdots, j_{kr} > \in [< j_{k1}, j_{k2}, \cdots, j_{kr} >]_n$, then $R_q(\mathscr{C}) = min(r_{<j_{11},j_{12},\cdots,j_{1r}>}, r_{<j_{21},j_{22},\cdots,j_{2r}>}, \cdots, r_{<j_{k1},j_{k2},\cdots,j_{kr}>})$.

Proof: **Case 1:** Without loss of generality let us consider the transform component indices $< j_{11}, j_{12}, \cdots, j_{1r} >=< j_{11}, j_{12}, \cdots, j_{1r} >, < j_{21}, j_{22}, \cdots, j_{2r} >=< j_{11}q^{s_1}, j_{12}q^{s_1}, \cdots, j_{1r}q^{s_1} >, \cdots, < j_{k1}, j_{k2}, \cdots, j_{kr} >=< j_{11}q^{s_{k-1}}, j_{12}q^{s_{k-1}}, \cdots, j_{1r}q^{s_{k-1}} >$, that are chosen from the cyclotomic coset $[< j_{11}, j_{12}, \cdots, j_{1r} >]_n$ of size r_{j_1}. The reciprocal polynomial $y_{<j_{11},j_{12},\cdots,j_{1r}>}(x)$ associated with $\alpha_{m_0}^{j_{11}}\alpha_{m_1}^{j_{12}}\cdots\alpha_{m_{r-1}}^{j_{1r}}$ will have representation as given in Eq. (2.8) with degree $e_j = r_{j_1}$ Roman (2005). Also, from (3.6) we have

$$c_i = C_{<j_{11},j_{12},\cdots,j_{1r}>}\Psi(i, j_1)^{-1} + \cdots + C_{<j_{11}q^{s_{k-1}},j_{12}q^{s_{k-1}},\cdots,j_{1r}q^{s_{k-1}}>}\Psi(i, j_1q^{s_{k-1}})^{-1} \tag{3.13}$$

Since the first $e_j = r_{<j_{11},j_{12},\cdots,j_{1r}>}$ codeword elements determine the rank of the codeword, for $\mathfrak{v} = 0$ in Eq. 3.12 we have

$$\sum_{i=0}^{r_{j_1}} b_i'(C_{<j_{11},j_{12},\cdots,j_{1r}>}\Psi(i, j_1)^{-1} + \cdots + C_{<j_{11}q^{s_{k-1}},j_{12}q^{s_{k-1}},\cdots,j_{1r}q^{s_{k-1}}>}\Psi(i, j_1q^{s_{k-1}})^{-1}) = 0 \tag{3.14}$$

We are interested in determining codeword **c** that has $r_c < e_j$ number of linearly independent

elements. To this extent let us consider a subfield $\mathbb{F}_{q^g}$ such that

$g = gcd(r_{<j_{11},j_{12},\cdots,j_{1r}>}, S_1, S_2, \cdots, S_{k-1}, m)$. Here S_u represents the separation between $< j_{11}, j_{12}, \cdots, j_{1r} >$ and $< j_{11+u1}, j_{12+u2}, \cdots, j_{1r+ur} >$ for $0 \leq u \leq k-1$. From the DFT description of Abelian codes we see that the free transform component assumes values from the field $\mathbb{F}_{q^{m\tau}}$. We know that there exists at least one element in the field $\mathbb{F}_{q^g}$ with $g|m\tau$. Let us consider $\mathbf{c}$ obtained from $C_{<j_{11},j_{12},\cdots,j_{1r}>}{}^{-1} = x \in \mathbb{F}_{q^g}$, then from Eq. (3.14) we have

$$\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1)^{-1} + \cdots + xC_{j_1 q^{s_{k-1}}} \left(\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1 q^{s_{k-1}})^{-1} \right) = 0 \tag{3.15}$$

$$\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1)^{-1} + \cdots + xC_{j_1 q^{s_{k-1}}} \left(\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1)^{-1} \right)^{q^{s_{k-1}}} = 0 \tag{3.16}$$

Since $x \in \mathbb{F}_{q^g}$ as seen earlier the element x can be expressed as $\sum_{i=0}^{g-1} d_i x_i$, with $d_i \in \mathbb{F}_q$. Eq. (3.15) can now be written as

$$\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1)^{-1} + \cdots + \left(\sum_{i=0}^{g-1} d_i x_i \right) C_{<j_{11},j_{12},\cdots,j_{1r}>q^{s_{k-1}}} \left(\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1)^{-1} \right)^{q^{s_{k-1}}} = 0 \tag{3.17}$$

Let us define $\delta_w = C_{<j_{11},j_{12},\cdots,j_{1r}>q^{s_{k-1}}} \left(\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1)^{-1} \right)^{q^{s_{w-1}}}$ for $w \in [1, k-1]$. Eq. (3.17) can now be written as

$$\sum_{i=0}^{r_u} b_i^{'} \Psi(i, j_1)^{-1} + (\delta_1 + \cdots + \delta_{k-1}) \sum_{i=0}^{g-1} d_i x_i = 0 \tag{3.18}$$

Following the definition of the Abelian code $C_{<j_{11},j_{12},\cdots,j_{1r}>}, C_{<j_{21},j_{22},\cdots,j_{2r}>}, \cdots, C_{<j_{k1},j_{k2},\cdots,j_{kr}>}$ take values independently from $\mathbb{F}_{q^{m\tau}}$, there exist a codeword $\mathbf{c}$ for $C_{j_1}, C_{j_2}, \cdots, C_{j_k}$ such that $\delta_1 \neq \delta_2 \neq \cdots \neq \delta_k$ then the set $\{\delta_1 x_0, \cdots, \delta_1 x_{g-1}, \cdots, \delta_k x_0, \cdots, \delta_k x_{g-1}, \}$ can form the set of kg linearly independent elements in the field $\mathbb{F}_{q^m}$ From the theory of Galois fields we know that if $\alpha^{-j_1} \in \mathbb{F}_{q^{r_{j_1}}}$ then $\{\alpha^{-j_1}, \alpha^{-2j_1}, \cdots \alpha^{-r_{j_1} j_1}\}$ forms the set of linearly independent elements in $\mathbb{F}_{q^{r_{j_1}}}$ and also in $\mathbb{F}_{q^m}$ since $r_{j_1}|m$. However according to Eq. (3.14) the summation should contain r_{j_1} terms, thus $r_u = r_{j_1} - kg = r_{j_1} - (k-1)g$. Since $r_{j_1|m}$ we have $r_{j_1} - (k-1)g < m$ linearly independent columns. Thus $R_q(\mathscr{C}) = r_{j_1} - (k-1)g$. If $r_{j_1} = m$ then $R_q(\mathscr{C}) = m - (k-1)g$.

Case 2: Since $< j_{11}, j_{12}, \cdots, j_{1r} > \in [< j_{11}, j_{12}, \cdots, j_{1r} >]_n \neq < j_{21}, j_{22}, \cdots, j_{2r} > \in [< j_{21}, j_{22}, \cdots, j_{2r} >]_n \neq \cdots, \neq < j_{k1}, j_{k2}, \cdots, j_{kr} > \in [< j_{k1}, j_{k2}, \cdots, j_{kr} >]_n$ the polynomial

$y_j(x)$ that has representation as given Eq. (3.8) has degree $e_j = r_{<j_{11},j_{12},\cdots,j_{1r}>} + r_{<j_{21},j_{22},\cdots,j_{2r}>} + \cdots + r_{<j_{k1},j_{k2},\cdots,j_{kr}>}$. From Eq. (3.7) we have

$$c_i = C_{<j_{11},j_{12},\cdots,j_{1r}>}\Psi(i,j_1)^{-1} + \cdots + C_{<j_{11}q^{s_{k-1}},j_{12}q^{s_{k-1}},\cdots,j_{1r}q^{s_{k-1}}>}\Psi(i,j_k)^{-1} \tag{3.19}$$

Since the first e_j codeword elements determine the rank of the codeword, for $\mathfrak{v} = 0$ in Eq. 3.12 we have

$$\sum_{i=0}^{e_j} b_i'(C_{<j_{11},j_{12},\cdots,j_{1r}>}\Psi(i,j_1)^{-1} + \cdots + C_{<j_{11}q^{s_{k-1}},j_{12}q^{s_{k-1}},\cdots,j_{1r}q^{s_{k-1}}>}\Psi(i,j_k)^{-1}) = 0 \tag{3.20}$$

Similar to analysis given in case 1, we are interested in determining the existence of a codeword $\mathbf{c}$ that has $r_u < e_j$ number of linearly independent elements. In this case since $< j_{11}, j_{12}, \cdots, j_{1r} >, < j_{21}, j_{22}, \cdots, j_{2r} >, \cdots, < j_{k1}, j_{k2}, \cdots, j_{kr} >$ are all chosen from different $q-$cyclotomic cosets modulo n, we consider g such that $g|r_{<j_{11},j_{12},\cdots,j_{1r}>}, g|r_{<j_{21},j_{22},\cdots,j_{2r}>}, \cdots, g|r_{<j_{k1},j_{k2},\cdots,j_{kr}>}$. Let us consider $\mathbf{c}$ obtained from $C_{<j_{11},j_{12},\cdots,j_{1r}>}{}^{-1} = x \in \mathbb{F}_{q^g}$, then from Eq. (3.20) we have

$$\sum_{i=0}^{r_u} b_i'\Psi(i,j_1)^{-1} + \cdots + xC_{<j_{k1},j_{k2},\cdots,j_{kr}>}\sum_{i=0}^{r_u} b_i'\Psi(i,j_k)^{-1} = 0 \tag{3.21}$$

Similar to the analysis given in case 1, let us define $\Delta_W = C_{j_W}\sum_{i=0}^{r_u} b_i'\Psi(i,j_w)^{-1}$ for $2 \le w \le k$. From the theory of cyclotomic coset we know that the number of $q-$cyclotomic cosets modulo n are upper bounded by $\lfloor n/m \rfloor$. Since free transform component indices are chosen from k different $q-$ cyclotomic cosets modulo n, this implies that $k \le n/m$. Following the analysis given in case 1, we see that $C_{<j_{11},j_{12},\cdots,j_{1r}>}, C_{<j_{21},j_{22},\cdots,j_{2r}>}, \cdots, C_{<j_{k1},j_{k2},\cdots,j_{kr}>}$ can take values independently from $\mathbb{F}_{q^{m\tau}}$ then the set $\left\{\delta_1 x_0, \cdots, \delta_1 x_{g-1}, \cdots, \delta_k x_0, \cdots, \delta_k x_{g-1}\right\}$ forms the set of kg linearly independent elements in the field $\mathbb{F}_{q^m}$. This set of linearly independent elements can be extended to form the non-trivial basis of $\mathbb{F}_{q^m}$ by choosing the remaining $m - kg$ linearly independent elements in $\mathbb{F}_{q^m}$. Since $\Psi(i,j_w)^{-1} \in \mathbb{F}_{q^{r_{<j_{11},j_{12},\cdots,j_{1r}>}}} \subseteq \mathbb{F}_{q^m}$, the elements $\{\Psi(i,j_1)^{-1}, \cdots, \{\Psi((m-g)i,j_1)^{-1}, \delta_1 x_0, \cdots, \delta_1 x_{g-1}, \cdots, \delta_k x_0, \cdots, \delta_k x_{g-1}\}$ can form the set of m linearly independent elements. According to Eq. (3.14) the summation should contain e_j terms, thus $r_u = e_j - (k-1)g = e_j - (m-1)g$. This implies that the codeword elements

starting from location e_j can be expressed as linear combination of previous e_j elements. If $e_j < m$ then the rank of this codeword is e_j. This is indeed the minimum rank because for any other values of $C_{<j_{11},j_{12},\cdots,j_{1r}>}, C_{<j_{21},j_{22},\cdots,j_{2r}>}, \cdots, C_{<j_{k1},j_{k2},\cdots,j_{kr}>}$ the rank will be greater than e_j. Also, if $e_j \geq m$ then rank of $\mathbf{c}$ is m. Since $C_{<j_{11},j_{12},\cdots,j_{1r}>}, C_{<j_{21},j_{22},\cdots,j_{2r}>}, \cdots, C_{<j_{k1},j_{k2},\cdots,j_{kr}>}$ take values independently, there exists codewords with only one non-zero free transform domain component, in which case the rank of the corresponding codeword is given by $r_{<j_{w1},j_{w2},\cdots,j_{wr}>}$ for $1 \leq w \leq k$. Thus in general

$R_q(\mathscr{C}) = min(r_{<j_{11},j_{12},\cdots,j_{1r}>}, r_{<j_{11},j_{12},\cdots,j_{1r}>}, \cdots, r_{<j_{11},j_{12},\cdots,j_{1r}>}, m)$.

Case 1: Example 3.2.1. Let the free transform components $C_{<1,0>}, C_{<2,0>}$. The component indices $\{< 1,0 >\} \in [< 1,0 >]_9$, $\{< 2,0 >\} \in [< 1,0 >]_9$. Here $r_{<1,0>} = r_{<1,2>} = 2$. Table 3.5 gives the list of all codewords over $\mathbb{F}_2$ of $(9,2)$ Abelian code. It can be seen that there are few non-zero codewords with rank 1. Hence $R_q(\mathscr{C}) = 1$.

Table 3.5: List of all codewords of $(9,2)$ Abelian code $\mathscr{C}$ over $\mathbb{F}_{2^2}$ corresponding to Example 3.2.1

$\begin{bmatrix}000000000\\000000000\end{bmatrix}$	$\begin{bmatrix}000111111\\111111000\end{bmatrix}$	$\begin{bmatrix}111111000\\111000111\end{bmatrix}$	$\begin{bmatrix}111000111\\000111111\end{bmatrix}$	$\begin{bmatrix}000111111\\111000111\end{bmatrix}$
$\begin{bmatrix}000000000\\000111111\end{bmatrix}$	$\begin{bmatrix}111000111\\000000000\end{bmatrix}$	$\begin{bmatrix}111111000\\111111000\end{bmatrix}$	$\begin{bmatrix}111000111\\111111000\end{bmatrix}$	$\begin{bmatrix}111111000\\000000000\end{bmatrix}$
$\begin{bmatrix}000111111\\000111111\end{bmatrix}$	$\begin{bmatrix}000000000\\111000111\end{bmatrix}$	$\begin{bmatrix}111111000\\000111111\end{bmatrix}$	$\begin{bmatrix}111000111\\111000111\end{bmatrix}$	$\begin{bmatrix}000000000\\111111000\end{bmatrix}$
$\begin{bmatrix}000111111\\000000000\end{bmatrix}$				

Case 2: Example 3.2.2. Let the free transform components $C_{<1,0>}, C_{<1,2>}$. The component indices $\{< 1,0 >\} \in [< 1,0 >]_9$, $\{< 1,2 >\} \in [< 1,2 >]_9$. Here $r_{<1,0>} = r_{<1,2>} = 2$. Table 3.6 gives the list of all codewords over $\mathbb{F}_2$ of $(9,2)$ Abelian code. All non zero codewords are of rank 2.

Theorem 3.2.2: Let $\mathscr{C}$ be an $(n,1)$ Abelian cyclic code of length $n|q^m - 1$ over $\mathbb{F}_{q^m}$ such that the transform domain component $C_{<jq^s>} \in C_{[<j>]}$ is free and all other transform

Table 3.6: List of all codewords of $(9, 2)$ Abelian code $\mathscr{C}$ over $\mathbb{F}_{2^2}$ corresponding to Example 3.2.2

$\begin{bmatrix}000000000\\000000000\end{bmatrix}$	$\begin{bmatrix}000111111\\111000111\end{bmatrix}$	$\begin{bmatrix}111000111\\111111000\end{bmatrix}$	$\begin{bmatrix}111111000\\000111111\end{bmatrix}$	$\begin{bmatrix}011110101\\101011110\end{bmatrix}$
$\begin{bmatrix}011001010\\010011001\end{bmatrix}$	$\begin{bmatrix}100110010\\010100110\end{bmatrix}$	$\begin{bmatrix}100001101\\101100001\end{bmatrix}$	$\begin{bmatrix}101011110\\110101011\end{bmatrix}$	$\begin{bmatrix}101100001\\001101100\end{bmatrix}$
$\begin{bmatrix}010011001\\001010011\end{bmatrix}$	$\begin{bmatrix}010100110\\110010100\end{bmatrix}$	$\begin{bmatrix}110101011\\011110101\end{bmatrix}$	$\begin{bmatrix}110010100\\100110010\end{bmatrix}$	$\begin{bmatrix}001101100\\100001101\end{bmatrix}$
$\begin{bmatrix}001010011\\011001010\end{bmatrix}$				

components are constrained to zero. Let $|[< j >]| = e_j$. Consider any non zero codeword $\mathbf{c} \in \mathscr{C}$

$\mathbf{c} = \{c_0, c_1, \cdots c_{e_j-1}, \cdots, c_{ke_j}, \cdots, c_{(k+1)e_j-1} \cdots c_{n-1}\}$.

There are two cases:

(i). $e_j|n$: If $e_j|n$, then $\frac{n}{e_j}$ sets $\{\{c_0, c_1, \cdots, c_{e_j-1}\}, \{c_{e_j}, \cdots, c_{2e_j-1}\} \cdots, \{c_{n-e_j}, \cdots, c_{n-1}\}\}$ are linearly independent sets over $\mathbb{F}_q$. If these sets are viewed as $m \times e_j$ matrices over $\mathbb{F}_q$, then each matrix has $\mathbb{F}_q$ rank equal to e_j.

(ii). e_j does not divide n: If e_j does not divide n, then $\lfloor \frac{n}{e_j} \rfloor$ sets

$\{\{c_0, c_1, \cdots, c_{e_j-1}\}, \{c_{e_j}, \cdots, c_{2e_j-1}\} \cdots, \{c_{n-\lfloor \frac{e_j}{n} \rfloor - e_j}, \cdots, c_{n-\lfloor \frac{e_j}{n} \rfloor - 1}\}\}$ are linearly independent sets over $\mathbb{F}_q$ and have rank e_j if these sets are viewed as $m \times e_j$ matrices over $\mathbb{F}_q$. The last set $\{c_{n-\lfloor \frac{e_j}{n} \rfloor}, \cdots, c_{n-1}\}\}$ consisting of $n - \lfloor \frac{e_j}{n} \rfloor$ terms is also linearly independent and has $\mathbb{F}_q$ rank equal to $n - \lfloor \frac{e_j}{n} \rfloor$ when viewed as $m \times n - \lfloor \frac{e_j}{n} \rfloor$ matrix over $\mathbb{F}_q$.

3.3 Puncturing of Abelian codes

In section 3.2 we have seen that for any codeword $\mathbf{c}$ the codeword elements from index e_j are a linear combination of first e_j elements. Hence the $(1 \times n)$ codeword vectors of an $\ell-$ Abelian code $\mathscr{C}$ can be punctured to $(1 \times e_j)$ codeword vectors without altering their rank and structural relationship.

Theorem 3.3.1: If $\mathscr{C}_p$ be rank$-m$ $(m, 1)$ punctured code obtained from $(n, 1)$ Abelian code

$\mathscr{C}$, then $\mathscr{C}_p$ is maximum distance separable (MDS) with $d = m$.

Proof: From Theorem 3.2.2, for $(n, 1)$ Abelian code $\mathscr{C}$ of rank m, the value of e_j is m resulting in punctured code $\mathscr{C}_p$ with $m \times m$ codeword matrices. Since rank is m, any two codewords in $\mathscr{C}_p$ will differ in m elements.In other words, the hamming distance d of $\mathscr{C}_p$ is equal to m. Also according to singleton bound $d \leq n - k + 1 = m - 1 + 1 = m$. Thus $\mathscr{C}_p$ is MDS.

3.4 Generator Matrix representation of rank-metric Abelian codes

Following the DFT (3.2) the codeword vector of Abelian code $\mathscr{C}$ can be represented as

$$\{c_0, \cdots, c_{n-1}\} = \left\{ \frac{1}{|G|} \sum_{y \in G} \Psi\left(< 0, j >\right)^{-1} C_{<j_{r-1}q^s, \cdots, j_0 q^s>}, \cdots \sum_{y \in G} \Psi\left(< n-1, j >\right)^{-1} C_{<j_{r-1}q^s, \cdots, j_0 q^s>} \right\} \tag{3.22}$$

Following the analysis given in Section 2.23 of Chapter 2, the generator matrix of the code $\mathscr{C}$ is given by,

$$\mathbf{G} = \begin{bmatrix} 1 & \Psi(1, j_1)^{-1} & \Psi(2, j_1)^{-1} & \Psi(3, j_1)^{-1} & \cdots & \Psi(n-1, j_1)^{-1} \\ 1 & \Psi(1, j_2)^{-1} & \Psi(2, j_2)^{-1} & \Psi(3, j_2)^{-1} & \cdots & \Psi(n-1, j_2)^{-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \Psi(1, j_k)^{-1} & \Psi(2, j_k)^{-1} & \Psi(3, j_k)^{-1} & \cdots & \Psi(n-1, j_k)^{-1} \end{bmatrix} \tag{3.23}$$

Similarly, the $(k \times e_j)$ generator matrix of the punctured (e_j, k) code $\mathscr{C}_p$ is given by,

$$\mathbf{G} = \begin{bmatrix} 1 & \Psi(1, j_1)^{-1} & \Psi(2, j_1)^{-1} & \Psi(3, j_1)^{-1} & \cdots & \Psi(e_j-1, j_1)^{-1} \\ 1 & \Psi(1, j_2)^{-1} & \Psi(2, j_2)^{-1} & \Psi(3, j_2)^{-1} & \cdots & \Psi(e_j-1, j_2)^{-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \Psi(1, j_k)^{-1} & \Psi(2, j_k)^{-1} & \Psi(3, j_k)^{-1} & \cdots & \Psi(e_j-1, j_k)^{-1} \end{bmatrix} \tag{3.24}$$

3.5 Parity check matrix

Following the analysis give in chapter 2, the parity check matrix of $(n, 1)$ Abelian codes is given by,

$$\begin{pmatrix} \Psi(1, jq^s)^{-1} & -1 & 0 & \cdots & 0 & 0 \\ 0 & \Psi(1, jq^s)^{-1} & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & \Psi(1, jq^s)^{-1} & -1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{3.25}$$

Similarly the parity check matrix of (n, k) Abelian codes can be given by

$$\begin{bmatrix} h_0 & h_1 & h_2 & \cdots & h_k & 0 & \cdots & 0 & 0 \\ 0 & h_0 & h_1 & \cdots & h_{k-1} & h_k & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & h_{k-1} & h_k \end{bmatrix} \tag{3.26}$$

Here the values $\{h_0, h_1, \cdots, h_k\}$ are obtained by convolution of k sets: $\{\Psi(1, j_1)^{-1}, -1\}$, $\{\Psi(1, j_2)^{-1}, -1\}, \cdots, \{\Psi(1, j_k)^{-1}, -1\}$ The check matrix in Eq. 3.26 is a band matrix with bandwidth $k + 1$.

3.5.1 Decoding in Rank metric

Let $\mathbf{R_x} = \mathbf{C} + \mathbf{E}$ be the received matrix with elements over $\mathbb{F}_q$. Equivalently, let $\mathbf{r} = \mathbf{c} + \mathbf{e}$ be the received vector with elements over $\mathbb{F}_{q^m}$. Decoding is realized by solving $\mathbf{H}r = \mathscr{S}$, where $\mathscr{S}$ is $e_j \times 1$ syndrome vector. Since the check matrix is of dimension $n - k \times n$, there exists q^{km} solutions for the same syndrome. Solutions can be obtained using numerical methods or computer program based interative simulations. The decoder selects the solution with minimum rank as an estimate of the error vector. This estimated error vector is then used to obtain an estimate of the transmitted vector. It can be noted that the decoder gives correct solution only if it has the knowledge of the transform component indices used at the transmitter. The solution of the decoding algorithm is unique if $R_q(\mathbf{e}) \leq \lfloor \frac{m-1}{2} \rfloor$: Without loss of generality let $\boldsymbol{x_1}$, $\boldsymbol{x_2}$ be two solutions of rank $\leq \lfloor \frac{m-1}{2} \rfloor$ such that $\mathbf{H} \cdot (\boldsymbol{x_1}) = \mathbf{H} \cdot (\boldsymbol{x_2}) \implies$

$\mathbf{H} \cdot (\boldsymbol{x_1} - \boldsymbol{x_2}) = \mathbf{H} \cdot \mathbf{d}_x = 0$. Since $\mathbf{H}$ is orthogonal to $\mathscr{C}$, this is true only if $\mathbf{d}_x = 0$ or $\mathbf{d}_x \in \mathscr{C}$ which means $R_q(\mathbf{d}_x) = m$. However, according to the rank inequality we have $R_q(\mathbf{d}_x) \leq R_q(\boldsymbol{x_1}) + R_q(\boldsymbol{x_2})$. Since $R_q(\boldsymbol{x_1}) = R_q(\boldsymbol{x_2}) \leq \lfloor \frac{m-1}{2} \rfloor$, $R_q(\mathbf{d}_x) \leq 2\lfloor \frac{m-1}{2} \rfloor < m$ contradicting the condition $R_q(\mathbf{d}_x) = m$. Thus, $\boldsymbol{x_1} = \boldsymbol{x_2}$, indicating that the proposed decoding algorithm gives unique solution if $R_q(\mathbf{e}) \leq \lfloor \frac{\mathbf{m-1}}{\mathbf{2}} \rfloor$.

3.6 Conclusion

In this chapter, we have analyzed the rank distance properties of Abelian codes that are more general class of cyclic codes. We have analyzed rank distance properties of (n, k) Abelian codes and demonstrated that (n, k) full rank Abelian codes can be obtained for any value of $k \geq 1$ and $1 \leq k \leq \lfloor \frac{n}{\mathfrak{e}} \rfloor$, for any length n which is not divisor of $q^m - 1$. We have stated and proved theorems that allow the determination of the exact rank of (n, k) Abelian codes. Using the underlying geometric progression property (in terms of character) of $(n, 1)$ Abelian codes we have constructed a parity check matrix for (n, k) Abelian codes. A check matrix based decoding strategy has been derived to correct rank errors. Applications of Abelian codes as full rank distance codes for MIMO systems has been discussed in chapter 4.

Chapter 4

(n, k) Cyclic codes and Abelian codes as Block codes for MIMO Systems

The $m \times e_j$ codeword matrices of full rank codes $\mathscr{C}$ can be used as space-time/frequency block codes in $N_T \times N_R$ MIMO systems with $N_T = m$ antennas. However, the codeword matrices that are obtained cannot be directly used in MIMO communication because the symbols of the code arise from the finite field $\mathbb{F}_q$, and the symbols of any constellation used in practice are drawn from the real number field $\mathbb{R}$ or complex number field $\mathbb{C}$. A rank-preserving map is used to map symbols of codeword matrices $\mathbf{C}$ between symbols from $\mathbb{F}_q$ and complex constellations (Konishi (2017)). In (Lusina et al. (2003)), the map between Galois field $\mathbb{F}_q$ with $q = 4\mathscr{K} + 1$, $\mathscr{K} \geq 0$ and the a residue class of Gaussian integers with $q = \mathrm{u} + i\mathrm{v}$ (u,v are integers) is shown to be rank preserving Huber (1994b). This map is used to construct STBCs from Gabidulin codes. Based on the analysis given in (Lusina et al. (2003)), Puchinger et al. (2016) has shown that for $q = 6\mathscr{K} + 1$ with $\mathscr{K} \geq 0$, the map between Finite field $\mathbb{F}_q$ and residue class modulo Eisenstein-Jacobi integer (Huber (1994a)) with $q = \mu + \rho\nu$, $\mu, \nu \neq 0$, $\rho = (-1 + i\sqrt{3})/2$ is rank preserving and is used to construct STBCs.

