ADDIS ABABA UNIVERSITY
RESEARCH AND GRADUATE PROGRAMS

ADDIS ABABA INSTITUTE OF TECHNOLOGY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

CODING AND DECODING OF PERFECT SPACE-TIME BLOCK CODES: ANALYSIS AND PERFORMANCE EVALUATION

BY

AREGAWI GEBRESILASSIE GEBREHIWOT

ADVISOR

Dr. HAILU AYELE

A thesis submitted to the Research and Graduate Programs of Addis Ababa University
In partial fulfillment of the requirements for the award of the degree of
Master of Science in Communication Engineering

Nov 2012
Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY
RESEARCH AND GRADUATE PROGRAMS

ADDIS ABABA INSTITUTE OF TECHNOLOGY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

CODING AND DECODING OF PERFECT SPACE-TIME BLOCK CODES: ANALYSIS AND PERFORMANCE EVALUATION

BY

AREGAWI GEBRESILASSIE GEBREHIWOT

ADVISOR

Dr. HAILU AYELE

ADDIS ABABA UNIVERSITY
RESEARCH AND GRADUATE PROGRAMS

ADDIS ABABA INSTITUTE OF TECHNOLOGY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

CODING AND DECODING OF PERFECT SPACE-TIME BLOCK CODES: ANALYSIS AND PERFORMANCE EVALUATION

By

Aregawi Gebresilassie Gebrehiwot

ADDIS ABABA INSTITUTE OF TECHNOLOGY
APPROVAL BY BOARD OF EXAMINERS

Dr.Getahun Mekuria	_____
Chairman, Dept. of Graduate Committee	Signature
Dr. Hailu Ayele	_____
Advisor	Signature
Ato Yalemzewd Negash	_____
Internal Examiner	Signature
Dr. Dereje H.mariam	_____
External Examiner	Signature

Declaration

I, undersigned, declare that this thesis entitled "**Coding and Decoding of perfect Space-time Block Codes: Analysis and Performance Evaluation**" is the result of my own work except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : _____

Name : Aregawi Gebresilassie Gebrehiwot

Date : _____

This thesis has been submitted for examination with my approval as a university advisor

Signature : _____

Advisor's Name : Dr. Hailu Ayele

Date : _____

Acknowledgments

Above all I thank my Lord, God & Savior Jesus Christ Who give me the strength to accomplish this task.

My second thanks goes to my advisor, Dr Hailu Ayele for all of his guidance. He is my second real mentor in my stay in academics. I am always surprised his commitment and dedication, his fatherly advice, even at class secessions', and his willingness to discharge his responsibilities. These are only few out of his qualities that exemplify him being a role model in my future career. His encouragement and appreciation words are motives in hard times.

My third gratitude is to Dr. Dereje Hailemariam who used to ask me critical questions, give me suggestions and recommendations during the seminar presentations, which helped me to separately see some details from general concepts. I would, also, like to thank Ministry of Education (MOE) to sponsor me to pursue this post graduate program. Next, it is my pleasure to thank the department of ECE to extend the deadline of submission understanding the constraint and insufficiency of the computer lab working hours that we had.

Thank you Higigat Aregawi, Tekleab Teka,Yonas Fisseha and Damtew Assfaw for your co-operation in giving me your laptops at times. It is my pleasure to thank my dwell mate Hailay Berihu for being understanding and considerate.

Really thank you my family to all of your genuine and immeasurable love that you always give me which keeps me strong, happy and motivated. Lastly, thank you all who have been on my side in all of my way in accomplishing this thesis work.

Abstract

Multiple-input multiple-output (MIMO) is one of the most significant advances in digital communication which enabled to increase the data rate as well as improve the reliability and robustness of the system to as compared to single antenna systems. This is achieved by deploying multiple antennas both at the transmitter and receiver sides [1]. However, various assumptions about channel state information (CSI) and channel fading lead to different capacity results [2]. Fading can be reduced substantially by using diversity techniques. Space-time diversity is the most economic technique. Space-time block codes (STBCs) are the most widely employed space-time codes. Perfect space-time block codes (PSTBCs) are families of STBCs that satisfy all of the following criteria: full diversity, high rate, good constellation shaping, uniform average transmitted energy per antenna, non-vanishing determinant (NVD) for increasing spectral efficiency and diversity-multiplexing tradeoff (DMT).

In this thesis, we investigate and demonstrate the coding and decoding of PSTBCs. We first give the design criteria of STBCs followed by the mathematical background of cyclic division algebra (CDA) as a constructing tool for PSTBCs. The PSTBCs are constructed and investigated to be the most efficient family of STBCs by the design criteria of STBCs.

Having considered conditional optimization maximum likelihood (COML) as a near optimal yet less complex decoding scheme of PSTBCs, we demonstrated the decoding of Golden code, a family of PSTBC, as an example. Simulation results show that the symbol error rate of the COML decoding of the Golden code is almost equal to ML decoding with decoding complexity of only $O(q^2)$ which is the order of, $O(q^4)$ for the conventional ML. Further, we considered the performance of the COML decoding under transmit, receive and both transmit and receive antenna correlations and found consistent complexity reduction. Although there is some deviation, in exact optimality of the COML decoding of the Golden code as of the previous works in the literature, which arise most probably due to the inaccuracy of the QAM quantization we used in this thesis, we conclude that an N_t transmit antenna PSTBC is near optimally COML decodable with a reduction in complexity of the order, $O(q^{N_t})$ from its respective ML.

KEY WORDS: STBC, CDA, PSTBC, COML.

Table of contents

TABLE OF FIGURES

List of Abbreviations and Symbols

List of Abbreviations

PSTBC	Perfect Space-time Block Code
NVD	Non-Vanishing Determinants
DMT	Diversity-Multiplexing Tradeoff
CDA	Cyclic Division Algebras
QAM	Quadrature Amplitude Modulation
HEX	Hexagonal
COML	Conditionally Optimized Maximum Likelihood Decoding
STC	Space-time Code
SNR	Signal-to-Noise Ratio
MIMO	Multiple Input Multiple Output
ML	Maximum Likelihood
MMSE-DFE-Fano	Minimum Mean Square Error Decision Feedback Equalizer Fano
V-BLAST	Vertical -Bell Laboratories Layered Space-time
CLPS	Closest Lattice Point Search
BB	Branch and Bound
PAM	Pulse-Amplitude Modulations
CSI	Channel State Information
PEP	Pair wise Error Probability
SER	Symbol Error Probability
STBC	Space-time Block Code
CG	Coding Gain
DG	Diversity Gain

List of Symbols

N_t	Number of transmit antennas
N_r	Number of receive antennas
T	total transmission time duration
$s_m[t]$	symbol transmitted from the m^{th} transmitter at time t
$y_n[t]$	symbol received by the n^{th} receiver at time t
$w_n[t]$	additive noise at the n^{th} receiver at time t
$h_{mn}[t]$	channel coefficient between the m^{th} transmitter and n^{th} receiver antenna at time t
M	a generating matrix
$\Re$	rate of a space-time block code

i	the square root of -1
m	the third root of unity
$d_{E,\min}$	Minimum Euclidean distance
R	rotational matrix
X	transmitted code matrix
Y	received signal matrix
H	matrix of channel coefficients
P(e)	error probability
Q(.)	Gaussian tail function
$\hbar$	Hermittan conjugate transpose
λ	eigenvalue of a square matrix
K	the rank of a matrix
d	diversity gain
r	multiplexing gain
β	bounding region in multidimensional constellation
γ_s	shaping gain of a bounding region
Z	the set of integers
Q	the set of rational numbers
C	the set of complex numbers
*	a multiplication operation
Λ	an algebra
E/B	E is a field extension of a base field B, read as "E field extension of B"
Q(i)	adding non-rational element to Q, which is read as "Q adjoint i"
Z[i]	Gaussian integers
Z[m]	Eisenstein integers
[E: B]	representation of a degree of a finite field extension
θ	generating (primitive)element of a number field
ψ	a homomorphism mapping element
φ	an embedding map of a number field in to a complex number
$\sigma_i(.)$	the i^{th} embedding (conjugate)of an element
Gal(.)	a Galois field extension
$\oplus$	direct sum of elements
e	a basis of a number field
γ	a non-norm code optimizing parameter
N(.)	norm of an algebraic element
Tr(.)	trace of an algebraic element
C_m	code matrix representation
O_E	ring of integers of E
L	Lattice representation
I	an ideal of a commutative ring
CB	space-time block code codebook

CHAPTER ONE

1 BACKGROUND AND INTRODUCTION

1.1 Introduction

From time to time the demand for high data rates is increasing drastically in all of the communication systems in general and in cellular, wireless local area networks and video and audio broadcasting services in particular. Especially providing wireless internet and multimedia services requires a much higher data rate than the existing technology so as to satisfy the ever growing communication need of the society.

Multiple-input multiple-output (MIMO) is one of the most significant advances in digital communication which not only increases the data rate but also improves the reliability and robustness of the system to as compared to single antenna systems. This is achieved by deploying multiple antennas both at the transmitter and receiver sides [1]. But one essential problem of a wireless channel is fading [2].

Fading occurs as the signal follows multiple paths between the transmit and the receive antennas. Depending on the magnitude, delay and phase of each signal, the effect could be that the signals cancel each other completely or significantly that attenuate the combined signal at the receiver. Such a signal may not correctly be detected by the receiver.

One remedy to multipath fading is employing *diversity techniques*. The basic idea of diversity is to send a multiple replica of the same signal in such a way that at least one of those different versions of the signal would reach the destination without fade. These multiple versions of the signal would be combined at the receiver to detect the correct signal. The most common combining techniques are *selection combining*, *switched combining*, *equal gain combining (EGC)* and *maximum ratio combining (MRC*). The choice of the combining technique depends on the trade-off between *system complexity* and *system performance*. While *Selection combining* is the least complex but the least reliable, MRC is the most complex but with the highest performance over all the combining techniques. EGC has a tolerable complexity and yet almost equal performance as of MRC [3] and [4].The diversity can be

achieved by sending the same signal in different time instants, across sufficiently spaced multiple antennas, using multiple frequency bands, or any two combination of them. Researchers have found that while time, frequency and time- frequency techniques are not preferred due to delay and high bandwidth consumption, *space-time diversity* is the most economic scheme that can be employed without consuming much additional network resources.

The most widely studied types of space-time codes (STCs) are turbo, V-BLAST, Trellis and block codes. Although Trellis codes have the highest performance, they are not preferred because of high decoding complexity [5]. In most of real world applications, space-time block codes (STBCs) are employed since lesser decoding complexity and comparable error performance to Trellis codes [6].

The interest of this thesis work is studying space-time block codes (STBCs). Much work has been done on these codes starting from their construction to different performance optimizations to satisfy the design criteria of STCs in general. Some of the most important desired characteristics of STBC are rate, multiplexing gain, diversity gain and coding gain and decoding complexity.

The *rate* of a STBC is defined as the number of information symbols transmitted per signaling interval. While *multiplexing gain (MG)* defines how fast the rate increases with the increase in the signal-to-noise ratio (SNR), the *diversity gain* (DG) determines how fast the error probability decreases with the increase in SNR. The *coding gain* (CG), which defines the power saved by sending a linear combination of the information symbols over sending the information symbols themselves for the same error probability, has the effect of decreasing the error probability. In any case, there is always a trade-off between DG and *MG* as determined in Zheng et al. [7] and other researches. The *MG* and the code rate, however, can be jointly maximized Gamal et al. [8]. On the other hand, decoding complexity is a measure of recovering the signal with the simplest processing, minimum implementation area or minimum power dissipation.

Intending to improve the performance of STBCs, two most important dimensions of constructing the codes have been investigated. The first dimension is building codes based on the traditional number system, the performance of which has many limitations as will be explored in Section 2.5. The second dimension, which is the interest of this thesis, is constructing codes based on *cyclic division algebra* (CDA), a family of modern number system (algebraic number system) to be discussed in Chater 3.

1.2 Problem Statement and Thesis Motivation

STBCs based on the traditional number system (non-algebraic) are inefficient in terms of many of the design criteria. The maximum rate they can achieve is one symbol per signaling interval. In addition, the constellation of the codes is not condensed and there is high energy inefficiency. As the constellation size increases, the minimum Hamming distance of the traditional coding scheme vanishes which degrades the error performance severely. As a result of this, constellation size independent or a minimum Hamming distance lower bounded by a nonzero value is an important requirement for STBC design.

However, algebraic codes, particularly CDA-based codes are found to overcome almost all of the limitations of traditional number- based codes. As these codes are efficient in terms of most of the design criteria, they are called *perfect space-time Block codes (PSTBCs)* [9] and [10].

But as it does in any life scenarios, an advantage comes with its own challenge as well as a cost. One challenge in the construction of codes based on CDA is, it requires a thorough knowledge and understanding of the vast algebraic number theory in general and CDA in particular.

Another big challenge of getting the perfect codes is their *decoding complexity*. Maximum likelihood (ML) decoding is the most optimal decoding scheme in terms of performance. Nevertheless, it is the most expensive method in terms of system complexity. Owing to this, any design of a communication system in general, and

STB coding and decoding in particular aims towards achieving a trade-off between performance and complexity. Aimed to exploit the best performance of the codes from CDA, a number of studies have be done in finding a decoding scheme that approaches the performance of ML, yet with a lesser decoding complexity. The objective of this thesis is, therefore, to address these two challenges of the PSTBCs.

1.3 Literature Review

PSTBC is a relatively recent research area, which is not more than half a decade. The very basic concept of PSTBCs is to define a STBC that satisfies the following design criteria:

- High rate codes.
- Full diversity.
- Have non-vanishing determinant (NVD) as the constellation size increases.
- Have energy efficient constellation.
- Have uniform average energy per antenna.
- Diversity-multiplexing trade-off (DMT) satisfying as well as near optimal in maximizing mutual information Hassibi et al [11].

The first PSTBC was found by Oggier et al. [10], for 2x2, 3x3, 4x4 & 6x6 antenna dimensions only. While investigating the performance of the codes, the authors considered a quasi-static Rayleigh fading channel for the sake of ease and simplicity of analysis.

Later, Elia et al. [12] have generalized the construction of PSTBCs for any number of antennas. In addition to the existing characteristics described by Oggier et al. [10], Elia et al. [12] had modified the full rate & non- vanishing determinant definitions and included additional attributes of the codes. The additional characteristics are the following:

- ***Approximate universality***: the codes have the property that they achieve the DMT criteria for any statistical description of the channel fading coefficients.

- ***Residual approximate universality***: the perfect codes have the property that if certain rows or columns (depending on the order of time and space domain dimensions of the code) each STBC code matrix are deleted, then the resultant code is approximately universal for the correspondingly lesser number of transmit antennas.

Before we proceed to address the proposed decoding schemes of PSTBC, let us highlight the decoding methods of general STCs. Targeted to approach ML, a number of lattice-based quasi-ML decoding algorithms have been proposed for vertical Bell Laboratories layered space-time (*V-BLAST*) model as described in Wolniansky et al.[13] and Damen et al. [14]. The most efficient of such decoders is the minimum mean-square error decision feedback equalizer (MMSE-DFE) Fano-search (abbreviated as "MMSE-DFE-Fano"), Murugan et al .[15]. It is a special case of the general frame work of *closest Lattice Point Search (CLPS)* algorithm. It is based on the analysis of the tree search algorithm for *joint detection & decoding*. The method involves two interrelated stages; namely, preprocessing & tree search. The former is concerned with exposing the underlying tree structure from the received noisy signal. The search stage, on the other hand, is based on the Branch & Bound (BB) algorithm [15]. Nevertheless, the bias introduced in *the MMSE processing* & the tree search scheme with *no boundary control* degrades its performance.

Improving the performance by 2dB over a wide range of SNR, Hu et al. [16] made a simple modification of the method of Murugan et al. [15] by *unbiased extension & boundary decoding*, a scheme called an equivalent Vertical- Bell Laboratories Layered Space-time (V-BLAST) decoding model. Yet it is limited to STCss that are transformable to their V-BLAST equivalent.

However, none of the above described decoders can be easily used to decode the PSTBC.

Oggier et al [10] pointed out that PSTBCs with an q-quadrature amplitude modulation $(q-\mathrm{QAM})$ or q-hexagonal $(q-\mathrm{HEX})$ constellation can be decoded based on an implementation of *sphere decoding* algorithm. The principle of the

algorithm is to search the closest lattice point to the received signal in a sphere of radius $\sqrt{c}$. However, the scheme has the following drawbacks:

- ✓ The algorithm's speed is highly affected by the choice of c, the radius.
- ✓ Whenever an error occurs, either the detected symbol is deleted or c is increased, which delays the processing time.
- ✓ The value of c is dependent on the noise status which should be adjusted frequently, particularly for time varying channels.
- ✓ For the Golden code, a 2x2 PSTBC, the worst case decoding complexity is found to be the fourth power of the constellation size. But even though there is no an analysis for the rest of the PSTBCs, the lattice point search is expected to degenerates to an exhaustive search as the preprocessing stage of the algorithm will yield a plane of possibilities rather than a single initial estimate when the channel matrix is close to singular.

Most recently, a fast and, yet an essentially maximum likelihood decoding of the PSTBCs has been found by Sirianunpiboon et al. [17, 18]. The decoding method is based on the conditional maximization of the ML by conditionally optimizing a certain set of the signals conditioned by the others [19].The scheme has been used in many wireless signal estimations and detections. The decoding complexity of the Golden code and 3x3 PSTBC, for example, is the second and sixth power of the constellation size whereas these have been a fourth and ninth power of the constellation size respectively for their conventional ML. In general this *conditionally optimized ML (COML)* decoding method reduces the power of the complexity order of the conventional ML by the order of the number of antennas used for the PSTBC.

1.4 Thesis Objectives

1.4.1 General objectives

This thesis has two main objectives. The first objective is to investigate the mathematical background necessary to construct the PSTBCs from CDA. While addressing the basic idea of the number system, the main focus will be on their

coding applications. At the end of having a full understanding of the concept, the perfect codes will be constructed showing how they satisfy those important design criteria. The second main objective of the thesis is to apply the COML decoding algorithm to test the performance of the PSTBCs.

1.4.2 Specific Objectives

As specific objectives, this thesis addresses modern number system in general and CDA in particular as a tool to design PSTBC. After studying the concept behind CDA, the algebraic structure of the number system is used to construct the perfect codes. We investigated that the algebraic properties of a number field working in its ring of integers gives, the non-vanishing determinant property, a necessary precondition characteristic of the codes to be DMT satisfying. In addition, we saw how rings of integers of number fields can be used to build algebraic lattices. The corresponding CDA, lattice, Gram & generator matrices, the codeword and minimum determinant of a PSTBC for antenna dimensions n=2,3,4,5 are demonstrated. The PSTBCs are investigated to satisfy almost all of the design criteria of STBCs. The performance of COML, in terms of the symbol error probability, is simulated using MATLAB. The simulation results showed as the PSTBCs are essentially ML decodable by using COML with slight deviation. As the approach is the same for all of the perfect codes, the performance of the Golden code under quasi-static Rayleigh fading channel is to be investigated as an example. Performance of the code will be studied in uncorrelated channel scenarios as well as realistic correlated antenna scenarios both at the transmission and reception side.

1.5 Organization of the Thesis

Chapter 2 presents background information related to STC. More specifically, we present the system and channel models, address the design criteria and discuss other properties of the codes to better optimize their performance in terms of constellation shaping, high rate, non-vanishing determinant (NVD) and DMT. Chapter 3 presents the mathematical background of CDA-based codes. By starting from definitions and giving notations of algebraic structures, it shows how algebras from number fields can yield high rate STBCs. In addition, Chapter 3 describes how the *norm* and the *ring of integers* of an algebraic element are related to the full diversity and NVD properties of STBCs. Chapter 4 is devoted to the explicit construction of the PSTBCs based on the algebraic concept developed in Chapter 3. The corresponding CDA, lattice, generator matrix, codeword and minimum determinant of PSTBC for antenna dimensions from two up to five is analyzed. Chapter 5 demonstrates, after giving necessary background of *conditional optimization*, the performance of COML as applied to Golden code under correlated and uncorrelated antenna conditions. Finally, Chapter 6 summarizes the conclusions from this research.

CHAPTER TWO

2 SPACE-TIME BLOCK CODES

2.1 Introduction

As its name implies, a STC is a coding scheme wherein the set of information symbols or their linear combination are transmitted across multiple antennas (space) and in different time slots. Before looking at the design of a STBC and some common families of STBCs, first consider how the concept of STCs in general and a STBC in particular came into existence.

The first inspiring event which paved a way to the development of STCs was the work of Wittenben [20], in which he found a bandwidth efficient transmit antenna modulation diversity scheme. But the key development of STCs is due to the work of Tarokh et al. in [5], wherein they proposed space-time Trellis codes. These codes are based on convolutional coding and Viterbi decoding. Even if they have highest performance, their decoding is complex and exhaustive. In addressing the high decoding complexity of trellis codes, STBCs were discovered. The first STBCs were found for smaller antenna dimensions. The first remarkable of such codes is the Alamouti STBC which employs two transmit and two receive antennas [6].

This coding scheme allowed the receiver to harness the spatial diversity of the transmit antennas while maintaining simple maximum-likelihood (ML) decoding at the receiver. This ease of decoding complexity comes owing to the orthogonality of the sequence of symbols transmitted from both antennas.

The work of Alamouti was later extended to any number of antennas by Tarokh et al. [21] by *theory of orthogonal designs*. But those codes had a limitation that complex orthogonal STBCs for more than four antennas can only achieve $1/2$ a rate. However, this constraint was solved after Liang [22] designed orthogonal codes with maximum rates. Nevertheless, orthogonal designs, in general, have a drawback that their maximum rate is less than one symbol per signaling interval for more than two antennas. Thus, we are sacrifying one important design

parameter, the *rate*. However, the *diagonal algebraic* [23] and *quasi-orthogonal* STBCs [24], [25], [26] achieved a transmission rate of one symbol per signaling interval, at the expense of an increase in decoding complexity.On the one hand, there is a penalty of data rate in orthogonal designs, on the other hand there is cost of decoding complexity in diagonal algebraic and quasi-orthogonal STBCs. The *semi-orthogonal algebraic* STBCs [27] were proposed as an alternative to quasi-orthogonal and diagonal algebraic STBCs as they achieve comparable bit-error rate performance yet they require a lower decoding complexity. Orthogonal, quasi-orthogonal, diagonal algebraic and semi-orthogonal algebraic STBCs achieve a maximum rate of one symbol per signaling interval.

In addressing the need for *higher rates*, the *threaded algebraic* [28] and *PSTBCs* [10] [29] were proposed. These high-rate STBCs achieve the maximum rate of the uncoupled parallel communication link. The formal definition of full and high data rates will be presented in Section 2.2 below.

In this chapter, first the MIMO communication system model and the channel fading model will be described. Next, a brief review of design criteria for STBCs in quasi-static fading channels and other properties that would improve the performance of the codes will be addressed.

2.2 Space-time Block code Model

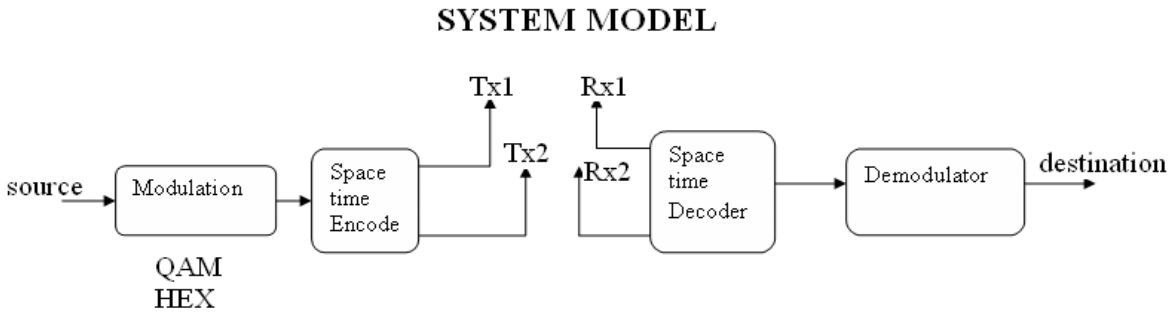


Figure 2.1: A Space-time Block code model

Consider a MIMO system with N_t transmit antennas and N_r receive antennas where each of the transmitters are sending for a certain duration of time, T. The pattern of transmitted symbols of a space-time block code forms an array of

matrices of the order $N_t x\, T$. While the transmitted symbols are the information signal themselves in uncoded system, they are a certain combination of the information signals in a coded system. A common way of forming the symbols is by making a linear combination of the information signals which is called linear space-time block coding. The energy required to transmit the information symbols may be over or below that is required to transmit the signals themselves. The difference in energy between the former and the latter for the same error probability is called the coding gain (CG) of the system. A coding technique with a higher CG is preferred in power limited systems.

STBC is a matrix formed by arranging those symbols across rows and columns. In our case the row refers to the *spatial domain* whereas the column refers to *temporal domain*. Thus, a certain row corresponds to a sequence of symbols transmitted by the corresponding transmitter throughout the whole transmission period and a certain column corresponds to the pattern of symbols transmitted at that particular time instant by all the transmitters.

Assuming that an information symbol transmitted by the ith transmit antenna at the jth transmission time slot is represented by x_i^j, the STBC codebook can be written in a simplified form as:

$$CB = \begin{bmatrix} x_1^1 & x_1^2 & \cdots & x_1^T \\ x_2^1 & x_2^2 & \cdots & x_2^T \\ \vdots & \vdots & \ddots & \vdots \\ x_{N_t}^1 & x_{N_t}^2 & \cdots & x_{N_t}^T \end{bmatrix} \tag{2.1}$$

Thus, the row $\begin{bmatrix} x_i^1 & x_i^2 & \ldots & x_i^T \end{bmatrix}$ is the sequence of information symbols transmitted by the ith transmit antenna in all transmission time slots while the column $\begin{bmatrix} x_1^t & x_2^t & \ldots & x_{N_t}^t \end{bmatrix}^T$ is the information pattern sent at the tth transmission time slot. The rate of STBC is the total number of symbols transmitted per signaling interval. If K number of symbols are transmitted within a time duration of T, the rate R is given

by K/T. An STBC is called *full rate* if $R = 1$. However, if $\Re > 1$, then the STBC is called a *high rate* STBC.

As mentioned in Section 2.1, most of STBCs from traditional number (non-algebraic) including Orthogonal, quasi-orthogonal, diagonal algebraic and semi-orthogonal algebraic STBCs achieve a maximum rate of $R = 1$. It is rare to get a full rate complex signal constellation STBCs for higher antenna dimensions. The only two STBCs which achieve high data rates are *threaded algebraic* and *PSTBCs*. Both of them give a maximum rate of the number of parallel interconnections between the transmitters and receivers. For equal n number of transmit and receive antennas, these two coding schemes can achieve a rate of data up to n [28] [29]. Although threaded algebraic and perfect STBCs are similar in most of the STBC design criteria, the former lack the NVD property which is a necessary precondition for the coding to be DMT satisfying. The NVD and DMT are some of the most important design criteria of STBCs which will be discussed in Section 2.4.

