On Coding Gain of STBC's from Field Extensions

A Project Report

Submitted in partial fulfilment of the

requirements for the Degree of

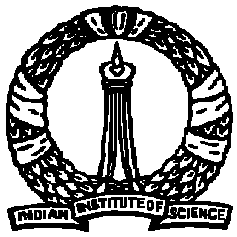
Master of Engineering (Telecommunications)

in

Electrical Communication Engineering

by

Subrahmanyam K



Department of Electrical Communication Engineering

Indian Institute of Science, Bangalore

Bangalore – 560 012 (INDIA)

JANUARY 2003

Acknowledgements

I am greatly indebted to my guide *Dr.B.Sundar Rajan*, who has guided me for this project work. His clear thinking and enthusiasm towards work have been really inspiring. Discussions with him have always motivated me to make deeper investigations into the problem. I would like to thank my lab mates Zafar, Sripati, Shashidhar, *Antenna* and *Proffie* for the technical as well as non-technical discussions. Working in the *Coding & Modulation Lab* has been enjoyable with Shashi, *Antenna* and *Proffie* around.

I would like to thank the IISc Community for giving me such a memorable time here for the past year and half. I owe my thanks to Kiran, who is truly a nice person to be with. Thanks are also due to Chash, CT, Sathish etc. of the *Bowschash Group* and Easwaran, Pandu, Siddu etc. of the *Crossword Fraternity*, for I had a great time with each and everyone of them.

I have to thank *Appa*, *Ammai* and *Vandukkutty* for being with me all along, and giving me constant encouragement.

Abstract

The rapid progress in Wireless Communication has created greater demand for better service, which motivates the need for higher data rates. As it has been shown, multiple antenna systems promise immense capacity and Space-Time Block Codes (STBC's) have emerged as a popular tool to tap the same. Research has been on for constructing transmission schemes providing better performance. Of late, algebraic techniques have come to the fore in the field of STBC Designs.

In this thesis work, we study the coding gains and certain other salient features of a class of STBC's from field extensions of the rational field $\mathbb{Q}$, the coding gain being the most important performance measure of an STBC after diversity. The relationship between codes from field extensions and certain other codes based on algebraic techniques, was also studied. We study the feasibility of certain Generalized transforms to improve the Peak-to-Average Power Ratio(PAPR) of Diagonal Algebraic Space-Time(DAST) codes.

Specifically, the contributions (new results) of this thesis are

- We provide a closed form expression for the coding gain for a sub-class of STBC's from field extensions [26].
- We provide an upper bound for the coding gain for a class of High-Rate STBC's which subsumes the High-Rate STBC's from field extensions.
- We show that DAST and Space-Time Constellation-Rotating(STCR) Codes are a subclass of the codes from field extensions [26].
- The Threaded Algebraic Space-Time(TAST) codes are shown to be *not* the same as High-Rate STBC's from field extensions.
- The Generalized Reverse Jacket Transform(GRJT) is shown *not* to provide any improvement in the PAPR of codes like DAST.

Contents

Chapter 1

Introduction

1.1 Motivation

The advancement in the area of Electronics and Telecommunication has been immense in the last couple of decades. The world saw revolutionary new methods of communication being implemented and more commonly used. Mobile communication has become more accessible to the common man. The increase in subscribers and the need for better services motivates the engineers into better wireless communication techniques.

The advent of Wireless Communication opened up a whole new set of challenges for the communication engineers. The main reason was because of the multipath fading channel. Other technical constraints were due to limited power availability in the hand-held devices, demand and competition for better QoS, restricted bandwidth etc. Research going on in various areas such as coded modulation, channel access protocols, receiver processing etc. have helped the above causes.

In this chapter, we discuss the main reason of concern for the engineers–the wireless channel. We discuss the so-called diversity schemes which promise to overcome the challenge posed by fading channels. We describe why multiple antenna systems help us to get better diversity and data rates and give a short introduction to Space-Time Codes. At the end of the chapter, we comment on how the rest of the thesis is organized.

1.2 The Wireless Channel

The wireless channel, due to the presence of various obstacles in the surroundings, is of unpredictable nature. Reflections and scattering of the radio waves results in multiple paths from transmitter to receiver. The multipaths interfere, combining waves of various strengths and phase, possibly in a destructive fashion, causing severe attenuation [8]. This phenomenon is called *fading*. The channel varies with time, which would bring down the performance (higher probability of error for a given SNR–*Signal to Noise Ratio*) of the system. Note that this is in addition to the additive Gaussian noise of the channel.

The most commonly assumed model for the fading channel is that of Rayleigh fading channel. The transmitted signal undergoes a fading, the magnitude of which is Rayleigh distributed. In the case of Rayleigh fading, for a single transmit and single receive antenna, the probability of error would go down as an inverse linear function of the SNR [7]. For an AWGN channel, the error probability falls down exponentially with respect to SNR. This means we have to provide a large increase in power to get good performance. Else, one could use diversity techniques by which we get better error performances.

1.3 Diversity

To circumvent the problem of fading, we use what is called as diversity. The idea is to send more than one copy of the message. By sending several copies, we reduce the probability of all being in deep fade. Diversity is used in one form or another in all kinds of reliable wireless communications. The introduction of diversity would cause the probability of error to fall in inverse polynomial rate with respect to the SNR rather than inverse linear rate.

Some commonly used diversity techniques are temporal diversity, frequency diversity and spatial diversity.

- *Temporal diversity* is essentially channel coding where you add more bits and also employ interleaving to make sure that they undergo different fades. Here we use

the fact the fading is time-varying and fades would be independent at instances well separated in time.

- *Frequency diversity* makes use of the fact that carriers at different frequencies undergo different fading levels. The signal is transmitted at different frequencies to reduce probability of error.

- *Spatial diversity* is using multiple antennas at transmitter and/or receiver, using the fact that antennas separated enough (spatially) shall experience independent fades.

1.3.1 Space-Time Coding

The work done by Emre Telatar [4] and Foschini and Gans [5] showed that multiple antenna systems possess high capacity over fading channels. The need to transmit in high data rates over wireless channels motivated the need for *Space-Time Codes*. As explained in the previous section, diversity techniques improve performance (probability of error) from the uncoded case. Space-Time codes combine two of the above discussed diversity techniques to get a new approach to combat fading and get high data rates. Here we use multiple transmit as well as receive antennas. Temporal diversity is also used here to improve the performance.

Space-Time Codes essentially consists of coding in both space and time. The input data is sent through multiple antennas, over different time intervals and received through multiple antennas as well [1]. Space-Time codes are broadly classified into two, like their conventional coding counterparts, ie. Space-Time Block Codes (STBC) and Space-Time Trellis Codes (STTC).

Space-Time Block Codes, as their name suggests, map blocks of input message into blocks of coded symbols. ie., coding of one block of input symbol is independent of the other blocks. This means that we have a mapping from blocks of input symbols to block transmission schemes (in space as well as time). Decoding schemes, are generally of polynomial complexity.

Space-Time Trellis Coding uses trellis coding which would indicate the dependence

on the previous blocks of data. The state of the trellis would change depending on the incoming symbols, and this change would determine on the transmitted signals from each antenna at different time instances. Viterbi algorithms are used for decoding.

1.4 Outline of the Chapters

In the next chapter, we look at various existing literature on Space-Time Block Codes and related work. We review the work done in STBC designs and compare the salient features of each. We look more closely into the codes based on algebra and algebraic number theory. Codes over field extensions are explained in detail and a background to Chapter 3 is formed. In Chapter 3, we derive a closed form expression for the coding gain for a special class of codes which form a subset of the codes from the codes over field extensions. Bounds on coding gains of certain other class of codes are also obtained. Chapter 4 looks at some comparison between the High-Rate codes over field extensions and Threaded Algebraic Space-Time codes (TAST). In the following chapter, we try to see the scope for any improvement in the Peak-to-Average Power Ratio(PAPR), for codes like DAST, STCR etc. by using different power distributing matrices. Chapter 6 consists of some concluding remarks. We also give an Appendix in which some background, to the mathematics used in this thesis, is provided.

Chapter 2

STBC's: An overview

In this chapter we shall review some work done on *Space-Time Block Codes* (STBC). First, we shall see the system model followed by the rank and determinant criterion for STBC's [1]. After that, we shall see different types of well known STBC designs.

2.1 System Model

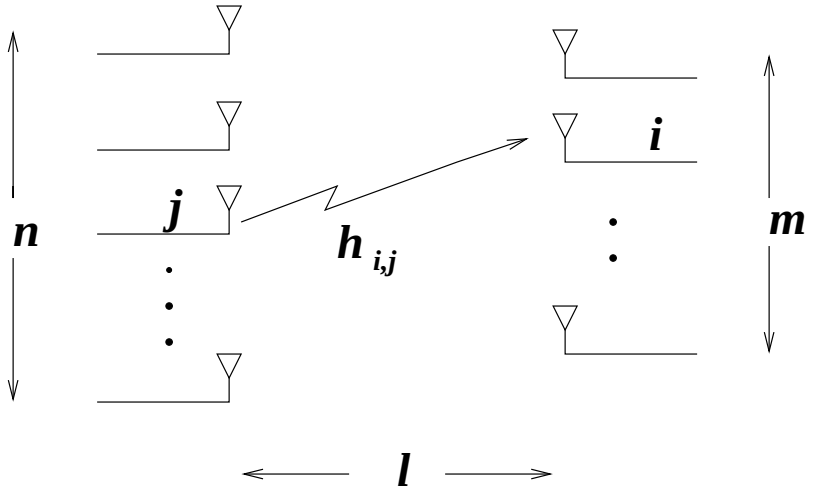


Figure 2.1: Multiple Antenna Transmission/Reception

We consider a system with n transmit antennas and m receive antennas. We shall assume a linear model in which the received vector $\mathbf{x} \in \mathbb{C}^m$ depends on the transmitted

vector $\mathbf{s} \in \mathbb{C}^n$ as follows.

$$\mathbf{x} = H\mathbf{s} + \mathbf{w} \tag{2.1}$$

Here $H \in \mathbb{C}^{m \times n}$ is the channel matrix. It contains the entries h_{ij} which are the fade coefficients from the jth transmit antenna to ith receive antenna. On either transmitter and receiver side, the antennas are sufficiently separated, which results in the fades for each transmit-receive antenna pair being independent. The channel is assumed to be *frequency non-selective* (flat fading). It is assumed that the fading is *quasistatic*, ie. the fade coefficients do not change for l time instances. All the entries of H are complex Gaussian random variables, independent with each other as well as in each dimension, identically distributed, with zero mean and a variance of 0.5 per dimension. Equivalently, each entry of H has magnitude Rayleigh distributed and phase uniformly distributed. Each component of the noise vector $\mathbf{w}$ is a zero mean Gaussian complex random variable with variance $N_0/2$ per dimension.

Definition 2.1 (Space-Time Block Code) *A Space-Time Block Code $\mathcal{C}$ is a finite set of $n \times l$ matrices, whose entries would be complex numbers. The entries of the codeword matrices can be restricted to points from a signal set $\mathcal{S}$. The code is said to* over $\mathcal{S}$ *if some of the entries are independently chosen from $\mathcal{S}$ and the other entries are functions of these. The code is said to be* completely over $\mathcal{S}$ *if all the entries of the codeword matrices are from $\mathcal{S}$. The* rate *of a Space-Time Block Code $\mathcal{C}$ is given by $\frac{1}{l}\log_{|\mathcal{S}|}(|\mathcal{C}|)$ in symbols per channel use.*

In the following sections, we shall see the capacity limits of multiple antenna systems and the code construction criteria for good performance.

2.2 Capacity of Multiple Antenna Systems

The motivation to use multiple antenna systems came mainly from the work done by Emre Telatar in [4] and Foschini and Gans in [5]. The capacity formulas were theoretically calculated and it was found that multiple antenna systems promise very high data rates.

Consider the system model of the previous section. The channel is given by the channel matrix H which is an $m \times n$ complex matrix. From [4], the capacity of the channel (in bits), when Channel State Information (CSI) is not known at the receiver, is given by

$$C = \log_2 \det \left(I_m + \frac{\rho}{n} H H^* \right) \tag{2.2}$$

where ρ is the SNR at each receive antenna.

An interesting case of the above is when $n = m$ and both are large. From [4], the capacity in that case is

$$C \approx n \log_2(1 + \rho) \tag{2.3}$$

We can see that when $n = m$, the capacity grows linearly with n. Further results in [4] show that for a fixed number of transmit (or receive) antennas, the capacity saturates even if we increase the number of receive (or transmit) antennas indefinitely. So capacity, virtually without any limit, can be obtained if one increases both the transmit and receive antennas simultaneously. The capacity aspects of Space-Time Block Codes were specifically studied in [9].