4.1 Preliminaries

- Gaussian Integers (Huber (1994b)):

  Gaussian integer is a complex number of the form $u + iv$ with u and v as integers.

Following Fermat's theorem, Huber (1994b) considered primes that are product of complex conjugate Gaussian Integers. If π is a Gaussian integer of the form $u+iv$ then a prime q can be expressed as $\pi\dot{\pi}^{'}$. Every prime number of the form $q = 4\mathscr{K} + 1$ can be expressed as the product of two complex conjugate Gaussian integers. Let $\mathcal{G}$ be the set of Gaussian Integers and let G_π residue class of $\mathcal{G}$ modulo π obtained using the modulo function μ defined as

$$\mu(\zeta) = \zeta - \left[\frac{\zeta\pi}{\pi\dot{\pi}^{'}}\right]\pi \tag{4.1}$$

Here $[\cdot]$ denotes the round-off operation.

Lusina et al. (2003) has shown that the map between Galois field $\mathbb{F}_q$ with $q = 4\mathscr{K} + 1$, $\mathscr{K} \geq 0$ and Gaussian integer field (residue class $\mathcal{G}_\pi$) with $q = \mathfrak{u}+i\mathfrak{v}$ is rank preserving. Here, $\mathfrak{u}$ and $\mathfrak{v}$ are integers. This map is used to construct STBCs from Gabidulin codes. Table 4.2 gives the Gaussian integer fields that are used in this chapter.

Table 4.1: Gaussian-Integers fields $\mathcal{G}_\pi$for various values of π.

$q(\pi)$	$\mathcal{G}_\pi$
$5\ (2+i)$	$\{0, 1, i, -1, -i\}$
$13\ (3+2i)$	$\{0, 1, 1+i, 2i, -i, 1-i, 2, -1, -1-i, -2i, i, -1+i, -2\}$
$17\ (4+i)$	$\begin{Bmatrix} 0, 1, 1+i, 2i, -1-2i, i, -1+i, -2, 2-i, \\ -1, -1-i, -2i, 1+2i, -i, 1-i, 2, -2+i \end{Bmatrix}$

- Eisenstein-Jacobi Integers (Huber (1994a)):

  Eisenstein-Jacobi integers Π are numbers of the form $\mathfrak{u} + \rho\mathfrak{v}$ where $\rho = \frac{-1+i\sqrt{3}}{2}$ and $\mathfrak{u}, \mathfrak{v}$ are integers. is a complex number with $\mathfrak{u}$ and $\mathfrak{v}$ as integers. It was shown that primes of the form $6\mathscr{K} + 1$ with $\mathscr{K} \geq 0$ can be written as $q = \mathfrak{u}^2 + 3\mathfrak{v}^2 = \Pi\dot{\Pi}^{'}$. Here $\Pi^{'} = \mathfrak{u}+\mathfrak{v}+\rho^2 2\mathfrak{v}$. Let $\mathcal{J}$ denote the set of Eisenstein-Jacobi Integers and let $\mathcal{J}_\Pi$ denote the residue class of $\mathcal{J}$ modulo Π obtained using modular operation

$$\mu(\zeta) = \zeta - \left[\frac{\zeta\pi}{\pi\dot{\pi}^{'}}\right]\pi \tag{4.2}$$

Based on the analysis given in Lusina et al. (2003), Puchinger et al. Puchinger et al. (2016) showed that for $q = 6\mathscr{K} + 1$, $\mathscr{K} \geq 0$ the map between Galois field $\mathbb{F}_q$ and Eisenstein-Jacobi integer field (residue class modulo Π) with $q = \mathfrak{u} + \rho\mathfrak{v}$, $\mathfrak{u}, \mathfrak{v} \neq 0$, $\rho = (-1 + i\sqrt{3})/2$ is rank preserving and can be used to construct STBCs. Table 4.2 gives the Residue classes of Eisenstein-Jacobi integers that are used in this chapter.

Table 4.2: Residue classes $\mathcal{J}_\Pi$ of Eisenstein-Jacobi Integers for various values of Π.

$q(\Pi)$	$\mathcal{J}_\Pi$
$7\,(3+\rho\cdot 2)$	$\{0, 1, 1+\rho, \rho, -1, -1-\rho, -\rho\}$
$13\,(3+\rho\cdot 4)$	$\begin{Bmatrix} 0, 1, 1+2\rho, 1+\rho, -1+\rho, \rho, -2-\rho, \\ -1, -1-2\rho, -1-\rho, 1-\rho, -\rho, 2+\rho, \end{Bmatrix}$

4.1.1 Space-Time Block Codes from Full Rank Codes

Space-time/frequency block codes (SFBC) can be obtained from codewords $\mathbf{C}$ of full rank code $\mathscr{C}$ by mapping each symbol of the codeword matrix $\mathbf{C}$ into symbol of Gaussian integer constellation or Eisenstein-Jacobi integer constellation. The resulting STBC/SFBC is shown below.

$$\mathbf{X}_\rho = \begin{bmatrix} \zeta(c_{00}) & \zeta(c_{01}) & \zeta(c_{02}) & \cdots & \zeta(c_{0\,e_j-1}) \\ \zeta(c_{10}) & \zeta(c_{11}) & \zeta(c_{12}) & \cdots & \zeta(c_{1\,e_j-1}) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \zeta(c_{m-1\,0}) & \zeta(c_{m-1\,1}) & \zeta(c_{m-1\,2}) & \cdots & \zeta(c_{m-1\,e_j-1}) \end{bmatrix}$$

Where, ζ is either Gaussian integer map or Eisenstein-Jacobi integer map based on the value q of the field $\mathbb{F}_q$. The obtained STBC/SFBC codewords have columns that are generally having non-orthogonal in nature. Hence, the resultant STBC/SFBC can be termed as non-orthogonal STBC/SFBC (NSTBC/NSFBC).

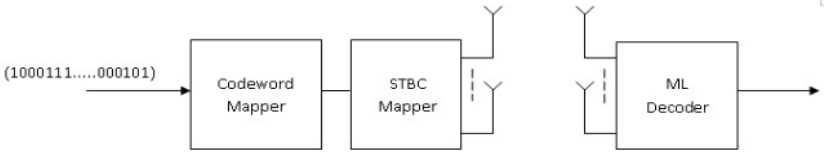


Figure 4.1: Block diagram of $N_T \times N_R$ MIMO system.

4.2 Application 1: Non-Orthogonal Space-Time Block codes for MIMO Systems

The block diagram of the conventional $N_T \times N_R$ MIMO transmitter and receiver is shown in Figure. 4.1. The number of transmit antennas N_T is considered to be equal to the value $\mathfrak{e}$ of the field $\mathbb{F}_{q^{\mathfrak{e}}}$. The incoming bit stream is split into frames of size $\left\lfloor log_2\left(q^{2\mathfrak{e}}\right)\right\rfloor$. The codeword mapper maps the frame to corresponding codeword matrix $\boldsymbol{c} \in \mathbb{C}$. STBC mapper maps the elements of codeword $\boldsymbol{C}$ to complex symbols (Lusina et al. (2003); Puchinger et al. (2016)). The mapping process is illustrated in (4.3)

$$(10111\cdots0111) \rightarrow \mathbf{X}_\rho = \begin{bmatrix} \zeta(c_{00}) & \zeta(c_{01}) & \zeta(c_{02}) & \cdots & \zeta(c_{0\,n-1}) \\ \zeta(c_{10}) & \zeta(c_{11}) & \zeta(c_{12}) & \cdots & \zeta(c_{1\,n-1}) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \zeta(c_{m-1\,0}) & \zeta(c_{m-1\,1}) & \zeta(c_{m-1\,2}) & \cdots & \zeta(c_{m-1\,n-1}) \end{bmatrix} \tag{4.3}$$

Each row of the NSTBC matrix $\mathbf{X}_\rho$ is transmitted through different transmit antenna.

4.2.1 Channel

The channel is assumed to be Quasi-Static Rayleigh fading channel with independent and identically distributed components.

4.2.2 Decoding

Decoding employs optimum Maximum Likelihood(ML) decoding algorithm The input at the MIMO receiver with N_R receiving antennas is given by,

$$\mathbf{Y} = \sqrt{\frac{E_s}{N_0}}\mathbf{H}\mathbf{X}_\rho + \eta_{AWGN} \tag{4.4}$$

Where,

$\mathbf{X}_\rho$ is STBC codeword of size $N_T \times n$

$\mathbf{H}$ is the channel matrix of size $N_R \times N_T$ which depends on the channel distribution.

$\eta_{AWGN}$is a $N_R \times n$ matrix of circularly symmetric i.i.d complex Gaussian random numbers.

Assuming that channel state information(CSI) is perfectly available at the receiver, an estimate $\widehat{\mathbf{X}_\rho}$ of the transmitted $\mathbf{X}_\rho$ can be obtained using,

$$\widehat{\mathbf{X}}_\rho = argmin \left\| \mathbf{Y} - \mathbf{H}\widehat{\mathbf{X}}_\rho^i \right\|^2 \quad 0 \leq i \leq q^m - 1. \tag{4.5}$$

4.2.3 Simulation Results

Simulations are performed under Quasi-Static Rayleigh fading channel environment. Table 4.3 gives the simulation parameters used for performance evaluation:

Table 4.3: Simulation Parameters

$m = N_T = 4$	$N_R = 1, 2$
$q = 7$	$m_0 = 2, m_1 = 5$
$n = m_0 m_1 = 10$	

Following Chapter 3, for length $n = 10$ Abelian codes we have exponent $\mathfrak{e} = lcm(2, 5) = 10$. Since $10|7^4 - 1$, we have considered codes over $\mathbb{F}_{7^4}$. The 7−cyclotomic cosets *mod* 10 are given below.

$[< 0, 0 >] = \{< 0, 0 >\}$

$[< 1, 0 >] = \{< 1, 0 >\}$

$[< 0, 1 >] = \{< 0, 1 >, < 0, 2 >, < 0, 4 >, < 0, 3 >\}$

$[< 1,1 >] = \{< 1,1 >, < 1,2 >, < 1,4 >, < 1,3 >\}$

The values of $j =< j_1, j_0 >$ are chosen to be $< 0,1 >$ and $< 1,1 >$ resulting in $(10,2)$ Abelian code $\mathbb{C}$. Figure 2. is the exponent table for $J_{3+2\rho}$ and Figure **??**. shows the constellation map $\zeta : F_7 \Rightarrow J_{3+2\rho}$. Here $\rho = \frac{-1+i\sqrt{3}}{2}$

$q = 7$	0	1	2	3	4	5
$\Pi = 3 + 2\rho$	1	$1 + \rho$	ρ	-1	$-1 - \rho$	$-\rho$

Spectral efficiency of proposed scheme can be calculated to be $\eta = \frac{\lfloor (log_2(7^8)) \rfloor}{10} = 1.9 bpcu$

Figure. 4.2 shows the comparisons ABER performance of 4×2, STBC-MIMO system over

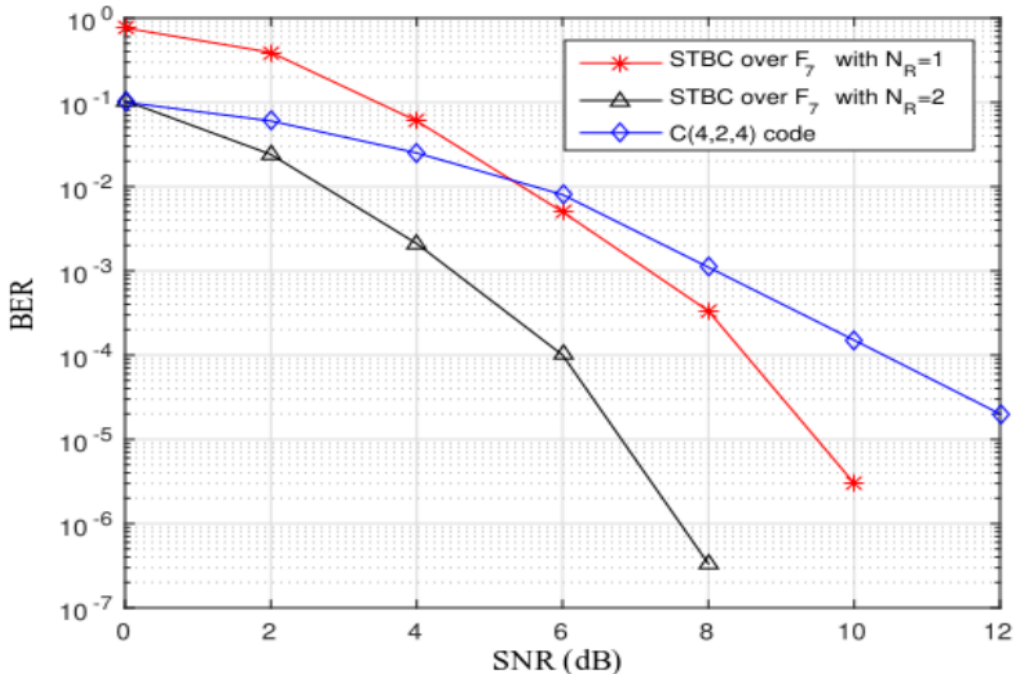


Figure 4.2: ABER of STBC over F_7

F_7 with C(4,2,4) code proposed in (Perişoară (2012)). It can be seen that with two free transform domain components the code provides a gain of approximately 4 dB when compared to C(4,2,4) code,, at a BER of 10^{-4}. The spectral efficiency is 1.9bpcu. In case of a 4×1 MIMO system the proposed STBC provides an asymptotic gain of approximately 2 dB.

4.3 Application 2: Non-orthogonal Space Frequency Block codes for MIMO-OFDM System

4.3.1 NSFBC Codebook Formulation

We have seen that the full rank codes over $\mathbb{F}_{q^m}$ can be constructed by choosing k free transform components, with each index chosen from a different $q-$cyclotomic coset of size m. If there are $\mathcal{L} \geq k$ $q-$ cyclotomic cosets, each of which are having size m, then we can have $\binom{\mathcal{L}}{k}$ possible choices of k $q-$ cyclotomic cosets that are grouped together. Of which, k free transform component indices can be chosen at a time with each from different $q-$ cyclotomic coset. Since the $q-$ cyclotomic cosets are of same size m, there are m^k possible choices of $k-$ free transform components. Each choice produces a full rank code (cyclic or Abelian) $\mathscr{C}_i$ with q^{km} codewords (matrices).

It can be stated that the rank distance between any two codewords (rank of difference matrix) of different codes such as $\mathscr{C}_i$ *and* $\mathscr{C}_j$ $0 \leq i, j \leq \binom{\mathcal{L}}{k} m^{k-1}$, $i \neq j$ may be less than m. The difference matrix which is obtained may not be a codeword and due to this, it is clearly understood that the rank goes down. However, from Case 2 of Theorem 6 in chapter 2, one can see that there exists a few codes whose codewords can be at a rank-distance m with respect to the codewords within the code and a few other codes as well (following Case 2 of Theorem 6, chapter 2). The reason here is that no two indices are chosen from the same $q-$cyclotomic coset. Thus, the codewords that belong to these two component codes of rank m can be grouped to form a composite code $\mathscr{X}$ having rank m. The composite code can be represented by $\mathscr{X} = \cup_{i=0}^{m^{\mathcal{L}}-1} \mathscr{C}_i$. A composite NSFBC code $\mathscr{X}_{NSFBC}$ corresponding to composite NSFBC code $\mathscr{X}$ has been obtained using rank preserving maps. Since all zero codeword is common for all component codes, the number of codewords in a composite NSFBC code $\mathscr{X}_{NSFBC}$ will be $\left(\binom{\mathcal{L}}{k} q^{km} - 1\right) + 1$.

The working of MIMO-OFDM-IM system employing the proposed composite NSFBCs is detailed in the next subsection.

4.3.2 Working principle NSFBC-MIMO-OFDM System

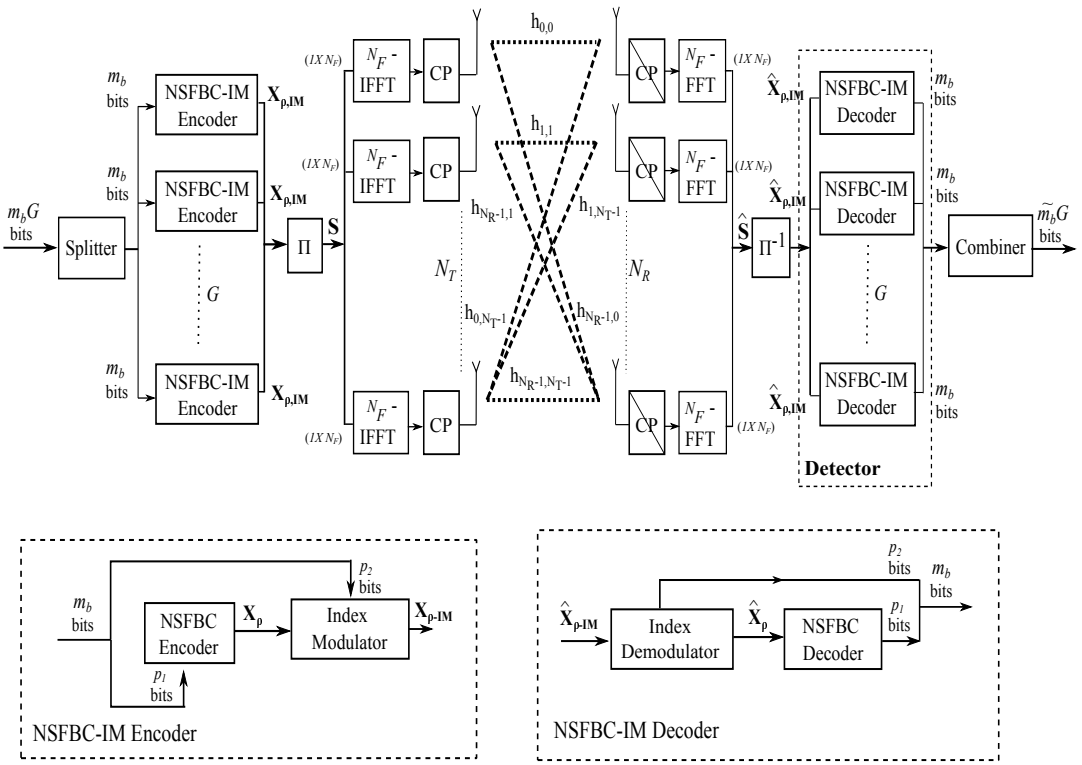


Figure 4.3: Block-Diagram of NSFBC based $N_T \times N_R$ MIMO-OFDM-IM system.

In this section we propose the NSFBC based MIMO-OFDM-IM system with $N_F = GN$ – OFDM carriers. Figure 4.3 illustrates the working of proposed NSFBC based MIMO-OFDM-IM system employing $N_F > N$ subcarriers. To facilitate the use of cyclic codes as NSFBCs, we consider the MIMO-OFDM system with $N_T = m$ – number of transmit antennas and N_R – number of receive antennas. Since there are $N_F = GN$ number of subcarriers that are available for communication, we use G – NSFBC-IM blocks at the transmitter, with each block providing $N_T \times N$ NSFBC-IM codeword. Thus, the available N_F carriers are divided among these G blocks, with $N = N_F/G$ subcarriers per block. The value of G is selected in such a way that the adjacent subcarriers are uncorrelated. i.e. B_c/G is less than subcarrier spacing. Here, B_c is the coherence bandwidth of the channel.

4.3.2.1 Transmitter

In Section 4.3.1, we have seen that there are $\binom{\mathcal{L}}{k}\left(q^{km}-1\right)+1$ codewords per $\mathscr{X}_{NSFBC}$. Since $N_T = m$, $m_bG = \left(log_2\left(\binom{\mathcal{L}}{k}(q^{kN_T}-1)+1\right) + n_m \cdot log_2\binom{N}{e_j}\right)G$ – number of input bits are con-

sidered at the input of block–splitter. These input bits are then split into G groups where, each group consisting of $m_b = log_2\left(\binom{\mathcal{L}}{k}(q^{kN_T}-1)+1\right) + n_m \cdot log_2\binom{N}{e_j}$ – number of information bits (Ib). At each NSFBC-IM block, the m_b information bits are further split into $p_1 = log_2\left(\binom{\mathcal{L}}{k}\left(q^{kN_T}-1\right)+1\right)$ – number of data bits (Db); and $p_2 = n_m \cdot log_2\binom{N}{e_j}$ – number of carrier selection bits (Csb). The p_1 data bits are processed by the NSFBC encoder to obtain the corresponding NSFBC codeword. The NSFBC codeword $\mathbf{X}_\rho$ is then considered as input for the index modulator (IM). Based on the carrier selection bits p_2, the index modulator select $N_A = e_j$ carriers out of available N subcarriers. The subcarriers that are chosen can be Same for all the rows of NSFBC (full rank mapping), or Different for each row of NSFBC (rank-deficient mapping).

1) In the first case, at any instance of time, the subcarriers that are chosen for all the rows of NSFBC codeword X_ρ are same . This process is to preserve the full rank property. Hence, $p_2 = log_2\binom{N}{e_j}$. This process give rise to $N_T \times N$ – NSFBC-IM codewords, with all symbols along each column being either zero (if the carrier frequency is not chosen) or non-zero (if the carrier frequency is chosen). An example representation of NSFBC-IM codeword $\mathbf{X}_{\rho-IM}$ is given as.

$$\mathbf{X}_{\rho,IM} = \begin{bmatrix} X_{0,0} & X_{0,1} & \cdots & X_{0,N-1} \\ X_{1,0} & X_{1,1} & \cdots & X_{1,N-1} \\ \vdots & \vdots & \cdots & \vdots \\ X_{N_T-1,0} & X_{N_T-1,1} & \cdots & X_{N_T-1,N-1} \end{bmatrix} = \begin{bmatrix} \zeta(c_{0,0}) & 0 & \cdots & \zeta(c_{0,e_j-1}) \\ \zeta(c_{1,0}) & 0 & \cdots & \zeta(c_{1,e_j-1}) \\ \vdots & \vdots & \cdots & \vdots \\ \zeta(c_{N_T-1,0}) & 0 & \cdots & \zeta(c_{N_T-1,e_j-1}) \end{bmatrix} \quad (4.6)$$

Thus, the symbols along each column of $\mathbf{X}_{\rho,IM}$ are either 0 or $\zeta(c_{k,l})$, with $0 \le k \le m-1$, $0 \le l \le e_j - 1$. The codewords obtained are termed as full rank NSFBC-IM codewords and corresponding codes as full rank NSFBC-IM codes (FR NSFBC-IM).

2) In the second case, the index modulator selects different subcarriers for different rows of NSFBC codeword. Hence, in this case $p_2 = mlog_2\binom{N}{e_j}$. This process gives rise to $N_T \times N$ NSFBC-IM codewords, with each symbol along each row being either zero (if the carrier frequency is not chosen) or non-zero (if the carrier frequency is chosen). An example repre-

sentation of NSFBC-IM codeword $\mathbf{X}_{\rho-IM}$ is given below:

$$\mathbf{X}_{\rho,IM} = \begin{bmatrix} X_{0,0} & X_{0,1} & \cdots & X_{0,N-1} \\ X_{1,0} & X_{1,1} & \cdots & X_{1,N-1} \\ \vdots & \vdots & \cdots & \vdots \\ X_{N_T-1,0} & X_{N_T-1,1} & \cdots & X_{N_T-1,N-1} \end{bmatrix} = \begin{bmatrix} \zeta(c_{0,0}) & \zeta(c_{0,1}) & \cdots & 0 \\ 0 & \zeta(c_{1,0}) & \cdots & \zeta(c_{1,e_j-1}) \\ \vdots & \vdots & \cdots & \vdots \\ \zeta(c_{N_T-1,0}) & \zeta(c_{N_T-1,1}) & \cdots & 0 \end{bmatrix} \tag{4.7}$$

From (4.7), based on the carrier selection bits, it is observed that the element $X_{i,j}$ ($0 \leq i \leq N_T - 1,\ 0 \leq j \leq N - 1$) of $\mathbf{X}_{\rho,IM}$ is either $\zeta(c_{k,l})$ $\left(0 \leq k \leq N_T - 1,\ 0 \leq l \leq e_j - 1\right)$ or 0. Hence, the codewords obtained are termed as rank deficient NSFBC-IM codewords and corresponding codes are termed rank deficient NSFBC-IM codes (RD NSFBC-IM).

In this work, we have considered FR-NSFBC-IMs for MIMO-OFDM-IM system with $N_R < 4$ antennas and RD-NSFBC-IMs for MIMO-OFDM-IM system with $N_R \geq 4$ antennas. In any case, the output of index modulator, $\mathbf{X}_{\rho,IM}$, is given by either (4.6) or (4.7). For convenience, let $\mathbf{X}_{\rho,IM}$ be represented as

$$\mathbf{X}_{\rho,IM} = \{\boldsymbol{X}_0, \boldsymbol{X}_1, \boldsymbol{X}_2 \cdots, \boldsymbol{X}_{N-1}\},$$

where, $\boldsymbol{X}_\rho$ is the ρ^{th} column of the NSFBC-IM codeword $\mathbf{X}_{\rho,IM}$. At the transmitter, each NSFBC-IM block gives rise to one NSFBC-IM codeword. Since there are G NSFBC-IM blocks, G NSFBC-IM codewords are available at the input of interleaver (Π). The interleaver stacks $G = N_F/N$ such NSFBC-IM codewords to form one NSFBC-OFDM-IM block $\mathbf{S}$, given by

$$\begin{aligned} \mathbf{S} &= \left\{\mathbf{X}^0_{\rho,IM}, \mathbf{X}^1_{\rho,IM}, \cdots, \mathbf{X}^{G-1}_{\rho,IM}\right\} \\ &= \left\{\boldsymbol{X}^0_0, \boldsymbol{X}^0_1, \cdots, \boldsymbol{X}^0_{N-1}, \boldsymbol{X}^1_0, \boldsymbol{X}^1_1, \cdots, \boldsymbol{X}^1_{N-1}, \boldsymbol{X}^{G-1}_0, \boldsymbol{X}^{G-1}_1, \cdots, \boldsymbol{X}^{G-1}_{N-1}\right\}. \end{aligned} \tag{4.8}$$

Where, $\mathbf{X}^{\mathcal{G}}_{\rho,IM}$ is the $\mathcal{G}^{th}, 0 \leq \mathcal{G} \leq G-1$, NSFBC-IM codeword of $\mathbf{S}$. $\boldsymbol{X}^{\mathcal{G}}_\rho$ is the ρ^{th} column of

the $\mathcal{G}^{th}$ NSFBC-IM codeword $\mathbf{X}^{i}_{\rho,IM}$, given by

$$X^{\mathcal{G}}_{\rho} = \left[X^{\mathcal{G}}_{0,\rho}, X^{\mathcal{G}}_{1,\rho}, X^{\mathcal{G}}_{2,\rho} \cdots, X^{\mathcal{G}}_{N_T-1,\rho}\right]^T ;\ 0 \leq \rho \leq N-1, 0 \leq \mathcal{G} \leq G-1$$

The terms $\mathcal{G}$ and ρ can be related as $\mathcal{G} = \lfloor \frac{\rho}{N} \rfloor$. Here, $G = N_F/N$, is number of NSFBC-IM codewords with N carriers per NSFBC-IM codeword.