The design criteria of a STBC depend on the availability of the channel state information (CSI) to the receiver. As a result, the design criteria for coherent and non-coherent receptions are different. The former is to mean that there is a perfect CSI at the receiver which can be done by sending pilot signals along the information symbols while the latter implies that the receiver has no knowledge (i.e blind) of the channel state.

The noisy received signal by the n^{th} receive antenna at the t^{th} time instant in a fading channel condition is given by:

$$y_n^t = \sum_{m=1}^{N_t} h^t{}_{m,n} x_m^t + w_n^t \tag{2.2}$$

Where,

- y_n^t is the received noisy signal by the n^{th} receive antenna at the t^{th} time instant.
- $h^t{}_{m,n}$ is the channel fading coefficient between the m^{th} transmit and the n^{th} receive antennas. w_n^t is a complex AWGN with zero mean, unit variance and power spectral density of N_0 at the n^{th} receiver at the t^{th} time instant.

In communication, there are different channel fading models of which *Rayleigh* and *Ricean* are the two most common fading channel models. A Rayleigh channel fading model is used when there is no-direct line of sight (NLOS) between the transmitter and the receiver that the received signal is substantially dominated by sufficiently many reflected components of the transmitted signal. In this case, the combined signal is complex, whose real and imaginary components are independent identically distributed (i.i.d) Gaussian random variables with zero mean and variance σ_s^2. The probability density function of the combined signal x is given as:

$$p(x) = \begin{cases} \frac{x}{\sigma_s^2} exp\left(\frac{-x^2}{2\sigma_s^2}\right), & x \geq 0 \\ 0, & otherwise \end{cases} \quad (2.3)$$

A channel is called Rician fading type if there is a direct signal component in addition to a Rayleigh distributed multiple reflected components.
The probability density function of a Rician fading signal is given by [30].

$$p(x) = \begin{cases} \frac{x}{\sigma_s^2} exp\left(\frac{-(x^2+D^2)}{2\sigma_s^2}\right) I_0\left(\frac{xD}{\sigma_s^2}\right), & x \geq 0 \\ 0, & otherwise \end{cases} \quad (2.4)$$

Where, D^2 is a direct signal power and $I_0(.)$ is a modified Bessel function of the first kind and Zero-order

As mentioned in the background part, the strength of the received combined signal is dependent on the phase, magnitude and delay spread of each component. *Delay spread* is the difference in propagation time between the longest and shortest paths which count for the resultant energy.

In addition to the nature of the impact of the environment on the magnitude and phase of the signal, a channel can also be classified based on the *rate of change of its nature* within the transmission duration.There are three models based on the speed of change of channel fading coefficients [30]:

- *Slow or Quasi-static fading*: In this case, the channel is assumed to behave constant throughout the transmission time duration. Thus, the channel

fading coefficients are chosen at the beginning of transmission. As a result, from Equation 2.2, $h^{t}_{i,n} = h^{\cdot}_{i,n}$.

- *Block fading*: the channel is assumed constant for a certain number of transmission instants only. Therefore, the channel fading coefficients are taken at the beginning of each block.

- *Fast fading:* the channel is thought to vary in every transmission time slot that the coefficients are taken to be the state of the channel at the beginning of each transmission time interval. In this thesis, we consider quasi-static Rayleigh fading channel.

In addition its dependancy on the availability of the CSI, the performance of the STBC is partly determined by the shape of the *bounding region* [10], as the complex information symbols of a STBC are elements of a multidimensional signal space. The symbols are required to be densely packed within a certain region. Such a property is called *shaping gain* of the coding scheme. This will be seen later in the constellation shaping part of Section 2.4.

2.3 Design Criteria of STBCs

After giving a back ground on the channel characteristic description, now it is possible to derive the code design criteria of STBCs. Here we see the design criteria of STBCs under quasi-static Rayleigh fading channel for coherent receiver. The two fundamental design criteria of STBCs are the *rank criterion* and the *determinant criterion* which will be discussed here in detail. These design criteria are derived based on the *union bound pair-wise error probability (PEP)* of the STBCs.

Assume that the received noisy signal vector is Y and the transmitted codeword of a STBC is X. The *maximum likelihood* (ML) decoder under an assumption of perfect *CSI* of the matrix H at the receiver tries to minimize the distance metric.

The distance metric is commonly written as the *squared Frobenius norm* which is given by [31]:

$$min \, \|Y - HX\|^2 \tag{2.5}$$

Where, $Y = HX + W$ compact form of Equation 2.2

An estimate of the error probability $p(e)$ is obtained by using the *union bound* as an average *PEP* over all elements of the constellation. An estimate of the error probability based on PEP is given by:

$$p(e) \le \frac{1}{|C\mathcal{B}|} \sum_{X \in C\mathcal{B}} \sum_{\hat{X} \ne X} p(X \to \hat{X}) \tag{2.6}$$

Where, $p(X \to \hat{X})$ is the *PEP*, i.e., the probability that when a codeword X is transmitted, the ML receiver decides erroneously in favor of another codeword $\hat{X}$, assuming only X and $\hat{X}$ are in the codebook. It can be shown that the PEP is a Gaussian tail function, Q(.), averaged over all realizations of the channel matrix H. Thus, it is given as

$$PEP = E\left[Q\left(\frac{\left\| H(X - \hat{X}) \right\|}{\sqrt{2N_0}} \right) \right] \tag{2.7}$$

Where $(X - \hat{X})$ is the *codeword difference matrix* and $N_0/2$ is the power spectral density (PSD) of the noise. The PEP will have different solutions depending up on the nature of the channel fading model considered. In the case of an independent Rayleigh fading, wherein the channel coefficients are assumed to be zero mean and unit variance complex Gaussian variables, the PEP can be rewritten as follows [31]:

$$PEP \le \det\left[I_{N_t} + \frac{E_s (X - \hat{X})(X - \hat{X})^{\hbar}}{4N_0} \right]^{-N_r} \tag{2.8}$$

Where, E_s is the average symbol energy and $\hbar$ is a Hermittan transpose of a matrix. Now let us denote the product of the codeword difference matrix and its complex transpose, $(X - \hat{X})(X - \hat{X})^{\hbar}$ by E and its rank by K. The value of K varies between 1 to N_t. If K= N_t for all of the pairs $(X, \hat{X})$, then the STBC is called a *full rank STBC*.

To state it differently, E has N_t Eigen values. If $\lambda_i, i = 1,...,K$ are the nonzero Eigen values of E, the PEP can be rewritten as follows.

$$PEP \le \prod_{i=1}^{K} \left(1 + \frac{Es\lambda_i}{4N_0}\right)^{-N_r} \tag{2.9}$$

For high SNR, the expression in the bracket may further be approximated such that the PEP can be rewritten in a more simplified form as

$$PEP \le \left(\frac{Es}{4N_0}\right)^{-KN_r} \left(\prod_{i=1}^{K} \lambda_i\right)^{-N_r} \tag{2.10}$$

Here, there are basically two variables which determine the PEP. Let us now reshape the expression so as to be in the form of parameters of our interest.

$$PEP \le \underbrace{\left(\frac{SNR}{4}\right)^{-KN_r}}_{1} \underbrace{\left\{\left(\prod_{i=1}^{K} \lambda_i\right)^{1/N_r}\right\}^{-Nr^2}}_{2} \tag{2.11}$$

In Equation 2.11, while KN_r is called the DG, $\left(\prod_{i=1}^{K} \lambda_i\right)^{1/N_r} / d_{eq}$ is called the CG. Where, d_{Eq} is the Euclidean distance of the uncoded reference signals [31].

Taking the logarithm of both sides, Equation 2.11can be rewritten as

$$\log(PEP) \le -\mathcal{DG}\log(SNR) - Nr^2 \log(\mathcal{CG}) - Nr^2 \log(d_{Eq}) + d \tag{2.12}$$

Where,

- DG is the diversity gain of the STBC
- CG is the coding gain of the STBC and d is a constant due to ¼.

2.3.1 Design criterion 1: the Rank Criterion

The upper bound PEP expression given in Equation 2.11 can be made as small as possible by making the DG as big as possible. DG is an approximate measure of the power gain of the system with diversity over without diversity at the same error probability [30]. As the number of receivers is fixed, DG can be maximized by maximizing K, the *rank order*. The maximum DG is achieved when $K = N_t$. Thus, the highest achievable DG is $N_t N_r$, obtained when the STBC is full rank with $K = N_t$.This criterion is called the *rank criterion*. DG determines how fast the PEP decays as a function of SNR. As can be seen from Equation 2.12, the DG is the *slope*

of the PEP against the SNR. Thus, the higher the *DG*, the lower the PEP. Consequently, a STBC is required to have the highest possible *DG* to offer the best error -free reception. Even though most of the family of STBCs described in Section 2.5 achieve fully diversity, only algebraic based STBCs achieve it with high rate and small number of transmit antennas.

2.3.2 Design Criterion 2: the Determinant Criterion

The PEP in Equation 2.11 can be made again as small as possible by playing around with the second term in the expression. As the exponent is negative, the term will have a minimum value when the product of the Eigen values is a big number. Thus, the PEP is inversely related to the CG of a STBC. CG can be taken as an approximate measure of the power gain of a coded system over that of uncoded system at the same DG and error probability [30]. As shown in Equation 2.12, the CG reduces the error probability by shifting the error rate curve to the left. As a result, an STBC with the high CG will have less probability of being in error. The term $\prod_{i=1}^{K}\lambda_i$ in Equation 2.11 is the absolute of the sum of the determinant of all the principal KxK cofactors of $(X-\hat{X})(X-\hat{X})^{\hbar}$,Tarokh [5]. This is called the *determinant criterion* of the STBC code design.

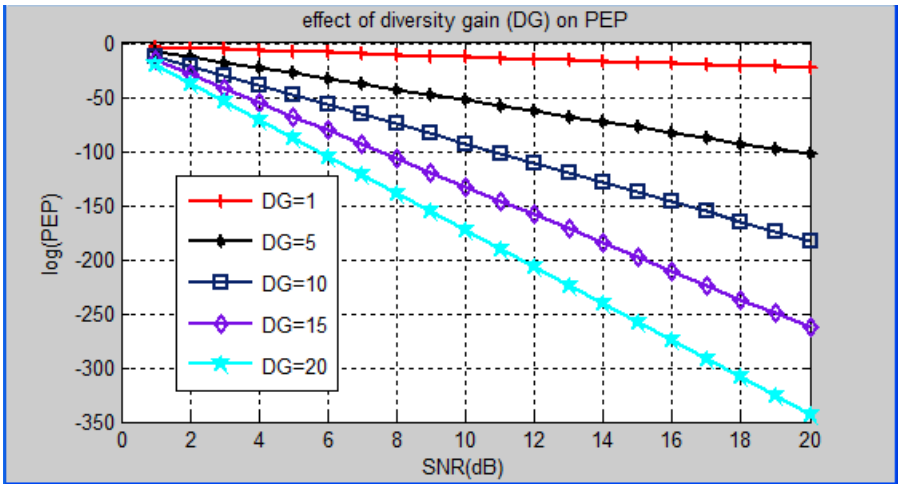


Figure 2.2 : The effect of DG on PEP for Nr=2, CG=2

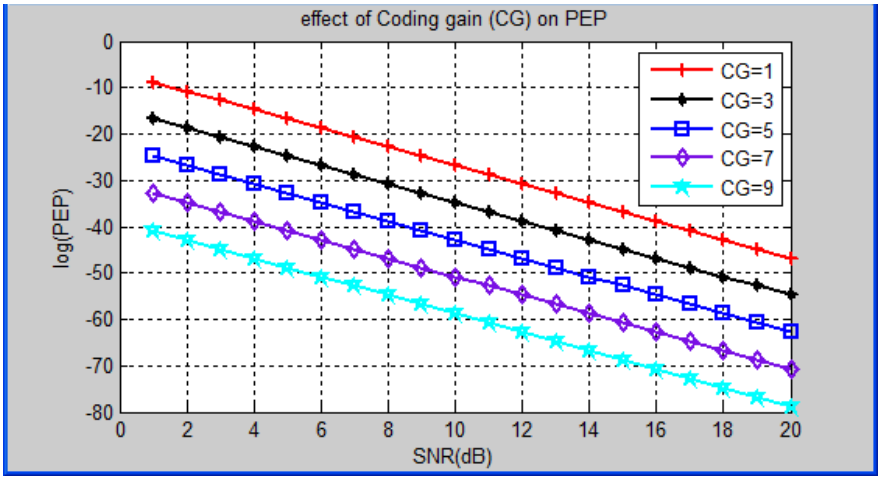


Figure 2.3: the effect of CG on PEP for Nr=2, DG=2

Figure 2.2 shows the effect of DG on PEP as described in Equation 2.12. Here, the slope of the PEP curve is approximately -5 for DG=5, -10 for DG=10, -12.5 for DG=15 and -17.5 for DG=20. Figure 2.3 shows the impact of CG on PEP as mentioned in Equation 2.12. It shows that for every 2 units increase of the CG, there is a 10 units shift of the PEP to the left.

2.3.3 Design criterion 3: the Decoding Complexity

It is not only how much a message is correctly decoded but also how easily it is decoded that matters in communication systems. This is so because the quality of a communication system is measured as a trade-off between *performance* and its *cost*. The decoding complexity contributes to the cost of a system in terms of hardware and signal processing. Thus, the design of a communication system in particular and STBC in particular should take into consideration both the *accuracy* and *simplicity* of decoding. Design criteria 1&2 cited above are based on the performance of STBC while design criterion 3 is based on the simplicity of decoding. As ML is the optimum decoding method, we use this as a base of comparison. Assuming perfect CSI, the ML decoder at the receiver chooses L complex information symbols, $x_i, i \in \{1,...,L\}$ that minimizes distance the metric:

$$F(\hat{x}_1,...,\hat{x}_L) = \arg\min\left\{\sum_{t=1}^{T}\sum_{n=1}^{N_r}\left|y_n^t - \sum_{i=1}^{N_t} h_{i,n}^t s_i^t\right|^2\right\} \tag{2.13}$$

The decoding complexity of an ML decoder is defined as the number of metric computations required to reach the ML decision. The worse-case decoding

complexity of an exhaustive ML is q^L as shown in [32], which corresponds to the maximum number of metric computations. Here q is the constellation size and L is the number of information symbols transmitted from that given constellation. The complexity of an algorithm is measured by the complexity of its hardware implementation. The hardware complexity in turn is measured by the number of logic gates, the area required to implement the algorithm and in terms of the power it dissipates.

Consequently, the number of metric computations should be as small as and as simplified as possible to reduce the implementation complexity of the algorithm. One way of doing this for linear STBCs is, by writing the ML computation in the form of linear sum of decoupled groups [32]. In such a case, each group would be a function of only certain fixed number of complex information symbols. Thus, a ML is called β-group decodable if it can be decomposed in to β decoupled groups. Let us see the following as an example. The ML decoding of Equation 2.13 assuming only three complex symbols is given as follows:

$$F(\hat{x}_1, \hat{x}_2, \hat{x}_3) = \arg\min\left\{\sum_{t=1}^{T}\sum_{n=1}^{N_r}\left|y_n^t - \sum_{i=1}^{N_t} h_{i,n}^t s_i^t\right|^2\right\} \tag{2.15}$$

Depending on the number of separable groups, we can have three sets of STBCs with the following ML expression.

$$\begin{aligned} STBC1 &: F(\hat{x}_1, \hat{x}_2, \hat{x}_3) = F_1(\hat{x}_1) + F_2(\hat{x}_2) + F_3(\hat{x}_3) \\ STBC2 &: F(\hat{x}_1, \hat{x}_2, \hat{x}_3) = F_1(\hat{x}_1) + F_2(\hat{x}_2, \hat{x}_3) \\ STBC3 &: F(\hat{x}_1, \hat{x}_2, \hat{x}_3) = F_1(\hat{x}_1, \hat{x}_2, \hat{x}_3) \end{aligned} \tag{2.16}$$

STBC1 is separable or three-group decodable since we can separate the decoding of the three transmitted symbols into three groups, each containing one complex symbol. Similarly, STBC2 is separable or two-group decodable as its ML decoding is separated in to two groups one of which containing one complex symbol while the other two complex symbols. Finally, STBC3 is not separable since the three symbols have to be decoded jointly.

2.4 Other important properties to further improve performance of STBCs

In addition to the three design criteria discussed in Sections 2.3.1-2.3.3, STBCs with the following characteristics will have better performance.

2.4.1 Constellation Shaping

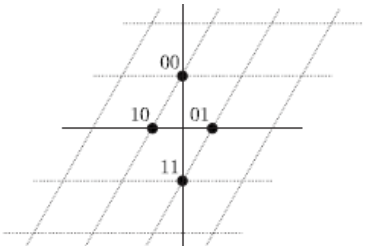
In design of signal constellation, the two fundamental operations are the *bit labeling* and the *constellation shaping*. The old problem of engineering mathematics was to maximize the number of spheres which fit a large box. The portion of the box occupied by the spheres is called the *sphere packing density* [33]. The optimal and densest sphere packing is known for dimensions one and two. In *lattice sphere coverings,* where the center of overlapping spheres form a lattice, it is possible to get an optimal and densest packing up to dimension eight [33]. *Lattice* is a discrete set of points in a multidimensional vector space. Thus, as STBC symbols correspond to points in multidimensional signal space, they can be packed as efficiently as possible inside a region which is characterized by the shaping gain of the code.

The *shaping gain* γ_s is defined relative to a *cubic bounding region* for which γ_s = 0 dB. The bounding region with maximal γ_s is spherical for any dimension, and for the dimension growing to infinity it can be shown that $\gamma_s \rightarrow$1.56 dB. On the contrary any skewed bounding region can result in a substantial shaping loss (i.e., $\gamma_s < 0$ dB) due to the higher average energy required to transmit the same number of constellation points.

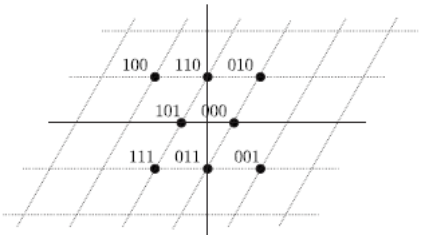
Although the spherical bounding region is attractive due to its shaping gain it has the drawback that labeling the constellation points requires a *huge look-up table*, which can be impractical for large constellations. Cubic constellations offer a better trade-off since they can easily be labeled and do not exhibit any shaping loss (i.e., γs = 0 dB). In order to save on the average transmitted energy, the cubic shaping of the STBCs is required. In addition, in order to get a balanced repartition of energy at the transmitter, the average energy per antenna is preferred to be uniform, which is commonly called *uniform average energy per antenna* (UAEPA).

The two famous and widely used alphabets from which a STBC symbols are taken are *quadrature amplitude modulation* (QAM) and *hexagona*l (HEX) alphabets. The q-QAM alphabet is a subset of the *Gaussian integer* $Z[i] = \{a + bi\}, a, b \in Z$, where $i = \sqrt{-1}$. The constellation is scaled to match $(k + 1/2) + i(l + 1/2)$ for some $k, l \in Z$ i.e., the minimum Euclidean distance $d_{E,\min} = 1$ and it is centered at the origin. The average energy *Es* is 0.5, 1.5 and 2.5 for *q* = 4,8,16. where $q = 2^n$ for some positive integer *n*, which offer great flexibility in terms of rates and are well suited for adaptive modulation schemes. Each of the real and imaginary parts of the q-QAM define a real alphabet known as *pulse amplitude modulation* (PAM).

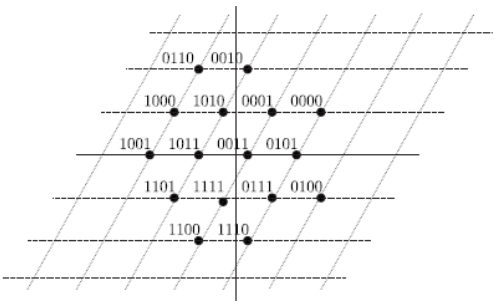
Hexagonal (HEX) alphabet. The $q - HEX$ alphabet is constructed from the two-dimensional hexagonal lattice $Z[m] = \{a + bm\}, a, b \in Z,$ where $m = e^{i2\pi/3}$. The constellations are taken from the translated hexagonal lattice A_2 . A lattice is a discrete set of points in a multidimensional vector space. It is fully described by its linearly independent *basis vectors*. This will be seen in Chapter 3, Section 3.4.



(a) 4-HEX constellation



(b) 8-HEX constellation



(c) 16-HEX constellation

Figure 2.4: optimal q-HEX constellations for q=4 ,8 and 16

The optimum hexagonal constellations, in terms of minimizing the error probability for a given SNR for 4-, 8- and 16-HEX are shown in the Figure 2.4(a), (b) and (c), where the respective translation vectors $(1/2,0), (1/2,0)\ and\ (1/4,0)$ guarantee a zero mean constellation. The bit labeling shown was optimized to mimic a Gray labeling as close as possible, in order to minimize bit error probability [31].

2.4.2 High Rate

As described in the introduction part, the demand of high data rate in modern communication is escalating from time to time. The provision of a broad range of services like wire-line voice quality and wireless date rates of about 64-128 Kb/s (ISDN) using cellular and PCs spectra are some of the growing interests of modern communication systems .In addition, the rapid growth of mobile computing is initiating many researches for high speed data services in the range of 144kb/s for microcellular wide area high mobility applications and up to 2Mb/s for indoor applications [5].

2.4.3 Non-Vanishing Determinant

Another property required for the design of STBCs is the *non-vanishing determinant* (NVD).This property is related to the adaptive modulation of STBCs. *Adaptive modulation* is the ability of a radio transmitter to switch between different modulating schemes to adapt to the varying signal conditions. For example, it can swap between PSK and QAM depending on the strength of the signal. In PSK a single wave form represents a single state while in QAM more states can be represented by a single wave form by varying the amplitude. The higher the number of states represented by a single wave form, the smaller the distances between the states and the greater the probability that the information will be lost during interference or noise. Thus, it is important that the CG, one measure of the minimum Hamming distance between the signal points, will not vanish as the constellation size increases. More importantly, infinite codes with nonzero CG are required to increase the throughput so as to meet the demand of high data rates.

STBC constructions from *non rotated vector space* & *quaternion lattices* give a CG decreasing with the constellation size and eventually vanishing for the infinite code [31]. NVD codes are also useful in bandwidth efficient concatenated coding schemes, where the outer code redundancy can be absorbed by a constellation expansion. A vanishing determinant can drastically reduce the overall CG [34]. The NVD property is a necessary and sufficient condition for a ST coding scheme to achieve the diversity-multiplexing trade-off [35] [36].

2.4.4 Diversity-Multiplexing Trade-off (DMT)

Introduction

Before looking at the trade-off, consider to first see what the intention of each is and how they are related. The intension of *diversity* is to maximize transmitting multiple replicas of the same information symbol in all of the available *tempora*l and *spatial* domains so as to improve the performance. On the other hand, the aim of *multiplexing* is to maximize the number of different symbols to be transmitted by all of the transmitters in all of time instants. Let us take an analogy of this in real world scenario. Assume that there is one fruit trader who has to cross an ocean to another place so as to get better profit. Assume again that he doesn't know the current market status that the price of the each fruit is unknown. He can take two extreme decisions. The *first option* is to take only one type of fruit possibly of different size, color, etc while the *second option* is to take a composite of different fruit types of few in number from each. Here, there is a probability that he can get better profit in both cases: if, when he makes the first choice the price of that particular fruit is high or when he makes the second decision, if the price of all is high and (or) the same. However, the probability of occurrence of these two extreme events is almost zero. As a result of this, the best decision that can be made is somewhere in between these two extremes, where both *making the profit* and *loss of an opportunity* of making a profit will be optimal. The analogy here is, the first decision of taking one type of fruit is analogous to diversity and that of the second decision of taking one from each is analogous to multiplexing. And *making a profit* is the advantage of having reliable communication from diversity or the advantage

of sending much information in multiplexing. Thus, the best practice is to make a trade-off between the two. The ideal thing is to get an inverse relation of each other which doesn't happen in real world scenarios. Before considering the DMT of STBCs, it is worth to clarify the two concepts; the rate in terms of the *channel capacity* and the diversity in terms of the *outage probability.*

2.4.4.1 Channel Capacity

Given a particular channel realization H, the theoretical limit of amount of data that can be transmitted via the channel reliably (with arbitrarily low error rate) is called the *channel capacity.* When one pass *separately- packed* but *forcefully -plugged* certain damageable products of different type through a narrow passage, it is expected that they will be deformed. The channel capacity can be thought of as the carrying ability of the channel to pass undamaged or unmixed data. For uniform power allocation at the transmitter, the capacity of a channel under no antenna correlation at both sides is given by [37], [38].

$$C_{channel}(SNR, H) = \log_2\left(\det\left(I_{Nr} + \frac{SNR}{N_t} HH^{h}\right)\right) \tag{2.17}$$

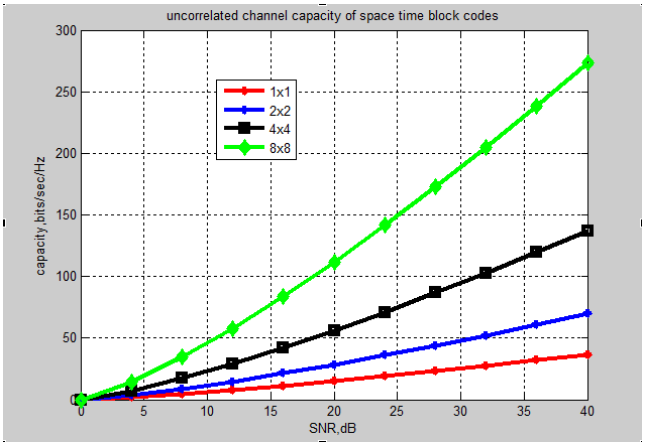


Figure 2.5: Uncorrelated antenna instantaneous channel capacity

The capacity expression in Equation 2.17 is the instantaneous capacity of the channel. The average or ergodic channel capacity is found by finding the average of the instantaneous channel capacity over different realizations of the channel fading coefficients. However, for a *quasi-static channel*, as the channel is expected to be constant within the transmission period, the instantaneous channel capacity can

be taken as the *realizable capacity* of the channel. The assumption of spatial uncorrelation is possible only if the antennas are adequately spaced. Antenna correlation can be a measure of the spatial diversity available in the MIMO system. The higher the correlation, the lower the diversity. There are two common antenna correlation models; while the first is *geometrically- based*, the second is *statistically-based* [38]. *Kronecker correlation model* is the simplest statistically-based correlation model which separates the full correlation matrix into transmit and receive antenna correlation matrices. The following transmit and receive antenna correlation matrices are used [38].