2.3 Performance Criterion

The performance criteria for Space-Time Codes were analysed by Vahid Tarokh *et al.* [1] and J-C Guey *et al.* [2] independently.

Let the signal points, ie. the entries of the matrices be taken from a signal set $\mathcal{S}$, the average signal energy being E_s. Let the additive noise, as mentioned in Section 2.1, have a variance of $N_0/2$ per dimension. Let $\mathbf{r}$ a received $m \times l$ matrix.

The Maximum Likelihood (ML) decoding, here is done by Exhaustive Search by computing the following metric, which is the squared Euclidean distance, over all $n \times l$ codeword matrices $\mathbf{c}$. The metric is

$$d^2(\mathbf{c} \to \mathbf{r}) = \sum_{j=1}^{m} \sum_{t=1}^{l} \left| \sum_{i=1}^{n} h_{j,i} c_t^i - r_t^j \right|^2 \tag{2.4}$$

where c_t^i is the element of codeword matrix $\mathbf{c}$ which was sent at the tth time instant from the ith antenna and r_t^j is an entry of $\mathbf{r}$, which is received at the the tth time instant at the jth antenna.

Let $\mathbf{c}$ and $\mathbf{e}$ be two codeword $(n \times l)$ matrices of the code. Assume Exhaustive Search ML decoding is done as above. In the case of Rayleigh fading and independent fade coefficients, the pairwise probability of error, ie., the probability that $\mathbf{c}$ is transmitted and is wrongly decoded as $\mathbf{e}$ is given by[1]

$$P(\mathbf{c} \to \mathbf{e}) \leq \left(\frac{1}{\prod_{i=1}^{n}(1 + \lambda_i E_s/4N_0)} \right)^m \tag{2.5}$$

where $B(\mathbf{c}, \mathbf{e}) = \mathbf{e} - \mathbf{c}$ and $A = BB^*$. The λ_i's are the eigenvalues of A.

We can simplify the expression in (2.5) as shown. Let r denote the rank of A. Then the kernel of A has dimension $n - r$ and exactly $n - r$ eigenvalues of A are zero. Let the nonzero eigenvalues of A be $\lambda_1, \lambda_2, \ldots, \lambda_r$, then from (2.5) and for high values of $E_s/4N_0$, we get

$$P(\mathbf{c} \to \mathbf{e}) \leq \left(\prod_{i=1}^{r} \lambda_i \right)^{-m} (E_s/4N_0)^{-rm} \tag{2.6}$$

The *diversity advantage* of the system is nothing but the power of the SNR in the denominator of the expression of pairwise error probability, here the diversity advantage is mr. The *coding advantage* is an approximate measure of the gain over an uncoded system operating with the same diversity advantage. Here we can see that a coding advantage of $(\lambda_1 \lambda_2 \cdots \lambda_r)^{1/r}$ is achieved. Note that the rank of A is the same as the rank of $B(\mathbf{c}, \mathbf{e})$. The criteria for good performance can be summarized as follows [1].

- *Rank Criterion:* In order to achieve the maximum diversity mn, the matrix $B(\mathbf{c}, \mathbf{e})$ has to be full rank for any two codewords $\mathbf{c}$ and $\mathbf{e}$. If $B(\mathbf{c}, \mathbf{e})$ has minimum rank of r over the set of any two tuples of distinct codewords, then a diversity of rm is achieved. This rank r is defined as the rank of the code.

- *Determinant Criterion:* Suppose that a diversity of rm is the target. The minimum of rth roots of the sum of the determinants of all $r \times r$ principal cofactors of $A(\mathbf{c}, \mathbf{e}) =$

$B(\mathbf{c},\mathbf{e})B(\mathbf{c},\mathbf{e})^*$ taken over all pairs of distinct codewords $\mathbf{c}$ and $\mathbf{e}$ corresponds to the coding advantage, where r is the rank of $A(\mathbf{c},\mathbf{e})$. For the special case of *full diversity* codes, ie. diversity nm, the minimum of the determinant of $A(\mathbf{c},\mathbf{e})$ taken over all pairs of distinct codewords $\mathbf{c}$ and $\mathbf{e}$ must be maximized.

When an $n \times l$ STBC has rank $r = \min(n, l)$, it is called a *full-rank code*. If the rank of an $n \times l$ STBC that is completely over $\mathcal{S}$ is r, then the transmission rate of this code in bits per second per hertz is upper bounded by $\frac{1}{l}\log_2[A_{|\mathcal{S}|^l}(n, r)]$ where $A_x(y, z)$ denotes the maximum size of a (conventional) code of length y and minimum Hamming distance z defined over an alphabet of size x [1]. It follows that for full-rank codes completely over $\mathcal{S}$ the rate in symbols per channel use is upper bounded by 1.

In the case when number of quasistatic intervals l is less than the number of transmit antennas n, there is wastage in the antennas since the maximum rank possible is n. Also if $l > n$, there would be a delay in decoding since the maximum possible rank would be n. So it is better if we get square designs, ie., $n = l$ with the same code size. Codes with this property ($n = l$) are called *minimal delay* codes. So the majority of the work was done on full-rank minimal delay codes.

The rank criterion holds good for the case of dependent fade coefficients as well as the case Rician Fading also. The determinant criterion for these cases are similar to the one above. The criteria for Rapid Fading channel are also derived in [1].

2.4 STBC Orthogonal Designs

In 1999, Tarokh *et al.* [3] studied the case of *STBC Orthogonal Designs* in detail. We shall reproduce some definitions and the main results of [3].

Definition 2.2 (Generalized Linear Processing Real Orthogonal Design) *A generalized linear processing real orthogonal design $\mathcal{G}$ of size n is an $l \times n$ matrix with entries as real linear combinations of the indeterminates $s_1, s_2, \cdots, s_n \in \mathbb{R}$, such that $\mathcal{G}^T\mathcal{G} = \mathcal{D}$, where $\mathcal{D}$ is diagonal matrix, with diagonal elements $\mathcal{D}_{ii}, i = 1, 2, \ldots, n$ of the form $(p_1^i s_1^2 + p_2^i s_2^2 +$*

$\ldots + p_k^i s_k^2$) and the coefficients $p_1^i, p_2^i, \ldots, p_k^i$ are strictly positive integers. The rate of $\mathcal{G}$ is $R = k/l$ symbols per channel use (PCU).

As special cases of the above, the following definitions can be obtained.

- If the entries are restricted to indeterminates $\pm s_1, \pm s_2, \cdots, \pm s_k$, we get a *Generalized Real Orthogonal Design* $\mathcal{G}$ of size n. $\mathcal{G}$ is a $l \times n$ matrix and $n \neq l \neq k$. The rate in this case is $R = k/l$.
- In particular, we can have a Generalized Real Orthogonal Design when $k = l \neq n$. The rate is 1 symbol PCU.
- We can have designs with $k \neq l = p$ also. Here rate is k/l.
- We get a *Linear Processing Real Orthogonal Design* of size n, when $k = l = n$. Here also rate is 1.
- A *Real Orthogonal Design* of size n is when $k = l = n$, entries are indeterminates $\pm s_1, \pm s_2, \cdots, \pm s_k$ themselves and the matrix is orthogonal.

The generalized real orthogonal designs enables decoupling of the symbols and each symbol can be decoded independently. This property is called *single symbol decodability.* Another beautiful property is that the indeterminates can take the values from any subset of the real field $\mathbb{R}$.

Tarokh *et al.* prove in [3] that a $l \times n$ Generalized Real Orthogonal Design in k indeterminates exists only when a Generalized Design $\mathcal{G}$ of the same size and the same number of indeterminates exist having $\mathcal{G}^T\mathcal{G} = (s_1^2 + s_2^2 + \ldots + s_k^2)I$. Even for the case of Linear Processing Real Orthogonal Designs, the same is true. The authors studied Real Orthogonal designs and they prove, using *Hurwitz-Radon Theory*, a special class of matrices, that a Linear Processing Real Orthogonal Design exists only for n =2, 4 or 8. For those values, Real Orthogonal Designs also exist. These schemes are given in [3]. Some of the Real Designs are reproduced below

Example 2.1 (Real Orthogonal Design) *The* 2×2 *Real Orthogonal Design is given by*

$$\begin{pmatrix} s_1 & s_2 \\ -s_2 & s_1 \end{pmatrix} \tag{2.7}$$

The Generalized Orthogonal Design for 3 *transmit antennas is*

$$\begin{pmatrix} s_1 & s_2 & s_3 \\ -s_2 & s_1 & -s_4 \\ -s_3 & s_4 & s_1 \\ -s_4 & -s_3 & s_2 \end{pmatrix} \tag{2.8}$$

Both the codes are of rate $R = 1$ *and are delay optimal designs also.*

From the real case, Tarokh *et al.* [3] proceeded to the respective complex counterparts.

Definition 2.3 (Generalized Complex Linear Processing Orthogonal Design) *A Generalized Complex Linear Processing Orthogonal Design* $\mathcal{G}_c$ *of size* n *is a* $l \times n$ *orthogonal matrix with entries the complex linear combinations of the indeterminates* $\pm s_1, \pm s_2, \cdots, \pm s_n \in \mathbb{C}$ *and their conjugates* $\pm s_1^*, \pm s_2^*, \cdots, \pm s_n^*$. *Also* $\mathcal{G}_c^* \mathcal{G}_c = \mathcal{D}_c$ *where* $\mathcal{D}_c$ *is a diagonal matrix with* (i,i)*th diagonal element of the form* $(p_1^i |s_1|^2 + p_2^i |s_2|^2 + \cdots + p_k^i |s_k|^2)$ *and the coefficients* $p_1^i, p_2^i, \ldots, p_k^i$ *are all strictly positive integers. The rate of such a design would be* $R = k/l$ *symbols PCU.*

From the above, we get the following definitions as special cases.

- *Generalized Complex Orthogonal Designs* are obtained when entries are restricted to the indeterminates $\pm s_1, \pm s_2, \cdots, \pm s_n \in \mathbb{C}$, their conjugates $\pm s_1^*, \pm s_2^*, \cdots, \pm s_n^*$ and their multiples with j. Here $k \neq l \neq n$ and rate is $R = k/l$.
- When $k = l \neq n$, we get a Generalized Complex Orthogonal Design of rate $R = 1$ symbol PCU.
- We can have designs with $k \neq l = n$, ie., rate $R = k/l$.

- We get *Linear Processing Complex Orthogonal Design* of size n, when $k = l = n$, and the entries are complex linear combinations of the indeterminates and their conjugates. The rate is $R = 1$ symbol PCU.

- A *Complex Orthogonal Design* of size n is when the matrix is orthogonal, and the entries are the indeterminates $\pm s_1, \pm s_2, \cdots, \pm s_n \in \mathbb{C}$, their conjugates $\pm s_1^*, \pm s_2^*, \cdots, \pm s_n^*$ and their multiples with j.

The most important advantage of Generalized Complex Orthogonal Designs is the *single symbol decodability*. That is, using simple linear processing, we can decouple the individual symbols. Since $\mathcal{G}_c^*\mathcal{G}_c$ is of the form as in Definition 2.3, we can separate each symbol which is being sent and decode them separately. The decoding will be *Maximum Likelihood (ML) Decoding*. This reduces the complexity immensely. Also, there is no restriction on the entries, they can be from any subset of $\mathbb{C}$.

Tarokh *et al.* tried to see the feasibility of Generalized Complex Orthogonal Designs and Linear Processing Complex Orthogonal Designs, on the same lines as the real designs. They proved that the existence of an $l \times n$ Generalized Linear Processing Complex OD in k variables implies the existence of a Generalized Linear Processing Complex OD $\mathcal{G}_c$ in the same dimension and number of variables having the property that $\mathcal{G}_c^*\mathcal{G}_c = (|s_1|^2 + |s_2|^2 + \ldots + |s_k|^2)I$, as in the case of Real Designs.

Further, it is proved in [3] that a Linear Processing Complex OD of size n exists if and only if a Linear Processing Real OD of size $2n$ exists. In other words, a Linear Processing Complex OD exists only for n =2 or 4. The existence of a design for $n = 4$ is disproved in [3], which means that Linear Processing Complex Designs exist only for $n = 2$, for which we have the *Alamouti Scheme*, which is the only Complex Orthogonal Design for $n = 2$.