Since the interleaving is in the frequency dimension, the number of rows of $\mathbf{S}$ remain same as that of $\mathbf{X}_{\rho,IM}$, i.e. equal to N_T. Each row of the NSFBC-IM-OFDM block $\mathbf{S}$ is then sent to the corresponding IFFT block. Further, the IFFT block computes $1 \times N_F$ time domain vector. The obtained N_F-point time domain vector is then padded with a cyclic prefix (CP) and then modulated onto $N_F + N_{CP}$ carriers. Since, the IFFT computation occurs at each transmit antenna (corresponding to each row of $\mathbf{S}$), N_T – IFFT vectors are available at the output of transmitter. These N_T – IFFT vectors are transmitted simultaneously over MIMO channel. For better resilience to inter-symbol interference (ISI), the length of cyclic prefix L, is chosen to be greater than the channel length L. The spectral efficiency is defined as the number of bits transmitted per channel usage per carrier frequency and is given by

$$\eta = \frac{G.\left(log_2\left(\binom{\mathcal{L}}{k}(q^{kN_T}-1)+1\right) + n_m \cdot log_2\binom{N}{e_j}\right)}{N_F + N_{CP}}, \qquad n_m = \begin{Bmatrix} 1 & FR\text{-}NSFBC\text{-}IM \\ N_T & RD\text{-}NSFBC\text{-}IM \end{Bmatrix} \tag{4.9}$$

4.3.2.2 Channel

The channel is considered to be frequency selective and time-flat with $L <$ L (length of cyclic prefix) – number of taps. Fading between each transmitting and receiving antenna is considered to be independent and identically distributed (I.I.D) with the Rayleigh distribution at a particular carrier frequency ρ. The Rayleigh distribution of channel coefficient h is given by

$$f_H(h) = \frac{2h}{\Omega} e^{-h^2/\Omega},\ h \geq 0 \tag{4.10}$$

Where, $\Omega = \mathrm{E}(H^2)$. The channel coefficients among various subcarriers are also considered to be identically distributed. Further assumption has been made that the wireless channels remain constant during the transmission of a MIMO-OFDM-IM frame.

4.3.2.3 Receiver

After removing the CP of length L per OFDM symbol and applying FFT at each branch of the receiver, the received $N_R \times N_F$ matrix at the input of deinterleaver is given by,

$$\begin{aligned}\mathbf{Y} &= \left\{\mathbf{Y}^0, \mathbf{Y}^1, \cdots, \mathbf{Y}^{\mathcal{G}-1}\right\} \\ &= \left\{\boldsymbol{Y}_0^0, \boldsymbol{Y}_1^0, \cdots, \boldsymbol{Y}_{N-1}^0, \boldsymbol{Y}_0^1, \boldsymbol{Y}_1^1, \cdots, \boldsymbol{Y}_1^{G-1}, \boldsymbol{Y}_0^{G-1}, \boldsymbol{Y}_1^{G-1}, \cdots, \boldsymbol{Y}_{N-1}^{G-1}\right\}\end{aligned}$$

with each column $\boldsymbol{Y}_\rho^{\mathcal{G}}$ representing the $N_R \times 1$ received vector at particular frequency ρ (after FFT), given by

$$\boldsymbol{Y}_\rho^{\mathcal{G}} = \begin{bmatrix} y_0^\rho \\ y_1^\rho \\ y_2^\rho \\ \vdots \\ y_{N_R-1}^\rho \end{bmatrix} = \begin{bmatrix} H_{0,0}^\rho & H_{0,1}^\rho & \cdots & H_{0,N_T-1}^\rho \\ H_{1,0}^\rho & H_{1,1}^\rho & \cdots & H_{1,N_T-1}^\rho \\ H_{2,0}^\rho & H_{2,1}^\rho & \cdots & H_{2,N_T-1}^\rho \\ \vdots & \vdots & \vdots & \vdots \\ H_{N_R-1,0}^\rho & H_{N_R-1,1}^\rho & \cdots & H_{N_R-1,N_T-1}^\rho \end{bmatrix} \begin{bmatrix} X_{0,\rho}^{\mathcal{G}} \\ X_{1,\rho}^{\mathcal{G}} \\ X_{2,\rho}^{\mathcal{G}} \\ \vdots \\ X_{N_T-1,\rho}^{\mathcal{G}} \end{bmatrix} + \begin{bmatrix} w_0^\rho \\ w_1^\rho \\ w_2^\rho \\ \vdots \\ w_{N_R-1}^\rho \end{bmatrix}$$

$$0 \leq \rho \leq N_F - 1 \tag{4.11}$$

Where, $H_{\omega\Omega}^\rho = \sum_{l=0}^{L-1} h_{\omega\Omega}(l) e^{-j\left(\frac{2\pi}{N_c}\right)l\rho}$; with $\mathbf{h}_{\omega\Omega} \equiv [h_{\omega\Omega}(0), h_{\omega\Omega}(1), \cdots, h_{\omega\Omega}(L-1)]$ representing the baseband equivalent impulse response of the channel between ω^{th} transmit antenna and Ω^{th} receive antenna, and L denoting the length of the channel impulse response. Following (4.8) , for simplicity, (4.11) can be written as

$$\boldsymbol{Y}_\rho^{\mathcal{G}} = \mathbf{H}_\rho^{\mathcal{G}} \boldsymbol{X}_\rho^{\mathcal{G}} + \boldsymbol{W}_\rho^{\mathcal{G}}\ ; \qquad 0 \leq \rho \leq N_F - 1\ \&\ \mathcal{G} = \left\lfloor \frac{\rho}{N} \right\rfloor \tag{4.12}$$

Where, $\boldsymbol{W}_\rho^{\mathcal{G}}$ is the $N_R \times 1$ vector of elements that are realizations of Gaussian random variable with zero mean. $\mathbf{H}_\rho^{\mathcal{G}}$ is $N_R \times N_T$ baseband equivalent impulse response of the channel matrix at a particular frequency ρ.

The deinterleaver (Π^{-1}) considers the received matrix, constructs a block of $N-$ columns, and feeds the $N_R \times N$ matrix to the detector. The detection employed is either a single-stage Maximum Likelihood (ML) detection of the entire NSFBC-IM code, or a two-stage mini-

mum mean square estimation (MMSE)-ML decoder. In the case of two-stage MMSE-ML decoder, the first stage is for the detection of carrier selection bits using Minimum Mean Square Estimation (MMSE), and the second stage is for the detection of data bits using Maximum Likelihood (ML) decoder. Thus the receiver is either

1. Single stage ML receiver or

2. Two Stage MMSE-ML receiver.

1. **Single Stage ML Receiver**

   In this case, the NSFBC-IM decoder is considered to be ML detector. At particular subblock G, the ML detector considers the $N_R \times N$ matrix $\mathbf{Y}^{\mathcal{G}}$ corresponding to that subblock G and obtains an estimate of the transmitted $N_T \times N$ matrix for estimating the transmitted NSFBC-IM codeword $\mathbf{X}_{\rho-IM}$. Following (4.11), the received $N_R \times N$ matrix can be given as,

$$\mathbf{Y}^{\mathcal{G}} = \hat{\mathbf{H}}^{\mathcal{G}} \left(\mathbf{X}^{\mathcal{G}}_{\rho,IM}\right)^T + \mathbf{W}^{\mathcal{G}}; \qquad 0 \leq \mathcal{G} \leq G-1 \tag{4.13}$$

   Where,

$$\mathbf{Y}^{\mathcal{G}} = \left[\boldsymbol{Y}^{\mathcal{G}}_0, \boldsymbol{Y}^{\mathcal{G}}_1, \cdots, \boldsymbol{Y}^{\mathcal{G}}_{N-1}\right]^T; \qquad \hat{\mathbf{H}}^{\mathcal{G}} = \begin{bmatrix} \hat{\mathbf{H}}^{\mathcal{G}}_0 & 0 & 0 & \cdots & 0 \\ 0 & \hat{\mathbf{H}}^{\mathcal{G}}_1 & 0 & \cdots & 0 \\ 0 & 0 & \hat{\mathbf{H}}^{\mathcal{G}}_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \hat{\mathbf{H}}^{\mathcal{G}}_{N-1} \end{bmatrix},$$

$$\mathbf{X}^{\mathcal{G}}_{\rho,IM} = \left[\boldsymbol{X}^{\mathcal{G}}_0, \boldsymbol{X}^{\mathcal{G}}_1, \boldsymbol{X}^{\mathcal{G}}_2, \cdots, \boldsymbol{X}^{\mathcal{G}}_{N-1}\right]; \qquad \mathbf{W}^{\mathcal{G}} = \left[\boldsymbol{W}^{\mathcal{G}}_0, \boldsymbol{W}^{\mathcal{G}}_1, \cdots, \boldsymbol{W}^{\mathcal{G}}_{N-1}\right]$$

   The ML decision required in estimating one transmitted NSFBC-IM codeword $\mathbf{X}^{\mathcal{G}}_{\rho,IM}$, is then given by

$$\left(\mathbf{X}^{\mathcal{G}}_{\rho,IM}\right)_{ML} = \arg\min\left(\left\|\mathbf{Y}^{\mathcal{G}} - \hat{\mathbf{H}}^{\mathcal{G}} \left(\mathbf{X}^{\mathcal{G}}_{\rho,IM}\right)^T\right\|^2_F\right); \qquad 0 \leq \mathcal{G} \leq G-1 \tag{4.14}$$

From the estimated NSFBC-IM matrix, the information bits (Ib) transmitted are then decoded.

2. **MMSE-ML Based Receiver**

   (a) In this case the detection is a two-stage process. At the first stage, the information conveyed using index modulator is obtained using MMSE based index demodulator. At the second stage, the modulated data is obtained using ML based NSFBC decoder. Assuming availability of perfect channel state information (CSI) at the receiver the MMSE estimation of $\hat{\mathbf{X}}_{\rho}^{\mathcal{G}}$ can be obtained in the following manner. At the first stage, MMSE estimation is performed for each column of the decoded NSFBC-OFDM-IM block $\mathbf{S}$. The estimated vector $\hat{\boldsymbol{X}}_{\rho}^{\mathcal{G}}$ is obtained using

$$\hat{\boldsymbol{X}}_{\rho}^{\mathcal{G}} = \mathbf{H}_{\rho}^{\mathcal{G}H}\left(\mathbf{H}_{\rho}^{\mathcal{G}}\mathbf{H}_{\rho}^{\mathcal{G}H} + \lambda\mathbf{I}\right)^{-1}\mathbf{Y}_{\rho}^{\mathcal{G}}\,; \qquad 0 \leq \rho \leq N_F - 1$$

$$\hat{\boldsymbol{X}}_{\rho}^{\mathcal{G}} = \mathbf{H}_{\rho}^{\mathcal{G}H}\left(\mathbf{H}_{p}^{\mathcal{G}}\mathbf{H}_{\rho}^{\mathcal{G}H} + \lambda\mathbf{I}\right)^{-1}\left(\mathbf{H}_{\rho}^{\mathcal{G}}\boldsymbol{X}_{\rho}^{\mathcal{G}} + \boldsymbol{W}^{\rho}\right) \tag{4.15}$$

   Where, λ is a constant and is equal to $\frac{N_T}{(\frac{E_b}{N_0})}$ in the case of linear MMSE estimators. An estimate of the transmitted NSFBC-IM is then given by

$$\hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}} = \left\{\hat{\boldsymbol{X}}_{0}^{\mathcal{G}}, \hat{\boldsymbol{X}}_{1}^{\mathcal{G}}, \hat{\boldsymbol{X}}_{2}^{\mathcal{G}}, \cdots, \hat{\boldsymbol{X}}_{N-1}^{\mathcal{G}}\right\}$$

   As seen from (4.15), $\hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}}$ contains Gaussian noise which is scaled by fading coefficients. From $\hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}}$, it is possible to obtain the carrier selection bits by finding locations of minimum magnitude. The remaining e_j high magnitude complex values of each row are considered to form an estimate of the $m \times e_j$ NSFBC matrix. This matrix is then fed as input to NSFBC decoder.

   (b) The second decoder (NSFBC decoder) considers the estimated $m \times e_j$ matrix and compares it with all the codewords of the corresponding composite NSFBC $\mathcal{X}_i$. The codeword which is at the minimum distance with this $m \times e_j$ matrix is then considered as $\hat{\mathbf{X}}_p$. The information corresponding to $\hat{\mathbf{X}}_p$ is considered as data bits.

The carrier selection and data bits together form an estimate of the transmitted information bits.

4.3.2.4 Computational Complexity

Below we discuss the computational complexity (in terms of number of complex multiplications) of the receiver in decoding information pertaining to one SFBC codeword.

1. MMSE-ML decoder.

   Computation of $\mathbf{H}_p^{\mathcal{G}H}\left(\mathbf{H}_p^{\mathcal{G}}\mathbf{H}_p^{\mathcal{G}H}+\lambda\mathbf{I}\right)^{-1}$: Since $\mathbf{H}_p^{\mathcal{G}}$ is of dimension $N_R\times N_T$ the number of complex multiplications required to compute $\mathbf{H}_p^{\mathcal{G}}\mathbf{H}_p^{\mathcal{G}H}$ is $N_R^2N_T$. Since the dimension of $\mathbf{H}_p^{\mathcal{G}H}\left(\mathbf{H}_p^{\mathcal{G}}\mathbf{H}_p^{\mathcal{G}H}+\lambda\mathbf{I}\right)^{-1}$ is $N_R\times N_T$, the estimation of one column of the SFBC-IM codeword requires N_RN_T complex multiplications. Since there are N columns per SFBC-IM, the total number of complex multiplications required in estimating one transmitted SFBC-IM is $N_R^2N_T+NN_RN_T$.

   Once the estimate of SFBC-IM is obtained, the decoding of data bits require comparison with SFBC codewords. This requires $\left(\binom{\mathcal{L}}{k}\left(q^{km}-1\right)+1\right)$ comparisons with each comparison resulting in $m\times e_j$ multiplications. Hence the total number of multiplications in estimating one block of information bits and carrier selection bits is $N_R^2N_T+NN_RN_T+\left(\binom{\mathcal{L}}{k}\left(q^{km}-1\right)+1\right).m\times e_j$. Therefore the computational complexity is given by

$$C_{MMSE}=N_R^2N_T+NN_RN_T+\left(\binom{\mathcal{L}}{k}\left(q^{km}-1\right)+1\right).m\times e_j \tag{4.16}$$

2. Single stage ML receiver:

   In this Section, the computational complexity (in terms of the number of complex multiplications) of the receiver in decoding information which is pertaining to one NSFBC codeword is discussed. The terms K, p_1, M mentioned in Table 4.4 are taken from Basar (2016). Where, K represents the number of subcarriers assigned per MIMO-OFDM-IM codeword, M is the order of QAM used, and p_1 is the number of data

bits per group in MIMO-OFDM-IM system. We outline the receiver complexity as the number of floating point operations (flops) needed per ML decision metric. As given in Trefethen and Bau III (1997), we consider every addition,subtraction, multiplication, division,and square-root operation as a single flop. Consider equation 4.14. Since N columns represent SFBC-IM codeword, following equation 4.14 the received matrix $\mathbf{Y}_p^{\mathcal{G}}$ corresponding to one SFBC-IM codeword can be given by

$$\mathbf{Y}_p^{\mathcal{G}} = \mathbf{H}_{\rho,IM}^{\mathcal{G}}(\mathbf{I}_{mn} \otimes \hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}}) + \mathbf{W}_{\rho,IM}^{\mathcal{G}} \; 0 \leq \mathcal{G} \leq G-1 \tag{4.17}$$

Where $\mathbf{H}_{\rho,IM}^{\mathcal{G}} = \left[\mathbf{H}_0^{\mathcal{G}}, \mathbf{H}_1^{\mathcal{G}}, \cdots, \mathbf{H}_{N-1}^{\mathcal{G}}\right]$ is $N_R \times N_T N$ matrix obtained by stacking N channel matrices corresponding to $\mathcal{G}^{th}$ SFBC-IM codeword.

$\hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}}$ represents $\mathcal{G}^{th}$ SFBC-IM codeword that is transmitted.

$\mathbf{W}_{\rho,IM}^{\mathcal{G}}$ represents $N_R \times N$ noise matrix whose columns are N vectors $\boldsymbol{W}_p^{\mathcal{G}}$ corresponding to $\mathcal{G}^{th}$ SFBC-IM codeword.

The Kronecker product $\left(\mathbf{I}_{mn} \otimes \hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}}\right)$ requires $N_T N$ multiplications and will result in $N_T N \times N$ matrix. Each complex multiplication requires 2 real multiplications. Since $\mathbf{H}_{\rho,IM}^{\mathcal{G}}$ is of dimension $N_R \times N_T N$ and $\left(\mathbf{I}_{mn} \otimes \hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}}\right)$ is of dimension $N_T N \times N$, computation of $\mathbf{H}_{\rho,IM}^{\mathcal{G}}\left(\mathbf{I}_{mn} \otimes \hat{\mathbf{X}}_{\rho,IM}^{\mathcal{G}}\right)$ requires $N_R N_T N^2$ complex multiplications with each complex multiplication requiring 4 real multiplications. Therefore each comparison requires $4N_R N_T N^2 + 2N_T N$ total number of real multiplications. There are $\binom{N}{e_j}^m \left(\binom{\mathcal{L}}{k}\left(q^{km}-1\right)+1\right)$ possible SFBC-IM codewords. Therefore the total number of computations (real multiplications) required are

$$C_{ML} = \binom{N}{e_j}^m \left(\binom{\mathcal{L}}{k}\left(q^{km}-1\right)+1\right)\left(N_R N_T N^2 + N_T N\right) \tag{4.18}$$

As seen from above, the single stage ML decoding complexity is exponential in $\binom{N}{e_j}$, increasing the decoding complexity with m. Hence this may not be suitable for codes over higher fields $\mathbb{F}_{q^m}$

The computational complexity of the proposed scheme and computational complexities of traditional MIMO-OFDM and MIMO-OFDM-IM is shown in Table 4.4 below.

Table 4.4: Computational complexity

Method	Complexity
MIMO-OFDM	$N_R(N_T+1)M^{N_T}$
MIMO-OFDM-IM	$N_R(N_T+1)(2^{p_1}M^K)^{N_T}$
Proposed Method (MMSE-ML)	$N_R N_T\,(N_R+N)+e_j m\left(\binom{\mathcal{L}}{k}\left(q^{km}-1\right)+1\right)$
Proposed Method(ML)	$\binom{N}{e_j}^m\left(\binom{\mathcal{L}}{k}(q^{km}-1)+1\right)\left(N_R N_T N^2+N_T N\right)$

4.3.3 Analytical Upper Bound

In Torabi et al. (2007), an upper bound on the probability of error of Alamouti based space-frequency block codes (SFBC) is provided. The bound is derived by exploiting the structure of Alamouti code which is resulting in a closed form expression. Because of the frequency selective nature of the channel and structure of the Alamouti code, joint detection of the symbols has been employed (Torabi et al. 2007). However, in this approach, as the structure is non-orthogonal and also because of the assumption that L > L, we have employed the use of BER analysis provided in Basar (2016).

Since the value of G is considered in such a way that the subcarriers are uncorrelated, the pairwise error events within different subblocks are identical (Basar (2016)). Hence, it is sufficient to estimate the PEP associated with one subblock to evaluate the performance of the proposed scheme. To derive the bound, we consider single stage ML detection of entire $N_T \times N$ NSFBC-IM codeword including joint detection of symbols along N_T rows of the received matrix, and for N consecutive columns that are corresponding to N columns of $\mathbf{X}_{\rho,IM}$.

Based on the analysis given in Basar (2016), the analytical upper bound (union bound) is derived with reference to (4.14) and is given as,

$$P_b \leq \frac{1}{N_c}\sum_{i=0}^{N_c-1}\sum_{j=0}^{N_c-1}\frac{P\left(\mathbf{X}^i_{\rho,IM}\rightarrow\mathbf{X}^j_{\rho,IM}\right)n_{i,j}}{N_b};\quad i\neq j \tag{4.19}$$

Where,

- $N_c = \left(\binom{\mathcal{L}}{k}(q^{kN_T} - 1) + 1\right)\binom{N}{e_j}^{n_m}$ – total number of NSFBC-IM codewords.
- N_b – total number of bits associated with the NSFBC-IM codeword.
- $n_{i,j}$ – number of bits in error between binary tuple associated with $\mathbf{X}^i_{\rho,IM}$ and $\mathbf{X}^j_{\rho,IM}$.
- $P\left(\mathbf{X}^i_{\rho,IM} \rightarrow \mathbf{X}^j_{\rho,IM}\right)$ represents the Pairwise Error Probability (PEP).

In (4.19), PEP is obtained by computing conditional PEP (CPEP) between two NSFBC-IM codewords and averaging the CPEP over all channel realizations. Following Simon and Alouini (2005), the CPEP $P\left(\mathbf{X}^i_{\rho,IM} \rightarrow \mathbf{X}^j_{\rho,IM} \mid \hat{\mathbf{H}}^{\mathcal{G}}_{\rho,IM}\right)$ is given by,

$$P\left(\mathbf{X}^i_{\rho,IM} \rightarrow \mathbf{X}^j_{\rho,IM} \mid \hat{\mathbf{H}}^{\mathcal{G}}_{\rho,IM}\right) = Q\left(\sqrt{\frac{\rho\left\|\mathbf{H}^{\mathcal{G}}_{\rho,IM}\left(\mathbf{X}^i_{\rho,IM} - \mathbf{X}^j_{\rho,IM}\right)\right\|^2}{2}}\right) \tag{4.20}$$

Using Craig's formula, this can be expressed as

$$P\left(\mathbf{X}^i_{\rho,IM} \rightarrow \mathbf{X}^j_{\rho,IM} \mid \hat{\mathbf{H}}^{\mathcal{G}}_{\rho,IM}\right) = \frac{1}{\pi}\int_0^{\pi/2} \exp\left(\frac{\rho\left\|\mathbf{H}^{\mathcal{G}}_{\rho,IM}\left(\mathbf{X}^i_{\rho,IM} - \mathbf{X}^j_{\rho,IM}\right)\right\|^2}{4sin^2\phi}\right)d\phi \tag{4.21}$$

The pairwise error probability (PEP) can be obtained by integrating (4.21) over probability density of $\Gamma = \left\|\mathbf{H}^{\mathcal{G}}_{\rho,IM}\left(\mathbf{X}^i_{\rho,IM} - \mathbf{X}^j_{\rho,IM}\right)\right\|^2$. Following Basar (2016); Simon and Alouini (2005), the PEP is given by

$$P\left(\mathbf{X}^i_{\rho,IM} \rightarrow \mathbf{X}^j_{\rho,IM}\right) = \frac{1}{\pi}\int_0^{\pi/2}\prod_{k=0}^{N_k}\left(\frac{1}{1 + \frac{E_b\lambda_{i,j,k}}{4N_0\sin^2\phi}}\right)^{n_R} d\phi \tag{4.22}$$

Where, N_k is the number of Eigen values, and $\lambda_{i,j,k}$ are the Eigen values of the difference matrix $\left(\mathbf{X}^i_{\rho,IM} \rightarrow \mathbf{X}^j_{\rho,IM}\right)\left(\mathbf{X}^i_{\rho,IM} \rightarrow \mathbf{X}^j_{\rho,IM}\right)^H$. It can be noted that, the value of $N_k = N_A = e_j$ in the case of FR-NSFBC-IM. Where as, the value of N_k can be less than e_j for RD-NSFBC-IM codewords.

Following (Simon and Alouini (2005)), using partial fraction expansion, a closed form solu-

tion of PEP can be given by,

$$P(\mathbf{X}^{i}_{\rho,IM} \rightarrow \mathbf{X}^{j}_{\rho,IM}) \leq \frac{1}{2} \prod_{l=1}^{N_k} \left(\frac{1}{(1+c_l)} \right)^{N_R} \tag{4.23}$$

Where, $c_l = \frac{E_b \lambda_{i,j,k}}{4N_O}$.

Substituting (4.23) in (4.19), union bound can be given by,

$$P_b \leq \frac{1}{N_c} \sum_{i=0}^{N_c-1} \sum_{j=0}^{N_c-1} \frac{\frac{1}{2} \prod_{l=1}^{N_k} \left(\frac{1}{(1+c_l)} \right)^{N_R} n_{i,j}}{N_b}; \quad i \neq j \tag{4.24}$$

$$P_b \leq \frac{1}{2N_c N_b} \sum_{i=0}^{N_c-1} \sum_{j=0}^{N_c-1} \prod_{l=1}^{N_k} \left(\frac{1}{(1+c_l)} \right)^{N_R} n_{i,j}; \quad i \neq j \tag{4.25}$$

4.3.4 Simulation Results

Based on the criteria given in Basar (2016); Martin and Taylor (2004), the number of transmit antennas N_T is considered to be two and four. We consider a 10-path frequency-selective Rayleigh fading MIMO channel with the maximum delay spread of $10T_s$ for fair comparison with existing results Basar (2016). Table 4.5 gives the values of various system parameters considered for simulations.

Table 4.5: MIMO-OFDM-IM system parameters (Basar (2016)).

Number of subcarriers(N_F)	512
Number of subcarriers per NSFBC-IM Block(N)	4,8,16
Subcarrier spacing(Δf)	15KHz
Sampling frequency(f_s)	7.68MHz
Cyclic prefix length (L)	36
Gaussian or Eisenstein Constellations	$\mathbb{F}(5), \mathbb{F}(7), \mathbb{F}(13)$

It is assumed that the channel state information (CSI) is unknown to the transmitter but, perfectly known to the receiver. The value of N is selected such that $B_c/\mathcal{G} = B_c N/N_F$ is less than the subcarrier spacing, resulting in uncorrelated channel coefficients associated with

adjacent subcarriers. Here, $B_c = (10T_s)^{-1}$. Since, $N_F = 512, \Delta f = 15KHz$ to meet the condition N is chosen to be $N = 4,\ 8,\ or\ 16$. Each value of N results in $G = G = N_F/N = 128,\ 64,\ or\ 32$ number of NSFBC-IM codewords per NSFBC-OFDM-IM block.

Table 4.6, Table 4.7, and Table 4.8 give spectral efficiencies that can be achieved by the proposed codes for various (e_j, k) codes over $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^4}$ respectively. From Table 4.6, it can be seen that a theoretical spectral efficiency of around 2.45 b/s/Hz can be achieved by using codes over $\mathbb{F}_{5^2}$ when compared to $1.87b/s/Hz$ offered by MIMO-OFDM-IM with BPSK (Basar (2016)). From Table 4.7, we note that the improvement in spectral efficiency achieved by FR-NSFBC-IM codes over $\mathbb{F}_{q^4}$ is around 0.2 b/s/Hz for most of the values of q when compared to the corresponding FR-NSFBC-IM codes over $\mathbb{F}_{q^2}$. From Table 4.8, we see that the proposed RD-NSFBC-IM codes achieve better spectral efficiencies which is almost >2 b/s/Hz while comparing with the corresponding FR-NSFBC-IM codes over $\mathbb{F}_{q^4}$. The reason is that the carrier selection bits per RD-NSFBC-IM codeword are n_m times more than FR-NSFBC-IM codeword.

Table 4.6: Spectrally efficiencies of proposed FR-NSFBC-IM codes over $\mathbb{F}_{q^2}$.

		$\eta_{theoretical}\ (bpcu)$			$\eta_{practical}\ (bpcu)$		
$\mathscr{C}_R - (e_j, k)$	N	q=5	q=7	q=13	q=5	q=7	q=13
$(2, 1)$	4	2.45	2.93	3.97	2.10	2.56	3.50
$(4, 2)$	8	2.44	2.92	3.79	2.33	2.80	3.73
$(8, 4)$	16	2.33	2.84	3.71	2.27	2.80	3.67

Table 4.7: Spectrally efficiencies of proposed FR-NSFBC-IM over $\mathbb{F}_{q^4}$.