$$\Theta_T = E_H\left\{H^T H^*\right\} = \begin{bmatrix} 1 & \sigma & \sigma^2 & \cdots & \sigma^{N_t-1} \\ \sigma & 1 & \sigma & \cdots & \sigma^{N_t-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma^{N_t-1} & \sigma^{N_t-2} & \cdots & \sigma & 1 \end{bmatrix} \tag{2.18}$$

$$\Theta_R = E_H\left\{HH^{\hbar}\right\} = \begin{bmatrix} 1 & \delta & \delta^2 & \cdots & \delta^{N_r-1} \\ \delta & 1 & \delta & \cdots & \delta^{N_r-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \delta^{N_r-1} & \delta^{N_r-2} & \cdots & \delta & 1 \end{bmatrix}$$

And the generalized correlated channel matrix $\tilde{H}$ is given by

$$\tilde{H} = \frac{1}{\sqrt{tr(\Theta_R)}}\Theta_R^{0.5} H\left(\Theta_R^{0.5}\right)^T \tag{2.19}$$

The ergodic channel capacity of Equation 2.17 assuming transmit and receive antenna correlations is as given, below, in Equation 2.20

$$C_{channel}(SNR, H) = \log_2\left(\det\left(I_{Nr} + \frac{SNR}{N_t}\left(\Theta_R^{0.5}\right)^{\hbar} H\left(\Theta_T^{0.5}\right)H^{\hbar}\right)\right) \tag{2.20}$$

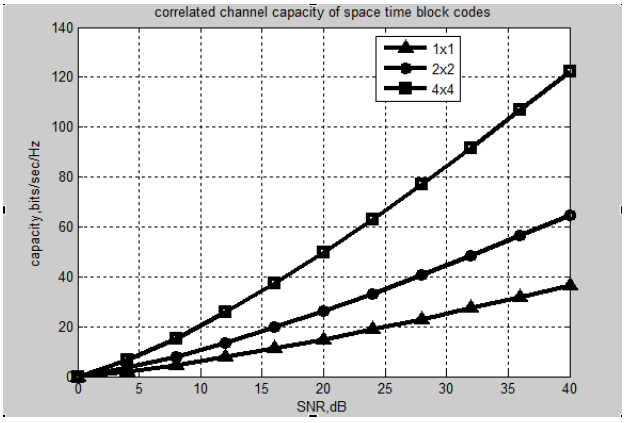


Figure 2.6: channel capacity under both transmit and receive antenna correlation coefficients $(\delta = \sigma = 0.95)$

2.4.4.2 Outage Probability

Another important concept in wireless communication is an *outage*. Whenever the channel matrix is random, the realizable channel capacity is random. In such conditions, it is difficult for the transmitter to adjust its rate in accordance to the realizable capacity that it must transmit at a fixed rate of $\Re$ bites/sec/Hz. This problem is particularly worse when the transmitter has no knowledge of the channel state. It happens, therefore, that when the realized channel capacity is below $\Re$, the receiver cannot decode correctly even for powerful codes.This situation can also be called the "*sender-receiver complete miscommunication event*." This event is called an *outage*. The occurrence of such miscommunication may be frequent or seldom depending on the nature of the surrounding environment and its probability of happening is called the *outage probability*. The probability of a MIMO channel being in outage is given by [31]

$$P_{out}^{MIMO}(\Re) = p\left\{\log_2\left(\det\left(I_{Nr} + \frac{SNR}{N_t} HH^{\hbar}\right)\right) < \Re\right\} \tag{2.21}$$

(a) Single Input-Single Output (SISO) Outage Probability

Assume that there is single transmitter and single receiver and the channel fading coefficient *h* is a zero mean and unit variance Gaussian random variable. The received, noise affected signal when a signal *s* is transmitted is given by

$$y = hs + w \tag{2.22}$$

The probability of an outage occurrence in this single link communication, according to Equation 2.21 is

$$p_{Out}^{SISO}(\Re) = \Pr\left\{\log_2\left(1 + SNR|h|^2\right) < \Re\right\} \tag{2.23}$$

For a Rayleigh fading channel, $|h|^2$ is exponentially distributed [31] that the outage probability will be

$$p_{Out}^{SISO}(\Re) = \Pr\left\{|h|^2 < \left(2^{\Re} - 1\right) SNR^{-1}\right\} \tag{2.24}$$

The cumulative distributive function of a unit parameter- exponentially distributed random variable *x* is determined to be $1 - \exp(-x)$. Applying this result to Equation 2.24, we get the outage probability:

$$p_{Out}^{SISO}(\Re) = 1 - \exp\left(-\left(2^{\Re} - 1\right)SNR^{-1}\right)$$
$$\approx \left(2^{\Re} - 1\right)SNR^{-1} \ (Pade\ approximation) \tag{2.25}$$

Taking logarithm of both sides of Equation 2.25, we get

$$\log\left(p_{Out}^{SISO}(\Re)\right) = -\log(SNR) + c_1 \tag{2.26}$$

The value of c_1 is constant for a fixed rate $\Re$.

(b)SIMO, MISO and MIMO Outage Probabilities

Similarly, the outage probabilities of SIMO, MISO and MIMO systems in their logarithmic scale are given respectively as follows [31]:

$$\log\left(p_{Out}^{SIMO}(\Re)\right) = -\mathcal{N}r\log(SNR) + c_2$$
$$\log\left(p_{Out}^{MISO}(\Re)\right) = -\mathcal{N}t\log(SNR) + c_3 \tag{2.27}$$
$$\log\left(p_{Out}^{MIMO}(\Re)\right) = -\mathcal{N}t\mathcal{N}r\log(SNR) + c_4$$

Where, c_2,c_3 and c_4 are constants due to the rate and the number of receive or/and transmit antennas. Moreover, the negative of the slopes of the outage probabilities in Equation 2.27 are the DG values for a *fully diverse system*.

Note that an *outage* implies an *error* even though the reverse is not always true, as it is possible to communicate while still making some tolerable error. Thus, we can say that an *outage* is the *worse error*. Under *full diversity*, comparing Equation 2.11 to Equations 2.26 and 2.27, we observe that the outage probability is *part of the PEP* regardless of the other constants in both cases. Rewriting Equation 2.11,

$$\log(PEP) \le \underbrace{-\mathcal{D}\mathcal{G}\log(SNR)}_{\mathcal{O}utage} - Nr^2C\mathcal{G} + \underbrace{-Nr^2\log(d_{Eq}) + d - c_i}_{constant}$$

$$\le \mathcal{O}utage - Nr^2C\mathcal{G} + \text{constant} \tag{2.28}$$

Keeping other parameters constant, and particularly under smaller receive antennas, the system performance approaches to outage when the CG approaches to zero, as can be seen from Equation 2.28.

From the worse case error event, outage probability of Equation 2.27 and the general PEP error expression of Equation2.28, the reliability of the system increases as the DG increases. However, increasing the DG has a penalty of decreasing the data rate as described at the introduction of Section 2.2.4. Since the link between

two communicating bodies is required to be highly reliable (*high performance*) as well as that provides to communicate much in a short period of time (*high data rate*), there should be a trade-off between these two. However, finding the trade-off is not a straight forward task and needs a skillful approach.

For a *scalar Gaussian channel*, the channel capacity in Equation 2.17 is given by [31]

$$C_{channel}(SNR) = \log_2(1 + SNR) \qquad (bits/Sec/Hz) \qquad (2.29)$$

Then, the channel capacity in bits per channel use (*bpcu*) at high *SNR* can be approximated to

$$C_{channel}(SNR) = \lim_{SNR\to\infty} \log_2(1 + SNR) = \log_2 SNR \qquad (2.30)$$

This shows that an increase of 3dB in SNR approximately increases the data rate by 1*bpcu*. Thus, asymptotically (SNR→∞), in order to have one more *bpcu*, we need 3dB more SNR.

Now let us consider *k* number of parallel (vector) channels where the CSI is not known by the transmitter. When the noise power decreases by 3dB, there will be an increase of 3dB in the SNR of each of the parallel channels.

This gives rise to an increase of the capacity of each by 1bpcu with an overall effect of increasing the system capacity by *k* bpcu. Thus, asymptotically, the capacity varies by $klog_2SNR$ [31].

A MIMO Rayleigh fading channel can be represented by *k* parallel uncoupled sub-channels such that their capacities add up. Therefore, the capacity in Equation 2.17 can be equivalently rewritten as [30] [31]

$$C_{channel}(SNR, H) = \sum_{i=1}^{k} \log_2\left(1 + \frac{SNR}{N_t}\lambda_i\right) \qquad (2.31)$$

Where, λ_i's are the singular values of HH^h and the instantaneous SNR of each sub-channel is $SNR\lambda_i/Nt$.

Thus, like the vector Gaussian channel, the MIMO Rayleigh fading channel will have *k* number of transmission modes when represented in the form of uncoupled parallel sub-channels. Where, $k=min\{Nt,Nr\}$ is the rank of the system. This also means the MIMO has *k* degrees of freedom that it can send *k bpcu* reliably. As a result of this, the rate of change of the *rate of data* for a MIMO Rayleigh fading

channel will be $k \log_2 SNR$. Here, the variable k is also called the *multiplexing gain (*MG*)* of the MIMO system.

In general, as the SNR approaches infinity, the error probability and the rate can be approximated to behave like the following:

$$\begin{aligned} p_e(SNR) &= -\mathcal{DG} \log SNR \\ \Re(SNR) &= \mathcal{MG} \log_2 SNR \end{aligned} \tag{2.32}$$

At a particular value of SNR, the error probability and the rate can be related as

$$\mathrm{p_e}(SNR) = -\frac{\mathcal{DG}}{\mathcal{MG}} \Re(SNR) \log_2 \tag{2.33}$$

Equation 2.33 shows that in order to minimize the error probability the ratio of the DG to MG must be maximized.

For an arbitrary diversity value *K*, which in turn means arbitrary DG, the maximum achievable DG for a fixed value of MG, and $T \geq Nt + Nr - 1$, in the case of Rayleigh fading is given by [7]

$$\mathcal{DG}(\mathcal{MG}) = (Nt - \mathcal{MG})(Nr - \mathcal{MG}) \tag{2.34}$$

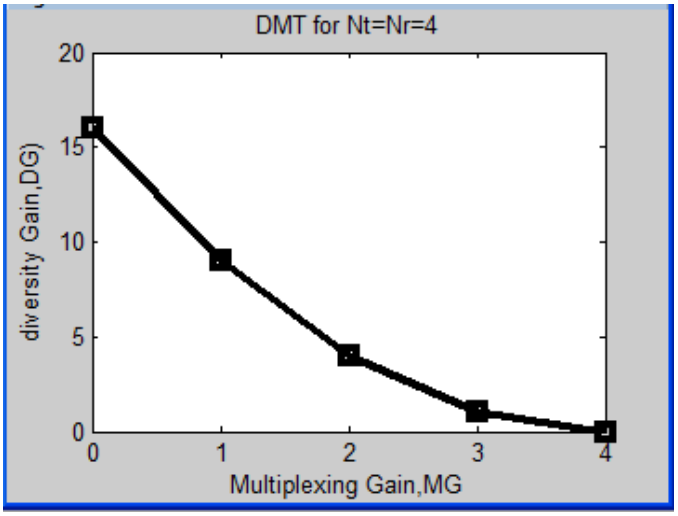


Figure 2.7: the DMT for Nt=Nr=4

In general, the design of STBCs is a trade-off between three conflicting goals: *minimizing the decoding complexity, maximizing the diversity gain* to improve reliability and *maximizing the multiplexing gain* to improve throughput.

2.5 A Review on the most common Families of STBCs

2.5.1 Orthogonal STBCs

Orthogonal STBCs (OSTBC) are the first family of STBCs to be discovered. Their ML decoding is separable due to the orthogonality of the array of symbols transmitted by each antenna. This property of the codes makes them the most easily decodable STBCs [32]. In general an OSTBC satisfies the following orthogonality property:

$$OSTBC^{*}OSTBC = I_{N_t}\sum_{i=1}^{L}\left|s_i\right|^2 \tag{2.35}$$

In addition to their decoding simplicity, OSTBCs are fully diverse. The first OSTBC was constructed by Alamouti [6] for two transmit antennas which was latter extended to any number of antennas by Tarokh et al.[21]. Particularly, Tarokh et al. developed full rate real OSTBCs for any number of antennas but with full rate complex OSTBC for two antennas, ¾ three and four antennas and ½ rate for more than four antennas [21]. OSTBCs for two [6], three and four transmit antennas [39] are given below.

$$OSTBC2_{1/1} = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix}, \quad OSTBC3_{3/4} = \begin{bmatrix} s_1 & 0 & s_2 & -s_3 \\ 0 & s_1 & s_3^* & s_2^* \\ s_2^* & -s_3 & s_1^* & 0 \end{bmatrix}$$

$$OSTBC4_{3/4} = \begin{bmatrix} s_1 & 0 & s_2 & -s_3 \\ 0 & s_1 & s_3^* & s_2^* \\ -s_2^* & -s_3 & s_1^* & 0 \\ s_3^* & -s_2 & 0 & s_1^* \end{bmatrix} \tag{2.36}$$

Where, in OSTBCi_j ,while i is the number o f transmit antennas, j is the rate of the code.

The construction of maximal rate complex OSTBC goes to the work of Liang [22]. His complex codes were not only maximal rate for any number of transmit antenna but also shown to be delay optimal for antennas less six. Delay optimality of STBCs is a desired property which minimizes the decoding delay at the receiver as the receiver has to receive the entire block before it starts decoding.

The maximal rate of a complex OSTBC for N_t transmit antennas is given by [22]

$$\Re = \frac{\lceil N_t/2 \rceil + 1}{2\lceil N_t/2 \rceil} \tag{2.37}$$

Regardless of some improvements, the Liang codes have the drawback that as the number of transmit antennas increases, the code rate approaches to ½ while the code length is getting too large for practical implementations. These limitations of the OSTBCs inspired for the creation of *diagonal algebraic* and *quasi-orthogonal* STBCs [26].

2.5.2 Diagonal Algebraic STBCs

Diagonal algebraic STBCs (DA-STBCs) are algebraic number field theory based linear STBCs formed from rotational constellations [23] [40]. Algebraic number field theory, as a basis of PSTBCs will be discussed in Chapter 3.The rotated complex information symbols are placed across the main diagonal of the square code matrix. These codes are both fully diverse and full rate for any number of transmit antennas. The improvement in performance of these codes over that of OSTBCs comes with a penalty of decoding complexity. QAM based –complex rotational matrix DA-STBCs are inseparable which makes them even more complex than real rotations [40]. The full rate DA-STBC for N_t number of transmit antennas is given as follows:

$$DA - STBCNt_{1/1} = diag(D = MS) = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & d_{Nt} \end{bmatrix} \tag{2.38}$$

Where

- diag(D) is the diagonal matrix with the vector $D = [d_1, d_2, ..., d_{Nt}]^T$ is on the diagonal
- $S = [s_1, s_2, ..., s_{Nt}]^T$ is a vector of complex information symbols taken from q-QAM.
- M is an NtxNt *unitary rotation* or *generator matrix* chosen to ensure a fully diverse DA-STBC.

2.5.3 Quasi-orthogonal STBCs

By relaxing the orthogonality constraint of Equation 2.35, quasi-OSTBCs (QOSTBC) enabled to achieve full rate codes at the expense of increasing the decoding

complexity. However, fully diverse- full rate QOSTBCs are possible by using constellation rotation which were proposed by Tirkkonen [41], Sharma et al. [25], and Su et al. [26]. These codes outperform the OSTBCs for four transmit antennas in terms of the SNR required to achieve a targeted error probability.

The full diversity- full rate QOSTBCs were latter generalized to any number of transmit antenna by Sharma et al [42]. The QOSTBC for the number of transmit antennas that are powers of two as constructed by Sharma [42] is given by

$$QOSTBC(s_1,...,s_{Nt}) = \begin{bmatrix} QOSTBC(r_1,...r_{\frac{Nt}{2}}) & -QOSTBC(r^*_{\frac{Nt}{2}},...,r^*_{Nt}) \\ QOSTBC(r_{\frac{Nt}{2}},...,r_{Nt}) & QOSTBC(r^*_1,...r^*_{\frac{Nt}{2}}) \end{bmatrix} \quad (2.39)$$

Where

- $r_n = \exp(i\omega_n)s_n$, $n \in \{1,...,Nt\}$ are the rotated q-QAM information symbols.
- $\omega_n, n \in \{1,...,Nt\}$ is the *rotation angle* chosen to ensure full diversity and that maximizes CG.
- $s_n, n \in \{1,...,Nt\}$ is the unrotated q-QAM information symbols.
- $QOSTBC(r_v,...,r_{v+\frac{Nt}{2}-1})$ is the QOSTBC for the first half transmit antennas in the rotated symbols ranging from r_v to $r_{v+Nt/2.}$
- By definition QOSTBC(s)=s.

For N_t transmit antennas, where N_t is not a power of two, the QOSTBC can be obtained by deleting any $N\tilde{t} - Nt$ rows of the code matrix $QOSTBC(r_1,...,r_{N\tilde{t}})$ for $N\tilde{t}$ antennas, where

$$N\tilde{t} = 2^{\lceil \log_2^{Nt} \rceil} \quad (2.40)$$

For example, the QOSTBC for three antennas is obtained by deleting any one row from the code matrix for four antennas. The STBCs for three and four transmit antennas are then given by [26]

$$QOSTBC3_{1/1} = \begin{bmatrix} s_1 & -s_2^* & -s_3^* e^{-i\omega} & s_4 e^{i\omega} \\ s_2 & s_1^* & -s_4^* e^{-i\omega} & -s_3 e^{i\omega} \\ s_3 e^{i\omega} & -s_4^* e^{-i\omega} & s_1^* & -s_2 \end{bmatrix}$$

$$QOSTBC4_{1/1} = \begin{bmatrix} s_1 & -s_2^* & -s_3^* e^{-i\omega} & s_4 e^{i\omega} \\ s_2 & -s_1^* & s_4^* e^{-i\omega} & -s_3 e^{i\omega} \\ s_3 e^{i\omega} & -s_4^* e^{-i\omega} & s_1^* & -s_2 \\ s_4 e^{i\omega} & s_3^* e^{-i\omega} & s_2^* & s_1 \end{bmatrix} \tag{2.41}$$

Here, the QOSTBC for three transmit antennas is found from the four transmit antenna by deleting the last row. The rotational angle that gives full diversity and that maximizes the CG is $\omega = \pi/4$. The improvement in performance of QOSTBCs over OSTBCs due to their full diversity and full rate is at the expense of decoding complexity as of DA-STBCs.

Semi-orthogonal algebraic STBCs (SOA-STBC) are other codes constructed from DA-STBC. They are constructed from DA-STBCs which have the same basic code structure as of QOSTBCs. They are called semi-orthogonal because half of the rows of the code matrix are orthogonal to the other half.

2.5.4 Threaded Algebraic and PSTBCs

All of the above described families of STBCs are at most *full rate*, i.e the maximal rate that they can achieve is one symbol per signaling interval. The only two STBCs that enable more than one symbol per signaling are *threaded algebraic* STBCs (TA-STBCs) and *PSTBCs*. They are called *high rate* STBCs. The construction of the TA(P)-STBCs and PSTBCs is the same, except for the choice of the *generator matrix*, the *non-norm element* and the *modulation alphabet* [26]. Thus, from this section then forth, the notation TA(P)-STBC is to mean TA-STBC or/both PSTBC. The algebraic terms will be discussed in Chapters 3 and 4.

The TA(P)-STBCs are fully diverse codes which guarantee arbitrary rate for arbitrary number of transmit antennas. Each layer of the thread of these codes transmit *one-DA-STBC* to achieve maximal rate of N_t symbols per signaling interval for N_t transmit antennas [26]. By doing so, it is possible to transmit a maximum number of Nt^2 symbols, which is achieved when each layer is carrying N_t number of symbols. Another basic feature of these codes is that it is possible to transmit any rate, below the maximal rate, by simply *deleting layers*. A particular rate $\Re$ of an *Nt* transmit antennas TA(P)-STBC is found by deleting $N_t - \Re$ number of layers.

For example, for three transmit and three receive TA(P)-STBC, the rates $\Re = \{1,2,3\}$ are found by deleting 3-$\Re$ layers.

Thus, a TA(P)-STBC encodes a total of $L = \Re N_t$ complex information symbols $s(\ell, nt)$ that are organized into $\Re$ layers where the ℓ^{th} layer is given by $S(\ell,) = \{s(\ell,1), s(\ell,2),..., s(\ell, Nt)\}$.

An $\Re$ rate TA(P)-STBC is written as [29] [31] [43]

$$TA(P) - STBC = \sum_{t=1}^{\Re} diag(D(t))R^{t-1} \tag{2.42}$$

Where

- diag (D(t)) is a diagonal matrix with vector D(t) on the diagonal
- D(t)=MS(t)=[d(t,1),d(t,2),…,d(t,Nt)]^T is the t^{th} thread
- M is NtxNt unitary *rotational* or *generator* matrix
- $R = [\gamma e_{Nt}, e_1, ..., e_{Nt-1}]$ is appropriate rotational matrix to meet the shaping constraint.
- e_j is the j^{th} column of the NtxNt identity matrix.
- γ is an algebraic unit-magnitude *non-norm* complex number whose value depends on the modulation alphabet size and the number of transmit antennas Nt.

In the construction of TA(P)-STBCs, while the first step is choosing the generator matrix M , the second step is selecting a suitable γ to ensure full diversity.

PSTBCs are different from TA-STBCs in that

- γ is independent of the *size* of the modulation alphabet. This makes them the only STBCs that satisfy the NVD which is a necessary condition for DMT.
- Their choice of M, γ and modulation alphabet is different. While the modulation alphabet is HEX for transmit antennas three and six, it is QAM for the rest. However, only QAM modulation is used in TA-STBCs.
- They have *good constellation shaping*, i.e., the energy required to transmit the linear combination of the information symbols is similar to the energy required to transmit the symbols themselves. This means there is no need of additional energy in encoding the information symbols [19].

- In addition, they possess uniform average energy per antenna in all time slots. It means also that the average energy of each entry of the code matrix is the same.
- The decoding complexity of PSTBCs not only depends on the transmission rate as of TA-STBCs but also on the type of modulation applied.

The comparison of different STBCs in terms of their rate ($\Re$), delay, number of real symbols detected per group (*number*) and the worse-case decoding complexity (*complexity*) as determined in [32] are given in Table 2.1.The worse-case decoding complexity is based on certain properties of the *triangular* part of the *orthogonal-triangular* decomposition of the effective channel matrix. The complexity is measured by *the average number of nodes* visited in a tree –based decoding algorithm called *Sphere decoder*.

Table 2.1 shows that TA-STBCs and PSTBCs are the most expensive in terms of decoding complexity. Fortunately, in the same year but six months ahead of the PhD thesis of Sinnokrot [32] , Sirianunpiboon et al. [11] came up with a lower decoding complexity of the PSTBCs based on conditional optimization; as an extension of the fast essentially ML decoding of the Golden code Sirianunpiboon et al. [17]. They found that the worse-case decoding complexity of PSTBCs is $o(q^2)$ for 2x2, $o(q^6)$ for 3x3 and $o(q^{12})$ 4x4.

In general, the worse-case ML decoding complexity of PSTBCs by using the *conditional optimization (COML)* concept is given by

$$COML = o\left(q^{Nt(Nt-1)}\right) \tag{2.43}$$

And the difference in the decoding complexity of the *sphere* and the *COML* decoding of PSTBCs is given by

$$\Delta = \underbrace{o\left(q^{Nt\left(Nt-\frac{1}{2}\right)-\frac{1}{2}}\right)}_{Sphere} - \underbrace{o\left(q^{Nt(Nt-1)}\right)}_{COML} = o\left(q^{\frac{Nt-1}{2}}\right) \tag{2.44}$$

In general, based on the three fundamental design parameters of STBCs, namely, *low decoding complexity*, maximum DG and maximum MG, PSTBCs are the best. The full diversity, high rate, good constellation shaping, uniform average energy per antenna, NVD and optimal DMT characteristics of PSTBCs supplemented by the

COML decoder make them the most preferred STBCs. Chapter 3 will give a mathematical background of CDA, a tool for PSTBCs.

Table 2.1: Rate, delay, number of separable groups and decoding complexity of the most common families of STBCs by using sphere decoding.

No	*STBC*	*Rate*	*Delay*	*Number*	*Complexity*
1	OSTBC	$\frac{\lceil N_t/2 \rceil + 1}{2\lceil N_t/2 \rceil}$	$\frac{1}{2\Re}\binom{Nt}{\lceil Nt/2 \rceil}$ f or $Nt = 4k$ $\frac{1}{\Re}\binom{Nt}{\lceil Nt/2 \rceil}$ fo r $Nt \neq 4k$	1	$o(1)$
2	QOSTBC	1	$2^{\lceil \log_2^{Nt} \rceil}$	$2^{\lceil \log_2^{Nt} \rceil}$	$o\left(q^{2^{\lceil \log_2^{Nt} \rceil - 1} - 1}\right)$
3	DA-STBC	1	Nt	Nt	$o\left(q^{\frac{Nt-1}{2}}\right)$
4	SOA-STBC	1	Nt	$\lceil N_t/2 \rceil$	$o\left(q^{\frac{\lceil Nt/2 \rceil - 1}{2}}\right)$
5	TA-STBC	{1,…,Nt}	Nt	$2\Re$ Nt	$o\left(q^{Nt\left(\Re - \frac{1}{2}\right) - \frac{1}{2}}\right)$
6	PSTBC	{1,…,Nt}	Nt	$2\Re$ Nt	$o\left(q^{Nt\left(\Re - \frac{1}{2}\right) - \frac{1}{2}}\right)$

CHAPTER THREE

3 CYCLIC DIVISION ALGEBRA AS APPLIED TO STBC

This chapter is devoted to give the necessary mathematical background of CDA which are the building block of PSTBCs. After highlighting the basic algebraic structures, the notion of division algebra will be introduced as it gives a way of building fully diverse STCs. The highest throughput codes are based on algebras over number fields. The number fields that will be used are those which allow encoding of QAM and HEX constellations. Then a particular family of algebras, namely cyclic algebras built over number fields, will yield, for N_t transmit antennas, $N_t x N_t$ Space–Time code words that send N_t^2 information symbols encoded into N_t^2 signals. Moreover, ring of integers of number fields are to be seen how they give NVD property and how they are used to build algebraic lattices. The lattice structure helps us to control the transmitted energy when encoding the STCs.

3.1 Algebraic Structures

An *algebraic structure* is defined by its *set* and by the *operations* on its set. The most common algebraic structures are *groups, rings and fields.*

3.1.1 Group

A group, $G = \langle \{\ \}, + \rangle$ is a set of elements with a binary operation that satisfies the following five properties:

a) Closure
b) Associability
c) commutability (only for commutative groups)
d) Existence of an identity
e) Existence of an inverse

Example 3.1: The set of residue integers with the addition operation, $G = \langle Z_n, + \rangle$, is a commutative group. Here, the subscript is to denote *modulo*. Thus, the set is $\{0,1,...,n-1\}$ while the operation is an addition. We can perform an addition operation without moving out of the set. If a subgroup of a group can be generated from the powers of an element, then the group is called a *cyclic group* and that

element is called a *generating element*. In other words, a cyclic group is a group that is its own cyclic group.