Example 2.2 (Generalized Complex Orthogonal Design) *Here we give examples of Generalized Complex OD. This square ($n = l$) design, from [13], has rate* 3/4*, for* 4 *transmit*

antennas.

$$\mathcal{C} = \begin{pmatrix} s_1 & s_2 & s_3 & 0 \\ -s_2^* & s_1^* & 0 & -s_3 \\ -s_3^* & 0 & s_1^* & s_2 \\ 0 & s_3^* & -s_2^* & s_1 \end{pmatrix} \tag{2.9}$$

The following design is of rate $1/2$ *for* 3 *transmit antennas.*

$$\mathcal{G}_c^3 = \begin{pmatrix} s_1 & s_2 & s_3 \\ -s_2 & s_1 & -s_4 \\ -s_3 & s_4 & s_1 \\ -s_4 & -s_3 & s_2 \\ s_1^* & s_2^* & s_3^* \\ -s_2^* & s_1^* & -s_4^* \\ -s_3^* & s_4^* & s_1^* \\ -s_4^* & -s_3^* & s_2^* \end{pmatrix} \tag{2.10}$$

2.4.1 The Alamouti Scheme

S.M.Alamouti in [6] had proposed his scheme for two antenna transmitter case in 1998. The scheme ensures diversity advantage equal to twice the number of receive antennas. The scheme is given by the following matrix.

$$\mathcal{O}_c = \begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix} \tag{2.11}$$

Alamouti also proposed a combining scheme at the receiver which would separate the two symbols s_1 and s_2. This is due to the fact that $\mathcal{O}_c^*\mathcal{O}_c = (|s_1|^2+|s_2|^2)I$. The Maximum Likelihood (ML) decoding would just amount to decoding the two separately, as in an uncoded system. He proves that his combining scheme provides the same performance as the $2m$ level maximum ratio combining, where m is the number of receive antennas. In [3], Tarokh *et al.* prove that this is the only Complex Orthogonal Design.

2.5 Variations of STBC Designs

Although [3] closed almost all the problems regarding the existence of Complex Orthogonal Designs, researchers and coding theorists all over started looking into other possibilities of improvement. Attempts were made to get better rate, more diversity, simpler decoding, more general signal set etc. by compromising on one of the above.

In [10], Jafarkhani proposed *Quasi-Orthogonal Codes* in which the rate is compromised. As a result of that, the decoding becomes easier. Though single symbol decodability is not obtained, some of the symbols get uncoupled from the rest. The code is not full diversity. There is no restriction on the signal set also. Two schemes were proposed, one for 4 transmit antennas and one for 8 transmit antennas. We shall reproduce an example from [10].

Example 2.3 (Quasi-Orthogonal Design) *This is the QOD suggested for* 4 *transmit antennas, with* 4 *variables.*

$$\mathcal{A} = \begin{pmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2^* & s_1^* & -s_4^* & s_3^* \\ -s_3^* & -s_4^* & s_1^* & s_2^* \\ s_4 & -s_3 & -s_2 & s_1 \end{pmatrix} \tag{2.12}$$

Note that the rank of the code is 2*, not full-rank. In the decoding, the symbols* (s_1, s_4) *gets decoupled from* (s_2, s_3)*. This is not single symbol decoding, but some improvement over Exhaustive Search ML decoding is obtained. The rate of the above code is* 1 *symbol PCU.*

Later, Su and Xia in [14] and Sharma and Papadias in [15], came up with 4×4 Quasi-Orthogonal Designs, very similar to each other. Both the schemes had full diversity and a rate of 1 symbol PCU. Basically, they proposed designs which gave partial decoupling. Unlike the scheme proposed by Jafarkhani, [14] and [15] gave schemes which had full diversity. But they had to restrict the signal constellation. Both the papers, had the same restriction on the signal constellation, ie., of the four symbols (s_1, s_2, s_3, s_4) used $s_1, s_3 \in \mathcal{S}_1$ and $s_2, s_4 \in \mathcal{S}_2$, where $\mathcal{S}_2$ is rotated version of $\mathcal{S}_1$ by an angle ϕ, where ϕ is such that the determinant of the difference of the codeword matrices is never zero.

In [11], Tarokh and Jafarkhani suggested a *Differential Detection* scheme for signal points restricted to 2^b-PSK constellations. The scheme was for 2 transmit antennas. Here the two symbols which are to be transmitted are coded based on the previous symbols. The advantage of this scheme is that *non-coherent detection* is possible, ie. the decoding can be done without knowing the channel matrix.

In [12], Hassibi and Hochwald studied a generalized class of codes called *Linear Dispersion Codes(LDC)* which get high rate. They construct codes which maximize the mutual information between the transmitter and the receiver. Thus they get close to the capacity. The construction is not based on the rank criterion for the probability of error. The scheme is a general scheme for any number of transmit/receive antennas. The construction is such that efficient decoding schemes are possible. The authors, in [12] defined a Linear Dispersion Code as follows.

Definition 2.4 (Linear Dispersion Codes) *A linear dispersion code is one for which the codeword is of the form*

$$\mathcal{C} = \sum_{q=1}^{Q} (s_q C_q + s_q^* D_q) \tag{2.13}$$

where $s_1, s_2, \ldots, s_Q$ are complex scalars from some signal set $\mathcal{S}$ and C_q and D_q are fixed *$l \times n$ complex matrices. Note that the code is completely determined by the set of dispersion matrices $\{C_q, D_q : q = 1, 2, \ldots, Q\}$ and the signal set $\mathcal{S}$. The rate of this code would be $R = Q/l$ symbols PCU.*

We can see that all the Orthogonal Designs (real as well as complex) discussed till now, form special cases of the Linear Dispersion Codes. Consider the Generalized Complex Orthogonal Design in equation (2.9), we can write it as an LDC as follows. The matrices C_i and D_i will be

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, C_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, C_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$D_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, D_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}, D_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

2.6 DAST & Similar Codes

2.6.1 DAST

Damen *et al.*[21] proposed *Diagonal Algebraic Space-Time Block Codes (DAST)* which have a normalized rate of 1 symbol per channel use and achieve full diversity over n transmit and m receive antennas. The DAST maintains the diversity and coding gain over all real or complex constellations carved from the ring of complex integers $\mathbb{Z}[j]$, such as PAM or QAM.

The DAST makes use of rotated constellations. The idea of rotations [22] is based on the fact that given a constellation Γ of dimension d, if any given vector $\mathbf{x} \in \Gamma$ has its components $x_1, x_2, \ldots, x_d$ different from all the other components of the vectors in Γ, then affecting $(x_1, \ldots, x_d)$ by independent fadings to give $(\alpha_1 x_1, \ldots, \alpha_d x_d)$, allows the receiver to recover $(x_1, \ldots, x_d)$ unless all the components fall in deep fading, ie. $|\alpha_j| \ll 1, \forall j$. This property is called *full modulation diversity* of the constellation Γ, and is measured by the *minimum product distance* of Γ.

DAST uses rotational matrices from [22] to generate constellations with full modulation diversity from constellations carved from $\mathbb{Z}[j]$. The rotational matrix Θ_n has all real entries. Let the n-tuple symbol that has to be sent be $(s_1, s_2, \ldots, s_n)$. It is rotated using the rotational matrix Θ_n as follows: $(x_1, \ldots, x_n)^T = \Theta_n (s_1, \ldots, s_n)^T$. If $s_1, \ldots, s_n$ belong to the basic constellation $\mathcal{S}$ which can be seen as a subset of the field of rational numbers $\mathbb{Q}$, then the rotated vector $(x_1, \ldots, x_n)$ has its components not from $\mathbb{Q}$ but from an *algebraic number field* which has a dimension n over $\mathbb{Q}$. Here instead of increasing the geometric dimension of the transmitted signal, we increase the algebraic dimension of the rotated constellation (The interested reader can refer the Appendix where a background

to algebra is provided.). Each component of the rotated vector contains information about all the transmitted symbols. The code is obtained as follows.

From the message vector $(s_1, \ldots, s_n)$, you get the rotated vector $(x_1, \ldots, x_n)$. We use this vector to get a diagonal matrix. This matrix is multiplied by a Hadamard matrix $\mathcal{H}_n$ and the resulting matrix Ξ_n is sent.

$$(x_1, \ldots, x_n)^T = \Theta_n (s_1, \ldots, s_n)^T \tag{2.14}$$

$$\Xi_n \stackrel{\triangle}{=} \mathcal{H}_n \text{diag}(x_1, x_2, \ldots, x_n) \tag{2.15}$$

The minimum product distance of this rotated constellation would be given by

$$d_{n,\min} = \min_{\mathbf{x}=\Theta_n(\mathbf{s}-\mathbf{s}'),\mathbf{s}\neq\mathbf{s}'\in\mathcal{S}} \prod_{i=1}^{n} |x_i| \tag{2.16}$$

where $\mathbf{s}$ and $\mathbf{s}'$ belong to the constellation $\mathcal{S} \subset \mathbb{Z}[j]$.

The most important aspect of the DAST codes are the rotation matrices used. The matrices need be of full modulation diversity. Towards that end, matrices from [22, 24] are used. Essentially, we extend the algebraic dimension of the constellation used. For $n = 2, 4$, some optimized rotation matrices are used (see [21]). For $n = 2^q$,$q \geq 3$ the rotation matrix extends the constellation from the rational field $\mathbb{Q}$ to $\mathbb{Q}(\cos\frac{2\pi}{8n})$. The matrix is given by

$$\Theta_n = [(\theta_n)_{ij}] = \sqrt{\frac{2}{n}} * \cos\left(\frac{\pi}{4n} * (4i-1)(2j-1)\right) \tag{2.17}$$

This particular rotation promises a full modulation diversity constellation with minimum product distance $d_{n,\min} = \frac{\sqrt{2}}{(2n)^{n/2}}$.

The code matrix Ξ_n is shown to have full diversity which is a result of the full modulation diversity of the rotated constellation. The Hadamard matrix does not cause any change in the diversity or coding gain. Damen *et al.* also give lower bounds for the coding gain. The DAST Codes are shown to be suitable for fast fading channels. The lattice structure of the code makes it decodable using Sphere Decoding [21, 31].

Example 2.4 (DAST Code for $n = 4$) *The DAST code for $n = 4$ is given below.*

$$\Xi_4 = \mathcal{H}_4 diag(x_1, x_2, x_3, x_4) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & -x_2 & x_3 & -x_4 \\ x_1 & x_2 & -x_3 & -x_4 \\ x_1 & -x_2 & -x_3 & x_4 \end{pmatrix} \tag{2.18}$$

where $\mathbf{x} = (x_1, x_2, x_3, x_4)^T$ is the rotated vector obtained using equation 2.14, the rotation matrix used is as given in [21] for $n = 4$. The minimum product distance is $\frac{1}{40}$.

2.6.2 STCR

Yan Xin *et al.* proposed a similar code[25] which was called *Space-Time Constellation-Rotating (STCR) Codes*. Again, full diversity and a rate 1 symbol per channel use is obtained. The scheme is for a range of number of transmit antennas and arbitrary number of receive antennas. The scheme is based on the same principles and properties as the DAST, such as the symbols being from a subset of $\mathbb{Z}[j]$, an n-length vector operated on by a matrix to get another vector having full modulation diversity, finally using this to get a diagonal matrix and transmitting the same after suitably power unifying it. Like DAST, the STCR Codes are also Sphere decodable.

Xin *et al.* constructed their code based on the theory of extending the rational field to a higher algebraic number field based on some irreducible polynomials. Here also rotation matrices are used (referred to as *unitary precoders* in [25]). They gave some bounds for the coding gains for their code for some values of n(number of transmit antennas). They prove an upper bound for the coding gain for a more general class of codes and prove that STCR Codes meet the upper bound for some cases. They also gave lower bounds for the coding gain for some cases.

The authors in [25] gave one construction technique for $n = 2^q$. For other values of n, they proposed a different scheme.

Example 2.5 (STCR Code for $n = 4$) *For $n = 4$, it can be seen that $4 = \phi(8)$ where $\phi(\cdot)$*

denotes the Euler's totient function. So the following rotational matrix is obtained.

$$\Theta_4 = \frac{1}{2}\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \alpha_0^3 \\ 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 \\ 1 & \alpha_3 & \alpha_3^2 & \alpha_3^3 \end{pmatrix} \tag{2.19}$$

where $\alpha = \alpha_0, \alpha_1, \alpha_2, \alpha_3$ are the roots of the minimal polynomial of $\alpha = e^{j\frac{2\pi}{16}}$, the primitive 16th root of unity, over $\mathbb{Q}$. The multiplication by $\frac{1}{2}$ is to normalize the power. The symbol vector $\mathbf{s} \in \mathcal{S}^4 \subset \mathbb{Z}[j]^4$ is operated on by this precoder (rotation matrix) to give $\mathbf{x} = \Theta_4\mathbf{s}$. Then, as in DAST, the diagonal matrix $D = diag(\mathbf{x})$ is suitably power unified and sent.