		$\eta_{theoretical}\ (bpcu)$			$\eta_{practical}\ (bpcu)$		
$\mathscr{C}_R - (e_j, k)$	N	q=5	q=7	q=13	q=5	q=7	q=13
$(2, 1)$	4	2.64	3.10	3.93	2.56	3.03	3.85
$(4, 2)$	8	2.66	3.12	3.96	2.62	3.03	3.91
$(8, 4)$	16	2.64	3.10	3.94	2.62	3.09	3.91

In Figure 4.4, the simulation results and upper bound of proposed (e_j, k) NSFBCs over

Table 4.8: Spectrally efficiencies of proposed RD-NSFBC-IM codes over $\mathbb{F}_{q^4}$.

		$\eta_{theoretical}\ (bpcu)$			$\eta_{practical}\ (bpcu)$		
$\mathscr{C}_R - (e_j, k)$	N	q=5	q=7	q=13	q=5	q=7	q=13
$(2,1)$	4	4.79	5.25	6.08	4.67	5.13	5.95
$(4,2)$	8	5.05	5.51	6.35	4.90	5.31	6.18
$(8,4)$	16	5.19	5.66	6.49	5.16	5.63	6.45

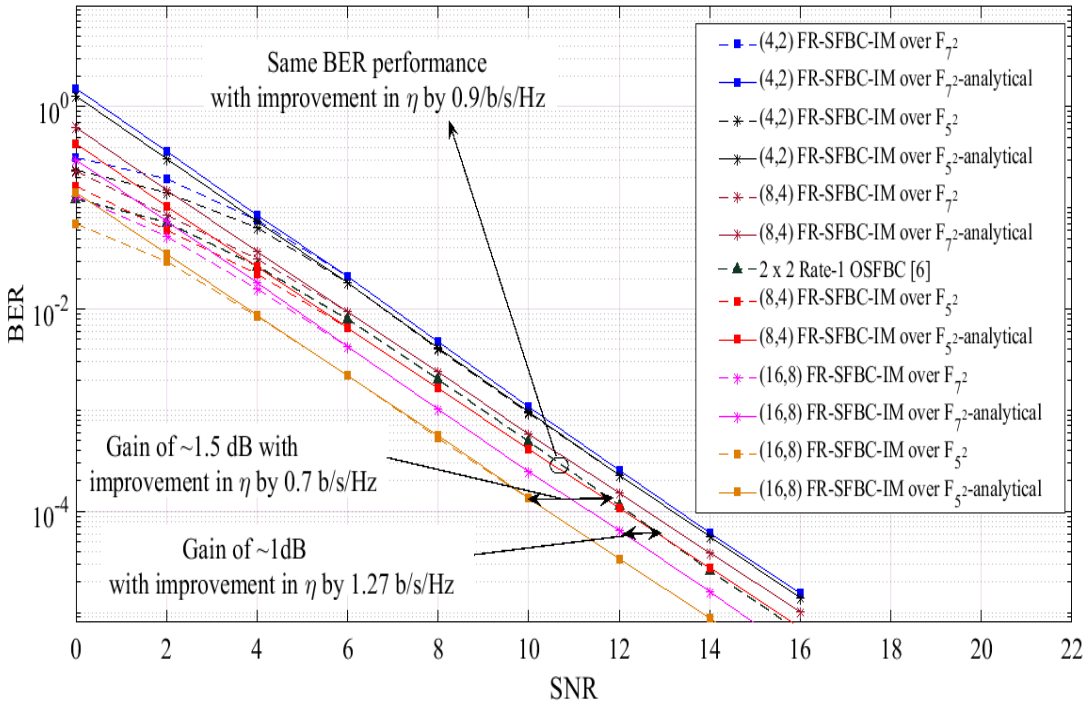


Figure 4.4: BER performance of FR-NSFBC-IMs over $\mathbb{F}_{5^2}, \mathbb{F}_{7^2}$ with N_T=2, N_R=2, $N = 4, 8, 16$ corresponding to $e_j = 2, 4, 8$ and ML-ML decoding.

$\mathbb{F}_{5^2}, \mathbb{F}_{7^2}$ are depicted. It can be seen that for a particular value of q, the BER performance improves with an increase in the values of e_j, k. It is observed that, $(16,8)$ codes over $\mathbb{F}_{5^2}$ provide a gain of around 1.5dB when compared to $(8,4)$ codes over $\mathbb{F}_{5^2}$. The above results are observed at a BER of 10^{-5}. A similar pattern is also observed in the case of codes over $\mathbb{F}_{7^2}$. In addition to that, we see that the codes over $\mathbb{F}_{5^2}$ achieve a spectral efficiency of around 2.4 $b/s/Hz$ from Table 4.12. Whereas, codes over $\mathbb{F}_{7^2}$ achieve a spectral efficiency of around codes over 2.9 $b/s/Hz$. From Figure 4.4, it can also be seen that the proposed $(8,4)$ FR NSFBC-IM codes provide similar BER performance when compared to Rate-1 Alamouti

code based MIMO-OFDM-IM. However, in a 2×2 MIMO-OFDM-IM system with $N_F = 512$ and $N = 4$, the Alamouti code with QPSK symbols (with rank preserving index modulation) provide a theoretical spectral efficiency of 1.5 b/s/Hz which is approximately 1 b/s/Hz less than the spectral efficiency provided by FR-NSFBC-IM codes over $\mathbb{F}_{5^2}$. Furthermore, it is observed that at lower values of (e_j, k), constructions over $\mathbb{F}_{7^2}$ provide similar performance with respect to constructions over $\mathbb{F}_{5^2}$. However, we see that the spectral efficiency is increased by about 0.3 b/s/Hz as shown in Table 4.12.

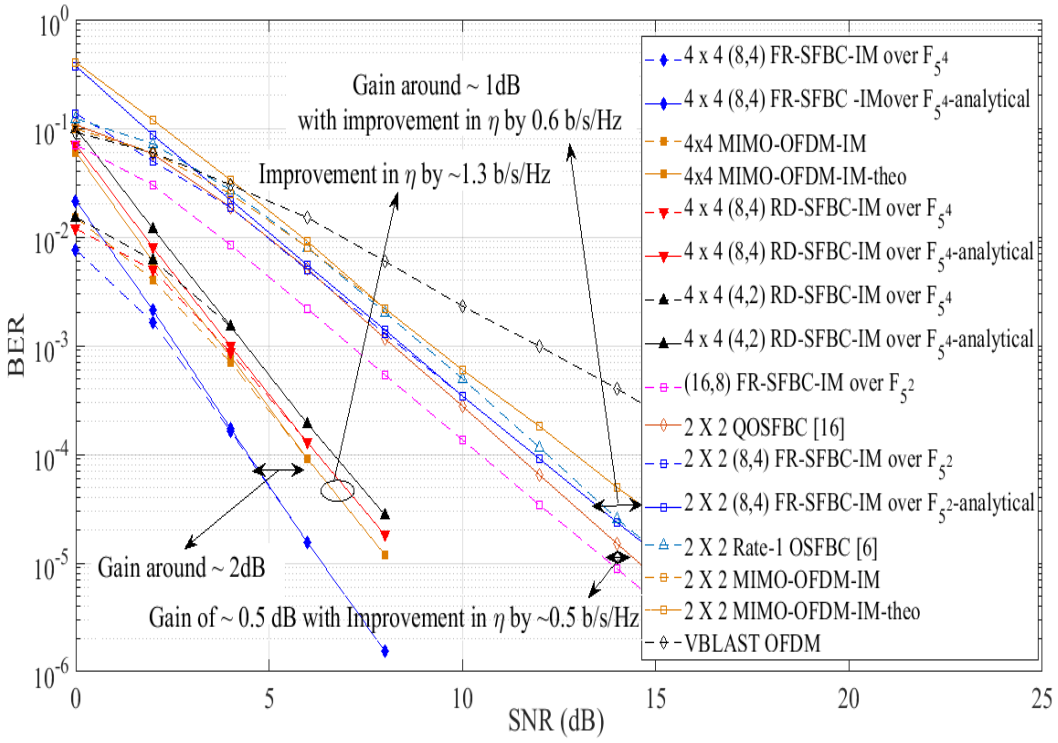


Figure 4.5: BER performance of NSFBC-IMs (FR and RD) over $\mathbb{F}_{5^2}$ and $\mathbb{F}_{5^4}$ for MIMO-OFDM-IM system with ML-ML decoding and $N_T = N_R$=2,4, N=4,8,16,32.

In Figure 4.5, we compare the BER performance of 2×2 MIMO-OFDM-IM system employing NSFBC codes over $\mathbb{F}_{5^2}$, Rate-1 OSFBC (Alamouti) codes (Torabi et al. (2007)) and full rate quasi-orthogonal space frequency block codes (QOSFBC) (Vakilian and Mehrpouyan (2016)). The detection is based on single-stage ML decoding. Moreover, VBLAST based MIMO-OFDM scheme is also considered for comparison. One can observe from Figure 4.5 that the proposed $(8, 4)$ FR-NSFBC-IM codes provide an asymptotic gain of around 1 dB when compared to MIMO-OFDM-IM with BPSK uncoded constructions (Basar (2016)). The

improvement in spectral efficiency is about 0.6b/s/Hz. A similar asymptotic performance is observed with $(8,4)$ NSFBC code with an improved spectral efficiency of around $0.9b/s/Hz$ when compared to Rate-1 Alamouti based MIMO-OFDM-IM (with rank preserving index mapping). It can be seen that $(16,8)$ NSFBC codes offer an asymptotic gain of around 0.5 dB when compared to QOSFBC (Vakilian and Mehrpouyan (2016)) based MIMO-OFDM-IM system. The performance is approximately 2 dB when compared to OSFBC based MIMO-OFDM-IM system. In this case, the improvement in spectral efficiency when compared to OSFBC-MIMO-OFDM-IM and QOSFBC-MIMO-OFDM-IM is 0.5 and 0.9 b/s/Hz respectively. In case of a 4×4 MIMO system, the asymptotic performance of $(8,4)$ RD-NSFBC-IM codes over $\mathbb{F}_{5^4}$ is observed to be similar at a BER of 10^{-4}. Here, both simulation and analytical performances have been realized to offer a gain difference of approximately 0.1 dB when compared to the existing method (Basar (2016)). However, from Table 4.8, the obtained spectral efficiency is found to be 1.3 b/s/Hz higher than the spectral efficiency quoted by MIMO-OFDM-IM system with BPSK (Basar (2016)). Hence, the proposed RD-NSFBC-IM codes offer higher spectral efficiency, when compared with the uncoded MIMO-OFDM-IM scheme (Basar (2016)). In this case, the BER performance is similar. In addition to that the proposed $(4,2)$ outperforms VBLAST OFDM. However, both the systems maintain the same spectral efficiency.

In Figure 4.6, the performance of 2×2 MIMO-OFDM-IM system employing MMSE detection has been depicted. We can see that the the proposed constructions over $\mathbb{F}_{5^2}$ provide a gain of approximately 2dB when compared to uncoded communication using BPSK (Basar (2016)). This is observed when BER is 10^{-3}. In the case of $(8,4)$ FR-NSFBC-IM codes over $\mathbb{F}_{13^2}$, $\mathbb{F}_{13^2}$, and $\mathbb{F}_{17^2}$, the BER performance gets deteriorated with an increase in the attribute q. However, Table 4.8 shows that the spectral efficiency of FR-NSFBC-IM codes over $\mathbb{F}_{7^2}$ is about 1.1 b/s/Hz higher than that of MIMO-OFDM-IM with BPSK (Basar (2016)). It is also observed that $(16,8)$ FR-NSFBC-IM code over $\mathbb{F}_{5^2}$ offer asymptotic gain of around $1dB$ when compared to $(8,4)$ FR-NSFBC-IM codes over $\mathbb{F}_{5^2}$. The spectral efficiency is same in both the cases.

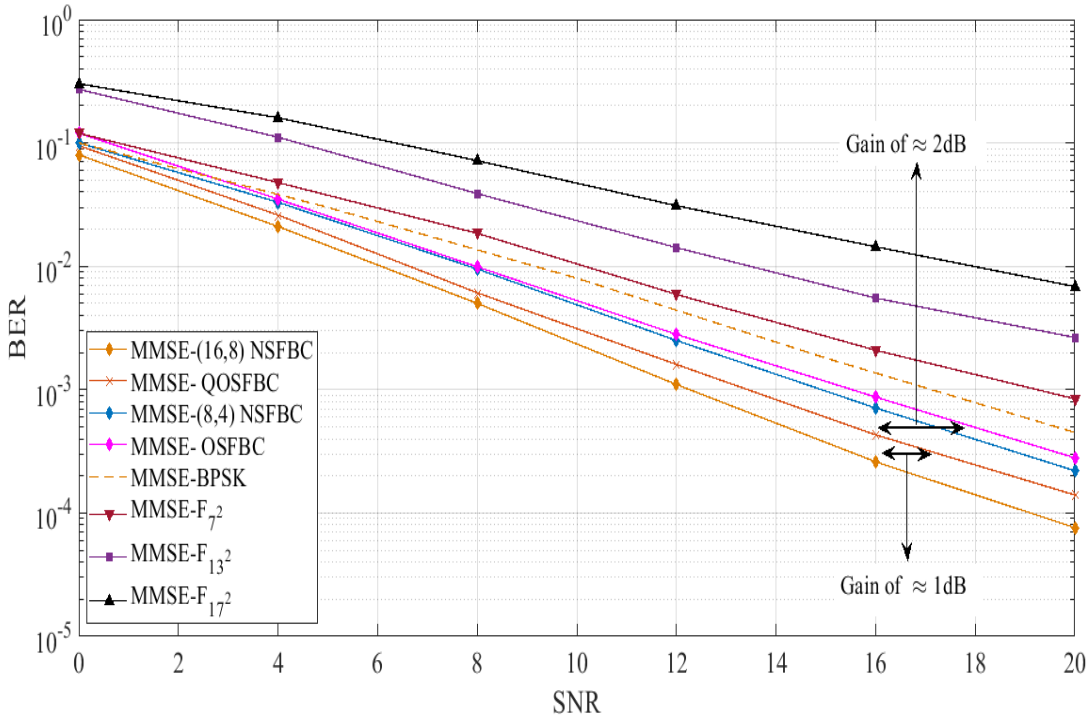


Figure 4.6: BER of the proposed NSFBC over $\mathbb{F}_{5^2}, \mathbb{F}_{7^2}, \mathbb{F}_{13^2}, \mathbb{F}_{17^2}$, for MIMO-OFDM-IM system with MMSE-ML decoding and $N_T = N_R$=2, N=4 corresponding to e_j =8.

We next consider an application that involves communication between source and sink through relay network. This scenario will allow us to examine the performance of the Block codes derived from rank codes in a two-fading channel.

4.4 Application 3: MIMO LOS communication using Relay network

Relay network based communication is gaining importance in application like surveillance and cellular communications in which communication coverage and reliability are important factors. In surveillance applications UAVs are considered for monitoring the border and transmit the information securely and reliably to the control and command station. In cellular communications Unmanned Aerial Vehicles are used as High Altitude Platforms that can increase the coverage radius. However due to altitudes at which the UAVs are placed, and the

frequency (wavelength) at which communication happens, the channels between UAV and the receiver is strongly Line of sight (LOS). However, it has been shown that spatial diversity can be created between UAV and ground station using relay network. The relay network provides virtual MIMO link between the source and the receiver. The growing demand for relay based services in case of LOS MIMO communications has created the need to examine the possibility of employing multiple antennas for realizing spatial diversity (Huo et al. (2019); Li et al. (2018)). In (Driessen and Foschini (1999); Liu and Springer (2015)), essential conditions required to obtain spatial diversity in LOS MIMO communication have been derived. It has been shown that if the inter-antenna separation at the transmitter (d_T) and the inter-antenna separation at the receiver (d_R) is such that $d_T d_R \geq \sqrt{\lambda R/4}$ (where R represents the transmitter-receiver separation and λ represents the operating wavelength), spatial diversity can be achieved. Thus, relay units can be located in a distributed manner to achieve spatial diversity, which can be brought about by ensuring proper separation between antennas placed on the relay unit and the antennas placed in the ground station or separation between relay units and the corresponding antennas in the ground station. In dense environments, spatial diversity combined with the use of STBCs and energy efficient spatial modulation strategies can result in reliable communication with improved spectral efficiency. In (Driessen and Foschini (1999)) authors have considered the creation of spatial diversity LOS MIMO channels. Hanna et al. (2019) proposed two distributed algorithms that adapt UAV position, to achieve multiplexing gain in cooperative communications containing UAV relay networks. One algorithm is based on gradient change and the other algorithm is based on brute force optimization. In (Liu and Springer (2015)) authors have proposed the use of space shift keying strategies in applications that involve spatially diverse LOS MIMO channels. In (Choi et al. (2016)) authors have attempted to use STBCs in a network of UAVs that act as relay nodes. The relay node UAVs work in cooperative mode to provide a virtual MIMO link (An effective MIMO link between the transmit and receive antenna systems with the repeater in between). The architecture in (Choi et al. (2016)) employs STBCs in a distributed manner. Following the analysis given in (Choi et al. (2016); Fotouhi et al. (2019)), in this work we propose two cooperative architectures that use relay units to achieve spatial diversity in LOS communi-

cation. The first design employs Space-Time Block Codes for 2×2 LOS MIMO network. The second design employs energy-efficient Space-Time Block Coded Spatial Modulation (STBC-SM) technique for 4×4 LOS MIMO network.

4.4.1 System model

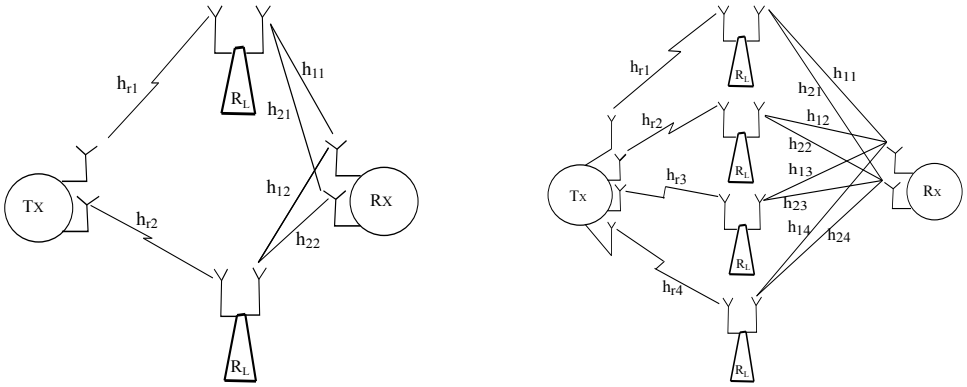


Figure 4.7: LOS MIMO architectures with cooperative relay network

The communication architectures that facilitate the use of NSTBC and NSTBC-SM are shown in Fig 4.7. The units labelled $\mathbf{R}_L$ are the relay units that provide virtual MIMO link between transmitter (**Tx**) and receiver (**Rx**). The arrangement of relay units, inter-unit distance d_1 and the minimum distance $\mathscr{R}$ between the relay network and the receiver are chosen to ensure orthogonality between relay units' signatures (Driessen and Foschini (1999); Liu and Springer (2015)). The orthogonality between signatures ensures spatial diversity and maximizes the diversity gain between transmitter and receiver. Further, the relay units are equipped with two directional antennas to support simultaneous transmission and reception using frequency division duplexing (FDD). In our work, the transmitter (**Tx**) is considered to UAV that possesses multiple directional antennas and supports beamforming (Fotouhi et al. (2019)). The transmitter UAV is either master drone (surveillance) or the mobile base station (cellular communications). The number of transmitter antennas N_T at **Tx** is equal the number of relay units. Further, the value of N_T is chosen to be equal to the number of rows of STBC, for STBC based communication. The value of N_T is chosen to be greater than the number of rows of STBC, for the case of STBC-SM. The relay units can be either ground-based relay

units or UAVs. In case of relay network formed by UAVs, the velocity of all the UAVs is constrained to provide minimal or negligible Doppler shift in the received signal. This can be achieved using additional sensors at UAVs, with each sensor sharing its coordinates with other sensors (Hanna et al. (2019)) so that the UAVs can maintain the same relative distance and orientation with respect to each other and the receiver (ground station). Alternatively, we can assume that the UAVs are firmly tethered to the ground so that they appear to be more or less stationary. In this work, we consider NSTBCs obtained in Section 4.1.1 and show that they can be used to enhance communication security. The reason for choosing these constructions is two-fold: a) rectangular STBCs of the desired length can be obtained, that can offer greater euclidean distance between codewords when compared with square constructions. b) the constructions provide an additional degree of freedom in choosing the free transform component indices that constitute the cyclic code. This can be used to construct a cryptographic key.

4.4.2 Transmitter

Consider a vector $\mathbf{c} = \{c_0, c_1, \cdots, c_{n-1}\}$ with $c_i \in \mathbb{F}_{q^r}$, $0 \leq i \leq n-1$. In Chapter 2, it was shown that the elements of vector $\mathbf{c}$ (i.e $c_i, 0 \leq i \leq n-1$) can be obtained using GFFT equation $c_i = \frac{1}{(n \bmod q)} \sum_{w=0}^{n-1} V_w \beta^{-iw}$ with $V_w \in \mathbb{F}_{q^m}$ for all $0 \leq w \leq n-1$. Here, β is the n^{th} root of unity in $\mathbb{F}_{q^r}$. It was shown that the rank of $\mathbf{c}$ depends on the choice of indices $w \in \mathscr{W} \subset [0, n-1]$ for which $V_w | w \in \mathscr{W}$ are free and rest of the indices are constrained to zero. More specifically it was shown that the rank of $\mathbf{c}$ depends on the size of the $q-$ cyclotomic cosets from which the index $w \in \mathscr{W}$ is chosen. The number of free transform indices k is equal to the size of the set $\mathscr{W}$ and the set of codeword vectors $\mathbf{c}$ obtained for all possible values of $V_w \in \mathbb{F}_{q^m}$ is called an (n, k) code $\mathscr{C}$. Since V_w take all possible values from $\mathbb{F}_{q^m}$ and since there are $k-$ V_ws, there will be q^{km} distinct vectors in $\mathscr{C}$. It was shown that if index subset $\mathscr{W}$ contains indices with each chosen from a distinct $q-$ cyclotomic coset of size r, then the matrix associated with each codeword vector $\mathbf{c}$ is of rank$-m$. The corresponding code $\mathscr{C}$ obtained for all possible values of V_ws is a rank$-r$ code . This (n, k) full row rank code $\mathscr{C}$ can be used as Space Time Block Code using suitable rank preserving maps. Following Theorem 1-6 in chapter 2, the

number of columns of STBC codeowrd is given by $e_j = |\mathscr{W}|r$. The elements of codeword matrix are over $\mathbb{F}_q$ and are mapped to complex constellation using rank preserving maps like Gaussian integer map (Huber (1994b)) or Eisenstein-Jacobi integer map (Huber (1994a)). Since the proposed architectures have 2/4 relay units, and since number of rows of STBC is equal to the number of transmit antennas, in this application we consider codewords over $\mathbb{F}_{q^2}, \mathbb{F}_{q^4}$.

4.4.2.1 Formation of index key

We see that the subset $\mathscr{W}$ contains $k-$ elements that are chosen from k different $q-$ different cyclotomic cosets of size m. From the definition of $q-$ cyclotomic cosets we see that for any integer set $Z = \{0, 1, \cdots, n-1\}$, if $\mathcal{L}$ represent the number of $q-$ cyclotomic coset of size m then we have $\binom{\mathcal{L}}{k}$ possible group of cyclotomic cosets of size r from which we can select k free transform component indices. From this group of k cyclotomic cosets we have m^k number of $k-$ tuple indices which each giving rise to unique full rank code $\mathscr{C}$. Thus in total we have $N_k = \binom{\mathcal{L}}{k} m^k$ number of possible $k-$ tuple combinations with each combination giving rise to rank$-m$ code and hence corresponding STBC. Each STBC, in turn, has q^{km} number of codeword matrices. Using this additional degree of freedom offered by the choice of free transform component indices, the transmitter and receiver can jointly establish an arrangement to follow through the set of component codes in a particular order. This arrangement is called the index key and is given by.

$$\{(\ell_0^0, \ell_1^0, \cdots, \ell_{k-1}^0), (\ell_0^1, \ell_1^1, \cdots, \ell_{k-1}^1), \cdots, (\ell_0^{L-1}, \ell_1^{L-1}, \cdots, \ell_{k-1}^{L-1})\} \tag{4.26}$$

The length of the key (represented by L) is defined as the number of combinations in the key. To illustrate this idea we consider the following example.

Example: Let $n = 15, l = 3, q = 2, m = 4$.

The $2-$ cyclotomic cosets *mod* 15 are given by:

$[0]_{15} = \{0\}$, $[1]_{15} = \{1, 2, 4, 8\}$, $[3]_{15} = \{3, 6, 12, 9\}$, $[5]_{15} = \{5, 10\}$ $[7]_{15} = \{7, 14, 13, 11\}$

The residue classes modulo $\frac{n}{m} = 5$ are given by

$(0)_{15,3} = \{0, 5, 10\}$, $(1)_{15,3} = \{1, 6, 11\}$, $(2)_{15,3} = \{2, 7, 12\}$, $(3)_{15,3} = \{3, 8, 13\}$, $(4)_{15,3} = \{4, 9, 14\}$.

Following case 2 of proposition 2 and also from (Dey and Rajan (2003)), we see that $(8, 2)$ quasi-cyclic codes of rank 4 can be obtained by choosing any one combination of indices listed in the table 4.9

Table 4.9: List of Combinations which can give rise to full rank codes

$(1, 6)$	$(1, 11)$	$(6, 11)$	$(2, 7)$	$(2, 12)$	$(7, 12)$	$(3, 8)$	$(8, 13)$	$(3, 13)$
$(4, 9)$	$(9, 14)$	$(4, 14)$	$(1, 7)$	$(1, 12)$	$(1, 3)$	$(1, 13)$	$(1, 9)$	$(1, 14)$
$(6, 2)$	$(6, 7)$	$(6, 8)$	$(6, 13)$	$(6, 4)$	$(6, 14)$	$(11, 2)$	$(11, 12)$	$(11, 3)$
$(11, 8)$	$(11, 4)$	$(11, 9)$	$(2, 3)$	$(2, 13)$	$(2, 9)$	$(2, 14)$	$(7, 3)$	$(7, 8)$
$(7, 4)$	$(7, 9)$	$(12, 8)$	$(12, 13)$	$(12, 4)$	$(12, 14)$	$(3, 4)$	$(3, 14)$	$(8, 9)$
$(8, 14)$	$(13, 4)$	$(13, 9)$	NA					

There are 48 number of free transform component indices indicated in table 4.9. Each choice of transform domain indices will give rise to a rank-4 3-quasi cyclic code, which we will refer to as a component code $\mathscr{C}_p$. An example representation of key obtained by following the rows of the row table one by one is given below.

$$(1, 6), (1, 11), \cdots, (3, 13), (4, 9), \cdots, (9, 14) \cdots, (1, 14), \cdots, \cdots, (8, 14), (13, 4), (13, 9).$$

In practice the order of key can be random, component indices can repeat and length of key can be users choice. The length of the key (represented by L) is defined as the number of combinations in the key. Each combination specifies a particular component code (or equivalently an entry in Table 4.9). Similar to cryptographic keys, the level of security of communication increases with randomness in the order of selection and length of the key. In addition to this security can be enhanced by dynamically changing the key during communication. This adds to the security in applications where secure transfer of tactical information is required.