Example 3.2: Four cyclic groups can be made from the group $G = \langle Z_6, + \rangle$. They are $H_1 = \langle \{0\}, + \rangle$, $H_2 = \langle \{0,2,4\}, + \rangle$, $H_3 = \langle \{0,3\}, + \rangle$ and $H_4 = G$. The only elements of the set whose integer powers can generate the group itself are *two* and *five.*

3.1.2 Ring

A ring $R = \langle \{\ \}, +, \bullet \rangle$ is an algebraic structure with two operations. The five properties defined for group are also applicable in a ring. Only the first three properties in Example 3.1 apply for the second operator. In addition, the second operation is distributive over the first. The set of elements of *R* that are invertible under the multiplication operation $\bullet$ is called the set of *units* of *R*, and is denoted by R^* . If $R^* = R/\{0\}$, then *R* is said to be a *skew field* or *division algebra.* This also means that every element except zero is invertible.

Example 3.3: The set of integers with the two operations addition and multiplication is a ring as addition satisfies the five while multiplication the first three properties. Thus, $R = \langle Z, +, \times \rangle$ is a ring.

3.1.3 Field

A field, $F = \langle \{\ \}, +, \bullet \rangle$ is a *commutative ring* in which the second operation satisfies all the five properties defined for the first operation except that there is no inverse for the identity element of the first operation. The distributive property of ring is also satisfied in fields. Thus, skew fields or division algebras only lack the commutability property *fields*.

Example 3.4: Z_p , R, Q and C are most well known commutative fields. Where, while Z_p refers modulo prime integers, R, Q and C are the set of real, rational and complex numbers respectively. Since commutative fields don't have much application in coding, the interest of this background is *non-commutative fields* from which division algebras are formed. The notations for the set of integers, real, rational and complex numbers used in Example 3.4 will consistently be used hereafter.

3.2 Algebras and Division Algebras

Algebra Λ is a set over a field F with operations of addition, multiplication, and multiplication by elements of F that have the following properties [31]:

a) Λ is a vector space with respect to addition and multiplication by elements of the field.

b) Λ is a ring with respect to addition and multiplication.

c) $(\lambda x)y = x(\lambda y) = \lambda(xy)$ for any $\lambda \in F, x, y \in \Lambda$

Example 3.5: The *Hamilton's quaternion* defined by $H_m = \{x + yi + zj + vk | x, y, z, v \in R\}$ with the basis $e = \{1, i, j, k\}$ for a vector space of *four* in R, is an example of a non-commutative algebra, i.e., every non-zero element of H_m is invertible. Like complex numbers, we can define the conjugate of a quaternion. Let $h_m = x + yi + zj + vk$ as $\bar{h}_m = x - yi - zj - vk$. By straight forward computation, we get the product of the element with its conjugate as $h_m \bar{h}_m = x^2 + y^2 + z^2 + v^2$. We call the product $h_m \bar{h}_m = |h_m|^2$ as the norm of the quaternion. The norm will never be zero unless all x, y, z, v are each zero. Thus the inverse of the quaternion is given by $h_m^{-1} = \frac{h_m}{h_m \bar{h}_m}$, which shows that all nonzero elements have an inverse. Next, we will see how high-dimensional algebras can be obtained from *number fields*.

3.3 Algebras on Number Fields

3.3.1 Introducing Number Fields

Consider the set of real numbers R and the set of complex C. C is found by "adding" a non-element i to R. In other words, C is an extension of R and can be represented by $C = R(i)$. In the same manner, we can extend the set of rational numbers, Q by adding a *non-rational* number. When we add the same non-element number i to Q, we obtain a new set $Q(i)$ that contains Q and i. So as to make the new set a field, all multiples and powers of i have to be included. By the same procedure, we can add $\sqrt{5}$ to $Q(i)$ to obtain $Q(i, \sqrt{5})$ as a new field. The dimension of $Q(i)$ as vector space over Q is two. Similarly, an element of $Q(i, \sqrt{5})$ can be written as $v = x + y\sqrt{5}$ with $x, y \in Q(i)$ or also $v = (a + ib) + \sqrt{5}(c + id)$, $a, b, c, d \in$ Q. Thus, $Q(i, \sqrt{5})$

is a vector space of dimension two over $Q(i)$, or a dimension of four over Q. A sample hierarchy of the field extension is shown in Figure 3.1.

In general, for two fields *B* and *E*, if $B \subseteq E$, then we call *E* is the *field extension* of the *base field B* and is denoted by E/B .The dimension of *E* as vector space over *B* is called the *degree* of *E* over *B* and is denoted by [*E:B*]. If [*E:B*] is finite, we say that *E* is a *finite extension of B*. We can have infinitely many field extensions depending on the choice of the bases and the number of added non-element objects. Fields with finite number of elements have crucial role in *cryptography*. Galois showed that for a field to be finite, the number of elements should be p^n , where *p* is a prime and *n* is a positive integer.

$$
\begin{array}{c}
Q(i,\sqrt{5},\sqrt{3}) \\
|2 \\
Q(i,\sqrt{5}) \\
|2 \\
Q(i) \\
|2 \\
Q
\end{array}
$$

Figure 3.1: A bottom-up hierarchy of field extensions with degrees on the branches

Example 3.6: The number of n-bit words for a binary, $\{0,1\}$ and tertiary, $\{0,1,2\}$ are 2^n and 3^n respectively.

Here, we will concentrate on finite field extensions whose base is Q. Finite field extensions of Q are called *number fields* and are generally represented by E/Q [31]. Thus, in all of the forth coming sections *E* is to represent a number field.

However, the question that may come to our mind is how we select those *non-element* numbers. We observe that the number i is the solution of the degree-two polynomial $X^2+1=0$. Thus, building $Q(i)$ means adding the solution of the polynomial equation whose coefficients are in Q, but which is not in Q. In the same way, $Q(i,\sqrt{5})$ is obtained from $Q(i)$ by adding the non-element $\sqrt{5}$, the root of the polynomial $X^2-5=0$, whose coefficients are in $Q(i)$. Let us generalize this concept.

For a field extension E/B, let $\beta \in E$ but $\beta \notin B$, if there exists a non-zero *irreducible monic* (the leading coefficient being 1) *polynomial* $P \in B[X]$ such that $P(\beta) = 0$,then we say that β is *algebraic over B* [31]. In other words, β is a root of a polynomial whose coefficients are in the base field *B*. Such a polynomial is called the *minimal polynomial* of β over B and is denoted by P_β. Thus, the polynomial $X^2 + 1$ is a minimal polynomial of i over Q and the number i is algebraic over Q. Similarly, the polynomial $X^2 - 5$ is minimal polynomial of $\sqrt{5}$ over $Q(i)$.

If all the elements of *E* are algebraic over *B* (all are roots of minimal polynomials whose coefficients in *B*), we say that *E* is an *algebraic extension* of *B*. As we saw shortly in this Section above, a number field is obtained by adding roots of minimal polynomials whose coefficients are in Q that all of its elements are algebraic over Q. Thus, we can equivalently say a number field is an algebraic number filed [44]. In the following Sub-section, we will see a particular family of fields which are generated by the powers of a single element in the same way as described for group in Section 3.1.1.

3.3.2 Embeddings and Galois Group

For a number field $E = Q(\theta)$ for some algebraic number $\theta \in E$ is called a *primitive* or *generating element*. Thus, *E* will be a Q -vector space generated by the powers of θ .To state it differently, we add all the integer powers and multiples of the primitive element which are not elements of Q. If the degree of *E* over Q is *n*, its basis is given by $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$. As a result of this, any $y \in E$ can be written as $y = \sum_{i=0}^{n-1} y_i \theta^i$, $y_i \in Q$ and the degree of the minimal polynomial of θ is *n*.

Next, we see how element of a number field can be represented in its different forms (commonly called *Homomorphs of an element*). For two rings *A* and *B*, a *ring homomorphism* is a map $\psi : A \to B$ that satisfies, for all $a, b \in A$ [31].

$$\begin{aligned} \psi(a+b) &= \psi(a) + \psi(b) \\ \psi(a*b) &= \psi(a) * \psi(b) \\ \psi(1) &= 1 \end{aligned} \tag{3.1}$$

Isomorphism is a special case of homomorphism wherein a given system *S* is said to be isomorphic to another system S' if and only if they have one-to-one correspondence and they satisfy the postulates that identify the system *S*. Thus, any system of numbers that satisfies all the postulates of another system of numbers is isomorphic to it.

In general if E/Q and B/Q are two field extensions of Q, we call $\Psi : E \to B$ a Q-*homomorphism* if Ψ is a ring homomorphism that satisfies $\Psi(a) = a$ for all $a \in$ Q, i.e., that *fixes* Q [31]. A Q -homomorphism $\Psi : E \to C$ called an *embedding* of *E* into *C*.

As is well known three are three types of mappings; the *injective map* (one-to-one correspondance), the *sujective map* (on –to correspondence) and the *bijective map* (both one-to-one and on-to correspondence). An *embedding* is an *injective map* that we can really understand it as a way of representing elements of *E* as complex numbers. As is *conjugation* to complex numbers *embedding* is to number fields. Thus, embeddings of element of a number field are all of its images when seen in the mirror of the base field.

Example 3.7: As $v = a + ib$ and $\bar{v} = a - ib$ are conjugates of each other in the field of *C*, $u = a + b\sqrt{5}$ and $\bar{u} = a - b\sqrt{5}$ are embeddings of each other in the field of $Q(\sqrt{5})$. It means that in both cases an element has exactly two forms; itself and another different one.

In general, for a number filed $E = Q(\theta)$ of degree *n* over Q, there are exactly *n* distinct embeddings of *E* into C ; $\sigma_i : E \to C$, $\sigma_i(\theta) = \theta_i$, $i = 1,2,..n$, where θ_i are the distinct zeros in C of the minimum polynomial of θ over Q [44]. As a result of this, the distinct zeros in *C* of the minimal polynomials of i and $\sqrt{5}$ ($X^2 + 1$ and $X^2 + 5$ resp.) are $\pm i$ and $\pm\sqrt{5}$ respectively.

Notice that one of the $\sigma_i's$, say σ_1, is the identity mapping, i.e., $\sigma_1(x) = x$ for all $x \in E$. When we apply the embedding σ_i to an arbitrary element $x \in E$, $x = \sum_{k=1}^{n} a_k \theta^k , a_k \in Q$, using the properties of Q –homomorphism in Equation 3.1, we get [31]

$$\sigma_i(x) = \sigma_i\left(\sum_{k=1}^{n} a_k \theta^k\right), a_k \in Q$$

$$= \sigma_i(a_k)\left(\sum_{k=1}^{n} \sigma_i(\theta)^k\right) = \sum_{k=1}^{n} a_k \theta_i^k \in C \tag{3.2}$$

From Equation 3.2, the image of any x under σ_i is uniquely identified by θ_i.

Thus, the concept in Example 3.7 can be described in compact form as:

$$\sigma_1 : Q(i) \to C \Leftrightarrow a+ib \mapsto a+ib \qquad \sigma_2 : Q(i) \to C \Leftrightarrow a+ib \mapsto a-ib$$

$$\sigma_1 : Q(i,\sqrt{5}) \to C \Leftrightarrow a+\sqrt{5}b \mapsto a+\sqrt{5}b \qquad \sigma_2 : Q(i,\sqrt{5}) \to C \Leftrightarrow a+\sqrt{5}b \mapsto a-\sqrt{5}b \tag{3.3}$$

From Equation 3.3, we observe that all their mappings are to themselves. When σi, i = 1, . . . , n are defined from E to E, it means that they are just a permutation of the roots of the minimal polynomial, or all roots of the minimal polynomial are in E. They are then bi-jective (and thus called Q -*automorphisms* of E, that is, maps from a field to itself that fix Q). Thus, we can define σ_1 and σ_2 as two Q- automorphisms of $Q(i)$, that is they satisfy $\sigma_j(x) = x$, $j = 1,2$, for all $x \in Q$. Similarly, we can define another σ_1 and σ_2 as two $Q(i)$- automorphisms of $Q(i,\sqrt{5})$ such that $\sigma_j(x) = x$, $j = 1,2$, for all $x \in Q(i)$. In a nutshell, the *automorphisms* of an extended field are those which have the same *interpretation* for an observer in the set of the base field.

For a field extension E/B, the set of *B-automorphisms* of E forms a group under composition of maps. This is fundamental for Galois Theory [44]. A number field extension E/B is a *Galois extension* if every irreducible polynomial over B which has at least one zero in E has in fact all its zeros in E. The *Galois group* of the extension E/B, denoted by $Gal(E/B)$, is the group of all B-automorphisms of E under composition of maps.

Relating this idea with the definition of group in Section 3.1.1, it tells us that, while the two embeddings σ_1, σ_2 of $Q(i)$ form elements of the group, the *binary operation* is the *mapping* (the law given by the composition of maps). To be called a group, all

the five properties in Section 3.1.1 have to be satisfied. It is forward and clear showing that the set is closed and associative. Let us now see whether there exists an *identity element* as well as an *inverse* for every element. Note that $\sigma_1(x) = x \forall x \in Q(i)$ showing that σ_1 is an identity. In addition, $\sigma_2(\sigma_2(x)) = x = \sigma_1(x)$ which shows that σ_2 is invertible under the mapping. Thus, $Gal(Q(i)/Q) = \{Id, a+ib \mapsto a-ib\}$. Similarly, $Gal(Q(i,\sqrt{5})/Q(i)) = \{Id, a+\sqrt{5}b \mapsto a-\sqrt{5}b\}$.

In both cases, as the Galois group is generated by one element, they are *cyclic groups*. In all the forth coming sections, a denotation $G = \langle\theta\rangle$ will represent a cyclic group generated by θ. We are now ready to construct cyclic algebras from cyclic Galois extensions. When the embedding is not to the field itself, then the embedding is called *relative embedding.*

Thus, if E/B is field extension of degree n, the *relative embeddings* are the n *B-homomorphisms* (i.e., homomorphisms fixing B) of E into C.

3.3.3 Introducing Cyclic Algebras

For a Galois extension E/B of degree *n* whose Galois group $G = Gal(E/B)$ cyclic with generator θ, choosing an element $\gamma \in B^*$, a *non-commutative (division) cyclic algebra* denoted by $\Lambda = (E/B, \theta, \gamma)$ is constructed as follows [31]:

$$\Lambda = E \oplus bE \oplus \ldots \oplus b^{n-1}E \tag{3.4}$$

Where, $b^n = \gamma$ and $\varepsilon b = b\sigma(\varepsilon)$ for all $\varepsilon \in E$ and $\oplus$ denotes a *direct sum*.
Thus, every element z in Λ is expressed by:

$$z = z_0 + bz_1 + \ldots + b_{n-1}z^{n-1} = \sum_{i=1}^{n-1} b^i z_i \tag{3.5}$$

The non-commutative property, i.e., $\varepsilon b = b\sigma(\varepsilon)$ of CDA tells us that a *left multiplication* of element of the algebra by another element is equal to *right multiplication* by the embedding of the element. For example, for the Hamilton's quaternion, we see that $ij = j\sigma(i) = j(-i) = -ji = k$ and $jk = k\sigma(j) = k(-j) = -kj = i$ .Thus, to define its *ring structure*, we need a multiplication.

CDA are particularly important for coding purpose as there is a correspondence between an element x of an algebra Λ and a matrix $X \in \mathcal{M}_n(E)$. To make it clear they are isomorphic to each other [31]. Let $x \in \Lambda$ and consider a left multiplication of an element of algebra by x in the basis $\{1, b\}$, i.e.. $n=2$.The matrix of left multiplication by x is shown below, in Equation 3.6. Note that $b^2 = \gamma$.

$$\begin{aligned} xz &= (x_0 + bx_1)(z_0 + bz_1) = x_0 z_0 + x_0 bz_1 + bx_1 z_0 + bx_1 bz_1 \\ &= x_0 z_0 + b\sigma(x_0) z_1 + bx_1 z_0 + \gamma\sigma(x_1) z_1 \\ &= (x_0 z_0 + \gamma\sigma(x_1) z_1) + b(\sigma(x_0) z_1 + x_1 z_0) \end{aligned} \tag{3.6}$$

In matrix form, in the basis $B = \{1, b\}$ the product will be,

$$xz = \begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix} \begin{bmatrix} z_0 \\ z_1 \end{bmatrix} \tag{3.7}$$

And for n=3, the matrix of left multiplication is given by

$$xz = \begin{bmatrix} x_0 & \gamma\sigma(x_2) & \gamma\sigma^2(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) \end{bmatrix} \tag{3.8}$$

Generally, for the basis $B = \{1, b, b^2, ..., b^{n-1}\}$, the matrix of left multiplication is given by:

$$\begin{bmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & \cdots & \gamma\sigma^{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{n-2} & \sigma(x_{n-3}) & \sigma^2(x_{n-4}) & \cdots & \gamma\sigma^{n-1}(x_{n-1}) \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \gamma\sigma^{n-1}(x_0) \end{bmatrix} \tag{3.9}$$

As we have seen in Chapters 1 and 2, STBCs are matrices whose entries are the transmitted information symbols (or combination of them) by a certain antenna at a certain time instant. The best practice is, unless there is difficulty in recovering later on, sending a combination of them, i.e., a blend which doesn't create confusion when required to be separated at the receiver. However, such strategy was not possible for a long a long time due to structure of the old number system. Luckily enough, the introduction of modern number system in general and CDA in

particular paved a way to a thought that their structure can be used for coding purpose. Thus, it can be concluded that the entries of matrices from CDA like Equation 3.9 can be taken as combination of information symbols carved from some constellation. Consequently, as the entries are from the extended field, the information symbols will be elements of the base field. The degree of the extended field will be equal with the number of antennas.

Example 3.8: The matrix in Equation 3.7 can be taken as a code book for two antennas

$$\mathcal{CB} = \left\{ \begin{bmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{bmatrix} \middle| x_0, x_1 \in E \right\} \tag{3.10}$$

If we suppose, for example, the information symbols are carved from QAM and HEX constellations, while the base fields will be $Q(i)$ and $Q(m)$ respectively, E will be any Galois extension of them. Where, $m = e^{2\pi/3}$. Considering $E = Q(i, \sqrt{5})$, we observe that its elements x_0 and x_1 can be given by $x_0 = a_0 + \sqrt{5}b_0, x_1 = a_1 + \sqrt{5}b_1 \middle| a_0, a_1, b_0, b_1 \in Q(i)$.

So both x_0 and x_1 encode two QAM information symbols, a_0, b_0 and a_1, b_1, respectively.

Owing to this, the codebook in Equation 3.10 can be rewritten as:

$$\mathcal{CB} = \left\{ \begin{bmatrix} a_0 + \sqrt{5}b_0 & \gamma(a_1 - \sqrt{5}b_1) \\ a_1 + \sqrt{5}b_1 & (a_0 - \sqrt{5}b_0) \end{bmatrix} \middle| a_0, b_0, a_1, b_0 \in q - QAM \right\} \tag{3.11}$$

Where, γ will be chosen in order to optimize the code performance as we will see in the following.

In general, if E/B has degree n, $x = \sum_{k=0}^{n-1} b^k x_k \in \Lambda$ has n coefficients each of which in turn can encode n information symbols. Thus, in sum x it encodes n^2 information symbols.

A *layer (thread)* [8] ℓ for $\ell = 1, \ldots, n$ of a codeword is the set of matrix entries in positions $(k, (\ell + k - 1) \bmod(n) + 1) \forall k = 1, \ldots, n$.

The codebook in Equation 3.11can is rewritten as the sum of its layers as:

$$\mathcal{CB}=\underbrace{\begin{bmatrix} a_0+\sqrt{5}b_0 & \\ & (a_0-\sqrt{5}b_0) \end{bmatrix}}_{Layer_0}+\underbrace{\begin{bmatrix} & \gamma(a_1-\sqrt{5}b_1) \\ a_1+\sqrt{5}b_1 & \end{bmatrix}}_{Layer_1} \tag{3.12}$$

Codebook 3.12 shows that the same *n* information symbols are distributed within one *layer* of the codeword.

3.4 Exploiting more the properties of CDA: Norm and Ring of Integers

In this subsection, we will see what *norm* and *ring of integers* are and how they are related to the properties of STBCs. The norm is used to show that CDA-based STBCs are fully diverse. Moreover, when the coefficients of the STBCs are taken from the rings of integers of a field extension, not only are the codes fully diverse but also they are NVD.

3.4.1 Norm and Full-Diversity

For an *n* degree field extension E/B, if $\sigma_1,\sigma_2,...,\sigma_n$ are the *n* embeddings of *E*, then the conjugates of an element $x \in E$ are given by $\sigma_1(x),\sigma_2(x),...,\sigma_n(x)$ and its *norm* and *trace* are as defined by [31] are given respectively as

$$N(x)=\prod_{i=1}^{n}\sigma_i(x) \quad \text{and} \quad Tr(x)=\sum_{i=1}^{n}\sigma_i(x) \tag{3.13}$$

The *reduced norm* of an element of a CDA is the determinant of its corresponding matrix, as given in Equation 3.9. Thus, in order to determine whether a code CB is fully diverse, we have to check whether $\det(X_i-X_j)\neq 0$, for any $X_i \neq X_j \in \mathcal{CB}$. By linearity of the algebra, codes from CDA satisfy $\det(X_i-X_j)=\det(X)$, $X_i \neq X_j$, $X \in \mathcal{CB}$. We are, thus, interested in knowing when $\det(X)=0 \forall x \neq 0$ .Let us see, by example, when the determinant is zero.

Example 3.9: Consider the determinant of codebook 3.10 obtained from CDA of degree n=2 as shown in Equation 3.7

$$\det\begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = x_0\sigma(x_0)-\gamma x_1\sigma(x_1) = N_{E/B}(x_0)-\gamma N_{E/B}(x_1) \tag{3.14}$$

The norm , *N(x)* of an element *x* cannot be zero unless the element is zero. The multiplicative property of norm and the additive property of trace has crucial role in simplifying algebraic computations. The algebraic norm and algebraic trace have the following properties [30].

$$N(x_1 x_2 ... x_n) = N(x_1)N(x_2)...N(x_n) \qquad (3.14)$$

$$Tr(x_1 + x_2 + ... + x_n) = Tr(x_1) + Tr(x_2) + ... + Tr(x_n)$$

Consequently, as we are considering nonzero elements, the only way Equation 3.14 can be zero is when the following condition is satisfied:

$$\det(X) = 0 \Leftrightarrow \gamma = N_{E/B}(x_0 / x_1) \qquad (3.15)$$

Thus, for a cyclic extension E/B of degree *n* with Galois group $Gal(E/B) = \langle \theta \rangle$, if $\gamma, \gamma^2, ..., \gamma^{n-1} \in B^*$ are not a norm of some element of *E*, then $(E/B, \theta, \gamma)$ is a *cyclic division algebra*. To sum up, the selection of non-norm element γ is the necessary condition for non-zero determinant, which is the basis of full diversity. By working more on the property of the algebra, it is also possible to determine the lower bound on the determinant of the difference of two matrices. Next, we see how the ring of integers gives such a property.

3.4.2 Ring of Integers and Non-Vanishing Determinants

We say that $\beta \in B$ is an *algebraic integer* if it is a root of a minimal polynomial with coefficients in Z . The set of algebraic integers of *B* is a ring called the *ring of integers* of *B*, and is denoted by O_B. The analogy between extension of Q and Z is that, while the set of algebraic extensions of Q form a field, the set of algebraic extensions of Z form a ring of integers. Thus, as *number field* is to Q, *ring of integers* is to Z. However, finding the algebraic integers and the corresponding minimal polynomial is not easy [46].

Example3.10: While the ring of integers of $Q(\sqrt{2})$ is the set $Z[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in Z\}$, the ring of integers of $Q(i)$ is given by $Z[i] = \{a + bi, a, b \in Z\}$.

Rings of integers can be found by taking only the algebraic integers of a number field. We will follow the later procedure, ring of integers of number fields. For

$B = Q(i)$ $O_B = Z[i]$, which means that O_B has a basis over Z given by $B = \{1, i\}$. We call B a Z-*module*. An R-module, where R is a ring, is a generalization of the notion of B-vector space, where B is a field. In our case, we have that B has a structure of vector space over the field Q, while we only have a structure of module for O_B over the ring Z.

In general, for a number field B of degree n, its ring of integers O_B forms a free Z–module (section) of rank n (that is, there exists a *basis* of n elements over Z). As previous, the analogy is that as *vector space* is to fields, *basis* is to rings. Let $\{b_i\}_{i=1}^n$ be a basis of the Z–module O_B, so that we can uniquely write any element of O_B as $\sum_{i=1}^n a_i b_i$ with $a_i \in Z$ for all i. We say that $\{b_i\}_{i=1}^n$ is an *integral basis* of B.

Example 3.11: (Ring of Integers and Basis). For $B = Q(\sqrt{5})$, any algebraic integer β in B has the form $a + b\sqrt{5}$ for some $a, b \in Q$ such that the minimal polynomial $X^2 - 2aX + a^2 - 5b^2$ has integer coefficients. And all the elements of O_B take the form $\beta = h + k(1+\sqrt{5})/2$ with both $h, k \in Z$ integers with the same parity, showing that $\{1, (1+\sqrt{5})/2)\}$ is an integral basis. The basis $\{1, \sqrt{5}\}$ is not integral since $a + b\sqrt{5}$ with $a, b \in Z$ is only a subset of O_B. This is because the norm of a basis element should always be unity which is not a matter in vector space. Note that, $(1+\sqrt{5})/2$ is also a primitive element of B with minimal polynomial $X^2 - X - 1$. Similarly, as it is an extension of degree 2 of Q(i), $E = Q(i, \sqrt{5})$ has Z[i]-basis for its ring of integers which is given by $O_E = Z[i][\left(1 + \sqrt{5}/2\right)] = \left\{u + v\frac{1+\sqrt{5}}{2} u, v \in Q(i)\right\}$. Thus $\{1, (1+\sqrt{5})/2)\}$ is a Z[i]-basis for O_E and telling us that $(1+\sqrt{5})/2$ is an algebraic integer since it has a minimal polynomial $X^2 - X - 1 \in Z[i][X]$.