2.6.3 TAST

In [28], El Gamal and Damen extended the concept of DAST to a more general system called *Threaded Algebraic Space-Time(TAST) Codes.* Here we use the concept of layering to get codes with rate upto n symbols per channel usage while the code retains full diversity. Here El Gamal and Damen have combined the principles of layered transmission approach[29] and that of DAST. The layering approach was generalized independent of the signal processing at the receiver in [30].

Threading

In the layering approach, the transmission matrix of size $n \times l$ is divided into a number of layers. There are some conditions which would ensure that each symbol interval within a layer is allocated to at most one antenna, and hence all spatial interferences experienced by the layer, comes from outside the layer. A layer with full spatial and temporal spans is referred to as a *thread.* The incoming message is split up into blocks and after encoding independently, each would be transmitted through a different layer.

In the threaded layering approach [30], the threads are designed so that each thread is active during all the available symbol transmission intervals and uses each of the n transmit antennas equally often. All of the codes considered in [28] have all their threads

of the same length and in the following form.

If the quasi static time intervals are $i \in (1, l)$, then the jth thread would be given by

$$\{((i+j-1)_n, i) : 1 \leq i \leq l\}, \quad 1 \leq j \leq n \tag{2.20}$$

where $(\cdot)_n$ denotes modulo n operation.

Example 2.6 (Threading) *In the following matrix A, we shall illustrate the threads.*

$$A = \begin{pmatrix} x_1 & y_2 & z_3 \\ z_1 & x_2 & y_3 \\ y_1 & z_2 & x_3 \end{pmatrix} \tag{2.21}$$

The entries (x_1, x_2, x_3) *are thread* 1, (y_1, y_2, y_3) *are thread* 2 *and* (z_1, z_2, z_3) *are thread* 3.

TAST Coding

Consider the case when $l = n$ and there is only one thread. We can see that transmission exists only in the principal diagonal of the $n \times n$ matrix. To get full diversity, and that too for the case where there are more thread, El Gamal and Damen use the principles of DAST (explained in Section 2.6). For the best performance, the minimum product distance (2.16) should be maximized. As in DAST, rotations from [22, 24] were considered.

When more than one threads are there, the TAST Codes are constructed by transmitting a scaled DAST Code in each thread, ie. in the jth thread you would send $\mathbf{s}_j$ which is encoded and sent as follows.

$$\phi_j \mathbf{x}_j = \phi_j \Theta^j \mathbf{s}_j \tag{2.22}$$

Where Θ^j is the rotation matrix for the jth thread and ϕ_j is a scaling. For TAST codes, the scaling numbers ϕ_j should be chosen to ensure full diversity and maximize the coding gain of the composite code. El Gamal and Damen in [28] give some conditions and methods to choose these ϕ_j's. They prove some lower bounds for the coding gains also. For decoding, they show that polynomial complexity decoding is achieved using sphere

decoding subject to the condition that number of threads should be at most $\min(n, m)$ where n and m are number of transmit and receive antennas respectively.

Example 2.7 (TAST Code for $n = 3$) *The TAST Code matrix for* 3 *transmit antennas is given below.*

$$\mathcal{T} = \begin{pmatrix} x_{11} & \phi^{2/3}x_{32} & \phi^{1/3}x_{23} \\ \phi^{1/3}x_{21} & x_{12} & \phi^{2/3}x_{33} \\ \phi^{2/3}x_{31} & \phi^{1/3}x_{22} & x_{13} \end{pmatrix} \tag{2.23}$$

where $\mathbf{x}_j = (x_{j1}, x_{j2}, x_{j3})^T = \Theta^j(s_{j1}, s_{j2}, s_{j3})^T$ *where* $\mathbf{s}_j = (s_{j1}, s_{j2}, s_{j3})^T$ *is the uncoded symbol vector in the* j*th thread.* Θ^j *is the rotation matrix used to rotate the* j*th thread,* ϕ *is a scaling factor, (referred to as* Diophantine number *in [28]) which has to properly chosen and optimized for full diversity and good coding gain.*

2.6.4 A Code based on Number Theory

In [20], Damen *et al.* proposed a Space-Time Block Code for 2 transmit antennas and 2 quasistatic symbol intervals. This code achieves full transmit diversity and a transmission rate of 2 symbols per channel use, the constellation being a subset of integer lattice $\mathbb{Z}[j]$. This code uses algebraic number theory for establishing full diversity and reaching good coding gain. This code, is a special case of TAST, but has the property that it achieves channel capacity for any number of receive antennas.

The code is as follows.

$$B_{2,\phi} = \frac{1}{\sqrt{2}} \begin{pmatrix} s_1 + \phi s_2 & \theta(s_3 + \phi s_4) \\ \theta(s_3 - \phi s_4) & s_1 - \phi s_2 \end{pmatrix} \tag{2.24}$$

where $\mathbf{s} = (s_1, s_2, s_3, s_4)^T \in \mathcal{C} = \mathcal{S}^4 \subset \mathbb{Z}[j]^4$ is the input symbol vector and $\theta^2 = \phi$ and $\phi = e^{j\lambda}$, where λ is a real parameter which has to be optimized. The scaling factor $\frac{1}{\sqrt{2}}$ is to normalize the Frobenius norm of the matrix. Damen *et al.* gave some conditions on ϕ for full diversity and better coding gains. The code, by virtue of its lattice structure, is Sphere Decodable at polynomial complexity.

2.7 STBC's based on Division Algebras

Sethuraman *et al.* in [16] provided a new approach to obtain Space-Time Block Codes using algebraic approach. They proposed a generalized method to construct a class of full-rank STBC's using embeddings of division algebras in matrix rings. They proposed various ways of applying the same to commutative as well as non commutative division algebras. (Background to necessary theory is provided in the Appendix.)

2.7.1 The Basic Principle

Definition 2.5 (Division Algebra) *A division algebra is a ring in which every nonzero element has a multiplicative inverse. A commutative division algebra is just a field.*

Example 2.8 (Hamilton's Quaternions) *The Hamilton's Quaternions was the first non-commutative division algebra discovered. The Quaternions, denoted by* $\mathbb{H}$ *is the four dimensional vector space over the field of real numbers* $\mathbb{R}$ *with the basis* $\{1, \hat{i}, \hat{j}, \hat{k}\}$*, with multiplication given by* $\hat{i}^2 = \hat{j}^2 = -1$ *and* $\hat{i}\hat{j} = \hat{k} = -\hat{j}\hat{i}$*. In other words,* $\mathbb{H}$ *is the set* $\{a + b\hat{i} + c\hat{j} + d\hat{k} : a, b, c, d \in \mathbb{R}\}$*. Addition is defined component wise. From the given relations, one can derive* $\hat{k}^2 = -1$*,* $\hat{j}\hat{k} = \hat{i} = -\hat{k}\hat{j}$ *and* $\hat{k}\hat{i} = \hat{j} = -\hat{i}\hat{k}$*. Multiplication is done term by term, then simplifying the expression using the above relations and finally combining like terms. We can see that multiplication is not commutative from the above relations themselves. Also for the non zero quaternion* $x = a+b\hat{i}+c\hat{j}+d\hat{k}$*, the multiplicative inverse is given by the quaternion* $\frac{a}{z} - \frac{b}{z}\hat{i} - \frac{c}{z}\hat{j} - \frac{d}{z}\hat{k}$*, where* $z = a^2 + b^2 + c^2 + d^2$*. Thus all non zero elements have a multiplicative inverse and* $\mathbb{H}$ *is a non-commutative division algebra. Note that the real field* $\mathbb{R}$ *and complex field* $\mathbb{C}$ *are a subset of* $\mathbb{H}$*, we get* $\mathbb{C}$ *when coefficients of any two of* $\hat{i}, \hat{j}, \hat{k}$ *go to zero, and* $\mathbb{R}$ *when coefficients of all the above three go to zero.*

The main principle that formed the basis of [16, 17, 18, 19] is the following.

Let D be a division algebra, and let $f : D \to M_n(F)$ be a ring homomorphism from D to the set of $n \times n$ matrices over some field F. Because it is a homomorphism and since D is a division algebra, we get the full rank code. This is due to the fact that, all

elements in D have an inverse, by definition. Essentially, we have $f(D)$ as an *embedding* of D in $M_n(F)$. This would ensure that the difference between any two matrices from the embedding in $M_n(F)$ would have full rank and hence satisfy the rank criterion.

Theorem 2.1 *Let $f : D \to M_n(F)$ be a ring homomorphism from a division algebra D to the set of $n \times n$ matrices over some field F. If E is any subset of the image of D under this map, then E will have the property that the difference of any two elements in it will be of full-rank.*

Using this principle, the authors proposed several ways of constructing full-rank codes using commutative as well as non-commutative division algebras. They took different types of division algebras and constructed codes using their structure.

2.7.2 Codes from Field Extensions

In [16, 17, 18], methods have been put forth to construct STBC's from embeddings of field extensions to matrix algebras. In [17], ways to construct rate-optimal STBC's over PSK constellations using *cyclotomic* field extensions were explained. STBC's from field extensions of the rational field $\mathbb{Q}$ were explained in [18]. The mathematics behind all of them are the same, which is explained as follows.

Let K be an extension field of F whose degree is $[K : F] = n$. K can be seen as a vector space over F, and a natural map L can be obtained from K to $End_F(K)$, which is the set of all F-linear transforms of the vector space K. This map is given by $k \mapsto \lambda_k$, where λ_k takes any $u \in K$ to to ku. It can be verified that $\lambda_k \in End_F(K)$ and the map L is a *ring homomorphism*. It can be said that K embeds in $M_n(F)$.

For a given choice of F basis $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ of K, one can write down the matrix corresponding to λ_k by just seeing what each basis element u_j is transformed to by the transformation λ_{u_i}. The expansion of the result in terms of the same basis would give the jth column of the matrix corresponding to u_i. For the other elements in F, the corresponding matrices will be the linear combinations of those of basis matrices.

Since every finite extension is a simple algebraic extension, we can say that K is generated over F by a primitive element α, we can consider the basis $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

Let the minimal polynomial of α over F be $h(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Then the matrix corresponding to λ_α, say M, is easily seen to be

$$M = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ 0 & 0 & 1 & \ldots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix} \tag{2.25}$$

It can be seen that the matrix corresponding to λ_{α^i} is nothing but M^i. This matrix is called the companion matrix of $h(x)$. Also it follows that the general element $k = f_0 + f_1\alpha + f_2\alpha^2 + \ldots + f_{n-1}\alpha^{n-1}$ will be mapped to the matrix $f_0 I_n + f_1 M + f_2 M^2 + \ldots + f_{n-1}M^{n-1}$. From this and Theorem 2.1, the following can be stated.

Theorem 2.2 *Let $K = F(\alpha)$ be an extension of the field F of degree n, and let the minimal polynomial of α over F be $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Let $M \in M_n(F)$ be the matrix defined in equation (2.25). Then the set of all matrices of the form $f_0 I_n + f_1 M + f_2 M^2 + \ldots + f_{n-1}M^{n-1}$, with $f_0, f_1, f_2, \ldots, f_{n-1} \in F$ is an embedding of K in $M_n(F)$. In particular, any finite subset E of such matrices will have the property that the difference of any two matrices in it will have full-rank.*

Example 2.9 (Code from Field Extension) *Here we give an example for a code from a field extension of the rational field $\mathbb{Q}$. Consider a QPSK signal set $\mathcal{S} = \{\pm 1, \pm j\}$. Consider polynomial $h(x) = x^3 - 2x - 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (see [33] and Theorem A.3 in the Appendix). Note that the constellation $\mathcal{S} \subset \mathbb{Q}(j)$, $\mathbb{Q}(j)$ is of degree 2 over $\mathbb{Q}$ and $(2, 3) = 1$. Hence the polynomial is irreducible over $\mathbb{Q}(j)$. Then the companion matrix of $h(x)$ is*

$$M = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix} \tag{2.26}$$

also, its square is given by

$$M^2 = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 2 & 2 \\ 1 & 0 & 2 \end{bmatrix} \tag{2.27}$$

Thus, the code, by the previous theorem, is given by

$$\mathcal{C} = \left\{ \begin{pmatrix} s_0 & 2s_2 & 2s_1 \\ s_1 & s_0 + 2s_2 & 2s_1 + 2s_2 \\ s_2 & s_1 & s_0 + 2s_2 \end{pmatrix} : s_i \in \mathcal{S}, i = 0, 1, 2 \right\} \tag{2.28}$$

2.7.3 Codes from Cyclotomic Extensions

One interesting special case of the above, is when the minimal polynomial of α is of the form $x^n - \gamma$ for some $\gamma \in F^*$. We can see that the matrix corresponding to λ_α, as a special case of equation (2.25), is given by

$$M = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & \gamma \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix} \tag{2.29}$$

From the above, it is easily seen [16] that the matrix corresponding to λ_k, where $k = f_0 + f_1\alpha + f_2\alpha^2 + \ldots + f_{n-1}\alpha^{n-1}$, is given by

$$\begin{bmatrix} f_0 & \gamma f_{n-1} & \gamma f_{n-2} & \dots & \gamma f_2 & \gamma f_1 \\ f_1 & f_0 & \gamma f_{n-1} & \dots & \gamma f_3 & \gamma f_2 \\ f_2 & f_1 & f_0 & \dots & \gamma f_4 & \gamma f_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ f_{n-1} & f_{n-2} & f_{n-3} & \dots & f_1 & f_0 \end{bmatrix} \tag{2.30}$$

The following can be stated as a special case of Theorem 2.2

Theorem 2.3 *Let F be a field, and let γ be a non zero element in F. Let the polynomial $x^n - \gamma$ is irreducible in $F[x]$. Then the set of all matrices of the form (2.30), with $f_0, f_1, \ldots, f_{n-1} \in F$ forms a field, isomorphic to $F(\sqrt[n]{\gamma})$. In particular, any finite set of such matrices will have the property that the difference between any two matrices in it will have full-rank.*

The following theorem [16] helps us to find irreducible polynomials over fields containing a wide range of signal constellations, for any number of antennas. These codes are referred to as codes over *cyclotomic extensions* of the rational field.