4.4.2.2 Transmission

One the index key is formed, the transmitter uses a secure channel to communicate the index key to the receiver. Initially a frame of length $\lfloor log_2(q^{kb}) \rfloor$ bits is considered at the input of the transmitter. Let the frame be represented as $\mathbf{u} = (u_{0,0}, \cdots, u_{0,b-1}, \cdots, u_{k-1,0}, \cdots, u_{k-1,b-1})$. The frame $\mathbf{u}$ is then split into k parallel streams each of length b given by $\mathbf{u^w} = (u_{w,0}, u_{w,1}, \cdots, u_{w,m-1})$ with $0 \leq w \leq k-1$. Each $\mathbf{u}^w$ is mapped onto $m-$ tuple vector with elements over $\mathbb{F}_q$. This is analogous to $m-$ tuple integer representation of $b-$ length binary vector with $b = qm$. This $m-$tuple vector is the assigned an equivalent symbol from $\mathbb{F}_{q^m}$ with $m = 2, 4$. $k-$ such symbols obtained are assigned to corresponding $k-$free transform components with free transform component indices obtained from index key. $m \times n$ full rank codeword is then obtained using the procedure mentioned Chapter 2. The codeword matrices obtained will have elements from the finite field $\mathbb{F}_q$. These elements are mapped onto two dimensional complex plane using rank preserving maps like Gaussian Integer map (Huber (1994b)) and Eisenstein-Jacobi Integer map (Huber (1994a)). This result in NSTBC codeword $\mathbf{X}$ with symbols from rectangular or hexagonal constellation as given by 4.1.1 and is rewritten below.

$$\mathbf{X} = \begin{bmatrix} \zeta(c_{00}) & \zeta(c_{01}) & \zeta(c_{02}) & \cdots & \zeta(c_{0\,e_j-1}) \\ \zeta(c_{10}) & \zeta(c_{11}) & \zeta(c_{12}) & \cdots & \zeta(c_{1\,e_j-1}) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \zeta(c_{m-1\,0}) & \zeta(c_{m-1\,1}) & \zeta(c_{m-1\,2}) & \cdots & \zeta(c_{m-1\,e_j-1}) \end{bmatrix} \tag{4.27}$$

If spatial modulation is employed then the transmitter considers s_a bits after the data frame to select the active transmit antennas through which the NSTBC codeword symbols are transmitted. The selected active antenna combination remain same throughout the NSTBC transmission. Since rows represent antenna dimension, the resulting NSTBC-SM codeword is

given as

$$\mathbf{X}_{IM} = \begin{bmatrix} \zeta(c_{00}) & \zeta(c_{01}) & \zeta(c_{02}) & \cdots & \zeta(c_{0\,e_j-1}) \\ 0 & 0 & 0 & \cdots & 0 \\ \zeta(c_{10}) & \zeta(c_{11}) & \zeta(c_{12}) & \cdots & \zeta(c_{1\,e_j-1}) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \\ \zeta(c_{m-1\,0}) & \zeta(c_{m-1\,1}) & \zeta(c_{m-1\,2}) & \cdots & \zeta(c_{m-1\,e_j-1}) \end{bmatrix} \tag{4.28}$$

Each row of NSTBC/NSTBC-SM codeword is then transmitted to its corresponding relay unit U_R which decodes and forwards to the receiver.

4.4.2.3 *Choice of index key*

In practice, the index key can be random, and the length of the index key ($\mathbf{L}$) can be chosen as per the requirement. From the formation of index key one can observe that if the index combinations are selected such that they have more than one common element (but not all) at different locations, then the amount of uncertainty in estimating the transmitted codeword, in the absence of index key is high. To illustrate this idea let us consider STBCs obtained from cyclic codes of length 15 over $\mathbb{F}_{2^4}$ constructed with $k = 2$ free transform component indices. 4.9 there are 48 choices of 2-tuple free transform component indices that will result in a rank-4 cyclic code. A possible index key with $k = 2$ is given by $\{(1,6),(1,3),(3,7)\cdots,(3,8),(4,9),\cdots,(1,13),\cdots\cdots,(8,9)\}$. The index key contains the combinations (1,3) and (3,7) with element 3 in common but at a different location. That is in the combination (1,3) element 3 is in the second place and in the combination (3,7) element 3 is in the first place. For the component code designed using a combination (1,3), the codeword obtained for the data sequence '00001010' and the codeword obtained for the data sequence '10100000' with (3,7) as the index combination is same. This means that in the absence of the knowledge of index key, there is uncertainty regarding the data sequence associated with the codeword. It can be noted that the amount of uncertainty increases with an increase in k as there can be more than one index element in common between the free transform domain combinations, and also depend on the length of index key $\mathbf{L}$ which is user

choice. In particular, there can be $N_k{}^{\mathbf{L}}$ number of possible index key combinations. For the example chosen above if the length of the key is full (i.e if $\mathbf{L} = 48$) then there can be $48^{48} = 2^{240} + 2^{192}$ possible number of index key combinations out of which one is legitimate. In the case of the AES-128 encryption scheme, the total possible combinations are 2^{126}. Thus, for an unintended user, the possibility of finding out the key and then the transmitted information in real time is highly complex and practically improbable and is almost impossible in case if index key hopping is employed. Table 4.10 gives the number of possible key combinations for various values of $q, m, \mathcal{L}, e_j, k, N_k$.

Table 4.10: Number of possible key combinations for codes over $\mathbb{F}_q$.

q	m	$\mathcal{L}$	(e_j, k)	N_k	# of possible key combinations
5	2	10	(4,2)	180	$180^{\mathbf{L}}$
7	2	21	(4,2)	840	$840^{\mathbf{L}}$

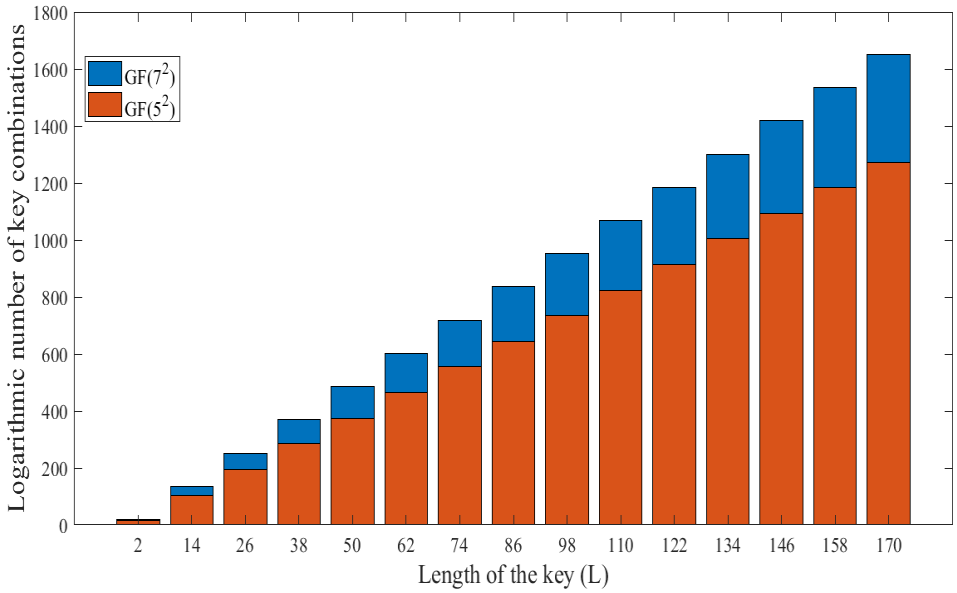


Figure 4.8: Number of possible keys in logarithmic scale

Figure4.8 gives the graph of a logarithmic number of possible keys (in terms of log_2) with respect to the length of the key. The length of the key is varied from 2 to 180. As can be seen from the figure the number of possible keys is around 2^{450} in case of codewords designed over $\mathbb{F}_{5^2}$ with an index key of length $\mathbf{L} = 62$. The number of possible keys is 2^{600} in

case of codewords designed over $\mathbb{F}_{7^2}$ for a key of length $\mathbf{L}$ =62. Thus, for the appropriate length of the index key, the illegitimate user will not be able to decode the information in real time in the absence of the index key. Further, for the appropriate choice of the index key, the ambiguity in the information in the absence of index key can be high. Thus making the proposed scheme best suitable for tactical communications involving relays. The output of each transmit antenna is then received by the corresponding relay unit.

4.4.3 Relay network

Assuming that all relay units receive the symbols simultaneously (cooperative), the received vector representing the received symbols at corresponding relay units is given by

$$Y^i = \mathbf{H}^i_{relay} X^i_{IM} \tag{4.29}$$

Here, X^i represents i^{th} column of the STBC codeword.

$\mathbf{H}^i_{relay} = diag(h_{0,0}, h_{1,1}, h_{2,2}, \cdots, h_{N_t-2,N_t-2}, h_{N_t-1,N_t-1})$. with $h_{i,i}$ representing the channel fading coefficient between transmitting antenna i and corresponding relay unit i. In this chapter we have considered the fading between transmitting antenna and the corresponding relay network unit to be Rician distributed. A Rician fading channel can be described by two parameters: K and Ω.K is the ratio between the power in the direct path and the power in the other, scattered, paths. Ω is the total power from both paths ($\Omega = \nu^2 + 2\sigma^2$), and acts as a scaling factor to the distribution.

The channel coefficient amplitude h is then Rice distributed with parameters $\nu^2 = \dfrac{K}{1+K}\Omega$ and $\sigma^2 = \dfrac{\Omega}{2(1+K)}$. The resulting PDF then is:

$$f(h) = \frac{2(K+1)h}{\Omega} \exp\left(-K - \frac{(K+1)h^2}{\Omega}\right) I_0\left(2\sqrt{\frac{K(K+1)}{\Omega}}h\right) \tag{4.30}$$

where, $I_0(\cdot)$ is the 0^{th} order modified Bessel function of the first kind. Each relay unit employs the decode and forward strategy. The MMSE estimated vector at the relay unit can be obtained by,

$$\hat{X}^i_{IM} = \mathbf{H}^{i^H}_{relay}(\mathbf{H}^i_{relay}\mathbf{H}^{i^H}_{relay} + \rho^{-1}I)Y^i \tag{4.31}$$

Each U_R then forwards the estimated symbols to the receiver.

4.4.4 Receiver

After n time slots, the received $N_R \times N_T$ matrix is given by

$$\mathscr{Y} = \mathbf{H}\hat{\mathbf{X}}_{IM} + \mathbb{N} \tag{4.32}$$

Here $\widehat{\mathbf{X}}_{IM} = \{\hat{X^0_{IM}}, \hat{X^1_{IM}}, \cdots, \hat{X^{n-1}_{IM}}\}$, is the estimated codeword forwarded by the relay network. $\mathbb{N}$ is the noise matrix of dimension $N_R \times n$ with elements that are realizations of circularly symmetric complex Gaussian distribution with zero mean and variance σ_n^2. $\mathbf{H}-$ represents the $N_R \times N_T$ channel matrix between relay network and the receiver. The general representation of $\mathbf{H}$ that can be used for both correlated and uncorrelated channels is given by $\mathbf{H} = R_{R_x}\mathbf{H}_u R_{U_R}$. Here R_{Rx} is the $N_R \times N_R$ receiver correlation matrix, is the $N_T \times N_T$ relay network correlation matrix, and $\mathbf{H}_u$ is the uncorrelated channel matrix representing the uncorrelated Rayleigh, Rician or Nakagami-m distribution. In case of uncorrelated Rayleigh and Rician fading, the channel magnitude follows (4.10), (4.30). When representing the uncorrelated Nakagami-m fading, the fading coefficient h_u follows the following density function

$$f(h_u;\, m, \Omega) = \frac{2m^m}{\Gamma(m)\Omega^m} h_u^{2m-1} \exp\left(-\frac{m}{\Omega}h_u^2\right), \forall h_u \geq 0. \;\; (m \geq 1/2, \text{ and } \Omega > 0) \tag{4.33}$$

Following (GD et al. (2017); Yacoub (2009)), a more realistic non uniform phase distribution has been considered to model the channel coefficients that exhibit Nakagami-m fading environment. Assuming the availability of perfect channel state information (CSI) at receiver end, the estimate of vector $\hat{\mathbf{X}}_{IM}$ is obtained by.

$$\widehat{\hat{\mathbf{X}}}_{IM} = argmin\left(\|\mathscr{Y} - \mathbf{H}\mathbf{X}_{IM}\|^2\right), \;\; \forall \mathbf{X}_{IM} \in \mathscr{X} \tag{4.34}$$

Here, $\widehat{\hat{\mathbf{X}}}_{IM}$ is an estimate of the transmitted codeword $\mathbf{X}_{IM}$ and $\mathscr{X}$ refers to the NSTBC-SM code $\mathscr{X}$ that is used at the transmitter. After obtaining $\widehat{\hat{\mathbf{X}}}_{IM}$ the receiver decodes antenna selection bits by finding rows with more number of zeros (in case of architecture supporting

STBC-SM) and data bits by searching nearest codeword of the component code. At this point it can be noted that the receiver can decode the data bits correctly only if the search is within the component code that is used at the transmitter. In the next section we derive an union bound on the probability of error of the proposed scheme.

4.4.5 Analytical Upper bound

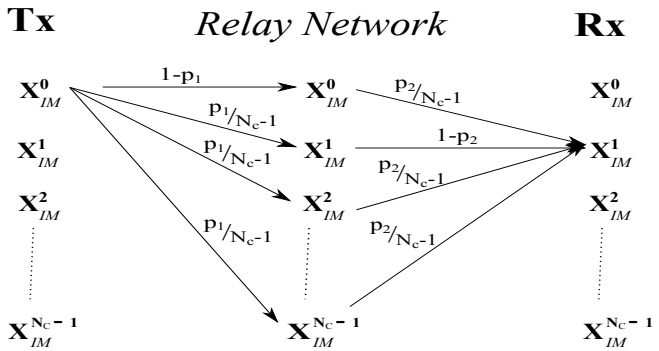


Figure 4.9: Graphical representation for Error computation

From the previous section, we infer that the decoding error at the receiver depends on two factors: 1) Symbols estimated at the relay network. 2) MIMO Channel between the relay network and receiver. The union bound on average BER can be expressed as

$$ABER = \frac{1}{N_c} \sum_{i=0}^{N_c-1} \sum_{j=0}^{N_c-1} \frac{N(X^i_{IM}, X^j_{IM})}{\eta} P_{error} \tag{4.35}$$

Here, $N(X^i_{IM}, X^j_{IM})$ represents the number of errors in the data sequences associated with X^i_{IM} and X^j_{IM}, η represents the spectral efficiency and N_c represents the number of codewords in component STBC. From Figure 4.9 we infer that P_{error} can be obtained by evaluating the probability that $\mathbf{X}^i_{IM}$ is decoded as $\mathbf{X}^k_{IM}$, $0 \leq i, k \leq N_c - 1$ and probability that $\mathbf{X}^k_{IM}$ is decoded as $\mathbf{X}^j_{IM}$, $k \neq j$. Let p_1 denote the probability of error at relay network and let p_2 denote the probability of error at receiver. It can be seen that the symbol estimation at each relay unit R_L is independent of the symbol estimations of other relay units and also independent with respect to symbol estimation in different time slots. The $r-$ independent symbol estimations at the $r-$ relay units, of a particular i^{th} column vector $\hat{X}^i_{IM}$ of $\hat{\mathbf{X}}_{IM}$, can be considered as an

estimation of $r-$length vector by the relay network. Since there is no interference between symbols of a column and between different columns of NSTBC/NSTBC-SM codeword, the conditional pdf of MMSE estimated $\hat{\mathbf{X}}_{IM}$, is given by (Basar (2016)).

$$f(\hat{\mathbf{X}}_{IM}|\mathbf{X}_{IM}) = \frac{\pi^{mn}}{det(\mathbf{C})} exp\{-(\hat{\mathbf{X}}_{IM} - \mu)^H \mathbf{C}^{-1} (\hat{\mathbf{X}}_{IM} - \mu)\} \tag{4.36}$$

Where, $\mu = E(\mathbf{X}_{IM})$ is the mean matrix of $\mathbf{X}_{IM}$ and $\mathbf{C} = cov(\mathbf{X}_{IM})$ is the covariance matrix of $\mathbf{X}_{IM}$. The simple MMSE detector decides onto the most likely codeword by maximizing the pdf $f(\hat{\mathbf{X}}_{IM}|\mathbf{X}_{IM})$, as (Basar (2016))

$$\begin{aligned} \hat{\mathbf{X}}_{IM} &= \underset{\mathbf{X}_{IM}}{arg\ max}\ f(\hat{\mathbf{X}}_{IM}|\mathbf{X}_{IM}) \\ &= \underset{\mathbf{X}_{IM}}{arg\ max}\ \sum_{i=0}^{r-1} \sum_{j=0}^{n-1} \frac{|\hat{x}_{IM}^{i,j} - Q_{i,j} x_{IM}^{i,j}|^2}{C_{i,j}} \end{aligned} \tag{4.37}$$

After the estimation of $n-$ columns vectors, following the analysis given in (Basar (2016)), p_1 can be given by

$$p_1 = E_H \left(P_1 \left(\hat{\mathbf{X}}_{IM} \rightarrow \mathbf{X}_{IM} | \mathbf{H}_{relay} \right) \right). \tag{4.38}$$

Here $E_H(\cdot)$ represents the expectation over $\mathbf{H}_{relay}$. $P_1 \left(\hat{\mathbf{X}}_{IM} \rightarrow \mathbf{X}_{IM} | \mathbf{H}_{relay} \right)$ is obtained by maximizing $f(\hat{\mathbf{X}}_{IM}|\mathbf{X}_{IM})$. Following (26) of (Basar (2016)) we have

$$P_1 \left(\mathbf{X}_{IM} \rightarrow \mathbf{E}_{IM} | \mathbf{H}_{relay} \right) = P_1 \left(\sum_{i=0}^{r-1} \sum_{j=0}^{n-1} \frac{|\hat{x}_{IM}^{i,j} - Q_{i,j} x_{IM}^{i,j}|^2 - |\hat{x}_{IM}^{i,j} - Q_{i,j} e_{IM}^{i,j}|^2}{C_{i,j}} > 0 \right) \tag{4.39}$$

Following complex constellation with i.i.d real and imaginary parts $P_1 \left(\mathbf{X}_{IM} \rightarrow \mathbf{E}_{IM} | \mathbf{H}_{relay} \right)$ given in 4.39 can be given by, (Basar (2016))

$$P_1 \left(\mathbf{X}_{IM} \rightarrow \mathbf{E}_{IM} | \mathbf{H}_{relay} \right) = Q \left(\sqrt{\sum_{i=0}^{m-1} \sum_{j=0}^{e_j - 1} V_{i,j} \delta_{i,j}} \right) \tag{4.40}$$

With $V_{i,j} = \frac{Q_{i,j}}{2C_{i,j}}$. Here, $C_{i,j}$ is $(i,j)^{th}$ element of a covariance matrix $\mathbf{C}$ of $\widehat{\mathbf{X}}_{IM}$. Similarly $Q_{i,j} \in Q = \mathbf{H}_{relay}^H (\mathbf{H}_{relay} \mathbf{H}_{relay}^H + \rho^{-1} I) \mathbf{H}^H \mathbf{H}$ and $\delta_{i,j} = |x_{IM}^{i,j} - e_{IM}^{i,j}|^2$. Since LOS MIMO

channels are considered, $Q_{i,j} \approx 1$ and $C_{i,j} \approx n_i(h_{i,j}^{relay})^{-1}((h_{i,j}^{relay})^{-1})^H$. Using Craig's formula

$$P_1\left(\hat{\mathbf{X}}_{IM} \rightarrow \mathbf{X}_{IM}|\mathbf{H}_{relay}\right) < 1/\pi \int_0^{\pi/2} exp\left(\frac{-\sum_{i=0}^{r-1}\sum_{j=0}^{n-1} Z_{i,j}\delta_{i,j}}{4N_0 sin^2(\theta)}\right)d\theta \tag{4.41}$$

Here $Z_{i,j} = 1/((h_{i,j}^{-1})^H h_{i,j}^{-1})$, has exponential distribution, Since N_T is equal to the number of relay units, the Moment Generating Function of $z_{i,j}$ is given by $M_z(t) = 1/(1-t)\ \ 0 \leq t \leq N_T - 1$(Basar (2016)). Averaging (4.41) over $\mathbf{H}_{relay}$, we have

$$p_1 = E_H\left(P_1\left(\hat{\mathbf{X}}_{IM} \rightarrow \mathbf{X}_{IM}|\mathbf{H}_{relay}\right)\right) < \frac{1}{\pi}\int_0^{\pi/2}\prod_{i=1}^{r}\prod_{j=1}^{n}\left(\frac{\sin^2\theta}{\sin^2\theta + \frac{\delta_{i,j}}{4N_0}}\right)d\theta \tag{4.42}$$

Equation (4.42) has a closed form expression given in appendix 5A of (Simon and Alouini (2005)). Similarly p_2 is evaluated at the receiver. Since ML decoding is employed, following (Simon and Alouini (2005)) the CPEP at receiver is given by

$$P_2\left(\mathbf{X}_{IM} \rightarrow \mathbf{E}_{IM}|\mathbf{H}\right) = Q\left(\sqrt{(\rho/2)}\,\|\mathbf{H}\left(\mathbf{X}_{IM} - \mathbf{E}_{IM}\right)\|\right) \tag{4.43}$$

Following (Simon and Alouini (2005)), p_2 is obtained by considering Craig's formula for $Q-$function and averaging over all possible channel realizations $\mathbf{H}$, given by

$$p_2 = E_H\left(P_2\left(\mathbf{X}_{IM} \rightarrow \mathbf{E}_{IM}|\mathbf{H}\right)\right) < \frac{1}{\pi}\int_0^{\pi/2}\prod_{n=1}^{N}\left(\frac{\sin^2\theta}{\sin^2\theta + \frac{\|\mathbf{H}(\mathbf{X}_{IM}-\mathbf{E}_{IM})\|^2}{4N_{0,F}}}\right)d\theta \tag{4.44}$$

Closed form expression of (4.44) for various channel models are given in chapter 5 of (Simon and Alouini (2005)). Following this, from 4.35 and Figure 4.9 ABER is then given by (4.45).

$$ABER = \frac{1}{N_c}\sum_{i=0}^{N_c-1}\sum_{j=0}^{N_c-1}\frac{N(X_{IM}^i, X_{IM}^j)}{\eta}(1-p_1)\frac{p_2}{N_c-1} + \frac{p_1}{N_c-1}(1-p_2)(N_c-2)\frac{p_1 p_2}{(N_c-1)^2} \tag{4.45}$$

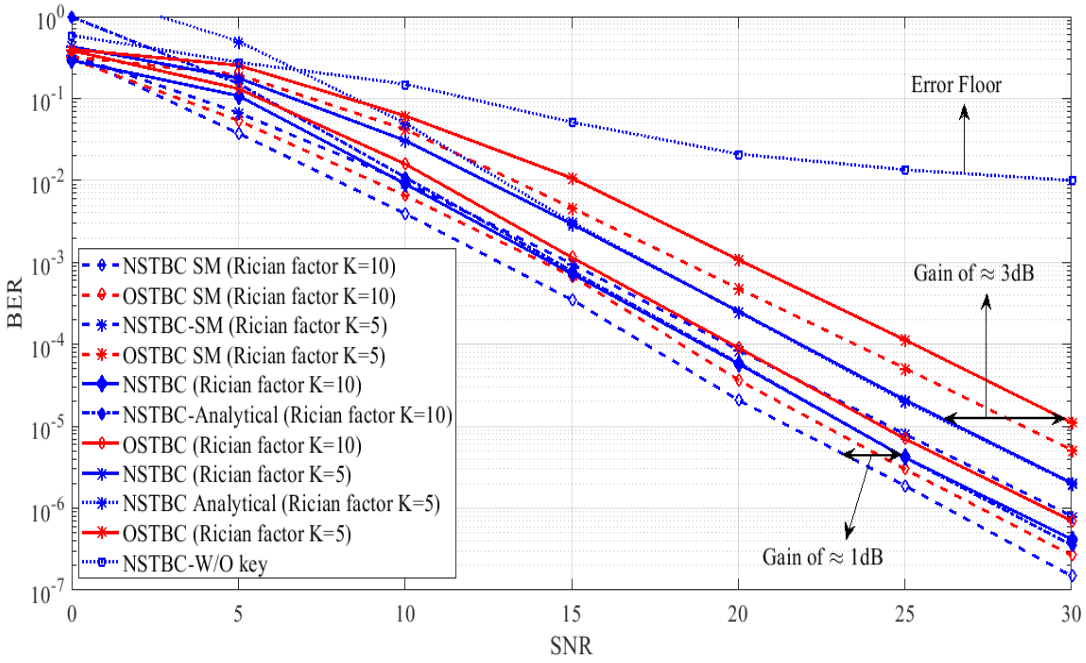


Figure 4.10: BER performance NSTBC-SM for LOS MIMO channel (Rician-Rician fading)