If E/B is a field extension, for any $x \in E$, $N_{E/B}(x)$ and $Tr_{E|B}(x) \in B$. Moreover, if $x \in O_E$, we have $N_{E/B}(x)$ and $Tr_{E/B}(x) \in O_B$ [44]. For example, as the roots of the minimal polynomial $X^2 - X - 1$ are $\theta = (1+\sqrt{5})/2$ and $(1-\sqrt{5})/2$, and since $\sigma_1(\theta) = (1+\sqrt{5})/2$ and $\sigma_2(\theta) = (1-\sqrt{5})/2$, the minimal polynomial expressed in terms of its embeddings is given by $\prod_{i=1}^{2}(X - \sigma_i(\theta)) = X^2 - Tr(\theta)X + N(\theta)$. As coefficients of the minimal polynomial of

ring of integers of $Q(\sqrt{5})$ are Z, then $Tr(\theta)$ and $N(\theta)$ are integers, which means that they are elements of the base field.

$$\det\begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix} = x_0\sigma(x_0) - \gamma x_1\sigma(x_1) \tag{3.16}$$

The non-vanishing determinant in two steps:

(1) First, since $x_0, x_1 \in E$, then $N_{E/B}(x_0)$ and $N_{E/B}(x_1)$ are in B. Since $\gamma \in B \subset E$, then

(2) Now, if we restrict $x_0, x_1 \in O_E$, we get that $N_{E/B}(x_0)$ and $N_{E/B}(x_1)$ are in O_B. By choosing $\gamma \in O_B$, we conclude that $\det(X) \in O_B$.

When transmitting QAM or HEX symbols, B has to be Q(i), resp. Q(m). Since Z[i], resp. Z[m] is included in O_E, by taking a suitable $\gamma \in O_B$, we have that

$\det(X) \in Z[i], Z[m] \Rightarrow |\det(X)|^2 \in Z$ so that $|\det(X)|^2 \geq 1, \; X \neq 0$

In other words, this means that prior to SNR normalization, the minimum determinant does not depend on the spectral efficiency, which motivated the term "*non-vanishing determinant*".

This procedure can be generalized to higher dimensions n. However, the first step cannot be proved the same way, since explicit computations of the determinant in higher dimension gets more complicated.

3.5 Shaping, Lattices and Discriminant

In this section, we first show how the structure of the ring of integers can be further exploited to construct an *algebraic lattice*. We then show how algebraic lattices can be useful to define a *shaping* property on the constellation to be sent.

3.5.1 Algebraic Lattices

Algebraic lattices are built using the so-called *canonical embedding* of a number field [43, 44]. If $\sigma_1, ..., \sigma_n$ are the n embeddings of a number field B, ordering the σ_i's so that, for all $x \in B$, $\sigma_i(x) \in$ R, $1 \leq i \leq r_1$,and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$, *canonical embedding* $\sigma : B \to R^{r_1+2r_2}$ is the isomorphism defined by [33]

$$\sigma(x) = (\sigma_1(x), ..., \sigma_{r_1}(x), \; \Re\sigma_{r_1+1}(x), \; \Im\sigma_{r_1+1}(x), \; ..., \; \Re\sigma_{r_1+r_2}(x), \; \Im\sigma_{r_1+r_2}(x)) \tag{3.17}$$

Note that $r_1 + 2r_2 = n$ .We can define a similar embedding if we consider instead of the extension B/Q a more general extension E/B $\sigma : E \rightarrow$

$C^n \Rightarrow x \mapsto \sigma(x) = (\sigma_1(x),...,\sigma_n(x))$

Where σ_i's are the relative embeddings of E/B (σ_i fixes B for all i)

A *lattice* is a discrete set of points in R^n or C^n . If $e_1, e_2,...,e_n$ are linearly independent set of vectors, then an *m-dimensional lattice* is given by

$$L = \left\{ x = \sum_{i=1}^{m} \lambda_i e_i, \lambda_i \in Z \right\} \tag{3.18}$$

Where , $\{e_1, e_2,...,e_n\}$ is called the *basis of the lattice*.

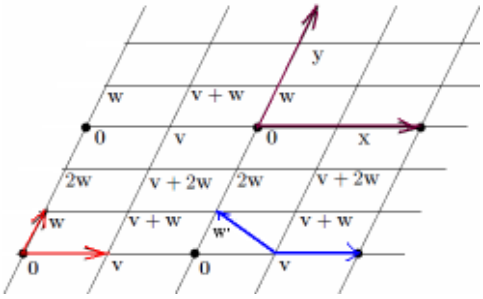
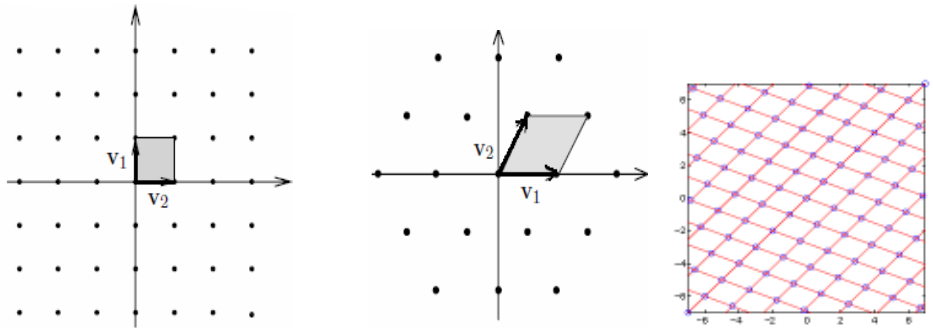


Figure 3.2: The points in the grid represent a lattice. The set of vectors {v,w} and {v,w'} are two examples of basis for this lattice. Points • represent a sub lattice. The set of vectors {x, y} form a basis for this sub lattice.

The two most common lattices are *integer lattices* (Z^n) and *hexagonal lattices* (A_2).



(a) (b) (c)

Figure 3.3: (a) Integer lattices, (b) hexagonal lattices and (c) algebraic lattices $Q(\sqrt{5})$

A lattice can be expressed by its generator matrix, M [27, 45] as

$$L = \{x = \lambda M \in R^n \,|\, \lambda \in Z^n\} \tag{3.19}$$

The lattice generator matrix of the lattice built from the canonical embedding of B is given by

$$M=\begin{bmatrix} \sigma_1(e_1) & \cdots & \sigma_{r_1}(e_1) & \Re\sigma_{r_1}(e_1), & \cdots; & \Im\sigma_{r_1+r_2}(e_1) \\ \vdots & & & & \vdots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_{r_1}(e_n) & \Re\sigma_{r_1}(e_n), & \cdots; & \Im\sigma_{r_1+r_2}(e_n) \end{bmatrix} \tag{3.20}$$

Where $\{e_1...,e_n\}$ is a basis of O_B and "$\Re$" and "$\Im$" are the real part and the imaginary part of a basis respectively. This gives a real lattice. Similarly, a complex lattice L^c is given by

$$L^c = \left\{x = \lambda M \in C^n \middle| \lambda \in Z[i]^n \, or Z[j]^n \right\} \tag{3.21}$$

Its generator matrix from the embedding $\sigma(x) = \{\sigma_1(x),...,\sigma_n(x)\}$ is given by

$$M^c = \begin{bmatrix} \sigma_1(e_1) & \sigma_2(e_1) & \cdots & \sigma_n(e_1) \\ \sigma_1(e_2) & \sigma_2(e_2) & \cdots & \sigma_n(e_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(e_n) & \sigma_2(e_n) & \cdots & \sigma_n(e_n) \end{bmatrix} \tag{3.22}$$

So far, we have used the ring of integers O_E to build algebraic lattices. In the following, we will show how algebraic lattices can be obtained in a more general manner, by considering *ideals of* O_E.

An *ideal* I of a commutative ring R is an additive subgroup of R which is stable under multiplication by R, i.e., $aI \subseteq I$ for all $a \in R$. Among all the ideals of a ring, some of them have the special property of being generated by only one element. These will be of particular interest for us. An ideal I is *principal* if it is of the form $I = (x)R = \{xy, y \in R\}, x \in I$ **[31].**

We can define the *norm* of an ideal. In the case of a principal ideal, it is directly related to the norm of a generator of the ideal. If $I = (x)O_E$ a principal ideal of O_E, its *norm* is defined by $N(I) = |N(x)|$.An algebraic lattice L' built from an ideal $I \subset O_E$ gives a sub lattice [27, 47] of the algebraic lattice L built from O_E. If $I = \beta O_E$, then the generator matrix M is given by

$$M = \begin{bmatrix} \sigma_1(\beta e_1) & \sigma_2(\beta e_1) & \cdots & \sigma_n(\beta e_1) \\ \sigma_1(\beta e_2) & \sigma_2(\beta e_2) & \cdots & \sigma_n(\beta e_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta e_n) & \sigma_2(\beta e_n) & \cdots & \sigma_n(\beta e_n) \end{bmatrix} \tag{3.23}$$

Matrix 3.23 is the matrix 3.22 multiplied by the diagonal matrix $D = diag(\sigma_1(\beta),..., \sigma_n(\beta))$.

Given the lattice generator matrix 3.23, we can compute the *determinant of the lattice* as follows

$$\det(L) = \left|\det(M)\right|^2 = \left|\det\left[\sigma_j(\beta e_i)\right]\right|^2 = \left|N(\beta)\right|^2 \left|\left[\det(\sigma_j(e_i)\right]\right| \qquad (3.24)$$

This number is related to an *invariant* of the number field, called the *discriminant*. If $\{e_1, e_2,..., e_n\}$ is an integral basis of E, the discriminant of B is defined as $d_B = \det\left[\sigma_j(e_i)\right]^2$ .It is found that the discriminant is independent of the choice of a basis [47].

For the codes that will be constructed in the Chapter 4, we will consider only extension fields of the kind $E/B = E'B/B$, i.e., E is the smallest field containing both E' and B. We call E the *compositum* of E' and B (see Figure 3.4). Furthermore, $E'B/B$ will have the property that its relative embeddings, $\sigma_1,...,\sigma_n$ are actually the same as the embeddings of E'/Q. However, this is not true in general.Under this assumption the determinant of the lattice is $\det(L) = \left|N_{B/Q}(\beta)\right|^2 \left|d_B\right|$ for a lattice built on B/Q while a lattice built on the compositum is given by $E'B/B$.

$$\det(L) = \left|N_{E/B}(\beta)\right|^2 \left|d_{E'}\right| \qquad (3.25)$$

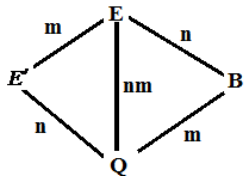


Figure 3.4: The structure of the compositum field of E′ and B

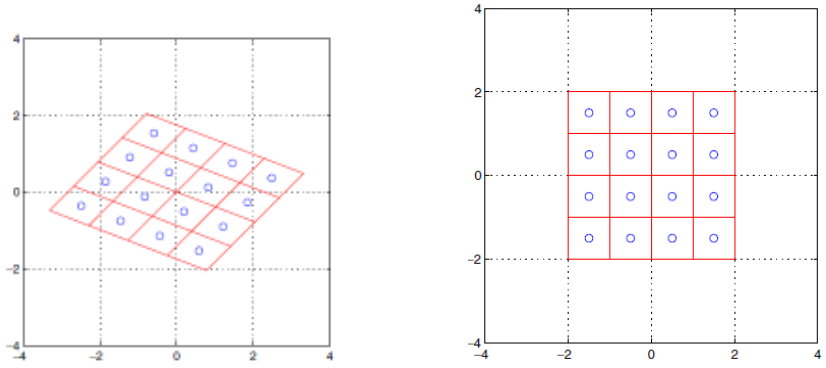
Example 3.12: the discriminant d_B of an algebraic lattice formed from $Q(\sqrt{5})$ by applying the two Q-homomorphisms to the integral basis $\{1,(1+\sqrt{5})/2\}$, is given as follows:

$$d_B = \det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ \left(\frac{1+\sqrt{5}}{2}\right) & \left(\frac{1-\sqrt{5}}{2}\right) \end{pmatrix}^2 = 5 \qquad (3.26)$$

3.5.2 Shaping

The inconsideration of the restriction on the shape of the lattice constellation resulted in either a complex bit labeling procedure or loss in the average energy [48]. The finding of rotated Z^n-lattices has solved this lattice constellation shaping problem by [48-49].

Example 3.13: Consider a two transmit and one receive antenna system with channel matrix $H = (h_1, h_2)$ and real independent Rayleigh fading coefficients to illustrate the trade-off among diversity, coding gain and constellation shaping. Figures 3.5(a), 3.5(b), and 3.6[31] show the transmitted signal set corresponding to different codes defined by the matrices M. In general the receiver will see a *compressed* or *expanded* signal set on the *x*- and *y*-axis depending on the fading coefficients *h*1 and *h*2. In what follows, $d_{E,\min}$ is to denote the *minimum Euclidean distance* the code and $d^2_{p,\min}$ is the *square minimum product distance* among all pairs of vectors.



(a) (b)

Figure 3.5: (a) the 16-QAM constellation with $d^2_{p,\min} = 0$, $d_{E,\min} = 1$, and $E_s = 2.5$, (b) an algebraic constellation with diversity, $d^2_{p,\min} = 4/25$, $d_{E,\min} = 0.8944$ and $E_s = 2.5$

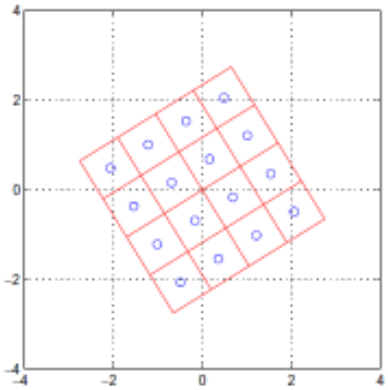


Figure 3.6: Algebraically rotated 16-QAM constellation with diversity, $d^2_{p,\min} = 1/5$, $d_{E,\min} = 1$ and $E_s = 2.5$

The 16-QAM constellation in Figure 3.5(a) with **M** the identity matrix and $d_{E,\min}=1$, has an average energy of $E_s=2.5$, but due to the lack of diversity, it cannot deliver the full information if one of the two channels is completely faded ($hi \approx 0$). In this case, the constellation points seen by the receiver collapse onto each other giving rise to systematic errors even in the presence of very little noise. Considering the algebraic constellation of Figure 3.5(b) with **M** given by the canonical embedding of $Q(\sqrt{5})$, full modulation diversity is achieved [31].

$$M = f\begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix} \tag{3.27}$$

The coefficient f is used for normalization purposes. Setting $f=1/\sqrt{2}$ we have $d_{E,\min}=1$ but this requires an average energy of $E_s=3.125(25\%more)$; alternatively with $f=\sqrt{2/5}$, we have the same energy $E_s=2.5$ but $d_{E,\min}=0.8944$. The same modulation diversity can be obtained by an algebraic rotation which also preserves the original average energy $E_s=2.5$ without sacrificing $d_{E,\min}$ (see Figure 3.6). The corresponding matrix is given by [31]

$$M = \frac{1}{\sqrt{5}}\begin{pmatrix} \sqrt{2+\frac{1+\sqrt{5}}{2}} & 0 \\ 0 & \sqrt{2+\frac{1-\sqrt{5}}{2}} \end{pmatrix}\begin{pmatrix} 1 & \frac{-1+\sqrt{5}}{2} \\ 1 & \frac{-1-\sqrt{5}}{2} \end{pmatrix} \tag{3.28}$$

Intuitively, the diagonal matrix is designed to skew the constellation in Figure 3.5(b) into the cubic shaped one in Figure 3.6 without losing the full diversity. The16-QAMconstellation in Figure 3.5(a) has $d^2_{p,\min}=0$, since it is not full rank, while the other two exhibit a positive $d^2_{p,\min}$. This can be estimated using the infinite lattice constellation and $\min\det(XX^{\hbar})$ for a codeword X. Using the theory of algebraic and ideal lattices [45], we find $d^2_{p,\min}=4/25$ for the algebraic lattice constellation and $d^2_{p,\min}=1/5$ for the algebraically rotated 16-QAM [31].

Several families of full diversity rotated Z^n–lattices from totally real algebraic number fields were given and analyzed for all dimensions in [48]. Here, we will see *cyclotomic construction* as one those families.

3.5.2.1 The Cyclotomic Construction

A cyclotomic field is a number field $B = Q(\zeta_m)$ generated by an m[th] root of unity, $\zeta_m = e^{2\pi i/m}$ as defined in [42, 50]. Let $B = Q(\zeta_p + \zeta_p^{-1})$ be a subfield of $Q(\zeta_p)$ generated by $\zeta_p^1 + \zeta_p^{-1} = 2\cos(2\pi/p)$, where ζ_p is a p^{th} root of unity. Since $[Q(\zeta_p) : B] = 2$ and B is totally real, it is called the *maximal real subfield* of a cyclotomic field. The degree of $Q(\zeta_p + \zeta_p^{-1})$ over Q is found by the *Euler function*, $\varphi(u)$ [51]. The Euler function of u is the number of non-negative integers $k \le u$ that are relatively prime to u. The following are examples of Euler functions of some positive integers that will be used in Chapter 4 while constructing the PSTBCs.

$$\varphi(5) = 4 \ , \ \varphi(7) = 6$$
$$\varphi(15) = 8 \ , \ \varphi(11) = 10 \tag{3.29}$$

Note: the set of non-negative integers which relatively prime to 15 is $\{0,2,4,7,8,11,13,14\}$

The degree, n of a cyclotomically constructed number field is given from the Euler function by

$$n = \frac{\varphi(u)}{2} \tag{3.30}$$

For some positive integer u. As a special case, $\varphi(p) = p - 1$, when the integer is a prime and its discriminant is given by

$$d_B = p^{\frac{n-2}{2}} = p^{\frac{p-3}{2}} \tag{3.31}$$

For a cyclotomic field $B = Q(\zeta_p + \zeta_p^{-1})$, its ring of integers is given by $O_B = Z[\zeta_p + \zeta_p^{-1}]$ [33]. The integral basis and the n embedding of $Q(\zeta_p + \zeta_p^{-1})$ into C are respectively

$$\{b_j = \zeta_p^j + \zeta_p^{-j}\}_{j=1}^n$$
$$\sigma_k(b_j) = \zeta_p^{kj} + \zeta_p^{-kj} = 2\cos(2\pi kj/p) \tag{3.32}$$

As the Gram matrix is identity matrix, the determinant of Z^n is 1 for $n \ge 2$ that its scaled version is of the form $(\sqrt{c}Z)^n$ for some integer c, so that its determinant is

$\det(G) = \det(M)^2 = c^n$. Thus, the general lattice determinant in Equation 3.25 for Z^n will be

$$N(I)^2 N(\beta) d_B = c^n$$
$$N(\beta) d_B = c^n = p^{(p-1)/2} \qquad \text{(for } I = O_B\text{)} \tag{3.33}$$

Thus, the basis in Equation 3.32 will be changed so as to obtain a Gram matrix which is *p_* times an identity matrix. The new basis B' obtained from an old basis B after transformation by a matrix T is given by TB. The elements of an *nxn* generator matrix of a rotated Z^n -lattice generated by the ring of integers after a basis *transformation matrix* from $\{b_j\}$ to $\{b'_j\}$ is given by

$$M_{kj} = \frac{1}{\sqrt{p}} \sigma_l((b'_k))_{k,l=1}^n \tag{3.34}$$

The main concern of a *shaping constraint* on the constellation to be sent in the case of cyclic algebra based codes obtaining a unitary matrix for CDA-based codes. Each layer of the codeword (3.9) has the form $\gamma\ (x_l, \sigma(x_l), ..., \sigma^{n-1}(x_l)), l = 0, ..., n-1$. Thus, the *shaping constraint* requires that each layer of the codeword is of the form *Mv*, where *M* is a unitary matrix and *v* is a vector containing the information symbols. Let $\{e_1, e_2, ..., e_n\}$ be a basis of O_E. Each layer of a codeword is of the form [31]:

$$\begin{pmatrix} e_1 & e_2 & \cdots & e_n \\ e_1 & \sigma(e_2) & \cdots & \sigma(e_n) \\ \vdots & \vdots & \ddots & \vdots \\ e_1 & \sigma^{n-1}(e_2) & \cdots & \sigma^{n-1}(e_n) \end{pmatrix} \begin{pmatrix} u_{l,1} \\ u_{l,2} \\ \vdots \\ u_{l,n} \end{pmatrix} = \begin{pmatrix} x_l \\ \sigma(x_l) \\ \vdots \\ \sigma^{n-1}(x_l) \end{pmatrix} \Rightarrow Mv_l = C_l \tag{3.35}$$

Where C_l is the l^{th} layer of the codeword and $x_l = \sum_{k=1}^n u_{l,k} e_k \in O_E$. Since $u_{l,k}$ takes discrete values, we can see the above matrix multiplication as *generating points* in a lattice. The matrix *M* is thus the *generator matrix* of the lattice, whose *Gram matrix* is given by MM^h.

M is required to be unitary, which translates into saying that the lattice we would like to obtain for each layer is a $Z[i]^n$ –lattice, resp. a $Z[m]^n$ –lattice, since QAM and HEX symbols are finite subsets of Z[*i*], resp. Z[*m*]. Note that the matrix *M* may be

viewed as a *pre-coding matrix* applied to the information symbols which amplifies their strength.

Finally, note that the $2n^2$-dimensional real lattice generated by the vectorized codewords, where real and imaginary components are separated, is either Z^{2n2} (for QAM constellation) or A_2^{n2}(HEX constellation),where A_2 is the hexagonal lattice [47], with generator matrix given by

$$M = \begin{bmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{bmatrix} \tag{3.36}$$

The unitary matrix M can be interpreted as the generator matrix of a lattice. The determinant of an algebraic lattice L built over a principal ideal $\mathrm{I} = (\beta)\mathrm{O}_\mathrm{E}$, where $E/B = E'B/B$ is given by $\det(L) = |N(\beta)|^2 |d_{E'}|$ In order to get $L = Z[i]^n$ (respectively $Z[m]^n$), or a scaled version $L' = [sZ[i]]^n$ –lattice, respectively $[sZ[m]]^n$, a necessary condition is to find in $\mathrm{O_E}$ an element β of suitable norm which will satisfy $\det[sZ[i]]^n = s^n$ for an integer *s*. Given an extension $E'B/B$, the discriminant is given that one has to find an element β such that $|N(\beta)|^2 |d_{E'}| = s^n$ .This condition, however, is not sufficient that once the element is found. The *Gram matrix* $G = MM^\hbar$ has to be computed for identity to assure whether the right lattice is obtained [31].

Since M is given by

$$M = \begin{bmatrix} \sigma_1(\beta e_1) & \sigma_2(\beta e_1) & \cdots & \sigma_n(\beta e_1) \\ \sigma_1(\beta e_2) & \sigma_2(\beta e_2) & \cdots & \sigma_n(\beta e_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta e_n) & \sigma_2(\beta e_n) & \cdots & \sigma_n(\beta e_n) \end{bmatrix} \tag{3.37}$$

Each entry of the Gram matrix is computed by the formula

$$g_{ij} = Tr_{E/B}(\beta b_i b'_j) \tag{3.38}$$

The two steps which form the method to obtain the shaping property on constellation are finding an element β with the right norm in $\mathrm{O_E}$ and computing the trace matrix $MM^\hbar$ for identity.

CHAPTER FOUR

4 EXPLICIT CONSTRUCTION OF PSTBCS

4.1 The Golden Code (2x2 Antenna Dimension)

The Golden code is a 2 *x*2 PSTBC. Its name, Golden code, comes from its algebraic construction which involves the Golden number $\theta_2 = (1+\sqrt{5})/2$. This perfect code has been found independently by the Belfiore et al. [52] and Dayal et al. [53]. It is built using the cyclic algebra

$$\Lambda_2 = (E = Q(i,\sqrt{5})/Q(i),\theta_2,i) \tag{4.1}$$

With $\sigma:\sqrt{5}\mapsto-\sqrt{5}$ and the ring of integer is given by $O_E = \{a+b\theta_2 | a,b\in Z(i)\}$ .Let us first define what an *infinite code is. An infinite code,* C_∞ *, is* the set of matrices of the form

$$C\mathcal{B}_\infty = \left\{ X_2 = \begin{bmatrix} a+b\theta_2 & c+d\theta_2 \\ i(c+d\bar{\theta}_2) & a+b\bar{\theta}_2 \end{bmatrix} : a,b,c,d \in Z[i] \right\} \tag{4.2}$$

4.1.1 The corresponding Cyclic Division Algebra (CDA)

The CDA of the Golden code is given by:

$$\Lambda_2 = L \oplus bL \tag{4.3}$$

Where $b\in\Lambda_2$ such that $b^2 = i$ and $ab = b\sigma(a)\forall a\in L$

4.1.2 The corresponding rotated $Z[x]^2$ -lattice: Z[i]²

Let us see now how to add the shaping property on the codebook built on Λ_2.

Noting from Equation 3.25, it is required to look at an element β_2 such that $\det(\Lambda_2) = |N_{E/B}(\beta_2)|^2 \left|d_{Q(\sqrt{5})}(\beta_2)\right|^2 = 5|N_{E/B}(\beta_2)|^2$.

In order to find such an element, we look at the factorization of 5 in O_E:

Since $5 = (1+i-i\theta_2)^2(1-i+i\theta_2)^2$, we choose $\beta_2 = 1+i-i\theta_2$.

4.1.3 The Gram and Generator matrices

As stated at the end of Section 3.4.2, after finding an appropriate element β_2, the Gram matrix should be checked for identity. Its generator matrix is given by

$$M_2 = \begin{pmatrix} \beta_2 & \beta_2\theta_2 \\ \sigma(\beta_2) & \sigma(\beta_2\theta_2) \end{pmatrix}. \tag{4.4}$$

A direct computation shows that $M_2 M_2^{\hbar} = 5I_2$. Thus $M_2/\sqrt{5}$ is a unitary matrix, yielding the shaping property.

4.1.4 The codeword

A codeword $X_2 \in C\mathcal{B}$ belonging to the Golden code after adding the shaping property has the form:

$$X_2 = \begin{bmatrix} \beta_2(a+b\theta_2) & \beta_2(c+d\theta_2) \\ i\sigma(\beta_2)(c+d\sigma(\theta_2)) & \sigma(\beta_2)(a+b\sigma(\theta_2)) \end{bmatrix} \tag{4.5}$$

where *a, b, c, d* are QAM symbols. When *a, b, c ,d* can take any value in Z[*i*], we say that we have an *infinite code* $C\mathcal{B}_\infty$ where the terminology recalls the case where finite signal constellations are carved from infinite lattices.

4.1.5 The Minimum Determinant

Let us now compute the minimum determinant of the infinite code. Since $\beta_2\sigma(\beta_2) = 2+i$, we have $\det(X_2) = (2+i)/5\left[(a+b\theta_2)(a+b\sigma(\theta_2)) - (c+d\theta_2)(c+d\sigma(\theta_2))\right]$ which will be simplified to $1/(2-i)\left[(a^2+ab-b^2-i(c^2=cd-d^2))\right]$. By the definition of *a, b ,c & d* we have that the non-trivial minimum of $\left|(a^2+ab-b^2-i(c^2+cd-d^2))\right|^2$ *is 1. Thus* $d_{p,\min}(C\mathcal{B}_\infty) = \min\left|\det(X_2)\right|^2 = 1/5$ .Therefore, the *minimum determinant* of the infinite code is bounded away from zero, as required. Another method of computing the minimum determinant is as follows:

$$X_2 = \frac{1}{\sqrt{5}}\begin{bmatrix} \beta_2 & 0 \\ 0 & \sigma(\beta_2) \end{bmatrix}\begin{bmatrix} a+b\theta_2 & c+d\theta_2 \\ i(c+d\theta_2) & (a+b\theta_2) \end{bmatrix} \tag{4.6}$$

Using the principle of determinant of product of matrices, we have

$$d_{p.\min} = \min_{X_2 \neq 0} \det(X_2) = 1/\sqrt{5}\, N_{E/B}(\beta_2) \min_{X_2 \neq 0} \det\begin{bmatrix} a+b\theta_2 & c+d\theta_2 \\ i(c+d\sigma(\theta_2)) & a+b\sigma(\theta_2) \end{bmatrix} \tag{4.7}$$

As the reduced norm of a CDA belongs to its base field, the determinant on the right-hand side is lower bounded by 1. Thus $d_{p,\min} = \min\left|\det(X_2)\right|^2 = 1/25\left|N_{E/B}(\beta_2)\right|^2 = 1/5$

In the entries of the codeword X_2 of Equationv4.6, the factor i guarantees uniform average transmitted energy per antenna as $|i|^2 = 1$.