Theorem 2.4 *Let n, m, l be such that the prime factors of n are a subset of those of m and $(l, m) = 1$. Then $x^n - \omega_m^l$ is irreducible over $\mathbb{Q}(\omega_m)$. Hence for any n, $\mathbb{Q}$ can be extended to include the chosen signal set with $x^n - \omega_m^l$ remaining irreducible over the extension.*

Example 2.10 (Code from Cyclotomic Extension) *Consider a 12-PSK signal set $\mathcal{S} = \{e^{j\frac{2\pi}{12}k} : 0 \leq k \leq 11\}$. For constructing an $n = 5$ transmit antenna STBC, an m is needed, such that m is a multiple of 12. Also the prime factors of n should be a subset of that of m. Hence $m = 60$ can be chosen. Consider the polynomial $h(x) = x^5 - \gamma$, where $\gamma = \omega_{60}$ is the primitive 60th root of unity. By the above theorem, this can be used to construct a code as follows. The code is given by*

$$\mathcal{C} = \left\{ \begin{pmatrix} s_0 & \gamma s_4 & \gamma s_3 & \gamma s_2 & \gamma s_1 \\ s_1 & s_0 & \gamma s_4 & \gamma s_3 & \gamma s_2 \\ s_2 & s_1 & s_0 & \gamma s_4 & \gamma s_3 \\ s_3 & s_2 & s_1 & s_0 & \gamma s_4 \\ s_4 & s_3 & s_2 & s_1 & s_0 \end{pmatrix} : s_i \in \mathcal{S}, i = 0, 1, 2, 3, 4 \right\} \tag{2.31}$$

Thus, one can construct STBC's with rate 1 symbol per channel use, using the above methods. The codes from field extensions have an inherent lattice structure and hence are Sphere Decodable at polynomial complexity [26]. The authors, in the remaining part of [16], explained various methods to use the above principles for constructing STBC's

from embeddings of commutative division algebras as well as non-commutative division algebras.

2.7.4 Codes from other minimal polynomials

Similar to the codes in the last section, codes can be constructed using other minimal polynomials also. If the polynomials are irreducible over a field which contains the constellation, from Theorem 2.2, a full diversity code can be constructed.

As a particular case of equation (2.25), we get the companion matrix for $x^n - px - p$, where p is a prime integer, as shown. If the minimal polynomial of α is of this form, the matrix corresponding to λ_α is as follows.

$$M = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & p \\ 1 & 0 & 0 & \dots & 0 & p \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix} \tag{2.32}$$

From the above, the matrix corresponding to λ_k for any $k = f_0 + f_1\alpha + f_2\alpha^2 + \ldots + f_{n-1}\alpha^{n-1}$ is given by

$$\begin{bmatrix} f_0 & pf_{n-1} & pf_{n-2} & \dots & pf_2 & pf_1 \\ f_1 & f_0 + pf_{n-1} & pf_{n-1} + pf_{n-2} & \dots & pf_3 + pf_2 & pf_2 + pf_1 \\ f_2 & f_1 & f_0 + pf_{n-1} & \dots & pf_4 + pf_3 & pf_3 + pf_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ f_{n-1} & f_{n-2} & f_{n-3} & \dots & f_1 & f_0 + pf_{n-1} \end{bmatrix} \tag{2.33}$$

For code construction, one can use the following theorem from [16].

Theorem 2.5 *Let $h(x)$ be an irreducible polynomial over $\mathbb{Q}$ of degree n. Suppose that F is an extension field of $\mathbb{Q}$ of degree m, and suppose that n and m are relatively prime.*

Then $h(x)$ remains irreducible over F.

Let the minimal polynomial of $\alpha \in \mathbb{C}$ be $h(x) = x^n - px - p$, where p is a prime number. By *Eisenstein's Criterion* (see [33] and Theorem A.3 of the Appendix), this polynomial is irreducible over $\mathbb{Q}$. Consider a QAM constellation $\mathcal{S}$, say 16-QAM. Thus $\mathcal{S} = \{(2y - 1 - 4) + j(2z - 1 - 4) : y, z = 1, 2, 3, 4\}$. It is easy to see that $\mathcal{S} \subset \mathbb{Q}(j)$. Since $\mathbb{Q}(j)$ is of degree 2 over $\mathbb{Q}$, the above polynomial $h(x)$ for any n odd would yield a full diversity code(since any odd n and 2 are relatively prime). The code constructed in Example 2.9, is an example for this type of construction.

2.7.5 High Rate Codes

One very interesting sub class of the codes explained in previous section was dealt with in [16, 19]. Here Sethuraman *et al.* developed Space-Time Block Codes having rate more than 1 (Symbols PCU) called *High-rate Codes.* While the codes continue to use the same basic principle as the previous section, it makes use of the following theorem also.

Theorem 2.6 *Let F be a field of characteristic zero, and let z be an indeterminate. Then, for any integer $n \geq 1$, the polynomial $x^n - z$ is irreducible in the ring $F(z)[x]$. (Here $F(z)$ is the rational function field over F in the indeterminate z, that is elements are of the form $a(z)/b(z)$ where $a(z)$ and $b(z) \neq 0$ are polynomials over F.)*

Since any transcendental number acts as an indeterminate over $\mathbb{Q}(\omega_m)$, we can have full-rank codes for any number of transmit antennas n, by replacing the γ in (2.30) by a transcendental number. Codes of this type are referred to as codes from *transcendental extensions.*

Example 2.11 (Code from Transcendental Extension) *Let $\mathcal{S}$ be an 8-PSK constellation. Let θ be an algebraic number, hence $\gamma = e^{j\theta}$ would be transcendental by Lindemann-Weierstrass Theorem [33] (Complete statement in Appendix as Theorem A.1). By the above theorem, $x^3 - \gamma$ is irreducible over $\mathbb{Q}(\omega_8)$ (where ω_8 is the primitive 8th root of unity. Note that $\mathcal{S} \subset \mathbb{Q}(\omega_8)$. The following would be the corresponding code, where γ is*

transcendental.

$$\mathcal{C} = \left\{ \begin{pmatrix} s_0 & \gamma s_2 & \gamma s_1 \\ s_1 & s_0 & \gamma s_2 \\ s_2 & s_1 & s_0 \end{pmatrix} : s_i \in \mathcal{S}, i = 0, 1, 2 \right\} \tag{2.34}$$

Corollary 2.7 *For any $n > 1$, the polynomial $x^n - z$ is irreducible in $\mathbb{Q}(\omega_p, z)[x]$.*

Since any transcendental number acts as an indeterminate over $\mathbb{Q}(\omega_p)$, we can replace z with a transcendental number. The High-rate STBC $\mathcal{C}$ obtained by using the polynomial $x^n - z$ is got by replacing each f_i in (2.30) by a polynomial $f_i(z) \in \mathbb{Q}(\omega_p)[z])$. That is

$$\mathcal{C} = \left\{ \begin{pmatrix} f_0(z) & f_{n-1}(z) & \dots & zf_1(z) \\ f_1(z) & f_0(z) & \dots & zf_2(z) \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1}(z) & f_{n-2}(z) & \dots & f_0(z) \end{pmatrix} : f_i(z) \in \mathbb{Q}(\omega_p)[z], i = 0, 1, 2, \dots, n-1 \right\} \tag{2.35}$$

Notice that each entry in the matrix codeword is a polynomial. Let each of $f_i(z) = \sum_{k=0}^{R-1} f_{i,k} z^k$, where $f_{i,k} \in \mathbb{Q}(\omega_p)$. Here R can be any arbitrary integer and hence the rate, which is R symbols per channel use, is arbitrary. Any degree polynomial will be fine since $\mathbb{Q}(z)$ is infinite dimensional over $\mathbb{Q}$. To get appropriate transcendental numbers z, one can make use of the *Lindemann-Weierstrass Theorem*[33] (also see Theorem A.1 in the Appendix), a consequence of which would be the fact that $e^{j\theta}$ would be a transcendental number for θ algebraic.

Example 2.12 (High-Rate Code from field extension) *Consider $\mathcal{S} = \{1, j, -1, -j\}$, a 4-PSK signal set. The following would be a rate $R = 2$ symbols PCU, 3×3 full-rank STBC over $\mathcal{S}$.*

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} f_{0,0} + f_{0,1}z & f_{2,0}z + f_{2,1}z^2 & f_{1,0}z + f_{1,1}z^2 \\ f_{1,0} + f_{1,1}z & f_{0,0} + f_{0,1}z & f_{2,0}z + f_{2,1}z^2 \\ f_{2,0} + f_{2,1}z & f_{1,0} + f_{1,1}z & f_{0,0} + f_{0,1}z \end{pmatrix} : f_{i,k} \in \mathcal{S}, i = 0, 1, 2, k = 0, 1 \right\} \tag{2.36}$$

The scaling factor $\frac{1}{\sqrt{2}}$ *is used to normalize power per antenna PCU. Since we are using* 4*-PSK, the bit rate is* 4 *bits per channel use.*

The High-rate STBC's are codes also have a lattice structure and are Sphere Decodable [27]. Though the decoding is of greater complexity than that of rate 1 codes, it is seen to be faster than the Exhaustive Search ML Decoding.

Chapter 3

Coding Gains of STBC's from Field Extensions

In this chapter, we look at coding advantages of some STBC's from Field Extensions. Here, we give closed form expressions for the coding gains for a sub class of codes given in the previous chapter, for certain signal sets. Also we state an upper bound for the coding gains of the High-rate codes.

3.1 Some useful definitions and results

We state the following results and definitions which would be useful for the rest of this chapter [24, 25, 33]. For all the following definitions as well as results, assume that the polynomial $f(x) \in \mathbb{Q}(j)[x]$ is irreducible over $\mathbb{Q}(j)$ and the roots of $f(x) = 0$ are $\alpha = \alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$.