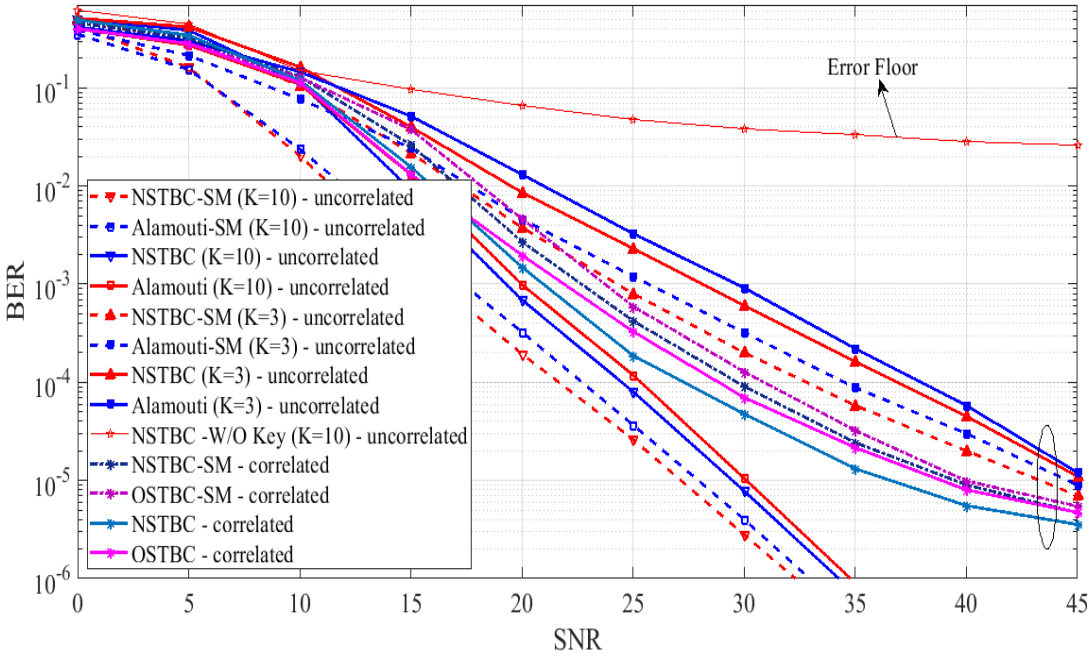


Figure 4.11: BER performance of NSTBC-SM for Rician-Rayleigh fading

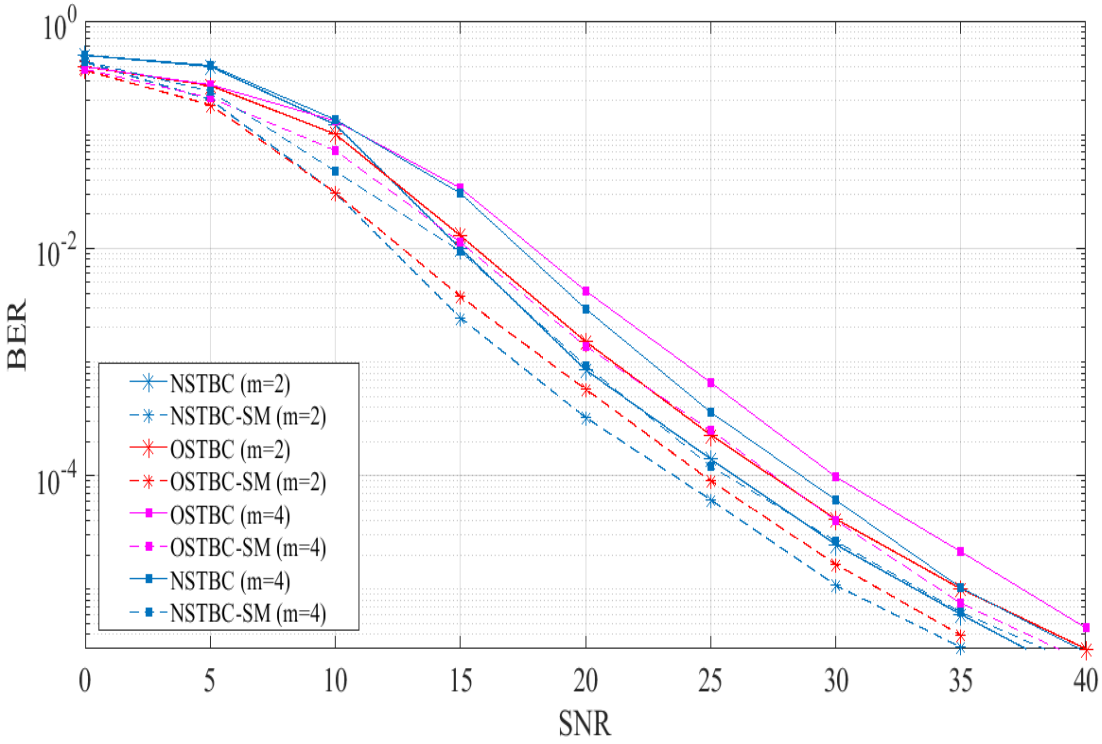


Figure 4.12: BER performance of NSTBC-SM for Rician-Nakagami-m fading

4.4.6 Simulation Results

Performance of the proposed codes is evaluated in an $N_T \times N_R$ system with the parameters specified in Table 4.11. These designs are based on full rank codes obtained from cyclic codes over $\mathbb{F}_{q^r}$ with $q = 5, 7$ and $r = 2$. Further, we choose $k = |\mathscr{W}| = 2$ resulting in $n = |\mathscr{W}|r = 4$. Each subset $\mathscr{W}$ is chosen such that the $(4, 2)$ component NSTBC is of rank $r = 2$. Since N_T is 4 in the second architecture, we have used 4 out of $\binom{4}{2} = 6$ combinations to obtain 4×4 NSTBC-SM codewords. For fair comparison we have considered codes that offer spectral efficiency of approximately $\eta = 3$ bpcu. The spectral efficiency of NSTBC over $GF(7^2)$ is 2.8 bpcu and NSTBC-SM over $GF(5^2)$ is 3.32 bpcu. To understand the performance of the proposed architectures in various environments that support spatial diversity, we have employed the empirical UAV channel described in (Khuwaja et al. (2018)). More specifically, due to the presence of strong LOS component, we consider Rician fading between the transmitting antennas and the corresponding relay unit. The channels between each relay unit and

Table 4.11: Simulation Parameters

Parameter	Value
N_T	2,4
N_R	2,4
q	5,7
r	2
Rician factor K	5,10

receiver are modelled using Rician/Nakagami-m fading that accommodates Rayleigh fading as a special case. For fair comparison in terms of spectral efficiencies, we have considered Alamouti STBC with 8-PSK and Alamouti STBC-SM with QPSK that result in $\eta = 3$ bpcu. Figure 4.10 shows the performance of the proposed scheme in case of Rician-Rician fading (LOS MIMO) between transmitter and receiver. That is the channel between the transmitter and relay units is considered as Rician fading with strong LOS and the channel between relay network and receiver is considered to be Rician with strong and weak LOS component. The Rician factor K is considered to be 5,10. Simulation results show that in the presence of index the proposed NSTBC codes over $\mathbb{F}_{5^2}$ provide an asymptotic gain of around 1dB with increased spectral efficiency of 0.32 bpcu when compared to Alamouti STBC. Further, the proposed NSTBC-SM codes are observed to offer a gain of around 3 dB when compared to corresponding NSTBC codes.

Figure 4.11 shows the performance of the proposed scheme in case of Rician-Rayleigh fading (both correlated and uncorrelated). In the case of correlated channels, the correlation is considered to be dense (inter antenna separation is 0.1λ). From the figure, it can be inferred that in the case of uncorrelated fading environment, the asymptotic performance of the proposed NSTBC-SM scheme is around 3dB greater than NSTBC codewords. Further, it can be noticed that the performance of the NSTBC/NSTBC-SM codes in the presence of Rician fading with K=10 between the transmitter and Relay units is 10dB better than its performance in Rician fading environment with K=3. In case of an environment characterized by the antenna correlation, the performance of the NSTBC scheme is better than NSTBC-SM. This may be due to an error in estimating antenna selection bits. Additionally, the proposed NSTBC is ob-

served to perform slightly better (0.5db SNR gain) with improved spectral efficiency of about $0.32bpcu$ when compared with Alamouti STBC. Figure 4.12 shows the performance of the proposed scheme in case of Rician-uncorrelated Nakagami-m fading channel. The results follow a similar trend as in Fig 4.10. From simulations (Figure 4.10,4.11,4.12) it can be observed that the BER of the proposed scheme reaches error floor at around 10^{-2} in the absence of index key. Thus, proper decoding can be performed only if the receiver has knowledge of the index key used at the transmitter. Thus, a layer of security can be added to the system by following this approach. Further, it can be noticed that for the same spectral efficiency, the proposed NSTBC/NSTBC-SM offers improved BER performance with improvement in SNR by about 0.5 to 1dB when compared with Alamouti code. Further, for similar BER performance, the NSTBC/NSTBC-SM offers increment in the η by about 0.3 to 0.5 bpcu.

4.4.6.1 Spectral efficiency

There are q^{km} possible $m \times e_j$codewords in a particular component code $\mathscr{C}$. If $N_T > m$ then there are $\binom{N_T}{m}$ possible choices of antennas for spatial modulation. Thus, The spectral efficiency can given by,

$$\eta = \frac{log_2\left(n_c q^{km}\right)}{n} \qquad \begin{Bmatrix} n_c = 1 & \text{NSTBC} \\ n_c = \binom{N_T}{m} & \text{NSTBC-SM} \end{Bmatrix} \tag{4.46}$$

Table 4.12 below gives the values of η that can achieved by the proposed codes and the traditional OSTBC. The codes considered are over $\mathbb{F}_{q^m}$ with $m = 2, 4$ and $q = 5, 7, 13, 17$. All codes have rate $\mathscr{R} = 1/m$. In table 4.12 $\mathcal{M}-$ represents the modulation order of $\mathcal{M} - PSK$

Table 4.12: Spectral efficiencies of cyclic codes ($l = 1 - quasi\text{-}cyclic\ codes$) in $m \times m$ MIMO systems

NSTBC				OSTBC		NSTBC				OSTBC	
q	m	(e_j, k)	η	$\mathcal{M}$	η	q	m	(e_j, k)	η	$\mathcal{M}$	η
5	2	(4,2)	2.32	4	2	13	2	(4,2)	3.70	16	4
5	4	(8,2)	2.32	4	2	13	4	(8,2)	3.70	16	4
7	2	(4,2)	2.8	4	2	17	2	(4,2)	4.08	16	4
7	4	(8,2)	2.8	4	2	17	4	(8,2)	4.08	16	4

or $\mathcal{M} - QAM$.

Table 4.13: Spectral efficiencies $l-$quasi-cyclic codes in $m \times m$ MIMO systems with $l = 2, 3$

			$l=2$	$l=3$				$l=2$	$l=3$
q	m	(e_j, k)	η_{NSTBC}	η_{NSTBC}	q	m	(e_j, k)	η_{NSTBC}	η_{NSTBC}
5	2	(4,2)	1.85	1.58	13	2	(4,2)	3.20	2.91
5	4	(8,2)	2.07	1.92	13	4	(8,2)	3.45	3.30
7	2	(4,2)	2.32	2.04	17	2	(4,2)	3.58	3.30
7	4	(8,2)	2.55	2.41	17	4	(8,2)	3.8	3.7

4.5 Rate Diversity trade-off

In this section, we will consider the Rate-Diversity trade-off for STBC/SFBC codes derived from quasi-cyclic (cyclic) codes. We will show that these codes achieve the upper bound derived by Lu and Kumar (2003) with equality. Consider $m \times e_j$ block code $\mathscr{C}$ employed in a MIMO system with $N_T = m$ transmit antennas. Let the channel be quasi-static. Since $m = N_T$ then $e_j \geq N_T$. Let ζ denote the signal alphabet (constellation) and $\mathbf{X} \subset (\zeta)^{N_T e_j}$ be a Space-time block code. Each codeword $\mathbf{X} \in \mathscr{X}$ is an $m \times e_j$ matrix. Following, let us define the rate R of the $m \times e_j$ STBC $\mathscr{X}$ as,

$$R = \frac{1}{e_j} log_{|\zeta|} |\mathscr{X}| \tag{4.47}$$

Under this definition, a rate 1 code corresponds to a Space-Time Block Code of size $|\zeta| e_j$, i.e a code which transmits on an average one symbol from the constellation $|\zeta|$ per time slot. For a given SNR ρ and a constant c the proposed STBC $\mathscr{X}$ achieves a diversity gain of $N_r \nu$ if the power series expansion of the maximum PEP is expressed as

$$PEP = c\rho^{-N_r \nu} + O(\rho^{-N_r \nu}) \tag{4.48}$$

The quantity ν is termed as the transmit diversity gain (Tarokh et al. (1998)). It has been shown (Tarokh et al. (1998)), that from the point of view of the PEP, an STBC $\mathscr{X}$ achieves a diversity gain ν if and only if for every $\mathbf{X}_1 \neq \mathbf{X}_2 \in \mathscr{X}$, the difference matrix $(\mathbf{X}_1 - \mathbf{X}_2)$ has rank at least ν over the field of complex numbers. In (Lu et al. (2003)), it has been shown

that the transmit diversity gain equals ν even when one replaces the pairwise error probability (PEP) criterion with either the codeword error probability or the symbol error probability. For a fixed signal constellation $\mathscr{X}$, it has been shown in (Lu and Kumar (2003)) that there is a trade- off between the rate R and the transmit diversity gain ν of a STBC code $\mathscr{X}$. Given the transmit diversity gain ν, the rate is upper bounded by,

$$\mathscr{R} \leq N_T - \nu + 1. \tag{4.49}$$

Lu and Kumar (2003) have given systematic code construction techniques for binary phase-shift keying (BPSK) and quaternary phase-shift keying (QPSK) signal constellations which are characterized by rate R which achieves the upper bound $\mathscr{R} \leq N_T - \nu + 1$ for every $\nu \leq N_T$ and for any N_T and e_j with $N_T \leq e_j \leq \infty$. The following observations follow from an inspection of 4.49.

- The trade-off between rate $\mathscr{R}$ and maximum transmit diversity gain ν is independent of the number of receive antennas N_R.
- For $N_T \leq e_j$, the trade-off is independent of e_j.
- Let $d*(\mathscr{R})$ be the maximum achievable diversity gain given rate $\mathscr{R}$. As the diversity gain ν must be an integer, we have from (6.3) that

$$d*(\mathscr{R}) \leq N_R \lfloor N_T - \mathscr{R} + 1 \rfloor \tag{4.50}$$

where $\lfloor \cdot \rfloor$ is the floor function. This is illustrated in Figure (7.1) for $N_T = 4$ and $N_R = 1$. In the following section, we will show that full-rank STBC codes derived from quasi-cyclic codes achieve the upper bound $\mathscr{R} \leq N_T - \nu + 1$ for given N_T and e_j. If the number of codewords is increased by relaxing the full-rank requirement, the upper bound $\mathscr{R} \leq N_T - \nu + 1$ can still be achieved under certain conditions.

Consider $\mathscr{C}$, a length n cyclic code over $\mathbb{F}_{q^m}$ where $q = 2$ or q is a prime of the form $4k + 1$ or $6k + 1$ for some constant $k \geq 1$. From chapter 2, we know that n length full-

rank quasi-cyclic codes over $\mathbb{F}_{q^m}$ having cardinality q^m can be obtained by having only one free transform component, C_j with $j \in [j]$ of cardinality $|[j]| = m$ and constraining all other transform domain components to zero. The non zero codewords of the code $\mathscr{C}_p$ can be viewed as $m \times e_j$ matrices over $\mathbb{F}_q$ having $\mathbb{F}_q$ - rank equal to m. Further, we know that in any non zero codeword $\mathbf{c} = \{c_0, c_1, \cdots, c_{m-1}, c_m, \cdots, c_{e_j-1}\} \in \mathscr{C}$ with $e_j > m$, then $\mathscr{C}_p$ is characterized by the diversity gain $\nu = m\, N_T = m$ and $e_j \geq m$. The symbol rate $\mathscr{R}$ is given by

$$\mathscr{R} = \frac{1}{e_j} log_q(q^{e_j}) = 1 \tag{4.51}$$

Further, $N_T - \nu + 1 = m - m + 1 = 1$. Hence $\mathscr{R} = 1 = N_T - \nu + 1$ and the rate-diversity trade off is met with an equality.

4.6 Conclusion

In this chapter, we have provided two applications which facilitate the use of proposed full rank codes. In applications 1 and 2, we have proposed the use of full rank codes as STBC for MIMO Systems and SFBCs for MIMO-OFDM-IM systems. The full rank codes that are derived from cyclic codes have been employed to synthesize space-frequency block codes that are non-orthogonal in nature (NSFBCs). The performance of MIMO-OFDM-IM system has been evaluated on a 10-path frequency selective MIMO channel. The results obtained through simulation says that the proposed RD-NSFBC-IM codes over $\mathbb{F}_{5^4}$ provide considerable improvement in spectral efficiency of about 1.3 b/s/Hz when compared to MIMO-OFDM-IM with BPSK, in the case of 4×4 MIMO scenario. Moreover, the BER performance is observed to be similar. For a 2×2 system, the proposed FR-NSFBC-IM codes over $\mathbb{F}_{5^2}$ provide an improvement in spectral efficiency of about 0.9 b/s/Hz when compared to MIMO-OFDM-IM system, with Rate-1 Alamouti code and QPSK. The BER performance is observed to be similar in this case as well. Additionally, in case of a 2×2 MIMO system, the proposed codes provide an improvement in spectral efficiency by 0.6 b/s/Hz with SNR gain of 1dB, when compared to QOSFBC based design.

In application 3, we have proposed two architectures containing cooperative relay networks that facilitate the use of full rank codes as Non-orthogonal STBCs (NSTBC) in LOS MIMO based communications. We have constructed an index key that is used to secure the communication between the transmitter and legitimate receiver. Simulation results show that the BER of the proposed codes reaches error floor at around 10^{-1} in the absence of index key. Further, simulation results indicate that in the presence of correlated fading, NSTBC codewords are observed to offer better performance as compared to NSTBC-SM codewords. An analytical upper bound on the average BER has been derived and presented. Designs derived from suitably truncated one-information symbol and two-information symbol e_j-length cyclic codes over $\mathbb{F}_{q^m}$ meet the rate-diversity trade-off with equality. In this chapter we have shown that the STBCs that are obtained from cyclic codes designed with transform components from different $q-$ cyclotomic cosets of size m, have rate diversity trade-off with equality. However, the rate decreases if STBCs are obtained from cyclic codes with transform component indices chosen from same $q-$ cyclotomic coset.

Chapter 5

Rank codes (RC) derived from (n, k)-Cyclic codes for correcting crisscross errors

In this chapter we have discussed the application of the rank codes derived from cyclic codes to protect the integrity of information when transferred over channels inducing crisscross errors. We have considered two main applications: 1) Multi-carrier power line communication. 2) Multilevel storage devices. In this chapter we consider (m, 1) rank codes obtained from GFFT description of cyclic codes.

5.1 Application 1: Power Line Communication

In this section, we consider multicarrier powerline communication system (mPLC) employing Index modulation (mPLC-IM). Power line communication is gaining importance in applications involving communication between appliances connected to power lines. In the case of mPLC, information is generally communicated in 2-D arrays, where symbols along a given row are modulated onto one subcarrier, and information symbols in different rows are transmitted using different subcarriers. Information is corrupted due to the presence of Narrowband noise, Impulse noise, Background noise and Frequency selective nature of the channel (Chee et al. (2013)). The effect of the channel on information transmission is modelled using various methods which are classified into two approaches: top-down approach and bottom-up approach (Zhu et al. (2013)). Many widely used channel models employ the top-

down approach. The frequency selective nature of the power line channel has been mimicked using the well-known characterization proposed by Zimmermann and Dostert (2002). The Background noise is modelled using the Nakagami-m model (Mathur et al. (2014)). Most of the work in literature uses BPSK modulation, where symbols belong to the set $\{1,-1\}$ (Mathur and Bhatnagar (2014); Mathur et al. (2014)). It has been shown that the PLC channel impairments can result in two types of errors: Random errors (due to background noise) and *Crisscross* errors (due to narrowband noise or impulse noise).

In multicarrier Power Line Communication (mPLC) with dominant Narrowband noise and Impulse noise, *crisscross* errors are predominantly observed. In case of dominant random noise or background noise, random errors are observed. Random errors can be corrected by using suitable Hamming metric based random error correcting codes. Burst errors can be corrected using the Reed Solomon codes or product codes. Similarly Crisscross errors can be corrected by using product codes, employing a complex interleaver. Alternately, crisscross errors can be corrected using rank codes (RC) (Gabidulin (1985)-Roth (1991)).

In this chapter, we have synthesized (n,k) cyclic codes with good rank distance properties for correcting criss-cross errors in an mPLC system with an added Index Modulation (IM) arrangement to yield information integrity as well as a degree of data security. We have employed the proposed rank-metric based decoding strategy for correcting criss-cross errors. The GFFT approach provides an additional degree of freedom, in the choice of free transform component indices. This has been used to design an index key based scheme that can enhance the physical layer security of a mPLC system . Thus, this arrangement is capable of providing an additional layer of security over and above its primary duty of preserving information integrity.

In Section 5.1.1 we revisit the details of Power Line Communication using Orthogonal Frequency Division Multiplexing (OFDM) and Low Rank Parity Check Codes (LRPC). In Section 5.1.2, we present the details of the proposed PLC system employing OFDM, Index Modulation and rank-metric based cyclic codes. The decoding strategy for correcting criss-cross errors that was presented in chapter 2, has been employed. In Section 5.1.3, we discuss the performance of the proposed scheme. We consider a 4-path frequency selective PLC

channel. For fair comparison we have considered RC codes over $\mathbb{F}_{2^m}$ with $m = 4, 6, 8$. In Section 5.2 we have synthesized few (n, k) cyclic codes that can be used in storage devices like LTO and TLC Flash drives. The chapter is concluded in Section 5.2.3 by comparing the performance of RC based schemes with conventional schemes (Chee et al. (2013); Kabore et al. (2015); Yazbek et al. (2017)) and quantifying the improvements obtained.

5.1.1 Coded PLC system with OFDM revisited

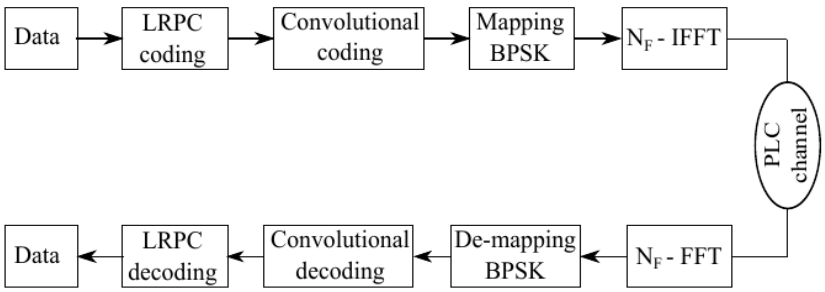


Figure 5.1: Block diagram of OFDM based PLC (Zhang and Cheng (2004))

Figure 5.1 shows the block diagram of OFDM based PLC employing Low-Rank Parity Check codes (Zhang and Cheng (2004)). The input data is encoded using Rate 1/2 LRPC encoder over $\mathbb{F}_2$. LRPC coding ensures the mitigation of crisscross errors. The LRPC coded output is encoded using convolutional coder, to mitigate the random errors due to background noise. To match the rate of LRPC encoder, the convolutional encoder of rate 1/2 is chosen. The encoded symbols, which are over base field $\mathbb{F}_2$, are mapped onto symbols in BPSK constellation and then passed onto 256 point IFFT, for OFDM modulation. The OFDM modulated data is then sent through the low voltage PLC channel. At the receiver, a soft decision Viterbi decoder is used to overcome the random errors due to background noise and LRPC decoder mitigates the effect of rank errors induced by narrowband noise and Impulse noise. We now discuss the details of the proposed secure multicarrier PLC system.

5.1.2 Secure Multicarrier PLC system with Index Modulation

5.1.2.1 Construction of Index key

In Section 4.4.2.1 we have seen that using this additional degree of freedom (freedom to chose the transform component indices) the transmitter and receiver can jointly establish an arrangement to follow through the set of component codes in a particular order. This arrangement was called the index key, given by $\{\mathbf{k_0}, \mathbf{k_1}, \cdots, \mathbf{k_{G-1}}\}$. Index key is used in this application to secure the communication between the legitimate user and smart grid that uses power line channel.

Transmitter

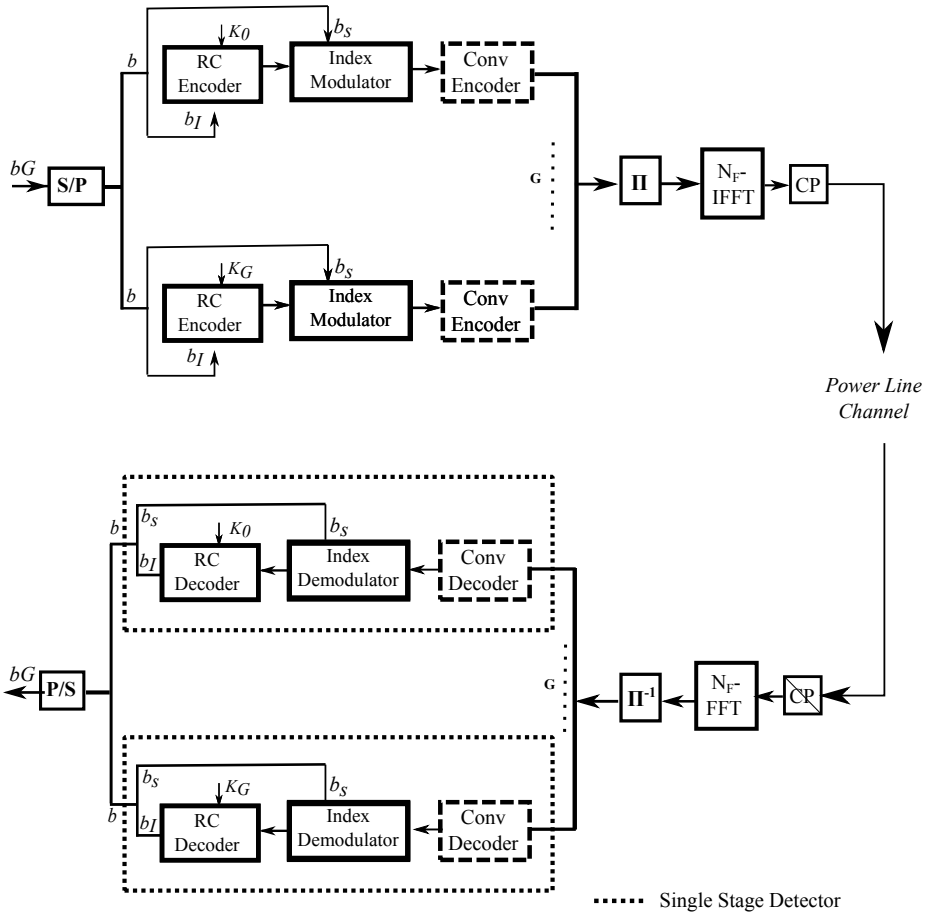


Figure 5.2: Proposed Secure PLC with index modulation

The block diagram of the proposed secure multicarrier PLC system is shown in Figure 5.2. Initially, the incoming $b\mathcal{G}$ bit stream is split into $\mathcal{G}$ parallel streams of length b (serial to parallel conversion). At each RC Encoder (RCE), $b_I = \lfloor m \cdot log_2(q) \rfloor$ bits out of b bits are considered to obtain codeword matrix. The remaining $b_s = \lfloor log_2\binom{N}{m} \rfloor$ bits out of b bits are considered for subcarrier selection. The b_I information bits at the encoder are encoded into $m \times m$ RC codeword by using the appropriate value of index key element ($\mathbf{k}_i$). Each encoder branch is assigned with $N = N_F/G$ number of subcarriers in a predetermined order. Index modulator (IM) now considers the b_s selection bits to select m subcarriers out of available N subcarriers, for transmitting symbols along each column of RC codeword. To maintain constant minimum weight (CW) and improve the performance, the m carriers chosen will be the same for the entire $m \times e_j$ RC codeword. This results in $(N \times e_j)$ Index Modulated RC (Im-RC) codeword. An example representation of IM-RC can be given by.

$$\mathbf{C} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,m-1} \\ 0 & 0 & \cdots & 0 \\ c_{1,0} & c_{1,1} & \cdots & c_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \\ c_{N-2,0} & c_{N-2,1} & \cdots & c_{N-2,m-1} \\ c_{N-1,0} & c_{N-1,1} & \cdots & c_{N-1,m-1} \end{bmatrix} \tag{5.1}$$

The $N \times m$ Im-RC codeword is then fed to the convolutional encoder. The convolutional encoder (CE) considers each row of the index modulated RC and encodes the data along

each row. The convolutionally encoded Im-RC is as given as

$$\mathfrak{C}_{IM} = \begin{bmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,m-1} & \cdots & c_{0,n-1} \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ c_{1,0} & c_{1,1} & \cdots & c_{1,m-1} & \cdots & c_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ c_{N-2,0} & c_{N-2,1} & \cdots & c_{N-2,m-1} & \cdots & c_{N-2,n-1} \\ c_{N-1,0} & c_{N-1,1} & \cdots & c_{N-1,m-1} & \cdots & c_{N-1,n-1} \end{bmatrix} \tag{5.2}$$

Traditionally the input to the OFDM modulator is a sequence of symbols obtained from a two-dimensional complex number plane. However, the elements of convolutionally encoded Im-RC are over $\mathbb{F}_q$ with q taking integer values. Hence, there is a need for one-to-one and onto-map to obtain a codeword with symbols over the complex plane. In literature, two well-known rank preserving maps have been defined: Gaussian Integer map and Eisenstein-Jacobi Integer map. The Convolutionally coded Im-RC obtained after using rank-preserving maps is given as,

$$\mathbf{X}_{IM} = \begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,m-1} & \cdots & x_{0,n-1} \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ x_{1,0} & x_{1,1} & \cdots & x_{1,m-1} & \cdots & x_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ x_{N-2,0} & x_{N-2,1} & \cdots & x_{N-2,m-1} & \cdots & x_{N-2,n-1} \\ x_{N-1,0} & x_{N-1,1} & \cdots & x_{N-1,m-1} & \cdots & x_{N-1,n-1} \end{bmatrix} \tag{5.3}$$

Where $x_{i,j} = \zeta(c_{i,j})$; $\quad 0 \leq i \leq m-1, 0 \leq j \leq m-1$, and

ζ is either Gaussian Integer map of Eisenstein-Integer map.