As an example of these PSTBCs, consider the Golden code to examine whether it satisfies the design criteria described in Section 2.3 or not.

(a)The rank criterion: as the minimum determinant $d_{p,\min}$ in Equation 4.7is not zero, the codeword matrix is full rank or full diversity. Thus, the Golden code satisfies the rank criterion.

(b)The determinant criterion: In general, as the higher determinant of a matrix, the higher the eigenvalues, this non-vanishing determinant code is expected to be higher.

(c) The decoding complexity criterion: As will be seen in Chapter 5, Section 5.2, the Golden code is ML decodable with a reduced complexity $o(q^{1/2})$ from sphere decoder, according to Equation 2.44.

(d) Good Constellation Shaping: The energy required to transmit the linear combination of the information symbols is equal to the energy required to send the themselves. This can be proven by considering writing the codeword as a sum of its layers of Equation 3.12. And note that each layer is given by, in terms of the generating matrix M_2 and a vector V containing the information symbols, MV as of Equation 3.35.Now, the average energy of their coded form is given by $E\{(M_2V)^h(M_2V)\} = E\{V^hV\} = E_s$ as M_2 is a unitary matrix, as explained in Section 4.1.3. Thus, there is no additional energy in the encoding process.

(e) UAEPA: As can be seen from the codeword Equation 4.5, the information symbols a and b are transmitted at the first transmit time slot by antenna one and their embedded form by the second transmit antenna at the second time slot. The same is true for the information symbols c and d. This shows that, on average, the energy used by each transmit antenna is equal. This is generally true as can be seen from the general codeword matrix of Equation 3.9. Thus, there is uniform average energy per antenna in PSTBCs.

(f) High rate: The Golden code transmits 4 QAM based symbols in two transmission slots giving a rate of $\Re = 2$, which is equal to the number of transmit

antennas. Thus, the Golden code is a high rate code, according to Table 2.1and definition of high rate in Section 2.2.

(g) NVD: As computed in Equation 4.7, the minimum determinant of the Golden code as the constellation size increases is lower bounded by a nonzero value $d_{p,\min} = 1/5$.

(h) DMT: Although it is a long and bulk process showing the optimality the Golden code, P. Elia et al. [54] showed that CDA-based codes are DMT optimal even for rectangular STBCs.

In general, the same analysis can be done to the rest of the PSTBCs as to show their optimality in many of the design criteria.

4.2 A PSTBC for 3x3 Antenna Dimension

For 3 antennas, we use HEX symbols. Thus, the base field is $B = Q(m)$,where $m = e^{2\pi i/3}$

Recall from Equation 3.29 that as *n*=*3*, the corresponding positive integer whose Euler value is twice of the degree is *u*=*7*. Thus, $\theta_3 = \zeta_7^{\,1} + \zeta_7^{\,-1} = 2\cos(2\pi/7)$) is the primitive element and the compositum of B and $Q(\theta_3)$ is the field extension is $E = Q(m,\theta_3)$.Its degree is denoted and represented by $[Q(\theta_3):Q] = 3$. As u=7 is prime, its discriminant is found by using Equation 3.31 as $d_{Q(\theta_3)} = p^{\frac{(p-3)}{2}} = 7^2 = 49$. The choice of basis independent parameter, discriminant is also given by $d_{Q(\theta_3)} = (\det(\sigma_l(b_k))^n{}_{k,l=1})^2$. The minimal polynomial of the generating element, θ_3 is given by $P_{\theta_3}(X) = \prod_{i-1}^{3}(X - \sigma_i(\theta_3)) = x^3 + x^2 - 2x - 1$.

4.2.1 The Corresponding CDA

The field extension E/B is cyclic with the generating element θ_3 and its embedding as given from Equation 3.32 is $\sigma : \zeta_7^{\,1} + \zeta_7^{\,-1} \mapsto \zeta_7^{\,2} + \zeta_7^{\,-2}$.We consider the cyclic algebra $\Lambda_3 = (E/B, \theta_3, m)$ of degree 3.

$$\Lambda_3 = L \oplus bL \oplus b^2 L \tag{4.8}$$

with $b \in \Lambda_3$ such that $b^3 = \gamma \in B^*$ and $ab = b\sigma(a) \forall a \in L$. The choice non- norm element γ=m gives a fully diverse code [31].

4.2.2 The Corresponding rotated $Z[x]^3$ -Lattice: Z[m]^3

Since we use HEX symbols, we look for a Z[m]-lattice which is a rotated Z[m] lattice which is a rotated Z[m]^3(= A_2^3) lattice. From the lattice determinant, $\det(\Lambda_3) = |N_{E/B}(\beta_3)|^2 |d_{Q(\theta_3)}| = 49|N_{E/B}(\beta_3)|^2$. The necessary condition to obtain a rotated Z[m]^3 lattice is the existence of an element β_3 whose norm is 7. The factorization of 7 in the ring of integers of this field is as follows: $7 = (1+m+\theta_3)^3(\overline{1+m+\theta_3})^3$ .Now we can let $\beta_3 = (1+m+\theta_3)$.

A Z[m] basis of its ideal, i.e. $(\beta_3)O_E$ is given by $\{\beta_3\theta_3^{\,k}\}_{k=0}^2$. In vector form,

$$B_3 = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 1+m+\theta_3 \\ (1+m)\theta_3 + \theta_3^{\,2} \\ 1+2\theta_3 + m\theta_3^{\,2} \end{bmatrix} \tag{4.9}$$

NB: $b_3 = (1+m+\theta_3)(\theta_3^{\,2}) = \theta_3^{\,2} + m\theta_3^{\,2} + \theta_3^{\,3}$ (see Appendix A.1)

4.2.3 The Gram and the generator Matrices

We have to use a basis transformation which will give us a Gram matrix which is p times an identity matrix. That is $G = PI_n$, where p and n are as defined above. The new transformed basis and the basis transformation matrix are given respectively as

$$T_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 2 & 1 & 0 \end{bmatrix} \quad , \quad B_3' = T_3 B_3 = \begin{bmatrix} b_1' \\ b_2' \\ b_3' \end{bmatrix} = \begin{bmatrix} 1+m+\theta_3 \\ (-1-2m) + m\theta_3^{\,2} \\ (-1-2m) + (1+m)(\theta_3 + \theta_3^{\,2}) \end{bmatrix} \tag{4.10}$$

Now let us check if we got an identity Gram matrix by computing its elements. The trace of $1, \theta_3$ and θ_3^2 by applying the embedding Equation 3.32 are respectively given as (see appendix A.2).

$$\begin{aligned} Tr_{Q(\theta_3)/Q}(1) &= \sum_{k=1}^{3} \sigma_k(1) = 3 \\ Tr_{Q(\theta_3)/Q}(\theta_3) &= \sum_{k=1}^{3} \sigma_k(\theta_3) = -1 \\ Tr_{Q(\theta_3)/Q}(\theta_3^{\,2}) &= \sum_{k=1}^{3} \sigma_k(\theta_3^{\,2}) = 5 \end{aligned} \tag{4.11}$$

Now, let us determine elements of the Gram matrix by using Equation 3.38. After normalization by p, we get $\frac{1}{7} Tr_{E/Q(j)}(b_l' \overline{b'}_k) = \delta_{lk}, l,k = 1,2,3$.

The diagonal elements of the Gram matrix are determined to be (see appendix A.3)

$$Tr_{E/Q(m)}(b_j'\overline{b_j'}) = \begin{cases} Tr(b_1'\overline{b_1'}) = Tr(1+\theta_3+\theta_3^2) = 7 \\ Tr(b_2'\overline{b_2'}) = Tr(2-\theta_3) = 7 \\ Tr(b_3'\overline{b_3'}) = Tr(4-\theta_3^2) = 7 \end{cases} \quad (4.12)$$

The generator matrix whose coefficients are given by $M_{kj} = \frac{1}{\sqrt{7}}\sigma_j((b_k'))_{k,j=1}^3$ as of the general expression of Equation 3.34 is shown below (appendix A.4):

$$M_3 = \begin{bmatrix} 0.66030+0.32733i & 0.20077+0.32733i & -0.49209+0.32733i \\ -0.29386-0.114567i & -0.037743-0.58982i & -0.61362+0.40817i \\ 0.59952+0.26250i & -0.04667-0.73550i & 0.27309-0.18164i \end{bmatrix} \quad (4.13)$$

4.2.4 The codeword

The codeword $X_3 \in C\mathcal{B}$ encodes nine HEX symbols $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$ as follows:

$$X_3 = \sum_{k=0}^{2} diag\left[\left(M_3(x_{3k}, x_{3k+1}, x_{3k+2})^T\right)\right] R_3^{\,k} \quad (4.14)$$

where, $R_3 = [0 \quad 1 \quad 0 \quad ; \quad 0 \quad 0 \quad 1 \quad ; \quad m \quad 0 \quad 0]$ is an appropriate rotational matrix to meet the desired shaping constraint.

The following Figure shows the uniform energy sharing of the transmit antennas (appendix A.5)

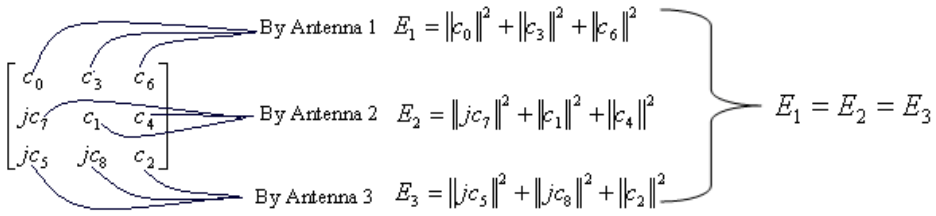


Figure 4.1: Uniform average energy transmitted per antenna

4.2.5 The minimum determinant

Using the same argument, the minimum determinant for this antenna dimension is given by the minimum of the square of the determinant of the code coke closest to the center of the constellation. Thus,

$$d_{p,\min} = \min\left|\det(X_3)\right|^2 = \frac{1}{7}\left|N_{E/B}(\beta_3)\right|^2 d_B = \frac{1}{7}\cdot\frac{1}{7^2}.7 = \frac{1}{49}$$

4.3 A PSTBC for 4x4 Antennas

We consider the transmission of QAM symbols that the base field is $Q(i)$. Recall again from Equation 3.29 that $\varphi(15)=8$ that $p=15$ in this case.

Thus, $\theta_4=\zeta_{15}^{1}+\zeta_{15}^{-1}=2\cos\left(2\pi/15\right)$ and $E=Q(i,\theta_4)$ is the compositum of $Q(i)$ and $Q(\theta_4)$.

Thus, we have its degree $[Q(i,\theta_4):Q(i)]=4$. The discriminant of $Q(\theta_4)$ is $d_{Q(\theta_4)}=1125$. Its minimal polynomial is given by $P_{\theta 4}(X)=\prod_{i=1}^{4}(X-\sigma_i(\theta_4))=X^4-X^3-4X^2+4X+1$.

4.3.1 The corresponding CDA

The field extension E/B is cyclic with the generator θ_4 with $\sigma:\zeta_{15}^{\ 1}+\zeta_{15}^{\ -1}\mapsto\zeta_{15}^{2}+\zeta_{15}^{-2}$. We consider the cyclic algebra $\Lambda_4=(E/B,\theta_4,i)$ of degree 4.

$$\Lambda_4=L\oplus bL\oplus b^2L\oplus b^3L \tag{4.15}$$

with $b\in\Lambda_4$ such that $b^4=\gamma\in B^*$ and $ab=b\sigma(a)\forall a\in L$. The choice of $\gamma=i$ yields a perfect code, as all of its integer powers are non norms in E/B. Thus, the code is fully diverse.

4.3.2 The Corresponding rotated $Z[x]^4$ -Lattice: Z[i]^4

Since we use QAM symbols, we look for a Z[i]-lattice which is a rotated Z[i] lattice. From the lattice determinant, $\det(\Lambda_4)=\left|N_{E/B}(\beta_4)\right|^2\left|d_{Q(\theta_4)}\right|=1125\left|N_{E/B}(\beta_4)\right|^2=5^3 3^2\left|N_{E/B}(\beta_4)\right|^2$.

The necessary condition to obtain a rotated Z[i]^4 lattice is the existence of an element β_4 whose norm is $3^2 5$ so that the the nth power of $\det(\Lambda_4)$ is an integer, as described at the end of Section 3.4.2. From the property of norm of an algebraic number of Equation 3.14, we note that the element whose norm is $3^2 5$ is a product of the two primes 3 and 5. In addition, as the number of embeddings are equal to the degree of field, the norm expression is the power of 4, here in this case. Gauss found that Gaussian primes have unique factorization and a Gaussian integers have unique prime factorization up to order [51].Now let's look for the ideal factorization of the primes 3 & 5, $3=\omega_3^2(\overline{\omega_3})^2$ & $5=\omega_5^4(\overline{\omega_5})^4$ .Consider the product $\beta_4=\omega_3\omega_5=(1+i(-3+\theta_4^{\ 2}))$.

Thus, $Z[i]$-basis of β_4, as above is $\{\beta_4\theta_4^{\ i}\}_{i=0}^{3}$. The basis transformation matrix and the new basis are given respectively in Equation 4.16, below.

$$T_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 1 \\ -1 & -3 & 1 & 1 \end{bmatrix} \qquad B_4' = \begin{bmatrix} b_1' \\ b_2' \\ b_3' \\ b_4' \end{bmatrix} = \begin{bmatrix} 1 + i(-3 + {\theta_4}^2) \\ \theta_4 + i(-3\theta_4 + {\theta_4}^3) \\ (-3\theta_4 + {\theta_4}^3) + i(-1 + 4\theta_4 - {\theta_4}^3) \\ (-1 + -3\theta_4 + {\theta_4}^2 + {\theta_4}^3) + i \end{bmatrix} \tag{4.16}$$

4.3.3 The Gram and the generator Matrices

Now let us compute the Gram & generator matrices. Determining the embeddings of the generating element and the trace of its lower integer powers is a necessary condition before computing the entries of the Gram as well as the generator matrices. The four embeddings are given by

$$\begin{aligned} \sigma_1(\theta_4) &= \sigma_1(\zeta_{15}^1 + \zeta_{15}^{-1}) = \zeta_{15}^2 + \zeta_{15}^{-2} = 2\cos\left(4\pi/15\right) \\ \sigma_2(\theta_4) &= \sigma_2(\zeta_{15}^1 + \zeta_{15}^{-1}) = \zeta_{15}^1 + \zeta_{15}^{-1} = 2\cos\left(2\pi/15\right) \\ \sigma_3(\theta_4) &= \sigma_3(\zeta_{15}^1 + \zeta_{15}^{-1}) = \zeta_{15}^7 + \zeta_{15}^{-7} = 2\cos\left(14\pi/15\right) \\ \sigma_4(\theta_4) &= \sigma_4(\zeta_{15}^1 + \zeta_{15}^{-1}) = \zeta_{15}^4 + \zeta_{15}^{-4} = 2\cos\left(8\pi/15\right) \end{aligned} \tag{4.17}$$

And the traces of some important terms are (See the Appendix B.1)

$$Tr(.) = \begin{cases} Tr(1) = \sum_{i=1}^{4} \sigma_1(1) = 4 \\ Tr(\theta_4) = \sum_{i=1}^{4} \sigma_1(\theta_4) = 1 \\ Tr(\theta_4^2) = \sum_{i=1}^{4} \sigma_1(\theta_4^2) = 9 \\ Tr(\theta_4^3) = \sum_{i=1}^{4} \sigma_1(\theta_4^3) = 1 \\ Tr(\theta_4^4) = \sum_{i=1}^{4} \sigma_1(\theta_4^4) = 29 \\ Tr(\theta_4^5) = \sum_{i=1}^{4} \sigma_1(\theta_4^5) = -4 \\ Tr(\theta_4^6) = \sum_{i=1}^{4} \sigma_1(\theta_4^6) = 99 \end{cases} \tag{4.18}$$

Again, using the formula in Equation 3.38, the off diagonal elements of the Gram matrix can be shown to zero. However, its diagonal elements, after normalization by 15, are computed to be

$$Tr_{E/Q(i)}(b_i'\overline{b_i'}) = Tr_{E/Q(i)}\left(\left|b_i'\right|^2\right) = \begin{cases} Tr(b_1'\overline{b_1'}) = Tr(10 - 6\theta^2 + \theta^4) = 15 \\ Tr(b_2'\overline{b_2'}) = Tr(1 + 3\theta + \theta^2 - \theta^3) = 15 \\ Tr(b_3'\overline{b_3'}) = Tr5 + 6\theta - \theta^2 - 2\theta^3) = 15 \\ Tr\left(b_4'\overline{b_4'}\right) = Tr(-5\theta + 2\theta^2 + 2\theta^3) = 15 \end{cases} \tag{4.19}$$

This shows that the Gram matrix can written in compact form as $G = 15I_4$.

Thus, we conclude that we got a rotated lattice as we got an element β_4 with a proper norm and

an identity Gram matrix. Now, we can determine the generator matrix whose entries are given by $M_{lk} = \frac{1}{\sqrt{15}}\sigma_l(b'_k)$. Where, M_{lk} is an element at the l^{th} row and k^{th} column.(see appendix B.2)

$$M_4 = \begin{bmatrix} 0.258 - i0.312 & 0.346 - i0.418 & -0.418 + i0.505 & -0.214 + i0.258 \\ 0.258 + i0.087 & 0.472 + i0.160 & 0.160 + i0.054 & 0.763 + i0.258 \\ 0.258 + i0.214 & -0.505 - i0.418 & -0.418 - i0.346 & 0.312 + i0.258 \\ 0.258 - i0.763 & -0.054 + i0.160 & 0.160 - i0.472 & -0.087 + i0.258 \end{bmatrix} \tag{4.20}$$

4.3.4 The codeword

A codeword $X_4 \in CB$ encodes 16 QAM symbols $x_0, x_1, ..., x_{15}$ which is given by [31]

$$X_4 = \sum_{k=0}^{3} diag(M_4(x_{4k,} x_{4k+1,} x_{4k+2,} x_{4k+3})^T) R_4^{\,k} \tag{4.21}$$

Where, R_4 is the appropriate rotational matrix given by $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ i & 0 & 0 & 0 \end{bmatrix}$

4.3.5 The minimum determinant

The minimum determinant of the infinite code is

$$d_{p,\min} = \min_{x_4 \neq 0}(\det(X_4)) = \min\left\{\frac{N_{E/B}(\beta_4)^2}{\det(\Lambda_4)}\right\} = \frac{3^2 * 5}{15^4} = \frac{1}{1125} = \frac{1}{d_{Q(\theta_4)}} \tag{4.22}$$

4.4 A PSTBC for 5x5 Antenna Dimension

For 5 antennas dimension we transmit QAM symbols. Thus, the base field is $B = Q(i)$.

As $\varphi(11) = 10$ from Equation 3.29, $p = 11$ that the generating element

$\theta_5 = \zeta_{11}^1 + \zeta_{11}^{-1} = 2\cos(2\pi/11)$ and $E = Q(i, \theta_5)$ be the compositum of B and $Q(i, \theta_5)$.

As $[Q(\theta_5) : Q] = 5$, and thus, $[Q(i,\theta) : B] = 5$.

The field extension E/B is cyclic with the generator θ_5 and with

$\sigma : \zeta_{11}^{\ 1} + \zeta_{11}^{\ -1} \mapsto \zeta_{11}^2 + \zeta_{11}^{-2}$.

4.4.1 The corresponding cyclic algebra

We consider the cyclic algebra $\Lambda_5 = (E/B, \theta_5, i)$ of degree 5.

$$\Lambda_5 = L \oplus bL \oplus b^2L \oplus b^3L \oplus b^4L \tag{4.23}$$

with $b \in \Lambda_5$ such that $b^5 = \gamma \in B^*$ and $ab = b\sigma(a) \forall a \in L$. The choice of $\gamma = i$ yields a perfect code, as all of its integer powers is non norms in E/B. Thus, the code is fully diverse [31].

In order to obtain a division algebra, we choose $\gamma = \gamma_n / \gamma_d = (3+2i)/(2+3i)$ which is non- norm and has unit magnitude in order not to affect the *uniform constellation* and *equal energy* properties as described by Elia et al. [12].

4.4.2 The Lattice Z[i]^5 and the generator matrix

The technique used to find Z[i]^5 is different from the previous methods and the generator matrix is given by [31]

$$M_5 = \begin{bmatrix} -0.3260 & 0.5485 & -0.455 & -0.5969 & -0.1699 \\ 0.5485 & -0.455 & -0.5969 & -0.1699 & -0.3260 \\ -0.455 & -0.5969 & -0.1699 & -0.3260 & 0.5485 \\ -0.5969 & -0.1699 & -0.3260 & 0.5485 & -0.455 \\ -0.1699 & -0.3260 & 0.5485 & -0.455 & -0.5969 \end{bmatrix} \tag{4.24}$$

4.4.3 The codeword

A codeword $X_5 \in C\mathcal{B}$ encodes 25 QAM symbols $x_0, x_1, ..., x_{24}$ which is given by which is given by

$$X_5 = \sum_{k=0}^{4} diag(M_5(x_{5k,}x_{5k+1,}x_{5k+2,}x_{5k+3}, x_{5k+4})^T) R_5^{\,k} \tag{4.25}$$

Where, the rotational matrix is given by $R_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ i & 0 & 0 & 0 & 0 \end{bmatrix}$

4.4.4 The minimum determinant

As the code construction is different, the method of calculating the minimum determinant is also a little bit different. By slightly modifying the method used for the Golden code, we obtain the following:

$$\det(X_5) = \det \begin{bmatrix} x_0 & x_1 & x_2 & x_3 & x_4 \\ \gamma\sigma(x_4) & \sigma(x_0) & \sigma(x_1) & \sigma(x_2) & \sigma(x_3) \\ \gamma\sigma^2(x_3) & \gamma\sigma^2(x_4) & \sigma^2(x_0) & \sigma^2(x_1) & \sigma^2(x_2) \\ \gamma\sigma^3(x_2) & \gamma\sigma^3(x_3) & \gamma\sigma^3(x_4) & \sigma^3(x_0) & \sigma^3(x_1) \\ \gamma\sigma^4(x_1) & \gamma\sigma^4(x_2) & \gamma\sigma^4(x_3) & \gamma\sigma^4(x_4) & \sigma^4(x_0) \end{bmatrix}$$

$$= \frac{1}{\gamma_d^4} \det \begin{bmatrix} x_0 & x_1 & x_2 & x_3 & x_4 \\ \gamma_n \sigma(x_4) & \sigma(x_0) & \sigma(x_1) & \sigma(x_2) & \sigma(x_3) \\ \gamma_n \sigma^2(x_3) & \gamma_n \sigma^2(x_4) & \sigma^2(x_0) & \sigma^2(x_1) & \sigma^2(x_2) \\ \gamma_n \sigma^3(x_2) & \gamma_n \sigma^3(x_3) & \gamma_n \sigma^3(x_4) & \sigma^3(x_0) & \sigma^3(x_1) \\ \gamma_n \sigma^4(x_1) & \gamma_n \sigma^4(x_2) & \gamma_n \sigma^4(x_3) & \gamma_n \sigma^4(x_4) & \sigma^4(x_0) \end{bmatrix} \tag{4.26}$$

$$= \frac{1}{\gamma_d^4} \det(\hat{X}_5)$$

Thus we have $\min\left|\det(X_5)\right|^2 = \frac{1}{(\gamma_d^4)^2} \min\left|\det(\hat{X}_5)\right|^2$. Since now $\hat{X}_5$ is a matrix with coefficients in Gaussian integers ($Z[i]$), the previous method works for $\hat{X}_5$.

$\min\left|\det(\hat{X}_5)\right|^2 = \frac{1}{11^5}\left|N_{E/Q(i)}(\beta_5)\right|^2 = \frac{1}{11^5}.11 = \frac{1}{11^4}$. And $\left|\gamma_d^4\right|^2 = \left|\gamma_d^2\right|^4 = (\left|2+3i\right|^2)^4 = 13^4$.

The minimum determinant of the code, therefore, is

$$d_{p,\min} = \frac{1}{11^4}.\frac{1}{13^4} = \frac{1}{(143)^4} \tag{4.27}$$

CHAPTER FIVE

5 COML DECODING OF THE PSTBCS

5.1 Introduction to Conditional Optimization

Conditional optimization is a technique which has been widely used in *statistical estimation* and *signal processing* in maximizing likelihoods [19]. The target of the technique is to reduce the complexity of the *maximization process* by reducing the number of maximization parameters. This reduction of the optimization parameters is possible by first finding some of the parameters being conditioned on the others. For example, if the received signal is function of the *magnitude* and *frequency* of another parameter, instead of maximizing with respect to both the magnitude and the frequency, it will be simpler to first analytically optimize over one of them conditioned on the other so that the overall maximization will be with respect to only one parameter. Finally, the actual value of the analytically found parameter will be determined from the optimizing value of the other.

Assume that the received signal is y and the set of parameters to optimize over is Φ. If the parameter set can be split as $\Phi = (\phi_1, \phi_2, \phi_3)$ such that optimization over ϕ_1 given ϕ_2 and ϕ_3 can be carried out analytically, then the optimization $p(y|\Phi)$ can be carried out in three consecutive steps as follows

$$\hat{\phi}_1(\phi_2, \phi_3) = \arg\max_{\varphi_1} p(y|\phi_2, \phi_3, \phi_1)$$

$$(\hat{\phi}_2, \hat{\phi}_3) = \arg\max_{\varphi_2, \varphi_3} p\left(y\middle|\phi_2, \phi_3, \hat{\phi}_1(\phi_2, \phi_3)\right) \tag{5.1}$$

$$\hat{\phi}_1 = \hat{\phi}_1(\hat{\phi}_2, \hat{\phi}_3)$$

Next, we will see sufficient conditions under which the conditional optimization leads to a reduction in decoding complexity of the PSTBCs. Writing Equation 2.2 in matrix form, the received signal matrix will be

$$Y = HX + w \tag{5.2}$$

Rearranging the entries of the received vector to form a row vector, it can be rewritten as

$$y = x\mathcal{h} + w \tag{5.3}$$

Where, *x* is the *transmitted information symbol vector* and *h is the induced channel Matrix*. *The* likelihood function of symbols *x* given the received signal *y* is given by

$$p(y|x) \propto \exp\left(\frac{-1}{2\delta^2}\left\|y - x\hbar\right\|^2\right) \tag{5.4}$$

Taking the prior distribution of symbols *x* to be uniform on the constellation *q*, we obtain the ML solution

$$\hat{x} = \arg \max_{x \in q^L} p(y|x) \tag{5.5}$$

Where, *L* is the number of transmitted symbols and *q* the constellation size.