Definition 3.1 (Integral over $\mathbb{Z}[j]$) *An element β of $\mathbb{Q}(j)(\alpha)$ is said to be integral over $\mathbb{Z}[j]$ if there exists a monic polynomial $g(x)$ with coefficients in $\mathbb{Z}[j]$, such that $g(\beta) = 0$. Clearly, every element in $\mathbb{Z}[j]$ is integral over $\mathbb{Z}[j]$.*

Example 3.1 (Integral over $\mathbb{Z}[j]$) *The number $\sqrt{2}$ is integral over $\mathbb{Z}[j]$ since it is a root of $x^2 - 2 = 0$. $\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}j\right)$ satisfies $x^4 + 1 = 0$, and hence is integral over $\mathbb{Z}[j]$.*

Result 3.1 (Minimal Polynomial) *If α is integral over $\mathbb{Z}[j]$, then there is a unique irreducible monic polynomial $M_\alpha \in \mathbb{Q}(j)[x]$, such that $M_\alpha(\alpha) = 0$. Also this will have $n = \deg M_\alpha$ distinct roots in $\mathbb{C}$.*

Example 3.2 (Minimal Polynomial) *From the Example 3.1, the minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ (note that it is irreducible in $\mathbb{Q}(j)[x]$. But the minimal polynomial of $\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}j\right)$ is not $x^4 + 1$ because it is further reducible in $\mathbb{Q}(j)[x]$. The minimal polynomial of $\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}j\right)$ is $x^2 - j$, which is irreducible in $\mathbb{Q}(j)[x]$.*

Definition 3.2 (Extension of an embedding) *An embedding η is a ring monomorphism of $\mathbb{Q}(j)(\alpha)$ in $\mathbb{C}$, and if η is an embedding of $\mathbb{Q}(j)(\alpha)$ in $\mathbb{C}$ such that $\eta(z) = z \forall z \in \mathbb{Q}(j)$, then η is called a $\mathbb{Q}(j)$-isomorphism of $\mathbb{Q}(j)(\alpha)$.*

Example 3.3 ($\mathbb{Q}(j)$-isomorphism of $\mathbb{Q}(j)(\alpha)$) *Consider the field $\mathbb{Q}(j)(\sqrt{2})$. We know that $\mathbb{Q}(j)(\sqrt{2})$ is of degree 2 over $\mathbb{Q}(j)$ and that every element $x \in \mathbb{Q}(j)(\sqrt{2})$ can be written as $x = a + b\sqrt{2}$, where $a, b \in \mathbb{Q}(j)$. Let us see the following mapping η*

$$\eta(a + b\sqrt{2}) = a - b\sqrt{2}, \quad (\textit{where } a, b \in \mathbb{Q}(j)) \tag{3.1}$$

We can see that $\forall z \in \mathbb{Q}(j)$, $\eta(z) = z$. Hence this is a $\mathbb{Q}(j)$-isomorphism of $\mathbb{Q}(j)(\sqrt{2})$.

Definition 3.3 (Relative norm of a field) *Let $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ be the complex roots of the minimal polynomial of α over $\mathbb{Q}(j)$. Let $\eta_m(\alpha) = \alpha_m$ for $m = 0, 1, 2, \ldots, n-1$. If $\beta \in \mathbb{Q}(j)(\alpha)$, then the relative norm of β from the field $\mathbb{Q}(j)(\alpha)$ is defined as $\mathcal{N}(\beta) := \mathcal{N}_{\mathbb{Q}(j)(\alpha)/\mathbb{Q}(j)}(\beta) = \prod_{m=0}^{n-1} \eta_m(\beta)$.*

Example 3.4 (Relative norm) *Let us consider the field $\mathbb{Q}(j)(\sqrt{2})$ which was considered in Example 3.3. The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$ from Example 3.2. The roots of $x^2 - 2 = 0$ are $\sqrt{2}$ and $-\sqrt{2}$. The $\mathbb{Q}(j)$-isomorphisms are identity map and the map η as given in Example 3.3. Then the relative norm from the field $\mathbb{Q}(j)(\sqrt{2})$ of $x = a + b\sqrt{2}$, where $a, b \in \mathbb{Q}(j)$ is*

$$\mathcal{N}(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \tag{3.2}$$

Note that the relative norm $\mathcal{N}$ can be negative also ($\mathcal{N}(\sqrt{2}) = -2$, for instance.)

Result 3.2 *If $\mathbb{Q}(j)(\alpha)$ is a finite extension of the field $\mathbb{Q}(j)$ with degree denoted by $[\mathbb{Q}(j)(\alpha) : \mathbb{Q}(j)] = n$, then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forms a basis of $\mathbb{Q}(j)(\alpha)$ over $\mathbb{Q}(j)$.*

Example 3.5 (Basis of extensions) *In the preceding examples, $\mathbb{Q}(j)(\sqrt{2})$ is of degree 2 over $\mathbb{Q}(j)$, ie., $[\mathbb{Q}(j)(\sqrt{2}) : \mathbb{Q}(j)] = 2$. We can see that, any element of $\mathbb{Q}(j)(\sqrt{2})$ can be written as $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}(j)$. Thus $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(j)(\sqrt{2})$ over $\mathbb{Q}(j)$.*

Similarly, consider $\mathbb{Q}(j)(\omega_{12}) = \mathbb{Q}(\omega_{12})$, where ω_{12} is the primitive 12th root of unity. The minimal polynomial of ω_{12} is $x^2 - jx - 1$. Hence $\mathbb{Q}(\omega_{12})$ is of degree 2 over $\mathbb{Q}(j)$ and $\{1, \omega_{12}\}$ form a basis of $\mathbb{Q}(\omega_{12})$ over $\mathbb{Q}(j)$.

Result 3.3 *The set of elements of $\mathbb{Q}(j)(\alpha)$ which are integral over $\mathbb{Z}[j]$ is a subring of $\mathbb{Q}(j)(\alpha)$ containing $\mathbb{Z}[j]$. This subring is called the ring of integers of $\mathbb{Q}(j)(\alpha)$ and denoted by $\mathcal{O}$.*

Example 3.6 (Ring of Integers) *Consider the field $\mathbb{Q}(j)(\sqrt{2})$. The above result says that all the elements of $\mathbb{Q}(j)(\sqrt{2})$ which are integral over $\mathbb{Z}[j]$ form a ring. For instance, since $\sqrt{2}$ and $\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}j\right)$ are integral over $\mathbb{Z}[j]$, their sum, difference, product etc. would also be integral over $\mathbb{Z}[j]$.*

Result 3.4 *If $\beta \in \mathbb{Q}(j)(\alpha)$ is integral over $\mathbb{Z}[j]$, then the relative norm of β from $\mathbb{Q}(j)(\alpha) \in \mathbb{Z}[j]$.*

Example 3.7 (Relative norm of integral β) *Consider $\sqrt{2} \in \mathbb{Q}(j)(\sqrt{2})$. As seen in Example 3.1, $\sqrt{2}$ is integral over $\mathbb{Z}[j]$ and from Example 3.4, the relative norm of $\sqrt{2}$ is $-2 \in \mathbb{Z}[j]$.*

Another example is $\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}j\right)$, which is integral by Example 3.1. We can write $\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}j\right)$ as $0 + \left(\frac{1}{2} + \frac{1}{2}j\right) \cdot \sqrt{2}$. The relative norm is $-j \in \mathbb{Z}[j]$.

3.2 Diagonalizing Codes from Field Extensions

In this section, we shall study the code by diagonalizing it. Note that we consider here codes from field extensions constructed using irreducible polynomials over $\mathbb{Z}[j]$ which are monic. The signal constellation is QAM, ie., scaled versions of constellations carved from $\mathbb{Z}[j]$.

The basic signal set is some $\mathcal{S}$ carved from $\mathbb{Z}[j]$ and normalized by $\sqrt{\mathcal{E}_s}$ such that the average symbol energy is unity. ie., $E[\|s\|^2]_{s\in\mathcal{S}} = 1$.

The code is constructed as shown in [16] and explained in Section 2.7.2. Consider a monic, irreducible polynomial $f(x) \in \mathbb{Z}[j][x]$ which is irreducible over $\mathbb{Q}(j)[x]$. Let the polynomial be

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \tag{3.3}$$

From Result 3.1, $f(x)$ does not have multiple roots. The companion matrix M of $f(x)$ is as given in equation (2.25). Also it is easily seen the characteristic polynomial of M is $f(\lambda)$.

We have to transmit through n transmit antennas and n quasistatic intervals. Let the symbol vector be $\mathbf{s} = (s_0, s_1, \ldots, s_{n-1})^T \in \mathcal{S}^n$. The transmitted code matrix is given by

$$T_{\mathbf{s}} = \frac{1}{\psi}[s_0 I_n + s_1 M + s_2 M^2 + \ldots + s_{n-1}M^{n-1}] \tag{3.4}$$

where ψ is a normalizing factor which makes the expected value of the Frobenius norm of $T_{\mathbf{s}}$ equal to n, ie.,

$$E = [\|T_{\mathbf{s}}\|^2] = E[\mathrm{tr}(T_{\mathbf{s}}^* T_{\mathbf{s}})] = n \tag{3.5}$$

We know that the characteristic equation of M will be $f(\lambda) = 0$. Since $f(x)$ is irreducible over $\mathbb{Q}(j)$(using Result 3.1), M is full rank and also $f(x) = 0$ has n distinct roots. So M is diagonalizable as follows.

$$M = P^{-1}DP \text{ where } D = \mathrm{diag}(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \tag{3.6}$$

and $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are the roots of $f(x) = 0$.

$$\begin{aligned} T_{\mathbf{s}} &= \psi^{-1}[s_0 I + s_1 M + s_2 M^2 + \ldots + s_{n-1} M^{n-1}] \\ &= \psi^{-1} P^{-1}[s_0 I + s_1 D + s_2 D^2 + \ldots + s_{n-1} D^{n-1}] P \\ &= \psi^{-1} P^{-1} D_{\mathbf{s}} P \qquad (3.7) \\ \text{where } D_{\mathbf{s}} &= \text{diag}(\mathbf{v}) \text{ and} \end{aligned}$$

$$\mathbf{v} = \begin{bmatrix} s_0 + s_1\alpha_0 + s_2\alpha_0^2 + \ldots + s_{n-1}\alpha_0^{n-1} \\ s_0 + s_1\alpha_1 + s_2\alpha_1^2 + \ldots + s_{n-1}\alpha_1^{n-1} \\ \vdots \\ s_0 + s_1\alpha_{n-1} + s_2\alpha_{n-1}^2 + \ldots + s_{n-1}\alpha_{n-1}^{n-1} \end{bmatrix} = \Theta \cdot \mathbf{s} \qquad (3.8)$$

We can see that $\mathbf{v} = \Theta \cdot \mathbf{s}$ where

$$\Theta = \begin{bmatrix} 1 & \alpha_0 & \alpha_0^2 & \ldots & \alpha_0^{n-1} \\ 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n-1} & \alpha_{n-1}^2 & \ldots & \alpha_{n-1}^{n-1} \end{bmatrix} \text{ and } \mathbf{s} = \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{bmatrix}$$

Example 3.8 (Diagonalization of code from Field Extensions) *Consider the code given in Example 2.9. One can see that the code is constructed using the polynomial* $x^3 - 2x - 2$. *As proved above, we can diagonalize the code* $\mathcal{C}$. *The diagonal matrix would be given by* $D_{\mathbf{s}} = diag(\mathbf{v})$, *where the vector* $\mathbf{v}$ *is given as follows.*

$$\mathbf{v} = \begin{bmatrix} s_0 + s_1\alpha_0 + s_2\alpha_0^2 \\ s_0 + s_1\alpha_1 + s_2\alpha_1^2 \\ s_0 + s_1\alpha_2 + s_2\alpha_2^2 \end{bmatrix} = \Theta \cdot \mathbf{s} \qquad (3.9)$$

where $(\alpha_0, \alpha_1, \alpha_2) = (1.77, -0.88 + j0.59, -0.88 - j0.59)$ *are the roots of* $x^3 - 2x - 2$. *We*

can see that $\mathbf{v} = \Theta \cdot \mathbf{s}$ *where*

$$\Theta = \begin{bmatrix} 1 & \alpha_0 & \alpha_0^2 \\ 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \end{bmatrix} \text{ and } \mathbf{s} = \begin{bmatrix} s_0 \\ s_1 \\ s_2 \end{bmatrix} \tag{3.10}$$

3.3 Calculation of Coding Gain

The described code is a full diversity code (as shown in Section 2.7.2 and [16]) and hence the coding gain [1] is defined as

Definition 3.4 (Coding Gain of a full-rank STBC) *The coding gain* Δ *of a full-rank Space-Time Block Code* $\mathcal{C}$ *of size* n *is defined as*

$$\Delta = \min_{\mathbf{c} \neq \mathbf{e} \in \mathcal{C}} |\det(\mathbf{c} - \mathbf{e})|^{2/n} \tag{3.11}$$

Example 3.9 (Coding Gain) *Consider the Alamouti Code in Section 2.4.1. This is a full diversity code for* $n = 2$ *transmit antennas. Consider that the entries come from a signal set* $\mathcal{S}$*. Then for* $x_1, x_2, y_1, y_2 \in \mathcal{S}$*, the difference between codeword matrices has the following form*

$$\mathcal{O}_x - \mathcal{O}_y = \begin{pmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{pmatrix} - \begin{pmatrix} y_1 & y_2 \\ -y_2^* & y_1^* \end{pmatrix} = \begin{pmatrix} (x_1 - y_1) & (x_2 - y_2) \\ -(x_2 - y_2)^* & (x_1 - y_1)^* \end{pmatrix} \tag{3.12}$$

The corresponding determinant is given by

$$\det(\mathcal{O}_{\mathbf{x}} - \mathcal{O}_{\mathbf{y}}) = |x_1 - y_1|^2 + |x_2 - y_2|^2 \tag{3.13}$$