Each branch of the transmitter results in a corresponding $\mathbf{X}_{IM}$. Since there are $\mathcal{G}$ branches, $\mathcal{G}-$ such $\mathbf{X}_{IM}$ matrices are considered column by column and interleaved. The interleaver (Π) stacks corresponding rows of $\mathcal{G}$ codewords one below the other (in row dimension). Each column of the interleaved codeword S, is considered as one frame. Since there are

n columns, n interleaved frames are obtained. The N_F point IFFT block considers each interleaved frames and then outputs the OFDM frame containing complex symbols. The OFDM-IM block is represented as S. In case of simple stacking based interleaver, S is given by

$$S = [\mathbf{X_{IM}}^0, \mathbf{X_{IM}}^1, \cdots, \mathbf{X_{IM}}^{\mathcal{G}-1}]^T \tag{5.4}$$

Where $\mathbf{X_{IM}^i}$ is as given in (5.3). Since there are $\mathcal{G}$ IM-RC codewords, the dimension of S is $N\mathcal{G} \times e_j = N_F \times e_j$. A cyclic prefix of suitable length is padded at the end of each N length OFDM frame (column of S), and then transmitted through PLC channel.

Rate of codes

Following (Chee et al. (2013)), the code rate is defined as

$$\mathcal{R} = \mathcal{R}_{IM-RC} \cdot \mathcal{R}_{conv} = \frac{\mathcal{G}\left(log_2\left(q^{km}\right) + log_2\binom{N}{m}\right)}{e_j\,(N_F + N_{CP})} R_{conv}$$

Here $\mathcal{R}_{IM-RC}$ represents overall rate of the RC and IM block together.

$\mathcal{R}_{conv}$ represents the rate of convolutional encoder.

5.1.2.2 Power Line Channel

The multipath power line channel is shown to be frequency selective with a complex frequency response given by Zimmermann and Dostert (2002),Katayama et al. (2006).

$$H(f) = \sum_{i=1}^{N} g_i e^{-(\alpha_0 + \alpha_1 f^\kappa)\mathrm{D}_i} . e^{-2\pi f(\mathrm{D}_i/\mathscr{V}_i)} \tag{5.5}$$

Here, g_i is the weighting parameter. α_0, α_1 are the attenuation parameters. D_i is the length of i^{th} path. $\mathscr{V}_i$ is the velocity of the wave propagating through i^{th} path. κ is the exponent. Besides frequency selective fading (η_f), noise in the PLC channel has three main components:

- Background noise (N_b): The background noise is assumed to be additive. The effect of background noise is most commonly characterized by Nakagami-m distribution (Mathur and Bhatnagar (2014)Mathur et al. (2014)).

- Narrowband noise (N_{nb}): In case of PLC narrowband interference is caused by ingress of signals from broadcast stations transmitting in Medium wave (MW), Short wave (SW) and Very High Frequency (VHF) bands. Various models have been proposed in literature to model the effect of narrowband noise. In this work, we use the model described in (Shongwe and Vinck (2013)) with narrow band interference probability p.

- Impulsive noise (N_i)- Impulse noise occurs mainly due to switching or surge in voltage. Based on the nature of the occurrence, the impulse noise can be periodic and asynchronous to mains, or periodic and synchronous to mains, or Asynchronous to mains. The most widely used channel description is Middleton class A model, with a pdf given by, Di Bert et al. (2011),Ndo et al. (2013).

$$p_\eta(v) = \sum_{k=0}^{\infty} \frac{e^{-A}A^k}{k!} \frac{1}{\sqrt{2\pi\sigma_k^2}} exp(-v^2/2\sigma_k^2) \tag{5.6}$$

  Here, A is impulse index.

  $\sigma_k^2 = \left(1 + \frac{1}{\Gamma}\right)\left(\frac{k/A+\Gamma}{1+\Gamma}\right)\sigma_b^2$

  σ_b^2 is the background noise variance.

  Γ is the Background to impulse noise ratio.

  In this work, the value of impulse index A is chosen to be 0.3 and the value of background to impulse noise ratio Γ as 0.1.

The effect of errors on 2D codeword matrices is shown below:

1. Errors due to the presence of dominant Background noise (N_b). These errors are termed as Random errors. The baseband 2D error matrix pertaining to background noise is as shown

$$N_b \rightarrow \begin{bmatrix} \mathbf{e} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{e} & \mathbf{e} \\ 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{e} & 0 & 0 & 0 \end{bmatrix}$$

Figure 5.3: Error Patterns due to various noises in PLC (Chee et al. (2013))

2. Errors due to presence of dominant Narrowband noise (N_{nb}) or Impulse noise (N_i). These errors are classified as *Burst* errors, and *Crisscross* errors. The baseband 2D error matrix pertaining to narrowband noise and impulse noise is as shown

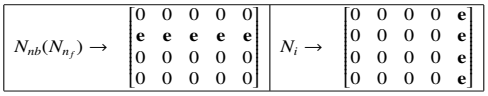


Figure 5.4: Error Patterns due to narrow band noise, impulse noise and frequency selective nature of PLC channel (Chee et al. (2013))

As seen in Figure 5.4, Impulse noise (N_i) disturbs all frequencies at a particular instant of time resulting in column errors, and Narrowband noise (N_{nb}) disturbs a specific frequency or a set of frequencies resulting in row errors.

5.1.2.3 Receiver

At the receiver the received block matrix corresponding to OFDM-IM block S is given by:

$$\mathbf{Y_S} = \mathbf{H}S + N \tag{5.7}$$

Where N is the additive noise comprising narrowband noise N_{nb}, Background noise N_b and Impulse noise N_i. The effect and distribution of various noise components are as discussed in section 1. Since FFT/IFFT is a linear process, following central limit theorem and the analysis given in (Meng et al. (2005)), the Noise matrix $\mathbb{N} = FFT(N)$ will have entries following Gaussian distribution with mean $\mu = \mu_x$ and variance $\sigma^2 = \sigma/sqrt(N_F)$. After the removal of CP and performing N_F point FFT, the deinterleaver rearranges the interleaved convolutionally encoded IM-RC codewords, before passing onto the Index demodulator block. The output of FFT block is a $N_F \times n$ matrix corresponding to transmitted OFDM block S. The de-interleaver splits the OFDM block into $\mathcal{G}-$ $(N \times n)$ $\hat{\mathbf{X}}_{IM}$s and then passes onto the bank of convolutional decoders. The convolutional decoder considers one row of the received Im-RC codeword and finds an estimate of the transmitted Im-RC codeword. This is then fed to Index Demodulator. The index demodulator considers $N \times e_j$ matrix and uses majority logic to estimate the carrier selection bits assigned to a particular RC. The resulting $m \times e_j$ matrix

is then fed to the proposed rank metric decoder. Following (Chee et al. (2013)) ,the $m \times e_j$ matrix at the input of proposed decoder, corresponding to $m_j \times e_j$ RC, can be modelled using the following equation:

$$\mathbf{Y} = \mathbf{X} + \mathbf{E_N} \tag{5.8}$$

With $\mathbf{E_N}$ representing the $m \times e_j$ error matrix reflecting the error patterns shown in Fig 5.3. and Figure 5.4, caused due to η_{nf},η_{nb},η_b and frequency selective nature of PLC. Using Inverse Rank-preserving map (5.8) can be equivalently represented as

$$\zeta^{-1}(\mathbf{Y}) \triangleq \mathbf{R} = \mathbf{C} + \mathbf{E} \tag{5.9}$$

The proposed rank metric decoder now refers to the index key value and estimates the transmitted RC and its corresponding b_s length binary data using the proposed decoding. At this point, it can be noted that the binary data at the output of the decoder will be a correct estimate of the corresponding binary data used at the transmitter, if and only if the index key value used at both encoder and corresponding decoder are same. The rank metric decoder uses the decoding method proposed in chapter 2 to find an estimate of the transmitted information.

5.1.3 Simulation Results

We have considered 4-path PLC channel with the parameters given in Table 5.1.

Table 5.1: Parameters of 4-path model

Attenuation Parameters					
k=1		α_0=0	α_1=7.8 × 10^{-8} m/s		
Path Parameters					
i	g_i	D_i/m	i	g_i	D_i/m
1	0.64	200	3	-0.15	244.8
2	0.38	222.4	4	0.05	267.5

In the presence of dominant narrowband noise and Impulse noise, the errors are considered to follow crisscross patterns (Chee et al. (2013); Yazbek et al. (2017)) as shown in Figure

5.4. Plass et al. (2008) proposed the use of rank-metric codes for applications involving narrowband noise, impulse noise and frequency selective fading. Chee et al. (2013) proposed the use of matrix codes for correcting crisscross errors in multitone power line communication. To have a fair comparison with the existing results (Chee et al. (2013); Yazbek et al. (2017)), we have considered the simulation of the Proposed system employing only the proposed rank-metric cyclic codes and decoding, with and without index modulation. Further, we have considered Multitone Frequency Shift Keying (FSK) modulation instead of OFDM. The proposed codes are compared with Constant Column Weight codes proposed by Chee et al. (2013)

For simulations we have considered RC(n, k) over $\mathbb{F}_{2^4}$ and $\mathbb{F}_{2^8}$, a 4-path PLC model with channel coefficients given in Table 5.1. The number of available data sub-carriers N_F =512. Table 5.2 gives rate comparisons of the proposed codes with the existing CCW codes. Figure 5.5 shows the BER performance of the proposed RC(4,1)$_{16}$, RC(8,3)$_{256}$ codes. From figure we infer that RC(4,1)$_{16}$ gives approx. 25% improvement in SER as compared to $CW(13,6,5)_2 \circ RS[15,14,2]_{16}$ (Chee et al. (2013)). Further, the proposed RC(8, 3) codes provide an improvement by about 30%, as compared to $CW(9,4,4)_2 \circ RS[15,14,2]_{16}$ codes. Table 5.2. gives the comparison of rates of codes used in Multitone FSK (Chee et al. (2013)).

Table 5.2: Comparison of Rates of RC and CCW codes

Code	n	N_f	$\mathcal{R}$
CW$(13,6,5)_2 \circ$ RS$[15,14,2]_{16}$	15	13	$log\|\mathbb{C}\|/nlog\binom{N_f}{w}$= 0.36
Im-RC$(4,1)_{2^4}$	4	8	0.31
CW$(9,4,4)_2 \circ$ RS$[15,14,2]_{16}$	15	9	$log\|\mathbb{C}\|/nlog\binom{N_f}{w}$= 0.53
RC$(6,3)_{2^6}$	6	6	0.50
RC$(8,3)_{2^8}$	8	8	≈ 0.40

Figure 5.6 shows the performance of the proposed scheme in the presence of dominant background, noise narrowband with probability p affecting two rows and impulse noise with probability $p = 0.05$. At a BER of 10^{-4}, in the presence of narrowband noise affecting two rows,

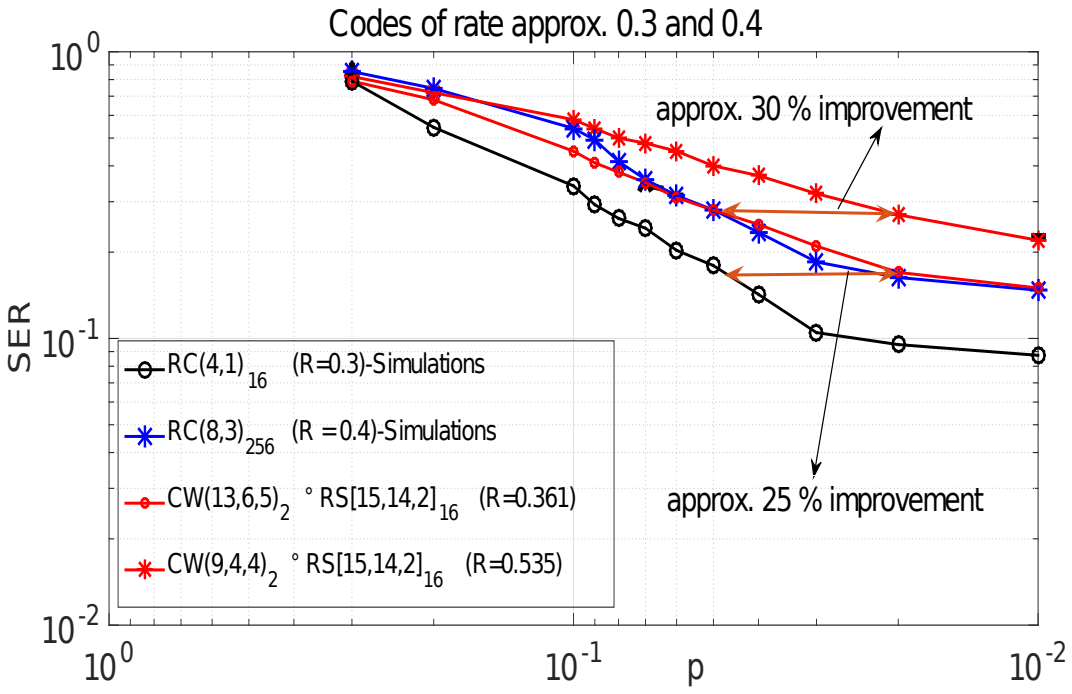


Figure 5.5: SER plot of RC(R=0.4,0.5) and CCW(R =0.361,0.535) codes

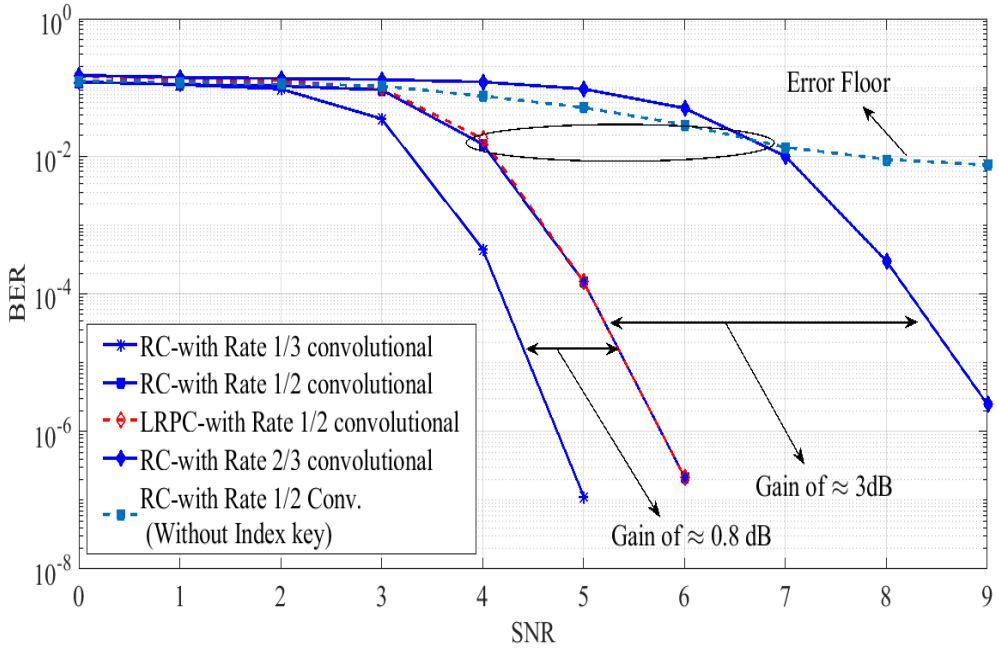


Figure 5.6: BER plot of RC-Conv. codes and LRPC/Gabidulin-Conv. codes

.

the proposed RC$(8, 3)_{2^8}$ code with rate 1/2 convolutional code provides a gain of approx. 3 dB as compared to the case of Rate 2/3 convolutional code. Further, in the case of rate 1/3 con-

volutional code along with the proposed RC$(8,4)_{2^8}$, an additional gain of 0.8 dB is achieved, when compared to RC$(8,3)$ codes. Additionally, it can be seen that in the absence of the exact knowledge of the index key at the receiver, the performance in the presence of rank three errors reaches the error floor at a BER of approximately 1×10^{-2}. When compared with the existing LRPC/Gabidulin based design with rate 1/2 convolutional code, the performance of the proposed scheme is slightly better. The use of the index key provides and additional layer of security. In terms of the complexity of encoding and decoding, the codes proposed by us enjoy a significant advantage over the codes proposed by Kabore et al. (2015); Yazbek et al. (2017). The computations required by the constructions in (Kabore et al. (2015); Yazbek et al. (2017)) are over the Galois field $\mathbb{F}_{2^{46}}$ whereas our constructions are based on computations over the Galois field $\mathbb{F}_{2^8}$. This brings about a significant reduction in the complexity of the encoding and decoding operations. Thus, these codes provide equivalent (slightly better) performance with significantly reduced computational complexity.

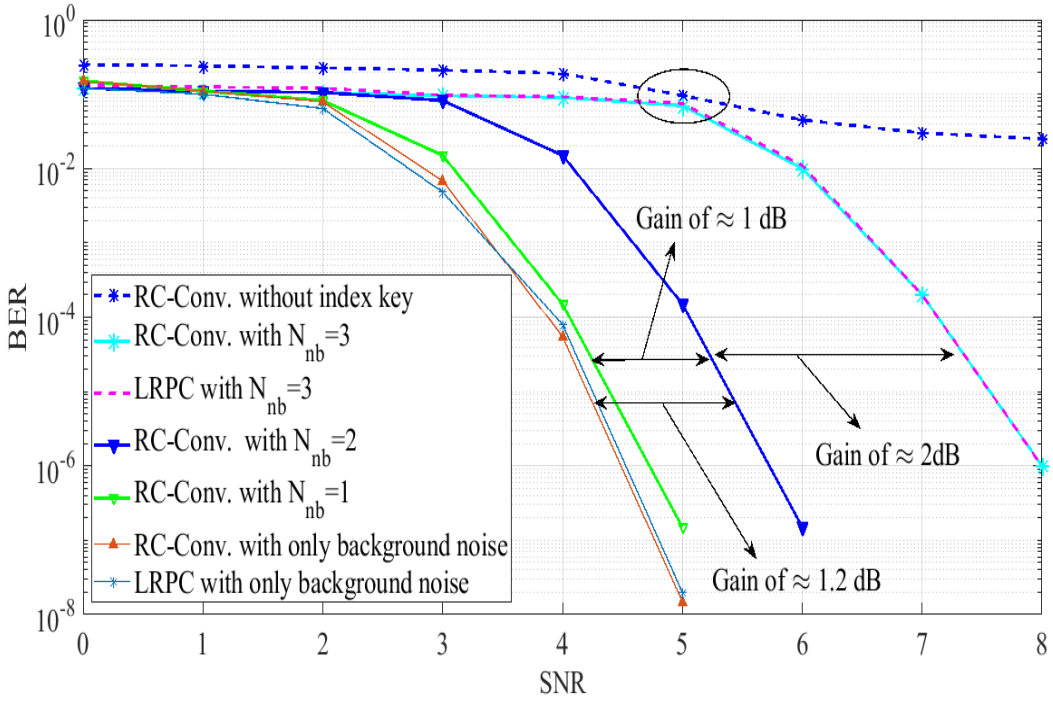


Figure 5.7: BER plot of RC-Conv. codes and LRPC/Gabidulin-Conv. codes for various values of N_{nb}

.

Figure 5.7 shows the BER performance of the proposed scheme in case of dominant

background noise, and background noise along with narrowband noise (N_{nb}) affecting one, two and three rows with impulse noise characterized by probability $p = 0.05$. It can be observed that the performance offered by the proposed scheme is similar in both the cases (with dominant background noise only and with background, impulse noise and narrowband noise). However, the proposed codes require knowledge of index key at the receiver, as seen from Figure 5.7.

In Figure 5.8 we have shown the performance of the proposed system in the presence of dom-

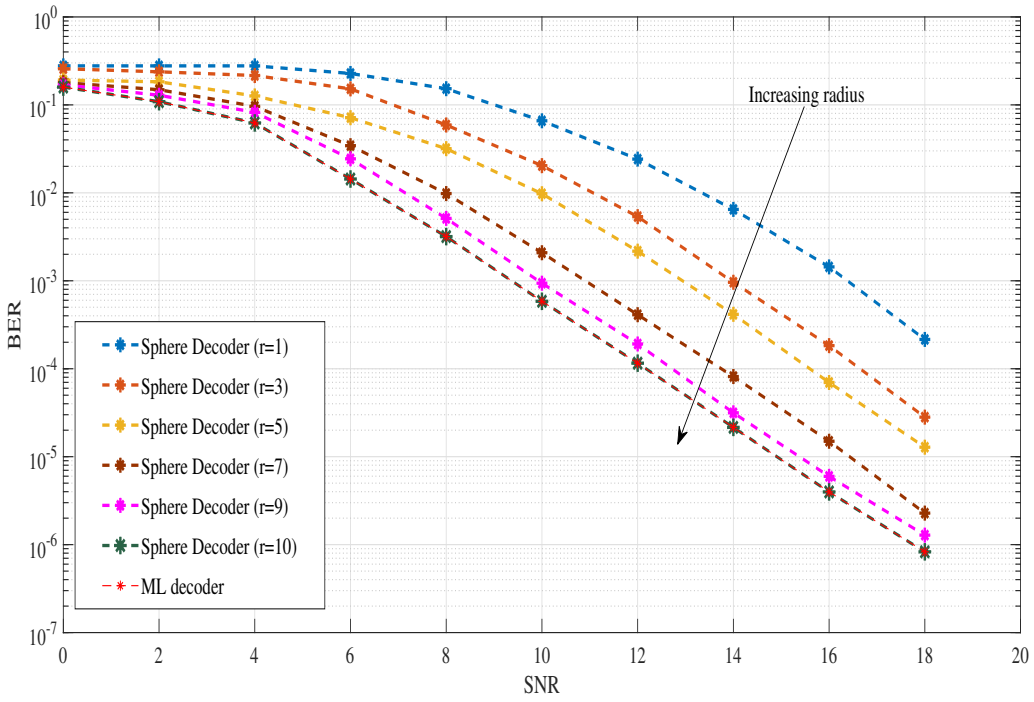


Figure 5.8: BER performance of proposed RC-codes in the presence of dominant background noise

inant background noise and in the absence of convolutional encoder/decoder. The decoding is single stage ML or Sphere decoding, for case of background noise, dominant narrowband noise affecting three rows, and impulse noise with probability $p = 0.05$. The BER curve for sphere radius $r = 10$ is similar to that of ML decoding. It can be observed that the performance of a single stage ML/Sphere decoder is inferior as compared to two-stage decoding,

because of the presence of rank errors and background errors. In the presence of errors with rank $< \lfloor m - 1/2 \rfloor$, but spread across all rows of the transmitted codeword, the proposed rank decoder can still decode without any error, however, the ML decoder can result in the wrong estimate as the decision metric is Euclidean distance and not rank distance, and the search space all possible Im-RC codewords, as evident from Figure5.8.

5.2 Application 2: Tape drives and MLC storage

In the introduction we have discussed that crisscross error can arise in tape drives and multi level cell flash drives. The standards defined for storage devices suggest the use of product code with Reed Solomon (RS) code as inner code and LDPC/RS code as outer code. We propose the use of RS codes for correcting burst errors (column errors) and the use of rank metric codes for correcting rank errors (especially row errors). The outer code can be a rank metric code and the inner code can be a RS code.

5.2.1 Linear Tape Open

Since cyclic codes like BCH codes and Reed-Solomon codes or product codes based on BCH/RS codes are most widely used in memory devices, in this section we synthesize some of the rank metric codes over $\mathbb{F}_{q^m}$.

The data layout of LTO drive is give as:

Number of Tracks per Tape-2176

Number of Data bands-4

Number of Servo Bands-5

Number of Write Heads/Data band-16

Number of wraps per/Data band-32.

Magnetic tape storage products are designed to ensure a Raw Bit Error Rate (RBER) of 10^{-17} to 10^{-20}. However, when aerial density increase the RBER tends to increase due to inter-bit interference. Linear block codes such as RS codes and LDPC codes are usually employed as inner and outer codes of product codes, to correct random and burst errors due

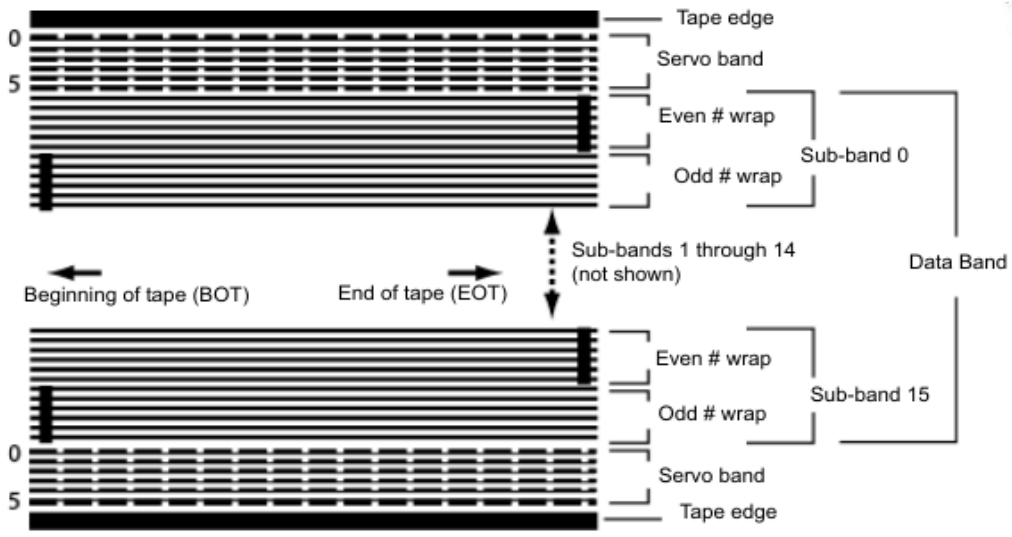


Figure 5.9: Data layout of tape drive LTO (Quantum-Corporation (2009))

to scratches or damage in certain part of the the tape. However, when viewed from the criss-cross perspective, it is evident that a code with good rank distance properties will possess the ability to correct criss-cross errors which are the most common types of errors encountered in tape drives. The tape head has $8, 16$, or 32 data read/write head elements and 2 servo read elements. Thus codes over $\mathbb{F}_{2^8}$ are best suitable for tape devices. Since Reed Solomon codes (constructed over $\mathbb{F}_{2^8}$) are the codes used in standards defined for storage devices, we synthesize rank-metric cyclic codes over $\mathbb{F}_{2^8}$. Below we synthesize $rank - d$ codes over $\mathbb{F}_{2^8}$. Since $n = 2^8 - 1$, the $q-$cyclotomic cosets modulo 255 are listed in Table 5.3 below Table 5.3 lists all possible $2-$ cyclotomic cosets modulo 255. We can see that there are 30 cosets of size 8. Following theorem 4 we see that rank-8 cyclic codes can be obtained by choosing $k = 30$ resulting in $(255, 30)$. These can be punctured to $(30, 30 * 8) = (240, 30)$ codes. Similarly $(240, 60)$ rank-7 codes, $(240, 90)$ rank -6 codes and $(240, 120)$ rank 5 codes can be obtained. It can observed that $(240, 30)$ and $(240, 60)$ have rank error correcting capability of $\lfloor \frac{d-1}{2} \rfloor = 3$ and burst error correcting capability of $155, 90$ respectively. Similarly the rank error correcting capability of $(240, 90)$ and $(240, 120)$ is 2 and the burst error correction capability of $75, 60$ respectively. The most commonly used RS code is $(255, 233)$ with burst error correction capability of 10 symbols. The maximum value of k that can be obtained for

Table 5.3: List of 2− cyclotomic cosets modulo 255

[0],	
[1, 2, 4, 8, 16, 32, 64, 128],	[3, 6, 12, 24, 48, 96, 129, 192],
[5, 10, 20, 40, 65, 80, 130, 160],	[7, 14, 28, 56, 112, 131, 193, 224],
[9, 18, 33, 36, 66, 72, 132, 144],	[11, 22, 44, 88, 97, 133, 176, 194],
[13, 26, 52, 67, 104, 134, 161, 208],	[15, 30, 60, 120, 135, 195, 225, 240],
[17, 34, 68, 136],	[19, 38, 49, 76, 98, 137, 152, 196],
[21, 42, 69, 81, 84, 138, 162, 168],	[23, 46, 92, 113, 139, 184, 197, 226],
[25, 35, 50, 70, 100, 140, 145, 200],	[27, 54, 99, 108, 141, 177, 198, 216],
[29, 58, 71, 116, 142, 163, 209, 232],	[31, 62, 124, 143, 199, 227, 241, 248],
[37, 41, 73, 74, 82, 146, 148, 164],	[39, 57, 78, 114, 147, 156, 201, 228],
[43, 86, 89, 101, 149, 172, 178, 202],	[45, 75, 90, 105, 150, 165, 180, 210],
[47, 94, 121, 151, 188, 203, 229, 242],	[51, 102, 153, 204],
[53, 77, 83, 106, 154, 166, 169, 212],	[55, 110, 115, 155, 185, 205, 220, 230],
[59, 103, 118, 157, 179, 206, 217, 236],	[61, 79, 122, 158, 167, 211, 233, 244],
[63, 126, 159, 207, 231, 243, 249, 252],	[85, 170],
[87, 93, 117, 171, 174, 186, 213, 234],	[91, 107, 109, 173, 181, 182, 214, 218],
[95, 125, 175, 190, 215, 235, 245, 250],	[111, 123, 183, 189, 219, 222, 237, 246],
[119, 187, 221, 238],	[127, 191, 223, 239, 247, 251, 253, 254]

designing rank 1 codes is $k = 186$. Thus the rank 1 error correcting code will be a $(255, 186)$ cyclic code with code $(186/255) = 0.7$

5.2.2 NAND FLASH

Crisscross errors can also be found in TLC NAND flash memories. In TLC memories each cell (FET) can hold 3 bits of data (equivalent to 8 voltage levels). The data layout of NAND FLASH is as given in Figure 5.10.