ML is achieved with $|q|^L$ computations of likelihood Equation5.5, but if the symbols are taken from an q-QAM and q-HEX constellations then dramatic reductions in complexity are possible.

If the induced channel matrix h has *n-rows* which are mutually orthogonal, for all channels H , then exact ML can be implemented with complexity $o(q^{L-n})$ [19].

While making the analytical computations in the *first* and *third* steps of Equation 5.1, there is *quantization* process. As a particular example, each complex symbol of an QAM or HEX is first separated into its *real* and *imaginary* parts. Next, each of them are quantized or rounded to the nearest PAM alphabet. As the quantization process introduces additional complexity to the decoding process, it should be taken into account.

For arbitrary constellation the quantization step is a search of at most $o(|q|)$, while if the constellation is a Cartesian product of two constellations, i.e., $q = \Re x \Re$ the search is at most $o\left(\sqrt{|q|}\right)$. However, if the constellation is QAM or HEX, the quantization step is $o(1)$. Thus, the quantization process in QAM or HEX adds nothing to the order of decoding complexity. As a result it is possible to decode the Golden code, 3x3 and 4x4 PSTBC with the order of complexity $o(q^2)$, $o(q^6)$ and $o(q^{12})$ respectively. This is because the all rows of the induced channel matrices of each are mutually orthogonal.

5.2 Coding and COML Decoding model of the Golden Code

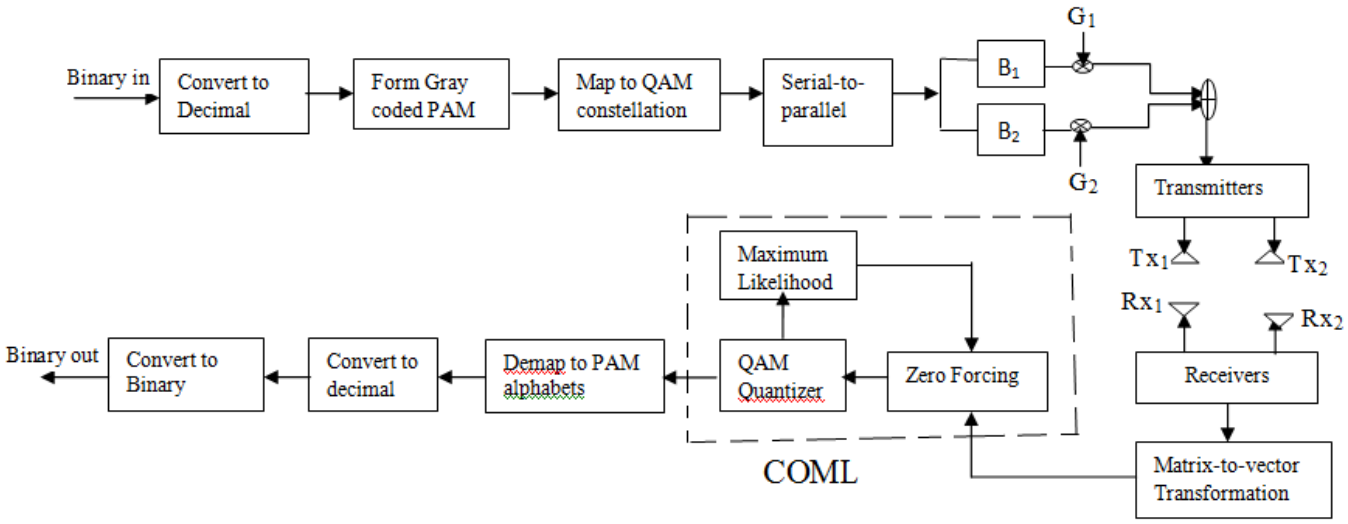


Figure 5.1: Coding and decoding model of the Golden code

The Golden code transmits 4-QAM complex symbols in two time slots by two transmit antennas. The transmit code words of the Golden code can be expressed as

$$X = \begin{bmatrix} \sigma(\beta) & 0 \\ 0 & \beta \end{bmatrix} \begin{bmatrix} x_1 & x_3 \\ ix_3 & x_1 \end{bmatrix} + \begin{bmatrix} \theta\sigma(\beta) & 0 \\ 0 & \beta\sigma(\theta) \end{bmatrix} \begin{bmatrix} x_2 & x_4 \\ ix_4 & x_2 \end{bmatrix} \tag{5.6}$$

Where,

$\theta = \frac{1+\sqrt{5}}{2}$, $\sigma(\theta) = \frac{1-\sqrt{5}}{2}$, $\beta = 1 + i\theta$ and $\sigma(\beta) = 1 + i\sigma(\theta)$

It can be written in a simplified form as

$$X = G_1 B_1 + G_2 B_2 \tag{5.7}$$

Where, the G_i's are pre-amplifying gain diagonal matrices and the B_i's are the cyclic Alamouti block codes. Assuming the channel state is known at the receiver and let h_{mn} be the channel gain coefficient from transmit antenna m to a receive antenna n. Thus, the received signal is given by

$$Y = HX + W \tag{5.8}$$

Where

$$H = \begin{bmatrix} h_{11} & h_{21} \\ h_{12} & h_{22} \end{bmatrix}$$

Equation 5.8 can be rewritten as

$$y = (x_1, x_3)\mathcal{H}_1 + (x_2, x_4)\mathcal{H}_2 + \mathrm{w} \tag{5.9}$$

Where $y=(y_1,y_2)$ contains the two received signal vectors and $y_i=(y_i^1,y_i^2)$ with the component y_i^j representing the received signal at antenna *i* at time slot *j*. The noise $w=(w_1^1,w_1^2,w_2^1,w_2^2)$ is i.i.d Gaussian with zero mean and covariance of $2\delta^2 I_2$. The channel matrix coefficients are given by

$$\mathcal{H}_1=(A_1,\mathrm{B}_1)\ ,\ \ \mathcal{H}_2=(A_2,\mathrm{B}_2) \tag{5.10}$$

Where A_i and B_i are the induced channel matrices from the two transmit antennas to the 1st and the 2nd receive antennas respectively. They are given as follows

$$A_1=\begin{bmatrix}\sigma(\beta)h_{11} & \beta h_{21}\\ i\beta h_{21} & \sigma(\beta)h_{11}\end{bmatrix}\ ,\ A_2=\begin{bmatrix}\theta\sigma(\beta)h_{11} & \sigma(\theta)\beta h_{21}\\ i\sigma(\theta)\beta h_{21} & \theta\sigma(\beta)h_{11}\end{bmatrix}$$

$$B_1=\begin{bmatrix}\sigma(\beta)h_{12} & \beta h_{22}\\ i\beta h_{22} & \sigma(\beta)h_{12}\end{bmatrix}\ ,\ B_2=\begin{bmatrix}\theta\sigma(\beta)h_{12} & \sigma(\theta)\beta h_{22}\\ i\sigma(\theta)\beta h_{22} & \theta\sigma(\beta)h_{12}\end{bmatrix} \tag{5.11}$$

The induced channel matrices have the following property which is the basis of the fast decoding approach [11].

$$\sum_{j=1}^{2} H_j H_j^{\hbar}=5\|H\|^2{}_F I_2 \tag{5.12}$$

Where, 5 is the corresponding pth root of unity for 2x2 antenna dimension and $\|H\|^2{}_F$ is the *Frobenius matrix norm* of a matrix given by $\|H\|^2{}_F=\sum_{i,j}^{n}\left|c_{ij}\right|^2=trace\left(HH^{\hbar}\right)$

In general, not only PSTBCs but also any STBC which satisfies Equation 5.12 is decodable with COML decoding approach with a reduced complexity [11].

Let

$$s=(x_1,x_3)\ \text{and}\ c=(x_2,x_4) \tag{5.13}$$

Substituting these expressions in equation (6.5), we obtain

$$y=s\mathcal{H}_1+c\mathcal{H}_2+w \tag{5.14}$$

The associated likelihood function is [17]

$$p(y|s,c)\propto\exp\left(-\frac{1}{2\delta^2}\left\|y-s\mathcal{H}_1-c\mathcal{H}_2\right\|^2\right) \tag{5.15}$$

Based on the *conditional optimization*, Equation 6.11 is first maximized with respect to ***c*** given ***s***

$$p(y|s,c)\propto\exp\left(-\frac{1}{2\delta^2}y'(I_4-\breve{\mathcal{H}}_1\mathcal{H}_1)y'^{\hbar}\right)$$

$$* \exp\left(\frac{-1}{2\delta^2}(s-\tilde{s}(c))\mathcal{H}_1\mathcal{H}_1^{\hbar}(s-\tilde{s}(c))\right) \tag{5.16}$$

Where,

$$y' = y - c\mathcal{H}_2 \ , \breve{\mathcal{H}}_1 = \mathcal{H}_1^{\hbar}(\mathcal{H}_1\mathcal{H}_1^{\hbar})^{-1} \text{, and}$$

$$\tilde{s}(c) = (y - c\mathcal{H}_2)\breve{\mathcal{H}}_1 \tag{5.17}$$

Equation 5.16 is exactly *zero forcing approximation* applied to get an approximate of *s* from Equation 5.14. A zero forcing is a *pseudo-inverse process* which helps to find the inverse of non-square matrices. Thus, in Equation 5.16 $\breve{\mathcal{H}}_1$ is the pseudo-inverse of H1. After multiplying both sides of Equation 5.14 by $\tilde{\mathcal{H}}_1$ and leaving *s* alone, get

$$s = \underbrace{(y - c\mathcal{H}_2)\breve{\mathcal{H}}_1}_{\tilde{s}(c)} - w\breve{\mathcal{H}}_1 \tag{5.18}$$

The first estimate of the pair *s* based on *c* is found by *quantizing* Equation 5.17 and is given as follows.

$$\hat{s}(c) = Q(\tilde{s}(c)) \equiv (Q(\tilde{x}_1(c)), \tilde{x}_3(c))) \tag{5.9}$$

The quantization here is to mean that the real and imaginary components of each complex value are *rounded off* to the nearest pulse amplitude modulation (PAM) alphabet, after separating to its components. For a QAM constellation whose PAM alphabets are $\pm 1, \pm 3, \pm 5, \ldots$, a certain value *x* somewhere between the alphabets can be rounded to the nearest alphabet by $2 * floor(x/2) + 1$.

Substituting the estimate of *S* in the likelihood function, the estimates of **c** will be:

$$\hat{c} = \underset{c \in q}{\arg\min} \left\| y - \hat{s}(c)\mathcal{H}_1 - c\mathcal{H}_2 \right\|^2 \quad , \tag{5.20}$$

$$\hat{s}(\hat{c}) = Q(\tilde{s}(\hat{c})) \equiv (Q(\tilde{x}_1(\hat{c})), \tilde{x}_3(\hat{c})))$$

If the likelihood function is maximized with respect to *s* given *c*, we obtain the estimate

$$\hat{s} = \underset{s \in q}{\arg\min} \left\| y - s\mathcal{H}_1 - \hat{c}(s)\mathcal{H}_2 \right\|^2, \tag{5.21}$$

$$\hat{c}(\hat{s}) = Q(\tilde{c}(\hat{s})) \equiv (Q(\tilde{x}_2(\hat{s})), \tilde{x}_4(\hat{s})))$$

where,

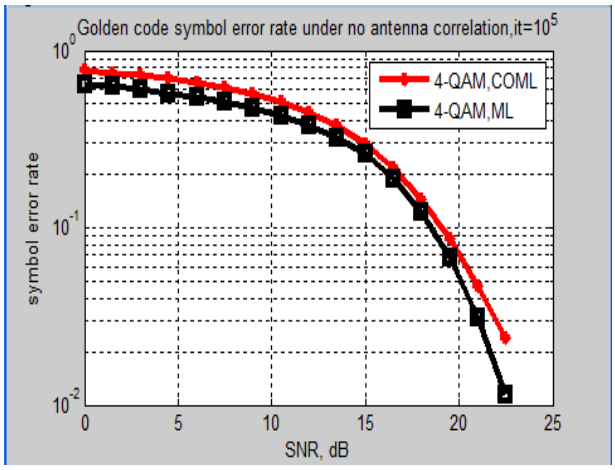
$$\tilde{c}(s) = (y - s\mathcal{H}_1)\breve{\mathcal{H}}_2 \tag{5.22}$$

Equations 5.20 and 5.21 each provide an algorithm for obtaining the estimate of x_i, i = 1, . . . , 4, each of which involves at most q^2 evaluations of the right hand side of their respective equation. Now we have both of them as possible decoding solutions. Whenever $\mathcal{H}_i\mathcal{H}_i^{\hbar}$'s are multiples of identity matrix, all of the optimizations Equations 5.20 and 5.21 would be exact ML and we would not need to make a choice. However, as we are making a zero forcing approximation, we need to choose the best alternative for each channel. One approach is to compute both alternatives and take the alternative which maximizes the likelihood. The key to the current algorithm is that due to the structure of the code one of the two estimates is good, i.e., essentially ML, with very high probability [17].

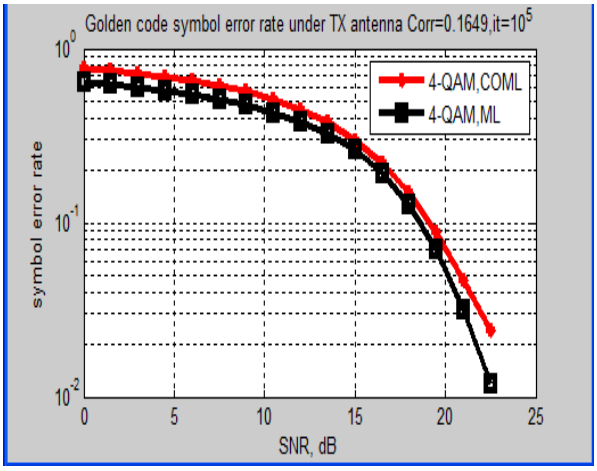
The accuracy of the quantization depends on both the *determinant* (which determines signal to noise ratio) and *condition number* (which determines the accuracy of the zero forcing approximation) of $\mathcal{H}_i\mathcal{H}_i^{\hbar}$ [17].

The computation can be reduced to two by deciding one of the two estimates based on the channel. A possible criterion is to choose to quantize the variables corresponding to the H_i with the largest value of $det(\mathcal{H}_i\mathcal{H}_i^{\hbar})$.

Thus, as the Golden code is constructed from QAM based information symbols, the computational complexity of the quantization is $o(1)$ that the algorithm involves at most q^2 evaluations of the likelihood function.



(a) Uncorrelated antenna case



(b) Transmit antenna correlated ($\sigma = 0.1649$)

Figure 5.2: Symbol error rate of COML and ML decoding of the Golden code under uncorrelated and transmit antenna correlated cases

5.3 Simulation Setup of the COML decoding of the Golden code

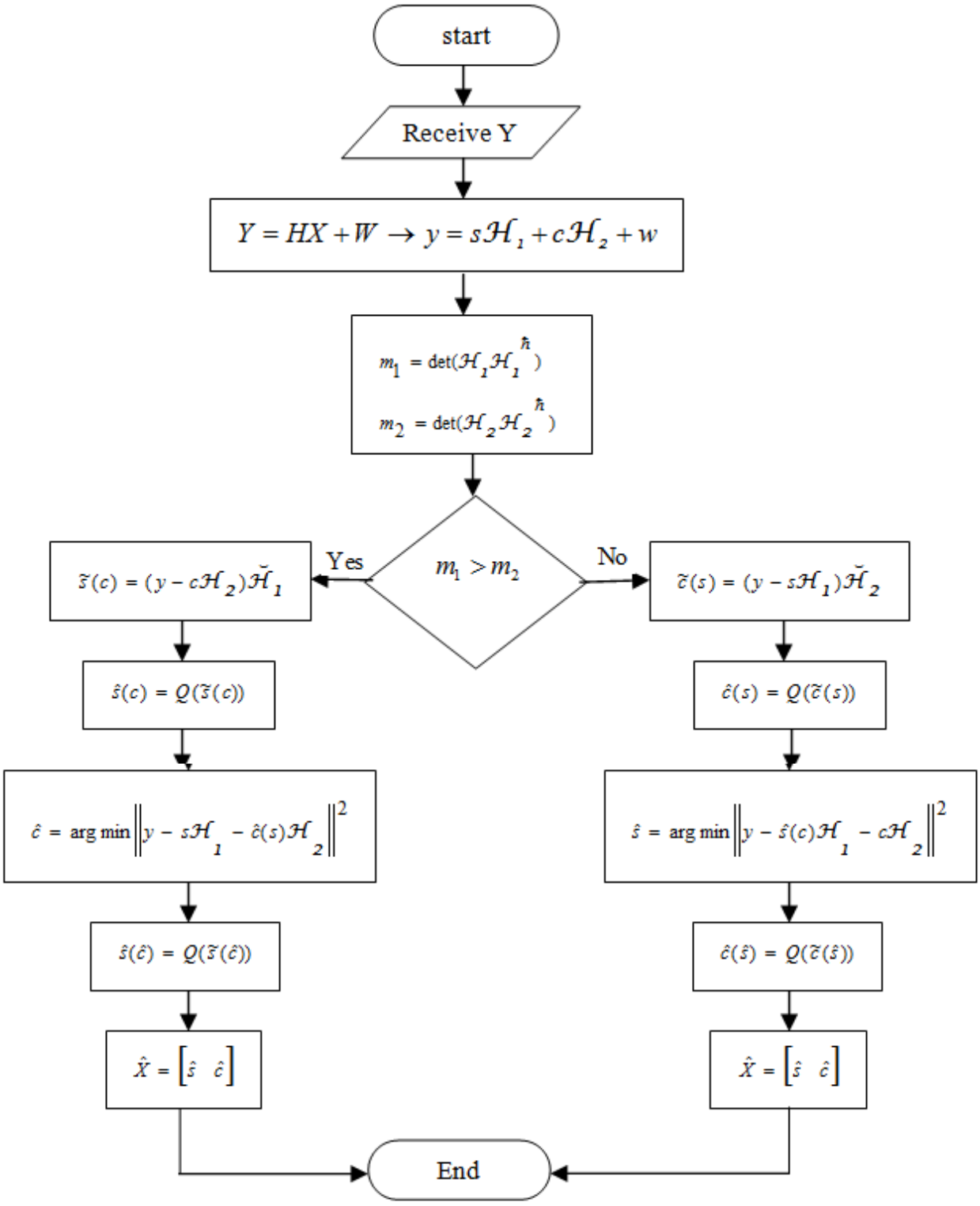


Figure 5.3: COML decoding set up of Golden code

5.4 Simulation results

We compared the performance of the COML decoder with ML for the Golden code. We assumed a Rayleigh fading quasi-static channel model that is known only by the receiver. The channel fading coefficients are considered to be samples of independent complex Gaussian variables with zero mean and variance of 0.5 for real dimension. And the noise is assumed to be a complex AWGN with zero mean and variance of N_0. The SNR at a receive antenna is given by

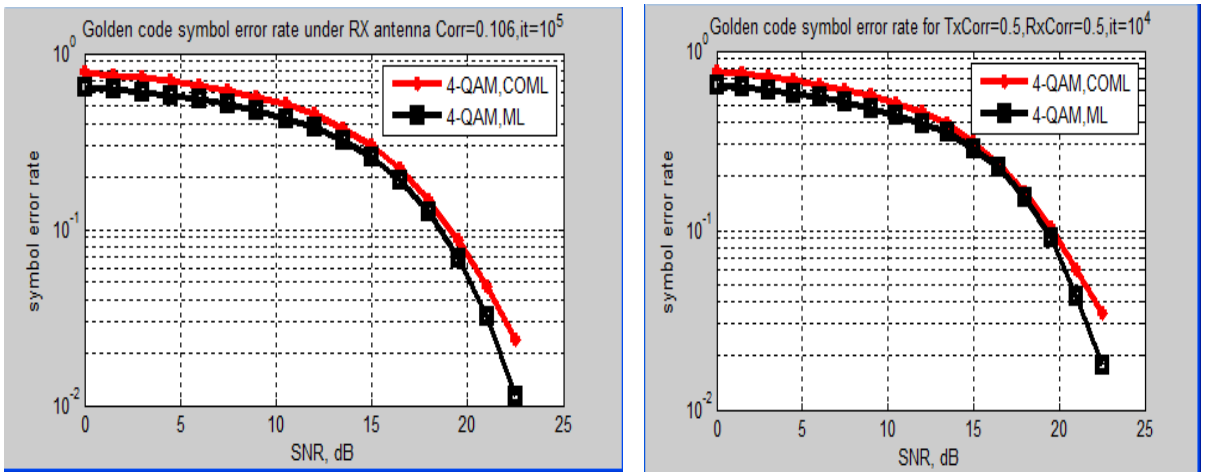
$$SNR(dB) = 10\log_{10}\left(\frac{P_s}{N_0}\right) \tag{5.23}$$

Where, P_s is the average signal power per symbol at a receive antenna which is given by

$$P_s = E_s\left(\left\|\mathcal{H}_1\right\|^2 + \left\|\mathcal{H}_2\right\|^2\right) \tag{5.24}$$

Where, E_s is the average energy per symbol.

In Figure 5.2, we show the symbol error rate of the Golden code under uncorrelated as well as transmit antenna conditions for 4-QAM as a function of SNR. The simulation shows that the performance of the Golden code using COML decoding is near ML. Next, we compared the performance of the code under receive antenna as well as both transmit and receive antenna correlations as shown in Figure 5.4.

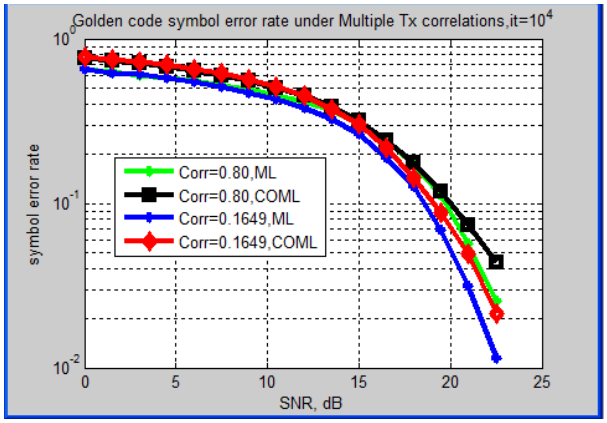


(a) Receiver antenna correlated ($\delta = 0.106$)

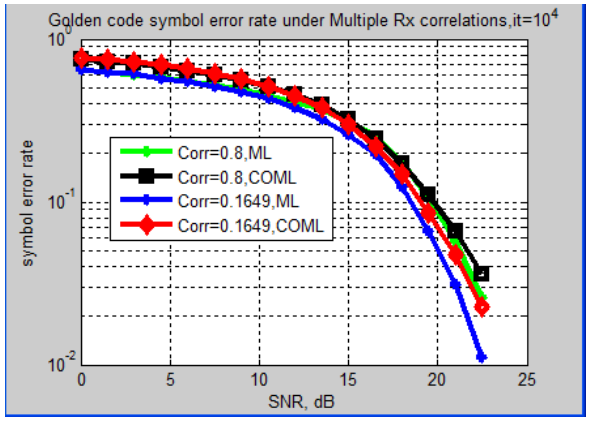
(b) Transmit and Receive antenna correlated ($\sigma = 0.5, \delta = 0.5$)

Figure 5.4: Symbol error rate of COML and ML decoding of the Golden code under receive and both transmit and receive antenna correlated cases

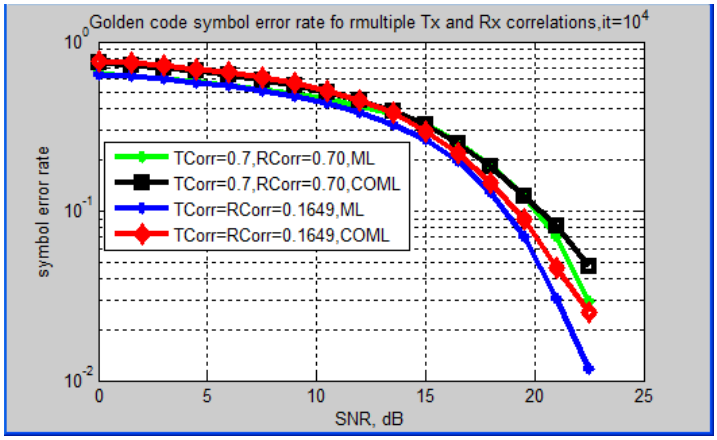
Further, in Figure 5.5, we simulated the performance of the Golden code under multiple correlation coefficients to show the relative impact on performance. We observed that the performance of the COML decoding of the Golden code is equally affected as of ML decoding by the nature of antenna correlations.



(a) Multiple transmit antenna correlations ($\sigma = 0.8, \sigma = 0.1649$)



(b) Multiple receive antenna correlations ($\delta = 0.8, \delta = 0.1649$)



(c)Multiple transmit and receive antenna correlations ($\sigma = 0.7, \delta = 0.7$) and ($\sigma = 0.1649, \delta = 0.1649$)

Figure 5.5: Symbol error rate of COML and ML decoding of the Golden code under multiple transmit, receive and both transmit and receive antenna correlated cases

The results in the literature are for uncorrelated antenna conditions only. Here, we also considered the impact of antenna correlation on performance of the COML against ML. Although our result of Figure 5.5 (a) is not exact as of the result of [17] in the literature, which could most probably be because of the accuracy of the QAM quantizer that we used, we conclude that the performance deviation of the COML decoding from the ML is negligible when compared with its high reduction in complexity.

CHAPTER SIX

6 CONCLUSION

In this thesis, we investigated the theory as well as the coding application of CDA with an aim of constructing PSTBCs which are the most efficient STBCs. Furthermore, we investigated the performance of COML as a near ML yet a lesser complexity decoding scheme for PSTBCs as taking Golden code as an example.

MIMO systems increase the rate as well as improve the reliability and robustness of a system compared to single antenna systems. We saw that employing *diversity techniques* enable to better harness MIMO systems to combat *multipath fading* problems. *Space-time diversity* is the best among different diversity techniques for its minimum delay, no additional band width and resource requirements. STBCs are preferred over other STCs due to their decoding simplicity as well as good performance.