For the coding gain, one has to minimize the above over all $(x_1, x_2) \neq (y_1, y_2)$ *in* $\mathcal{S}$*. We can see that this amounts to minimizing one of the terms, since both terms are positive. One of the term can go to zero, but not both since we are searching for distinct vectors.*

Hence the coding gain for the Alamouti scheme is given by

$$\Delta = \min_{\mathbf{x}\neq\mathbf{y}\in\mathcal{S}} |\det(\mathcal{O}_{\mathbf{x}} - \mathcal{O}_{\mathbf{y}})|^{2/2} = \min_{x\neq y\in\mathcal{S}} |x-y|^2 \tag{3.14}$$

For the codes analysed in the previous section, given by equation (3.4), the above definition can be modified as follows.

$$\Delta = \min_{\mathbf{s}\neq\tilde{\mathbf{s}}} [|\det T_{\mathbf{s}-\tilde{\mathbf{s}}}|]^{2/n} \tag{3.15}$$

$$\begin{aligned} \text{But } |\det T_{\mathbf{s}-\tilde{\mathbf{s}}}| &= |\psi^{-n} \det P^{-1} \det D_{\mathbf{s}-\tilde{\mathbf{s}}} \det P| \\ &= \psi^{-n} |\det D_{\mathbf{s}-\tilde{\mathbf{s}}}| \\ &= \psi^{-n} \prod_{m=0}^{n-1} |\theta_m^T \cdot (\mathbf{s}-\tilde{\mathbf{s}})| \end{aligned} \tag{3.16}$$

where θ_m^T is the m^{th} row of Θ. Thus the coding gain will be

$$\Delta = \min_{\mathbf{s}\neq\tilde{\mathbf{s}}} \frac{1}{\psi^2} [\prod_{m=0}^{n-1} |\theta_m^T \cdot (\mathbf{s}-\tilde{\mathbf{s}})|^{2/n}] \tag{3.17}$$

Theorem 3.1 (Lower bound on coding gains) *For a code as in Section 3.2, constructed using a monic polynomial over $\mathbb{Z}[j]$ and where the constellation is carved from $\mathbb{Z}[j]$ and normalized by $\sqrt{\mathcal{E}_s}$, the coding gain $\Delta \geq \frac{1}{\psi^2 \mathcal{E}_s}$.*

Proof: For any distinct $\mathbf{s}$ and $\tilde{\mathbf{s}}$, define $g(\alpha) := \sum_{k=0}^{n-1} \sqrt{\mathcal{E}_s}(\mathbf{s}-\tilde{\mathbf{s}})\alpha^k$. As n is the degree of minimal polynomial of $\alpha_i (0 \leq i \leq n-1)$ over $\mathbb{Q}(j)$, $\{1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{n-1}\}$ are linearly independent over $\mathbb{Q}(j)$ (Result 3.2). Hence $g(\alpha_i) \neq 0,\ (0 \leq i \leq n-1)$.

The relative norm of $g(\alpha_0)$ is

$$\mathcal{N}(g(\alpha_0)) := \prod_{m=0}^{n-1} \eta_m(g(\alpha_0)) = \prod_{m=0}^{n-1} g(\alpha_m) \neq 0 \tag{3.18}$$

By Result 3.3, $g(\alpha_0)$ is integral over $\mathbb{Z}[j]$. Using Result 3.4, $\mathcal{N}(g(\alpha_0)) \in \mathbb{Z}[j]\backslash\{0\}$ which together imply $|\mathcal{N}(g(\alpha_0))| \geq 1$. Hence

$$\begin{aligned}
\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s}-\tilde{\mathbf{s}})| &= \prod_{m=0}^{n-1} |\sum_{k=0}^{n-1} \sqrt{\mathcal{E}_s}(s_k - \tilde{s_k})\alpha_m^k| \\
&= |\prod_{m=0}^{n-1} g(\alpha_m)| \\
&= \mathcal{N}(g(\alpha_0)) \geq 1 \qquad (3.19) \\
\text{Coding Gain } \Delta &= \min_{\mathbf{s}\neq\tilde{\mathbf{s}}} \frac{1}{\psi^2}[\prod_{m=0}^{n-1} |\theta_m^T \cdot (\mathbf{s}-\tilde{\mathbf{s}})|^{2/n}] \\
&= \min_{\mathbf{s}\neq\tilde{\mathbf{s}}} \frac{1}{\psi^2\mathcal{E}_s}[\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s}-\tilde{\mathbf{s}})|^{2/n}] \\
&\geq \frac{1}{\psi^2} \cdot \frac{1}{\mathcal{E}_s} \cdot 1 = \frac{1}{\psi^2\mathcal{E}_s}
\end{aligned}$$

□

Example 3.10 (Coding Gain Lower Bound) *Consider the following code. We use $n = 3$ antennas and the code is constructed using the polynomial $x^3 - 2$. Using Theorem 2.5 and since $(2, 3) = 1$, we can say that we can construct codes as in equation (2.30) where γ is replaced by 2, provided the constellation used $\mathcal{S} \subset \mathbb{Q}(j)$. Here, due to the restriction in Theorem 3.1, we have to have $\mathcal{S} \subset \mathbb{Z}[j]$ which ensures $\mathcal{S} \subset \mathbb{Q}(j)$. The code is given by*

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{6}} \begin{pmatrix} s_0 & 2s_2 & 2s_1 \\ s_1 & s_0 & 2s_2 \\ s_2 & s_1 & s_0 \end{pmatrix} : s_i \in \mathcal{S}, i = 0, 1, 2 \right\} \qquad (3.20)$$

where the constellation $\mathcal{S} \subset \mathbb{Z}[j]$. The $\frac{1}{\psi} = \frac{1}{\sqrt{6}}$ multiplication factor is to normalize the Frobenius norm of the codeword matrix to 3. Also assume $\mathcal{S}$ has been normalized by $\sqrt{\mathcal{E}_s}$ to give $\mathcal{S}'$ so that $E[||s||^2]_{s\in\mathcal{S}'} = 1$. Then by the above theorem, the coding gain is lower bounded as

$$\Delta \geq \frac{1}{6 \cdot \mathcal{E}_s} \qquad (3.21)$$

If we use constellation $\mathcal{S}$ itself, without normalizing the expected signal energy, then the

coding gain is lower bounded as $\Delta \geq \frac{1}{6}$.

Theorem 3.2 *For a constellation* $\mathcal{S}$ *containing two neighbour points of* $\mathbb{Z}[j]$ *and normalized by* $\sqrt{\mathcal{E}_s}$*, coding gain* $\Delta = \frac{1}{\psi^2 \mathcal{E}_s}$.

Proof: For $\mathcal{S}$ as above, we can choose $\mathbf{s}$ and $\tilde{\mathbf{s}}$ such that $|\mathbf{s} - \tilde{\mathbf{s}}| = \frac{1}{\sqrt{\mathcal{E}_s}}(1, 0, 0, \ldots, 0)^T$. Then

$$\begin{aligned}
\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s} - \tilde{\mathbf{s}})| &= \prod_{m=0}^{n-1} |\sum_{k=0}^{n-1} \sqrt{\mathcal{E}_s}(s_k - \tilde{s_k})\alpha_m^k| \\
&= \prod_{m=0}^{n-1} |\sqrt{\mathcal{E}_s} \cdot \frac{1}{\sqrt{\mathcal{E}_s}}| = 1 \\
\text{Coding Gain } \Delta &= \min_{\mathbf{s} \neq \tilde{\mathbf{s}}} \frac{1}{\psi^2} [\prod_{m=0}^{n-1} |\theta_m^T \cdot (\mathbf{s} - \tilde{\mathbf{s}})|^{2/n}] \\
&= \min_{\mathbf{s} \neq \tilde{\mathbf{s}}} \frac{1}{\psi^2 \mathcal{E}_s} [\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s} - \tilde{\mathbf{s}})|^{2/n}] \\
&\leq \frac{1}{\psi^2} \cdot \frac{1}{\mathcal{E}_s} \cdot 1 = \frac{1}{\psi^2 \mathcal{E}_s} \qquad (3.22) \\
&\quad \text{(Since minimum would be less than a special case)}
\end{aligned}$$

Using both the above theorems, we can see that for a constellation which has two neighbour points of $\mathbb{Z}[j]$ the coding gain will be

$$\Delta = \frac{1}{\psi^2 \mathcal{E}_s}$$

□

Example 3.11 (Coding Gain) *Consider the same code as in Example 3.10. We can use Theorem 3.2 here, if the constellation* $\mathcal{S}$ *has two neighbour points of* $\mathbb{Z}[j]$*. Consider the constellation given in Figure 3.1, which has neighbour points in* $\mathbb{Z}[j]$*. We can use the the theorem to get the coding gain for the above constellation as*

$$\Delta = \frac{1}{6\mathcal{E}_s} \qquad (3.23)$$

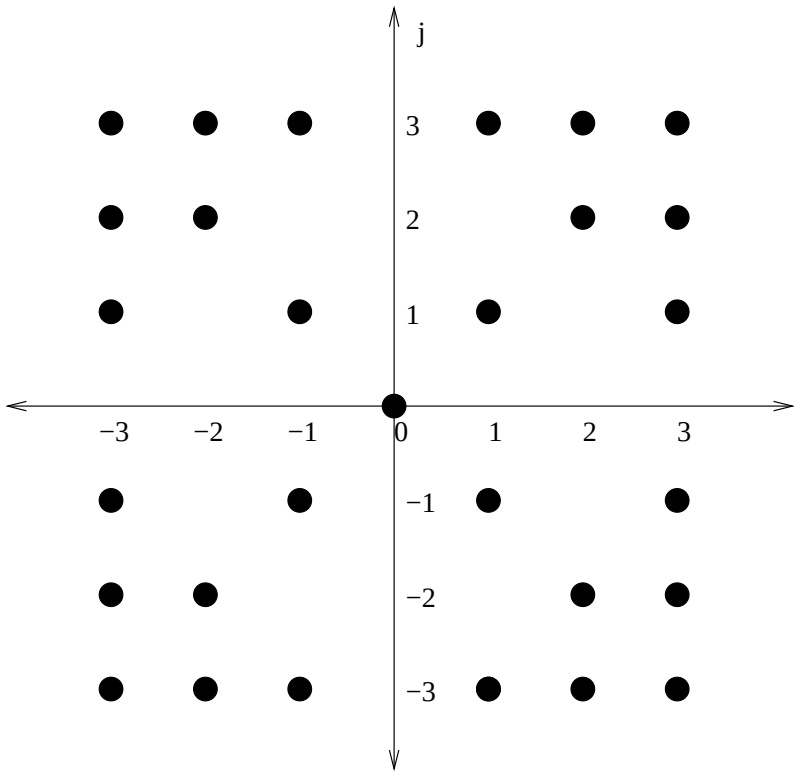


Figure 3.1: Constellation carved from $\mathbb{Z}[j]$ having neighbour points of $\mathbb{Z}[j]$

assuming the constellation is normalized by $\sqrt{\mathcal{E}_s}$ *to make average symbol energy unity. However, if the constellation was used as such, the coding will be given by* $\Delta = \frac{1}{6}$.

3.3.1 Codes over QAM Constellations

Here we consider a special case of the calculation done in the previous section. We determine a closed form expression for the coding gains for codes over QAM Constellations constructed using monic polynomials over $\mathbb{Z}[j]$.

Theorem 3.3 *Consider a QAM Constellation* $\mathcal{S}$ *with signal points from* $(2k-1-Q)d + j(2l-1-Q)d$ *where* $k, l \in \{1, 2, \ldots, Q\}, d \in \mathbb{N}$ *and normalized by* $\sqrt{\mathcal{E}_s}$. *Then coding gain* $\Delta = \frac{4d^2}{\psi^2 \mathcal{E}_s}$.