Referring to Figure 1.2,1.3 we see that retention errors can lead to crisscross error patterns. Since the current generation NAND flash drives are MLC (4 voltage levels) and TLC (8 voltage levels), each cell can hold 2 and 3 bits respectively. Also referring to Figure 1.3 we see that errors are mostly confined to upper row (LSB) resulting in rank-1 errors. Thus rank−3 codes over $\mathbb{F}_{2^3}$ can be synthesized for NAND FLash memories. The details of which can be found below: The 2− cyclotomic cosets modulo 7 are given by,

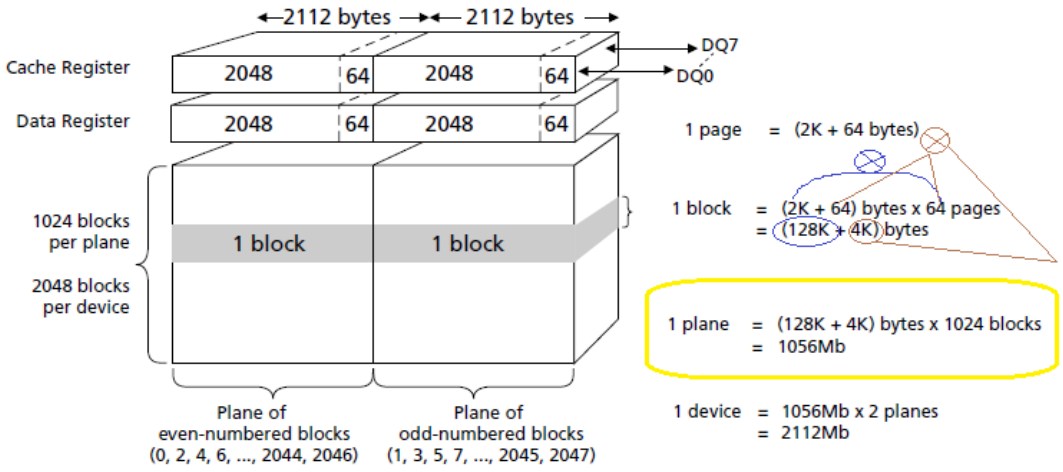


Figure 5.10: NAND Flash memory organization Micron (2006)

$[0] = \{0\},$	$[1] = \{1, 2, 4\},$	$[3] = \{3, 5, 6\}$

As we can see that there are two 2− cyclotomic cosets of size $m = 3$. Various possible rank 3 codes that can correct rank-1 crisscross errors are given in the Table 5.4 below. These

Table 5.4: List of number of rank-3 codes

(n, k)	Number of possible codes
$(3, 1)$	6
$(6, 2)$	9

are rate 1/3 rank−1 error correcting codes that can be used as inner code along with burst error correcting RS outer codes. However since the MLC flash cell can hold 4 voltage levels. We can define a quantization table to map 4 voltage levels to 3 integer values and then construct codes over $\mathbb{F}_{3^m}$. The mapping Table is as given below:

Table 5.5: Encoding/Mapping table from binary to $\mathcal{Z}_3$

bits	0	01	11
value	0	1	2

Table 5.6: List of 3− cyclotomic cosets mod 242 in $\mathbb{F}_{3^5}$

[0],	[1, 3, 9, 27, 81],	[2, 6, 18, 54, 162],
[4, 12, 36, 82, 108],	[5, 15, 45, 135, 163],	[7, 21, 63, 83, 189],
[8, 24, 72, 164, 216],	[10, 28, 30, 84, 90],	[11, 33, 55, 99, 165],
[13, 39, 85, 109, 117],	[14, 42, 126, 136, 166],	[16, 48, 86, 144, 190],
[17, 51, 153, 167, 217],	[19, 29, 57, 87, 171],	[20, 56, 60, 168, 180],
[22, 66, 88, 110, 198],	[23, 69, 137, 169, 207],	[25, 75, 89, 191, 225],
[26, 78, 170, 218, 234],	[31, 37, 91, 93, 111],	[32, 46, 96, 138, 172],
[34, 64, 92, 102, 192],	[35, 73, 105, 173, 219],	[38, 58, 100, 114, 174],
[40, 94, 112, 118, 120],	[41, 123, 127, 139, 175],	[43, 95, 129, 145, 193],
[44, 132, 154, 176, 220],	[47, 59, 141, 177, 181],	[49, 97, 113, 147, 199],
[50, 140, 150, 178, 208],	[52, 98, 156, 194, 226],	[53, 159, 179, 221, 235],
[61, 65, 101, 183, 195],	[62, 74, 182, 186, 222],	[67, 103, 115, 119, 201],
[68, 128, 142, 184, 204],	[70, 104, 146, 196, 210],	[71, 155, 185, 213, 223],
[76, 106, 116, 200, 228],	[77, 143, 187, 209, 231],	[79, 107, 197, 227, 237],
[80, 188, 224, 236, 240],	[121],	[122, 124, 130, 148, 202],
[125, 133, 157, 203, 229],	[131, 149, 151, 205, 211],	[134, 160, 206, 230, 238],
[152, 158, 212, 214, 232],	[161, 215, 233, 239, 241]	

The 3− cyclotomic cosets mod 242 can be given in Table 5.6. As can be seen from the table there are 48 3− cyclotomic cosets from which $(5, 3)$ rank-3 cyclic codes can be constructed. The rate of these codes is $3/5 = 0.6$.

From the analysis given in Chapter 2, we can observe that the rank error correction capability of the proposed rank codes depend on the number of rows and not on the number of columns. Thus, for the same rank error correction capability (m, k) codes are preferred than (e_j, k) codes. These codes are analogous to Gabidulin codes.

5.2.3 Conclusion

In this chapter, we have tested the performance of the proposed codes in applications that induce crisscross errors. At first we have proposed a PLC communication scheme employing OFDM and Index Modulation. The proposed scheme employs cyclic codes with good rank distance properties for correcting crisscross errors, and convolutional codes for correcting random background errors. We have used the proposed rank-metric based decoding strategy for rank codes obtained from transform domain description of cyclic codes. Performance of RC with the proposed decoding strategy is evaluated in a multicarrier power line communication system employing Index modulation. In case of PLC with OFDM-IM simulation results show that a coding gain of approximately 2dB can be achieved with RC over F_{2^8} in the presence of rank-2 errors as compared to the performance in the presence of rank three errors. Additionally, a coding gain of 1dB can be achieved by using the proposed codes with rate 1/3 convolutional code as compared to that using rate 1/2 convolutional code. Additionally, it was shown that in the absence of index key the receiver could not decode correct information, resulting in the error floor in the BER performance. In the case of PLC with multitone FSK, simulation results show that with RC codes SER graph shows an improvement of about 25-30% as compared to CCW codes proposed by Chee et al. Additionally, the codes proposed in this work offer additional layer of security, equivalent (slightly superior) error performance and reduced computational complexity when compared with LRPC/Gabidulin codes.

As part of the second application we have considered storage devices: Linear Tape Open (LTO) and MLC/TLC Flash drives. We have proposed few code constructions over $\mathbb{F}_{2^8}$ that can be used in these devices to overcome crisscross errors. Exploiting the underlying linear structure a parallel decoding method can be used to overcome the decoding delay. However,

since the rank error correction capability of the proposed codes depend on the number of rows (and not on number of columns), rank codes obtained from various $(m, 1)$ codes can be used in memory devices inducing crisscross errors.

Chapter 6

Conclusions and Suggestions for Future Work

The work started with a study of rank-metric codes with an intent to apply these constructions for correcting *crisscross* errors. Crisscross errors are commonly found in multi-carrier communication, storage devices like tape drives and multi level flash memories. During this phase, we became interested in analysing the rank distance properties of $[n \times n, k]$ $\ell-$ Quasi cyclic codes (general class of widely used cyclic codes). After completing this work we decided to study the rank properties of $n-$length Abelian codes over $\mathbb{F}_{q^m}$ by making use of the DFT domain description of these codes. In Chapter 2, we have given theorems for constructing $n-$length ℓ QC codes over Galois field $\mathbb{F}_{q^m}$ with desired rank. We have given closed form expressions for the $\mathbb{F}_q-$ rank of a $n-$length quasi cyclic code over $\mathbb{F}_{q^m}$ characterized by a single free transform domain component. For such codes, we have shown that the codeword vector can be divided into $\lfloor \frac{n}{e_j} \rfloor$ sets of size e_j , whose components are linearly independent. Thus, each of these sets can be viewed as $m \times e_j$ matrices over $\mathbb{F}_q$ having terms which has $\mathbb{F}_q-$ rank equal to e_j. The last set comprises of $(n - \lfloor \frac{n}{e_j} \rfloor e_j)$ linearly independent terms which has $\mathbb{F}_q-$ rank $(n - \lfloor \frac{n}{e_j} \rfloor e_j)$ when viewed as an $m \times (n - \lfloor \frac{n}{e_j} \rfloor e_j)$ matrix over $\mathbb{F}_q$. In the case of (n, k) rank metric code constructions if the free transform components are confined to single $q-$ cyclotomic coset of size e_j, we have shown that the first e_j components of the codeword completely determine it's rank. This result has been used to obtain full rank punctured codes. We have obtained a procedure for designing constant rank codes for $k > 1$. Also we have

provided a check matrix construction that has properties of band matrix and provided a decoding strategy using this check matrix. A class of MRD codes were obtained when the free transform components are drawn from more than one $q-$cyclotomic coset.

In Chapter 3, we have characterized Abelian codes using the rank-metric. We have been able to generalize many of the results obtained for quasi cyclic codes into the more general setting of Abelian codes. We have obtained exact results for the $\mathbb{F}_q-$rank of an $n-$length Abelian code over $\mathbb{F}_{q^m}$ characterized by a tow or more free transform components drawn from different q-cyclotomic cosets of size e_j. We have been successful in obtaining exact results which determine the rank of Abelian codes characterized by two free transform components drawn from the same/different $q-$cyclotomic coset. In the second part of the thesis, we have applied the theorems associated with the rank characterization of cyclic codes to derive designs for STBCs/SFBCs. Also we have analyzed their performance in applications involving *crisscross* errors. In Chapter 4, we have derived designs for quasi-static fading channels from full-rank cyclic codes. In Chapter 5, we have derived designs for applications involving crisscross errors. In simulations, these codes are observed to have performed very well. In this section which deals with directions for further research, we have briefly discuss several possible extensions for further study.

FUTURE SCOPE

- In Chapter 2, we have been able to derive exact expressions for the rank of a (n, k) quasi-cyclic code when the free transform components are confined to a single and/ or multiple $q-$ cyclotomic cosets. However we were unable to obtain the weight spectrum of the codes.

- In Chapter 3, we have been able to extend to a general class of multivariate polynomial codes called Abelian codes. However, these results can be extended to a more general class of multivariate polynomial codes called Quasi-Abelian codes. Also, it will be of interest to explore the rank distance properties of other general classes of cyclic codes such as constacyclic coded, and a special class called negacyclic codes.

- In carrying out simulations to determine the error performance of STBCs derived from cyclic codes, we have performed check matrix based decoding. It will be interesting to know whether list based decoding algorithms can be designed which admit lower decoding complexity and better error correcting capability.

- Array codes are two dimensional codes which can be of either Block or Convolutional type. These have been extensively used for providing error protection in storage devices. Roth has shown that a rank $\mu - [n \times n]$ array code over a finite field F is a k-dimensional linear space of n × n matrices over F , such that every non zero matrix has rank $\geq \mu$. Further, he has given a decoding algorithm to retrieve $\Gamma \in C$, given a possibly erroneous received array $\Gamma + E$, as long as $R_q(E) \leq \mu - 1$. These codes have found application in decoding criss-cross errors in $n \times n$ arrays. Similar to MRA codes, the codewords of a linear $n-$length cyclic code over $\mathbb{F}_{q^m}$ can be viewed as $m \times n$ matrices over $\mathbb{F}_q$. With the help of the characterization for $n-$length cyclic codes over $\mathbb{F}_{q^m}$, we can construct full-rank $(= m)$ cyclic codes over $\mathbb{F}_{q^m}$. It would be interesting to study how effective these codes can be in correcting errors in semiconductor memories and tape drive systems where the dominant error mechanisms are burst row errors and data erasures.

- Multiuser MIMO and Non-orthogonal Multiple Access is gaining importance in the study of Massive MIMO and Multiuser MIMO. The proposed codes are non-orthogonal in nature and can be considered as suitable candidates for synthesizing non-orthogonal designs for Massive MIMO and Multiuser MIMO.

- Due to their full rank property constant full rank codes could find application in network coding. We have not addressed this aspect in this thesis. This could be considered as a fertile avenue in the search for channel codes for network coding.

References

Asif, H. M., Honary, B., and Hamayun, M. T. (2017). Gaussian integers and interleaved rank codes for space–time block codes. *International Journal of Communication Systems*, 30(1):e2943.

Basar, E. (2016). On multiple-input multiple-output ofdm with index modulation for next generation wireless networks. *IEEE Transactions on Signal Processing*, 64(15):3868–3878.

Berman, S. (1967). On the theory of group codes. *Cybernetics and Systems Analysis*, 3(1):25–31.

Blahut, R. E. (1983). *Theory and practice of error control codes*. Addison-Wesley.

Cai, Y., Haratsch, E. F., Mutlu, O., and Mai, K. (2012). Error patterns in mlc nand flash memory: Measurement, characterization, and analysis. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 521–526. EDA Consortium.

Chee, Y. M., Kiah, H. M., and Purkayastha, P. (2013). Matrix Codes and Multitone Frequency Shift Keying for Power Line Communications. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2870–2874. IEEE.

Choi, M., Lee, H., and Nam, H. (2016). Cooperative uav networks based on distributed space-time block codes. In *2016 13th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*, pages 454–458. IEEE.

Dey, B. K. and Rajan, B. S. (2003). Dft domain characterization of quasi-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing*, 13(6):453–474.

Di Bert, L., Caldera, P., Schwingshackl, D., and Tonello, A. M. (2011). On noise modeling for power line communications. In *Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on*, pages 283–288. IEEE.

Ding, Y. (2015). On list-decodability of random rank metric codes and subspace codes. *IEEE Transactions on Information Theory*, 61(1):51–59.

Driessen, P. F. and Foschini, G. J. (1999). On the capacity formula for multiple input-multiple output wireless channels: A geometric interpretation. In *1999 IEEE International Conference on Communications (Cat. No. 99CH36311)*, volume 3, pages 1603–1607. IEEE.

Fotouhi, A., Qiang, H., Ding, M., Hassan, M., Giordano, L. G., Garcia-Rodriguez, A., and Yuan, J. (2019). Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials*.

Gabidulin, E. M. (1985). Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16.

GD, G. S., Shriharsha, K., Raghavendra, M., and Acharya, U. S. (2017). A comprehensive framework for double spatial modulation under imperfect channel state information. *Physical Communication*, 25:519–526.

Guruswami, V. and Xing, C. (2013). List Decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin Dubcodes up to the Singleton Bound. In *Proceedings o[1]-[6]f the forty-fifth annual ACM symposium on Theory of computing*, pages 843–852. ACM.

Hanna, S., Yan, H., and Cabric, D. (2019). Distributed uav placement optimization for cooperative line-of-sight mimo communications. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 4619–4623. IEEE.

Huber, K. (1994a). Codes over eisenstein-jacobi integers. *Contemporary Mathematics*, 168:165–165.

Huber, K. (1994b). Codes over gaussian integers. *IEEE Transactions on Information Theory*, 40(1):207–216.

Huo, Y., Dong, X., Lu, T., Xu, W., and Yuen, M. (2019). Distributed and multi-layer uav networks for next-generation wireless communication and power transfer: A feasibility study. *IEEE Internet of Things Journal*.

Kabore, A. W., Meghdadi, V., Cances, J.-P., Gaborit, P., and Ruatta, O. (2015). Performance of gabidulin codes for narrowband plc smart grid networks. In *Power Line Communications and its Applications (ISPLC), 2015 International Symposium on*, pages 262–267. IEEE.

Katayama, M., Yamazato, T., and Okada, H. (2006). A Mathematical Model of Noise in Narrowband Power Line Communication Systems. *IEEE Journal on Selected areas in Communications*, 24(7):1267–1276.

Khaleghi, A., Silva, D., and Kschischang, F. R. (2009). Subspace codes. In *IMA International Conference on Cryptography and Coding*, pages 1–21. Springer.

Khuwaja, A. A., Chen, Y., Zhao, N., Alouini, M.-S., and Dobbins, P. (2018). A survey of channel modeling for uav communications. *IEEE Communications Surveys & Tutorials*, 20(4):2804–2821.

Konishi, T. (2017). Integer Space–Time Block Codes With Large Trace Metrics. *IEEE Wireless Communications Letters*, 6(5):686–689.

Li, B., Fei, Z., and Zhang, Y. (2018). Uav communications for 5g and beyond: Recent advances and future trends. *IEEE Internet of Things Journal*.

Liew, T. and Hanzo, L. (2002). Space-time codes and concatenated channel codes for wireless communications. *Proceedings of the IEEE*, 90(2):187–219.

Liu, P. and Springer, A. (2015). Space shift keying for los communication at mmwave frequencies. *IEEE Wireless Communications Letters*, 4(2):121–124.

Loidreau, P. (2006). A Welch–Berlekamp like Algorithm for Decoding Gabidulin Codes. In *Coding and cryptography*, pages 36–45. Springer.

Lu, H.-f. and Kumar, P. V. (2003). Rate-diversity tradeoff of space-time codes with fixed alphabet and optimal constructions for psk modulation. *IEEE Transactions on Information Theory*, 49(10):2747–2751.

Lu, H.-f., Wang, Y., Kumar, P. V., and Chugg, K. M. (2003). Remarks on space-time codes including a new lower bound and an improved code. *IEEE Transactions on Information Theory*, 49(10):2752–2757.

Lusina, P., Gabidulin, E., and Bossert, M. (2003). Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760.

Martin, P. A. and Taylor, D. P. (2004). High-throughput error correcting space-time block codes. *IEEE communications letters*, 8(7):458–460.

Mathur, A. and Bhatnagar, M. R. (2014). Plc performance analysis assuming bpsk modulation over nakagami-*m* additive noise. *IEEE Communications Letters*, 18(6):909–912.

Mathur, A., Bhatnagar, M. R., and Panigrahi, B. K. (2014). Plc performance analysis over rayleigh fading channel under nakagami-*m* additive noise. *IEEE Communications Letters*, 18(12):2101–2104.

Meng, H., Guan, Y. L., and Chen, S. (2005). Modeling and analysis of noise effects on broadband power-line communications. *IEEE Transactions on Power delivery*, 20(2):630–637.

Micron (2006). *NAND Flash Memory*. Micron, https://media.digikey.com/pdf/Data

Moon, T. K. (2005). Error correction coding. *Mathematical Methods and Algorithms. Jhon Wiley and Son*, pages 2001–2006.

Ndo, G., Labeau, F., and Kassouf, M. (2013). A Markov-Middleton Model for Bursty Impulsive Noise: Modeling and Receiver design. *IEEE Transactions on Power Delivery*, 28(4):2317–2325.

Perişoară, L. A. (2012). Ber analysis of stbc codes for mimo rayleigh flat fading channels. *Telfor Journal*, 4(2):78–82.

Plass, S., Richter, G., and Vinck, A. H. (2008). Coding schemes for crisscross error patterns. *Wireless Personal Communications*, 47(1):39–49.

Puchinger, S., Stern, S., Bossert, M., and Fischer, R. F. (2016). Space-time codes based on rank-metric codes and their decoding. In *2016 International Symposium on Wireless Communication Systems (ISWCS)*, pages 125–130. IEEE.

Quantum-Corporation (2009). *LTO-5 User's guide*. Quantum Corporation,http://4rgroup.com/sanpham/product-doc/Quantum-LTO-5

Rajan, B. S. and Siddiqi, M. (1992). Transform domain characterization of abelian codes. *IEEE transactions on information theory*, 38(6):1817–1821.

Roman, S. (2005). *Field theory*, volume 158. Springer Science & Business Media.

Roth, R. M. (1991). Maximum-rank array codes and their application to crisscross error correction. *IEEE transactions on Information Theory*, 37(2):328–336.

Roth, R. M. (2018). On decoding rank-metric codes over large fields. *IEEE Transactions on Information Theory*, 64(2):944–951.

Shannon, C. E. (1948). A mathematical theory of communication. *Bell system technical journal*, 27(3):379–423.

Shongwe, T. and Vinck, A. H. (2013). Interleaving and nulling to combat narrow-band interference in plc standard technologies plc g3 and prime. In *Power Line Communications and Its Applications (ISPLC), 2013 17th IEEE International Symposium on*, pages 258–262. IEEE.

Simon, M. K. and Alouini, M.-S. (2005). *Digital communication over fading channels*, volume 95. John Wiley & Sons.

Sripati, U. and Rajan, B. S. (2003). On the rank distance of cyclic codes. In *IEEE International Symposium on Information Theory, 2003. Proceedings.* IEEE.

Sripati, U., Rajan, B. S., and Shashidhar, V. (2004a). Full-diversity stbcs for block-fading channels from cyclic codes. In *IEEE Global Telecommunications Conference, 2004. GLOBECOM'04.*, volume 1, pages 566–570. IEEE.

Sripati, U., Shashidhar, V., and Rajan, B. S. (2004b). Designs and full-rank stbcs from dft domain description of cyclic codes. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, pages 338–338. IEEE.

Tarokh, V., Seshadri, N., and Calderbank, A. R. (1998). Space-time codes for high data rate wireless communication: Performance criterion and code construction. *IEEE transactions on information theory*, 44(2):744–765.

Torabi, M., Aissa, S., and Soleymani, M. R. (2007). On the ber performance of space-frequency block coded ofdm systems in fading mimo channels. *IEEE Transactions on Wireless Communications*, 6(4):1366–1373.

Trefethen, L. N. and Bau III, D. (1997). *Numerical linear algebra*, volume 50. Siam.

Vakilian, V. and Mehrpouyan, H. (2016). High-rate and low-complexity space-time block codes for 2 x 2 mimo systems. *IEEE communications Letters*, 20(6):1227–1230.

Wachter-Zeh, A. (2014). List Decoding of Crisscross Error Patterns. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 1236–1240. IEEE.

Yacoub, M. D. (2009). Nakagami-m phase-envelope joint distribution: an improved model. In *2009 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC)*, pages 335–339. IEEE.

Yazbek, A. K., EL Qachchach, I., Cances, J.-P., and Meghdadi, V. (2017). Low Rank Parity Check Codes and Their Application in Power Line Communications Smart Grid Networks. *International Journal of Communication Systems*, 30(12):e3256.

Zhang, Y. and Cheng, S. (2004). A novel multicarrier signal transmission system over multipath channel of low-voltage power line. *IEEE Transactions on Power Delivery*, 19(4):1668–1672.

Zhu, W., Zhu, X., Lim, E., and Huang, Y. (2013). State-of-art power line communications channel modelling. *Procedia Computer Science*, 17:563–570.

Zimmermann, M. and Dostert, K. (2002). A Multipath Model for the Powerline Channel. *IEEE Transactions on communications*, 50(4):553–559.

List of Publications

Accepted (Journals)

1. **Raghavendra M.A.N.S** and U. Shripathi Acharya, "Non Orthogonal Space-Frequency-Block Codes from cyclic codes for wireless systems employing MIMO-OFDM with Index Modulation." *Elsevier Physical Communication* 34 (2019): 174-187

2. **Raghavendra, M. A. N. S**, and U. Shripathi Acharya. "Index Modulation Aided Multi-Carrier Power Line Communication Employing Rank Codes from Cyclic Codes." *Elsevier Physical Communication* 39 (2020): 100975.

Accepted (Conference Proceedings)

1. **Raghavendra M.A.N.S**, G.D Goutham Simha, and U. Shripathi Acharya. "Non-orthogonal full rank space-time block codes over Eisenstein-Jacobi integers for MIMO systems." *In Electronics and Communication Systems (ICECS), 2017 4th International Conference on,* pp. 83-87. IEEE, 2017.

2. **Raghavendra M.A.N.S**, G.D Goutham Simha, and U. Shripathi Acharya. "Abelian Codes over Eisenstein-Jacobi Integers for MIMO Systems." *In Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on,* pp. 1909-1912. IEEE, 2017.

Journals(Under preparation)

1. **Raghavendra M.A.N.S** and U. Shripathi Acharya, "On the Rank Distance Properties of Quasi-Cyclic Codes." to be submitted to *IEEE Transactions on Communications*

2. **Raghavendra M.A.N.S** and U. Shripathi Acharya, "On the Rank Metric Abelian Codes." to be submitted to *IEEE Transactions on Information Theory*

3. **Raghavendra M.A.N.S** and U. Shripathi Acharya, "Cooperative Relay Assisted LOS MIMO Communication: A Space-Time Block Coded Spatial Modulation Approach." to be submitted to *Wireless Personal Communications, Springer*.

Brief Bio-Data

Name: Raghavendra M.A.N.S

Address
Raghavendra M.A.N.S
Research Scholar, Department of Electronics and Communication Engineering,
National Institute of Technology Karnataka, Surathkal, India-575025.
e-mail: mans.raghavendra@rediff.com

Qualification

- M.Tech - Communication Systems, National Institute of Technology Karnataka, Surathkal.
- B.E - Electronics and Communication Engineering, Visvesvaraya Technological University (VTU), Belgaum.

Research Interests

Error Control Coding, MIMO Wireless Communications.