The most important desired characteristics of STBCs are rate, MG, DG, CG and decoding complexity. Based on these desired characteristics, we saw three fundamental design criteria: the *rank criterion*, the *determinant criterion* and the *decoding complexity*. The rank criterion, related to the DG of the system, is an approximate measure of the power saved when using diversity over without diversity. In Figure 2.2, the slope of the error curve decreases as the CG increases which shows that STBCs with higher DG have a *steep descent curve* of error probability characteristics than lower DG codes. On the other hand, in Figure 2.3, the whole error probability plot is shifted down as the CG increases, which means that the determinant criterion seeks high CG so as to improve the performance of the system by *completely shifting* the error curve to the left. Decoding complexity, as a third design criterion, is measure of the number of metric computations to reach ML decision or the area required to implement an algorithm should be small as possible. We saw that for the same number of decodable information symbols, STBCs *with highest number of separable groups* are the least complex. In addition, STBCs with good constellation shaping, NVD and that satisfy DMT have better performance.

Thus, based on the performance matrices, we showed that PSTBCs are the most efficient STBCs; they are fully diverse, high rate, NVD, DMT satisfying with energy efficient constellation shaping and with uniform power per transmit antenna. We also saw the mathematical algebra necessary to construct the PSTBCs. The three most common algebraic structures are groups, rings and fields. *Non-commutative* Rings whose non-zero elements are all invertible are called *skew field* or *division algebra*. CDAs, single element generated finite field extensions of Q, have a structure that is suitable for coding purpose. The norm of an algebraic element is away to verify the diversity property of CDA-based codes. In addition, we saw that the integer part (*ring of integers*) of number fields have a structure which is suitable to achieve NVD codes. They have special patterns, called *lattices* which help to control the power of transmitted signals. By further properly restricting the shape of the algebraic lattices, simple *bit labeling procedure* and high power saving can be achieved. We saw that one way of achieving this is by rotating Z^n lattices. *Cyclotomic* constructions are families of rotated lattices which are obtained by dividing a circle into equal parts.

Then after, we investigated the explicit construction of the PSTBCs for lower antenna dimensions based the concept of CDA. We showed the respective generating element, CDA, rotated lattice, codeword and the minimum determinant of the PSTBCs. We observed that most of the PSTBCs are fully diverse when the information symbols are taken from of $Z[i]^n$ or QAM constellation.

Moreover, in this thesis, we investigated the performance of Golden code, as an example of the PSTBCs, by applying COML decoder. The simulation results showed that the COML decoding of Golden code has almost equal performance as of ML with a reduced complexity of $o(q^2)$, which is $o(q^4)$ for an exhaustive ML. The performance of the Golden code was simulated under uncorrelated and correlated antenna conditions. We conclude that the impact of transmit antennas and receive antenna s correlations on the performance of the Golden code are almost similar. Moreover, in all cases, the performance of COML decoding against

ML, is consistent that it is not affected by the variation of antenna correlation scenarios.

In general, in this thesis, we investigated that the PSTBCs are the most optimal codes in terms of the design criteria of STBCs as of the objective of the thesis. In addition, the COML decoding of the PSTBCs is essentially ML, with slight deviation, yet with complexity reduction of $o(q^n)$ from the conventional ML decoding.

Appendix A

Detail computations related to 3x3 PSTBC

The basis reduction in Equation 4.9 is given as follows:
Note that

$$\sum_{k=0}^{p-1}\zeta_p^k = 1+\zeta_p^1+\ldots+\zeta_p^{p-1}=0 \iff 1+2\sum_{k=1}^{n=(\frac{p-1}{2})}\cos(\frac{2\pi k}{p})=0$$

Thus, $\theta_3^{\,2}+\theta_3^{\,3}=\theta_3^{\,2}(1+\theta_3)=(\zeta_7^1+\zeta_7^{-1})^2(1+\zeta_7^1+\zeta_7^{-1})$

$$=(1+\zeta_7^1+\zeta_7^2+\zeta_7^3+\zeta_7^{-3}+\zeta_7^{-2}+\zeta_7^{-1})+1+2(\zeta_7^1+\zeta_7^{-1})$$

From $\zeta_7^7=1$ and multiplying both sides by ζ_7^{-1}, ζ_7^{-21} & ζ_7^{-3} respectively, we get the equivalent positive exponent & negative exponent expressions: $\zeta_7^6=\zeta_7^{-1}$, $\zeta_7^5=\zeta_7^{-2}$ & $\zeta_7^4=\zeta_7^{-3}$.

Substituting their equivalent for the negative exponents, we obtain

$$\theta_3^{\,2}+\theta_3^{\,3}=\underbrace{(1+\zeta_7^1+\zeta_7^2+\zeta_7^3+\zeta_7^4+\zeta 5+\zeta_7^6)}_{0}+\underbrace{1+2(\zeta_7^1+\zeta_7^{-1})}_{1+2\theta_3}=1+2\theta_3.$$

The reduced expression will be

$$b_3=1+2\theta_3+m\theta_3^{\,2} \tag{A.1}$$

The determination of the trace of $1,\theta_3$ and θ_3^2 in Equation 4.11 can be done as follows:

$$Tr_{Q(\theta_3)/Q}(1)=\sum_{k=1}^{3}\sigma_k(1)=\sigma_1(1)+\sigma_2(1)+\sigma_3(1)=1+1+1=3$$

$$Tr_{Q(\theta_3)/Q}(\theta_3)=\sum_{k=1}^{3}\sigma_k(\theta_3)=\sigma_1(\theta_3)+\sigma_2(\theta_3)+\sigma_3(\theta_3)=2\cos(\frac{2\pi}{7})+2\cos(\frac{4\pi}{7})+2\cos(\frac{6\pi}{7})=-1.$$

$$Tr_{Q(\theta_3)/Q}(\theta_3^{\,2})=\sum_{k=1}^{3}\sigma_k(\theta_3^{\,2})=\sigma_1(\theta_3^{\,2})+\sigma_2(\theta_3^{\,2})+\sigma_3(\theta_3^{\,2})$$

Using property of ring homomorphism in Equation 3.1, we obtain

$$=\sigma_1(\theta_3)\sigma_1(\theta_3)+\sigma_2(\theta_3)\sigma_2(\theta_3)+\sigma_3(\theta_3)\sigma_3(\theta_3)$$

$$=\sigma_1(\theta_3)^2+\sigma_2(\theta_3)^2+\sigma_3(\theta_3)^2$$

$$Tr(\theta_3^2)=4\cos^2(\frac{2\pi}{7})+4\cos^2(\frac{4\pi}{7})+4\cos^2(\frac{6\pi}{7})=4.992\approx 5. \tag{A.2}$$

Next, Let us find the elements of the Gram matrix in Equation 4.12. The elements are given by $g_{ij}=Tr_{E/Q(j)}(b_i'\overline{b_j'})$. As the matrix is an identity matrix, only we need to compute the diagonal elements.

$$g_{11}=Tr_{E/Q(j)}(b_1'\overline{b_1'})=Tr((1+m+\theta_3)(\overline{1+m+\theta_3})),$$

Note that $b_1' = 1 + j + \theta_3 = (\frac{1}{2} + \theta_3) + i\frac{\sqrt{3}}{2}$ and $\overline{b_1'} = (\frac{1}{2} + \theta_3) - i\frac{\sqrt{3}}{2}$.

So, $b_1'\overline{b_1'} = \left((\frac{1}{2} + \theta_3) + i\frac{\sqrt{3}}{2}\right)\left((\frac{1}{2} + \theta_3) - i\frac{\sqrt{3}}{2}\right) = 1 + \theta_3 + \theta_3^2$

Thus, $g_{11} = Tr_{E/Q(j)}(b_1'\overline{b_1'}) = Tr(1 + \theta_3 + \theta_3^{\,2}) = Tr(1) + Tr(\theta_3) + Tr(\theta_3^{\,2}) = 3 - 1 + 5 = 7$

Similarly, $g_{22} = Tr_{E/Q(j)}(b_2'\overline{b_2'}) = Tr(2 - \theta_3) = 7$

$$g_{33} = Tr_{E/Q(j)}(b_3'\overline{b_3'}) = Tr(4 - \theta_3^2) = 7 \qquad \text{(A.3)}$$

The Gram matrix, therefore, is given by $G = 7I_3$.

Elements of the generator matrix in Equation 4.13 are given by $M_{kl} = \frac{1}{\sqrt{7}}\sigma_l((b_k'))_{k,l=1}^3$.

$$M_{11} = \frac{1}{\sqrt{7}}\sigma_1(b_1') = \frac{1}{\sqrt{7}}\sigma_1(1 + m + \theta_3) = \frac{1}{\sqrt{7}}(1 + \frac{(-1 + i\sqrt{3})}{2} + 2\cos(\frac{2\pi}{7}))$$

$$= \frac{1}{\sqrt{7}}\left(\left[\frac{1}{2} + 2\cos(\frac{2\pi}{7})\right] + \frac{i\sqrt{3}}{2}\right) = 0.6603 + 0.32733i$$

$$M_{12} = \frac{1}{\sqrt{7}}\sigma_2(b_1') = \frac{1}{\sqrt{7}}\sigma_2(1 + m + \theta_3) = \frac{1}{\sqrt{7}}(1 + \frac{(-1 + i\sqrt{3})}{2} + 2\cos(\frac{2(2\pi)}{7}))$$

$$= \frac{1}{\sqrt{7}}\left(\left[\frac{1}{2} + 2\cos(\frac{4\pi}{7})\right] + \frac{i\sqrt{3}}{2}\right) = 0.02077 + 0.32733i$$

$$M_{13} = \frac{1}{\sqrt{7}}\sigma_3(b_1') = \frac{1}{\sqrt{7}}\sigma_3(1 + m + \theta_3) = \frac{1}{\sqrt{7}}(1 + \frac{(-1 + i\sqrt{3})}{2} + 2\cos(\frac{3(2\pi)}{7}))$$

$$= \frac{1}{\sqrt{7}}\left(\left[\frac{1}{2} + 2\cos(\frac{6\pi}{7})\right] + \frac{i\sqrt{3}}{2}\right) = -0.49209 + 0.32733i \qquad \text{(A.4)}$$

The rest of the entries are determined and in the same manner.
By Considering the rotational matrix, $R_3 = [0 \quad 1 \quad 0 \quad ; \quad 0 \quad 0 \quad 1 \quad ; \quad m \quad 0 \quad 0]$, the expansion of the codeword, X_3 in Equation 4.14 is shown below, in appendix A.5.

Let us evaluate the expansion for each value of k. For the sake of simplicity, let's represent the entries of the generator matrix as

$$, M_3 = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

For k=0, $X_0 = diag\left(M_3 \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} \right) R^0 = diag\left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} \right)$

$$\Rightarrow X_0 = diag\left(\begin{bmatrix} a_{11}x_0 + a_{12}x_1 + a_{13}x_2 \\ a_{21}x_0 + a_{22}x_1 + a_{23}x_2 \\ a_{31}x_0 + a_{32}x_1 + a_{33}x_2 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} \right) = \begin{bmatrix} c_0 & 0 & 0 \\ 0 & c_1 & 0 \\ 0 & 0 & c_2 \end{bmatrix}$$

For k=1,

$$X_1 = diag\left(M \begin{bmatrix} x_3 \\ x_4 \\ x_5 \end{bmatrix} \right) R^1 = diag\left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} c_3 \\ c_4 \\ c_5 \end{bmatrix} \right) \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ m & 0 & 0 \end{bmatrix}$$

$$\Rightarrow X_1 = \begin{bmatrix} c_3 & 0 & 0 \\ 0 & c_3 & 0 \\ 0 & 0 & c_3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ m & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & c_3 & 0 \\ 0 & 0 & c_4 \\ mc_5 & 0 & 0 \end{bmatrix} \quad \text{and}$$

For k=2,

$$X_2 = diag\left(M_3 \begin{bmatrix} x_6 \\ x_7 \\ x_8 \end{bmatrix} \right) R^2 = diag\left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} c_6 \\ c_7 \\ c_8 \end{bmatrix} \right) \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ m & 0 & 0 \end{bmatrix}^2$$

$$\Rightarrow X_2 = \begin{bmatrix} c_6 & 0 & 0 \\ 0 & c_7 & 0 \\ 0 & 0 & c_8 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ m & 0 & 0 \\ 0 & m & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & c_6 \\ mc_7 & 0 & 0 \\ 0 & mc_8 & 0 \end{bmatrix}$$

The codeword for 3x3 PSTBC is, therefore, given by

$$X_3 = X_0 + X_1 + X_2 = \begin{bmatrix} c_0 & c_3 & c_6 \\ mc_7 & c_1 & c_4 \\ mc_5 & mc_8 & c_2 \end{bmatrix}. \qquad \text{(A.5)}$$

Note the pattern of the entries along the diagonals. Only entries below the main diagonal are multiplied by *m* required to obtain full diversity yet satisfy the uniform power allocation for each transmit antenna or average energy of each symbol.

$$E_1 = \|c_0\|^2 + \|c_3\|^2 + \|c_6\|^2 \quad E_2 = \|mc_7\|^2 + \|c_1\|^2 + \|c_4\|^2 \quad E_3 = \|mc_5\|^2 + \|mc_8\|^2 + \|c_2\|^2$$

Appendix B

Detail computations related to 4x4 PSTBC

The trace of some important terms in Equation 4.18 are computed as:

$$Tr(1) = \sigma_1(1) + \sigma_2(1) + \sigma_3(1) + \sigma_4(1) = 4$$

$$Tr(\theta_4) = \sigma_1(\theta_4) + \sigma_2(\theta_4) + \sigma_3(\theta_4) + \sigma_4(\theta_4).$$

$$= 2[\cos(48) + \cos(24) + \cos(168) + \cos(96)] = 1$$

$$Tr({\theta_4}^2) = \sigma_1({\theta_4}^2) + \sigma_2({\theta_4}^2) + \sigma_3{\theta_4}^2) + \sigma_4({\theta_4}^2)$$

$$= 4[\cos^2(48) + \cos^2(24) + \cos^2(168) + \cos^2(96)] = 9$$

$$Tr({\theta_4}^3) = \sigma_1({\theta_4}^3) + \sigma_2({\theta_4}^3) + \sigma_3({\theta_4}^3) + \sigma_4({\theta_4}^3)$$

$$= 8[\cos^3(48) + \cos^3(24) + \cos^3(168) + \cos^3(96)] = 1$$

$$Tr(\theta^4) = \sigma_1(\theta^4) + \sigma_2(\theta^4) + \sigma_3(\theta^4) + \sigma_4(\theta^4)$$

$$= 16[\cos^4(48) + \cos^4(24) + \cos^4(168) + \cos^4(96)] = 29$$

$$Tr({\theta_4}^5) = \sigma_1({\theta_4}^5) + \sigma_2({\theta_4}^5) + \sigma_3({\theta_4}^5) + \sigma_4({\theta_4}^5)$$

$$= 32[\cos^5(48) + \cos^5(24) + \cos^5(168) + \cos^5(96)] = -4$$

$$Tr({\theta_4}^6) = \sigma_1({\theta_4}^6) + \sigma_2({\theta_4}^6) + \sigma_3({\theta_4}^6) + \sigma_4({\theta_4}^6)$$

$$= 64[\cos^6(48) + \cos^6(24) + \cos^6(168) + \cos^6(96)] = 99 \qquad \text{(B.1)}$$

Some of entries of the generator matrix in Equation 4.20 are computed as follows:

$$M_{11} = \frac{1}{\sqrt{15}}\sigma_1(b_1') = \frac{1}{\sqrt{15}}\sigma_1[1 + i(-3 + {\theta_4}^2)] = \frac{1}{\sqrt{15}}[1 + i(-3 + 4 * \cos^2(48))] = 0.258 - i0.31228$$

$$M_{12} = \frac{1}{\sqrt{15}}\sigma_1(b_2') = \frac{1}{\sqrt{15}}\sigma_1[\theta_4 + i(-3\theta_4 + {\theta_4}^3)] = \frac{1}{\sqrt{15}}[2 * \cos(48) + i(-3 * \cos(48) + 8 * \cos^3(48))] = 0.346 - i0.418$$

$$M_{13} = \frac{1}{\sqrt{15}}\sigma_1(b_3') = \frac{1}{\sqrt{15}}\sigma_1[(-3\theta_4 + {\theta_4}^{3)} + i(-1 + 4\theta_4 - {\theta_4}^3)]$$

$$= \frac{1}{\sqrt{15}}[(-6 * \cos(48) + 8 * \cos^3(48)) + i(-1 + 8 * \cos(48) - 8 * \cos^3(48))] = -0.418 + i0.5051$$

$$M_{44} = \frac{1}{\sqrt{15}}\sigma_4(b_4') = \frac{1}{\sqrt{15}}\sigma_4[(-1 - 3\theta_4 + {\theta_4}^2 + {\theta_4}^3) + i]$$

$$= \frac{1}{\sqrt{15}}[(-1 - 6 * \cos(96) + 4 * \cos^2(96) + 8 * \cos^3(96) + i] = -0.8734 + i0.2582 \qquad \text{(B.2)}$$

The rest of the entries are found in the same manner.

REFERENCES

[1] I.E.Telatar, "Capacity of Multi-Antenna Gaussian Channels", AT&T Bell Labs, http://mars.belllabs.com/cm/ms/what/mars/papers/proof, 1995.

[2] G. J. Foschini, M. J. Gans, "On Limits of Wireless Communications in Fading Environments when Using Multiple Antennas", Wireless Personal Communications, vol. 6, pp. 311-335, March 1998.

[3] M. K. Simon, M.-S. Alouini, *Digital Communication over Fading Channel: A Unified Approach to Performance Analysis*, John Wiley & Sohn, 2000.

[4] T. S. Rappapot, *Wireless Communications: Principles and Practice*, Prentice Hall, 1996.

[5]. V. Tarokh, N. Seshadri, A. R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction", IEEE Trans. Inform. Theory, vol. 44, no. 2, pp. 744-765, March 1998.

[6] S. Alamouti, "A Simple Transmitter Diversity Technique for Wireless Communications", IEEE Journal on Selected Areas of Communications, Special Issue on Signal Processing for Wireless Communications, vol.16, no.8, pp.1451-1458, Oct. 1998.

[7] L. Zheng and D. Tse, "Diversity and Multiplexing: A Fundamental Trade-off in Multiple Antenna Channels," IEEE Trans. on Inf. Theory, vol. 49, no 4, pp. 1073-1096, May 2003.

[8] H. E. Gamal and M. O. Damen, "Universal Space-Time Coding," IEEE Trans. Inf. Theory, vol. 49, no. 5, pp. 1097-1119, May 2003.

[9]. B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate s pace-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596– 2616, October 2003.

[10]. F. Oggier, G. Rekaya, J.C. Belfore, and E. Viterbo, "Perfect Space Time Block Codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, Sep.2006.

[11] B. Hassibi and B.M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol.48, no.7, pp. 1804-1824, July 2002.

[12]. P. Elia, B. A. Sethuraman, and P.V. Kumar, "Perfect Space–Time Codes for Any Number of Antennas," *IEEE Trans. Inf. Theory*, Vol. 53, No. 11, 2007.

[13] P. W. Wolniansky, G. J. Foschini, G. D. Golden, and R. A. Valenzuela, "V-BLAST: An architecture for realizing very high data rates over the rich-scattering wireless channel," *in Proc. ISSSE*, 1998, pp. 295–300

[14] M. O. Damen, A. Chkeif, and J. C. Belfiore, "Lattice codes decoder for space-time codes," *IEEE Comm. Lett.*, vol. 4, no. 5, pp. 161–163, May 2000.

[15] A. D. Murugan, H. E. Gamal, M. O. Damen, and G. Caire, "A unified framework for tree search decoding: rediscovering the sequential decoder," *IEEE Trans. Inf. Theory*, vol.52, no. 3, pp.933-953, Mar. 2006.

[16] J.Hu and H. Zhang, "Efficient Decoder for Perfect Space-Time Codes," *Communication Networks and Services Research Conference*, pp. 249 – 254, 2008

[17] S. Sirianunpiboon, A. R. Calderbank, and S. D. Howard, "Fast essentially maximum likelihood decoding of the golden code," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, June 2011.

[18] S. Sirianunpiboon, A. R. Calderbank, and S. D. Howard, "Low complexity essentially maximum likelihood decoding of perfect space-time block codes," *submitted to IEEE Trans. Inf. Theory*, 2008

[19] S. Sirianunpiboon, Y. Wu, A. R. Calderbank, and S. D. Howard, "Fast optimal decoding of multiplexed orthogonal designs by conditional optimization, "*IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1106–1113,Mar. 2010.

[20] A. Wittneben, "A New Bandwidth Efficient Transmit Antenna Modulation Diversity Scheme for Linear Digital Modulation," *IEEE International Conference on Communications*, vol. 3, pp. 1630-1634, Geneva, Switzerland, May 1993.

[21]V. Tarokh, H. Jafarkhani and A. Calderbank, "Space-Time Block Codes From Orthogonal Designs," *IEEE Trans. on Inf. Theory*, vol. 45, no. 5, pp. 1456-1467, July 1999.

[22] X.-B. Liang, "Orthogonal Designs with Maximal Rates," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 24682503, Oct. 2003.

[23] M. O. Damen, K. Abed-Meraim, and J.C. Belfiore, "Diagonal Algebraic Space-Time Block Codes," *IEEE Trans. on Inf. Theory*, vol. 48, no. 3, pp. 628-636, Mar. 2002

[24] H. Jafarkhani, "A Quasi-orthogonal Space-Time Block Code," *IEEE Trans. Communications*, vol. 49, no. 1, pp. 14, Jan. 2001.

[25] N. Sharma and C. Papadias, "Improved Quasi-orthogonal Codes through Constellation Rotation," *IEEE Trans. Communications*, vol. 51, no. 3, pp. 332-335, Mar. 2003.

[26] W. Su and X.-G. Xia, "Signal Constellations For Quasi-orthogonal Space-Time Block Codes With Full Diversity," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2331-2347, Oct. 2004.

[27] D. Dao, C. Yuen, C. Tellambura, Y. Guan, T. T. Tjhung, "Four-Group Decodable Space-Time Block Codes," *IEEE Trans. Signal Processing*, vol. 56, pp. 424-430, Jan. 2008

[28] M. O. Damen, H. E. Gamal and N. C. Beaulieu, "Linear Threaded Algebraic Space- Time Constellations," *IEEE Trans. Inf. Theory*, vol. 49, pp. 2372-2388, Oct. 2003.

[29] P. Elia, B. A. Sethuraman and P. Kumar, "Perfect Space-Time Codes with Minimum and Non-Minimum Delay for any Number of Transmit Antennas, *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853-, Nov. 2007.

[30] V. Branka, Y.Jinhong, *space time coding,* John Wiley's and Sons, 2003, available in hard copy at Addis Ababa Institute of technology main library.

[31] J.-C. Belfore, F. Oggier and E.Viterbo, Cyclic Division Algebras: a Tool for Space-Time Coding, Jan. 2007.

[32] M. O. Sinnokrot,"space-time block codes with low maximum-likelihood decoding complexity," dissertation, Georgia Institute of Technology, Dec. 2009.

[33] F. Oggier and E.Viterbo, "Algebraic Number Theory and Code Design for Rayleigh Fading Channels,"*Foundations and Trends in Communications and Information Theory*, 2004.

[34] F. Oggier and B. Hassibi, "An algebraic coding scheme for wireless relay networks with multiple-antenna nodes," *submitted to IEEE Trans. on Signal Processing*, Mar. 2006.

[35] P. Elia, K. Raj Kumar, S.A. Pawar, P. Vijay Kumar, and H.-F. Lu., "Explicit, minimum-delay space-time codes achieving the diversity-multiplexing gain trade-off," *Proceedings of Wireless Communications*, 2005.

[36] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar and H.-F. Lu, "Explicit, Minimum- Delay Space-Time Codes Achieving the Diversity-Multiplexing Gain Trade-off," *IEEE Trans. on Inf. Theory*, vol. 52, pp. 3869-3884, 2006.

[37] D. Gesbert, *M.* Shafi, D.Shiu, P.T. Smith and A. Naguib, "From Theory to Practice: An Overview of MIMO Space–Time Coded Wireless Systems," *IEEE journal on selected areas in communications*, vol. 21, no. 3, Apr.2003.

[38] Space-Time Block Coding for Multiple Antenna Systems, Wien university PhD dissertation, November 2005.

[39] G. Ganesan and P. Stoica, "Space-Time Block Codes: A Maximum SNR Approach," *IEEE Trans. on Inf. Theory*, vol. 47, pp. 1650-1656, May 2001.

[40] M. O. Damen and N. C. Beaulieu, "On Diagonal Algebraic Space-Time Block Codes, *IEEE Trans. Communications*, vol. 51, no. 6, pp. 911-919, June 2003.

[41] O. Tirkkonen, "Optimizing Space-Time Block Codes By Constellation Rotations," *in Proc.Finnish Wireless Commun. Workshop (FWCW)*, Finland, pp. 59-60, Oct. 2001.

[42] N. Sharma and C. Papadias, "Full Rate Full Diversity Linear Quasi-Orthogonal Space-Time Codes For Any Transmit Antennas," *EURASIP Journal Applied Signal Processing*, no. 9, pp. 1246-, Aug. 2004.

[43] M. O. Damen, H. E. Gamal and N. C. Beaulieu, "Linear Threaded Algebraic Space-Time Constellations," *IEEE Trans. Inf. Theory*, vol. 49, 2003.

[44] I.N. Stewart and D.O. Tall, *Algebraic Number Theory*, Chapman and Hall, 1979.

[45] E. B.-Fluckiger, *Lattices and number fields*, *Contemporary Mathematics*, 1999.

[46] E. B.-Fluckiger, F. Oggier, and E. Viterbo, "New algebraic constructions of rotated Z^n lattice constellations for the Rayleigh fading channel," *IEEE Trans. on Inf. Theory*, vol. 50, no. 4, pp.702-714, 2004.

[47] J. H. Conway and N.J.A Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1988.

[48] J. Boutros and E. Viterbo,"Rotated multidimensional QAM constellations for Rayleigh fading channels," *IEEE Proceedings on Inf. Theory Workshop*, 1996.

[49] X. Giraud, E. Boutillon, and J.-C. Belfiore, "Algebraic tools to build modulation schemes for fading channels," *IEEE Trans. on Inf. Theory*, vol. 43, n. 3, pp. 938–952, 1997.

[50] L. C. Washington, Introduction to Cyclotomic Fields. Springer-Verlag, New York,1982.

[51] R.J. Goodman, the queen of mathematics: a historically motivated guide to number theory, Welesley, 1998, available in hard copy at AAU Science Faculty Library.

[52] J.-C. Belfiore, G. Rekaya, and E. Viterbo, "The golden code: A 2x2 full-rate space-time code with non- vanishing determinants," *IEEE Trans. on Inf. Theory*, vol. 51, no. 4, Apr. 2005.

[53] P. Dayal and M.K. Varanasi,"An optimal two transmit antenna space-time code and its stacked extensions," *Proceedings of Asilomar Conf. on Signals, Systems and Computers*, 2003.

[54] P Elia, K. Raj Kumar, H.-F. Lu,"Explicit Space-Time Codes that Achieve the Diversity-Multiplexing Gain Tradeoff," *IEEE*, 2005.