Proof:We can write $\sqrt{\mathcal{E}_s}(s_k - \tilde{s_k}) = 2dz_k$ where $z_k \in \mathbb{Z}[j]$.

$$\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s} - \tilde{\mathbf{s}})| \quad = \quad (2d)^n \prod_{m=0}^{n-1} |\theta_m^T \cdot \mathbf{z}|$$

$$
\begin{aligned}
&= (2d)^n \prod_{m=0}^{n-1} |\sum_{k=0}^{n-1} z_k \alpha_m^k| \\
&= (2d)^n |\mathcal{N}(\sum_{k=0}^{n-1} z_k \alpha_0^k)| \\
&\geq (2d)^n \qquad (3.24) \\
\text{Coding Gain } \Delta &= \frac{1}{\psi^2 \mathcal{E}_s} \min_{\mathbf{s} \neq \tilde{\mathbf{s}}} [\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s} - \tilde{\mathbf{s}})|^{2/n}] \\
&\geq \frac{1}{\psi^2 \mathcal{E}_s} (2d)^2 = \frac{4d^2}{\psi^2 \mathcal{E}_s} \qquad (3.25)
\end{aligned}
$$

Now consider the case when $\mathbf{s}$ and $\tilde{\mathbf{s}}$ are such that $(\mathbf{s} - \tilde{\mathbf{s}}) = \frac{2d}{\sqrt{\mathcal{E}_s}}(1, 0, 0, \ldots, 0)^T$. As in Theorem 3.2 we can show that $\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s} - \tilde{\mathbf{s}})| = (2d)^n$ and hence coding gain, being the minimum, will be at most $\frac{4d^2}{\psi^2 \mathcal{E}_s}$. Since we have shown the lower bound, we can make it an equality for the coding gain.

$$\text{Coding Gain } \Delta = \frac{4\mathrm{d}^2}{\psi^2 \mathcal{E}_\mathrm{s}}$$

□

Thus coding gains for codes over constellations carved from $\mathbb{Z}[j]$ and constructed using any monic polynomial over $\mathbb{Z}[j]$ are determined.

Example 3.12 (Coding Gain for QAM Constellations) *Here also we consider the same code as in Example 3.10. But we take a different constellation this time, we choose the* $16 - QAM$ *constellation given by* $\mathcal{S} = \{(2x - 5) + j(2y - 5) : x, y = 1, 2, 3, 4\}$ *as shown in Figure 3.2. For this constellation, we have* $d = 1$*, where* d *is a parameter of the constellation defined in Theorem 3.3. The coding gain is given by*

$$\Delta = \frac{4}{6\mathcal{E}_s} = \frac{2}{3\mathcal{E}_s} \quad \textit{(since } d = 1\textit{)} \qquad (3.26)$$

If the constellation is not normalized for unit average energy, we have coding gain $\Delta = \frac{2}{3}$.

Note that this theorem holds for codes constructed using non-cyclotomic polynomials also. Consider the code given in Example 2.9 also. Recall that, the code there is also usable

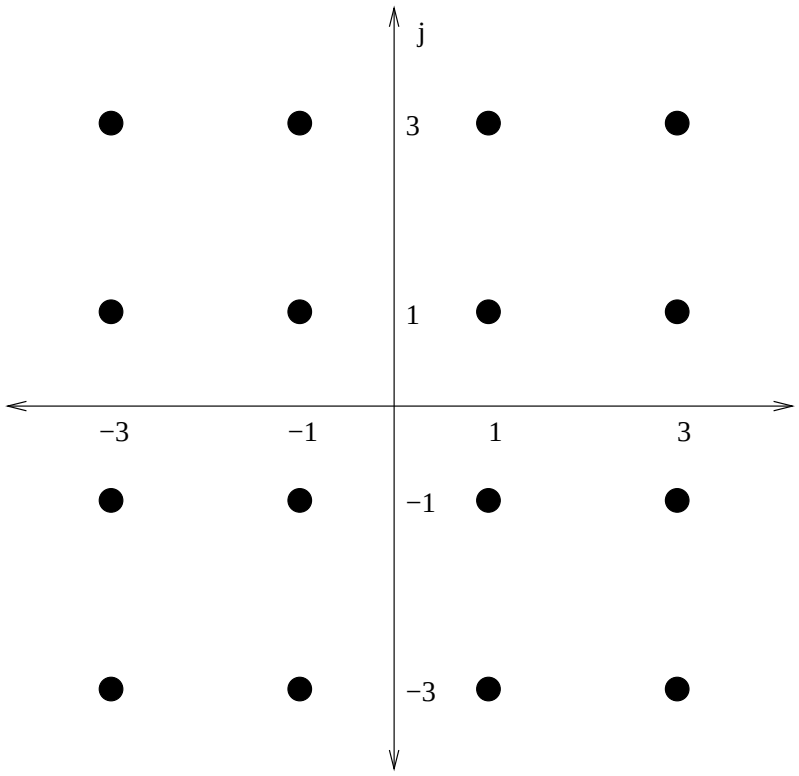


Figure 3.2: 16-QAM Constellation

for QAM constellations. This code is constructed using a non-cyclotomic polynomial. Here the normalizing factor needed is $\psi = \sqrt{10}$. *So here, if we use the above constellation, we can say that the coding gain* $\Delta = \frac{2}{5\mathcal{E}_s}$.

3.3.2 Codes over rotated QAM Constellations

We extend the calculation of the coding gain, to rotated QAM constellations.

Definition 3.5 (Rotated QAM Constellation) *A constellation* $\mathcal{S}$ *with signal points from* $[(2k-1-Q)d + j(2l-1-Q)d]e^{j\phi}$ *where* $k, l \in \{1, 2, \ldots, Q\}, d \in \mathbb{N}$ *and* $\phi \in [0, 2\pi]$ *is a rotating angle. The constellation would be a QAM constellation rotated anticlockwise by* ϕ *radians.*

Theorem 3.4 *Consider a code over a rotated QAM constellation* $\mathcal{S}$ *as defined above and energy normalized by* $\sqrt{\mathcal{E}_s}$. *Then the coding gain is the same as that stated in Theorem 3.3 and is given by* $\Delta = \frac{4d^2}{\psi^2 \mathcal{E}_s}$.

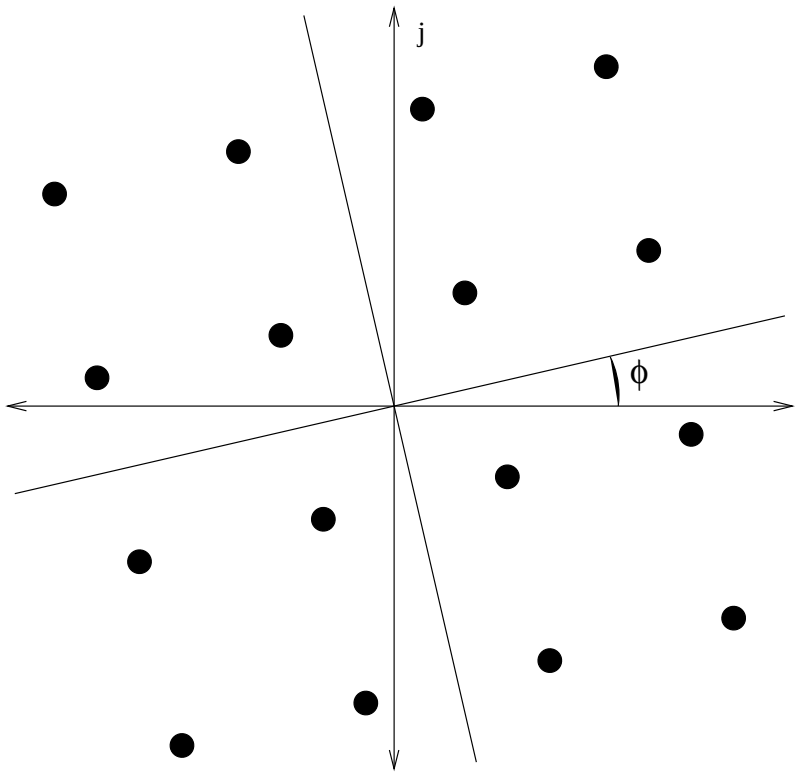


Figure 3.3: Rotated 16-QAM Constellation

Proof: The code is constructed in exactly the same way as in Theorem 3.3, the constellation has the same structure but every signal point has a multiplicative factor of $e^{j\phi}$ along with it. Hence $\sqrt{\mathcal{E}_s}(s_k - \tilde{s_k}) = 2dz_k \cdot e^{j\phi}$, where $z_k \in \mathbb{Z}[j]$.

$$\begin{aligned}
\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s}-\tilde{\mathbf{s}})| &= (2d)^n |e^{nj\phi}| \prod_{m=0}^{n-1} |\theta_m^T \cdot \mathbf{z}| \\
&= (2d)^n \prod_{m=0}^{n-1} |\theta_m^T \cdot \mathbf{z}| \\
\text{(from (3.24))} \quad &\geq (2d)^n \qquad (3.27) \\
\text{Coding Gain } \Delta &= \frac{1}{\psi^2 \mathcal{E}_s} \min_{\mathbf{s}\neq\tilde{\mathbf{s}}} [\prod_{m=0}^{n-1} |\theta_m^T \cdot \sqrt{\mathcal{E}_s}(\mathbf{s}-\tilde{\mathbf{s}})|^{2/n}] \\
&\geq \frac{1}{\psi^2 \mathcal{E}_s}(2d)^2 = \frac{4d^2}{\psi^2 \mathcal{E}_s} \qquad (3.28)
\end{aligned}$$

Now consider the case when $\mathbf{s}$ and $\tilde{\mathbf{s}}$ are such that $(\mathbf{s}-\tilde{\mathbf{s}}) = \frac{2d}{\sqrt{\mathcal{E}_s}} e^{j\phi}(1,0,0,\ldots,0)^T$. Like in the previous theorem, this would give us an upper bound. Combining both, we get

equality for the coding gain $\Delta = 4d^2/\psi^2\mathcal{E}_s$. □

Example 3.13 (Coding Gain for Rotated QAM Constellations) *Consider the same code as in Example 3.10. We can use that code over a rotated QAM constellation. A rotated* 16*-QAM constellation is given in Figure 3.3. Note that here also, the parameter* $d = 1$*. Assuming the constellation is normalized to unit energy by* $\sqrt{\mathcal{E}_s}$*, the coding gain is given by*

$$\Delta = \frac{4}{6\mathcal{E}_s} = \frac{2}{3\mathcal{E}_s} \tag{3.29}$$

When the constellation is not normalized, the coding gain $\Delta = \frac{2}{3}$*.*

Note that this holds good for non-cyclotomic extensions also. For instance, we can apply this to the code described in Example 2.9. It must be noted that the code remains full-diversity over the rotated constellation also. If we use the code in Example 2.9 over the constellation shown in Figure 3.3, the coding will be $\Delta = \frac{2}{5\mathcal{E}_s}$*. (The normalizing factor to be used in Example 2.9 is* $\psi = \sqrt{10}$*.)*

3.4 Codes from Transcendental Extensions

These codes are mentioned in [16] and was discussed in Section 2.7.5. A point that can be noted here is that, we are able to get bounds over the coding gains only because the extensions done here over the base field are algebraic in nature. If we are extending using transcendental numbers, we cannot assert anything about the coding gains. An example of codes from transcendental extensions is given in Example 2.11. The following example shall illustrate that.

Consider extension using the polynomial $x^n - \gamma$ where γ is a transcendental number. We can try to construct a code over this polynomial, the resulting code will be as in equation (2.30). If the constellation used is some subset of $\mathbb{Q}[j]$ or $\mathbb{Z}[j]$, we can see that the determinant would be a polynomial in γ with rational coefficients. And since γ is transcendental, this would never go to zero. So we are assured of full-rank and diversity. But if we do not carry out any maximization/optimization for the coding gain, we would not get any lower bounds on the coding gain. We can be see that as follows.

As a consequence of the *Lindemann Weierstrass Theorem* [33](Theorem A.1 in the Appendix), any number of the form $e^{j\theta}$ would be transcendental for θ algebraic. Let us choose the constellation to be a subset of $\mathbb{Z}[j]$, say 16-QAM. For the two antenna ($n = 2$) case, the code is given by $\begin{pmatrix} s_0 & \gamma s_1 \\ s_1 & s_0 \end{pmatrix}$. The coding gain would be given by $|s_0^2 - \gamma s_1^2|$. If we choose θ to be a rational close to π, and $s_1 = 1 + j, s_2 = -1 + j$, we can see that the coding gain becomes arbitrarily small. So we cannot make assertions on the coding gains, for codes over transcendental extensions, unless optimization has been carried to ensure the same.

3.5 High-Rate Codes from Field Extensions

High-rate codes were explained in [16, 19] and Section 2.7.5. In this section, we shall propose an upper bound to the coding gain achieved by a class of codes which subsumes the High-Rate codes. This is a generalization of the upper bound for coding gain given in [25]. We shall specify a class of codes and then propose the bound.

Consider vectors of the form $\mathbf{s} = (s_0(z), s_1(z), s_2(z), \ldots, s_{n-1}(z))^T$ where each $s_i(z) = \sum_{k=0}^{R-1} s_{i,k} z^k$ and $s_{i,k} \in \mathcal{S} \subset \mathbb{Z}[j] \forall i, k$. Consider rotational matrices Θ which would take $\mathbf{s}$ to $\mathbf{u}$ where $\mathbf{u} = \Theta\mathbf{s}$.

$$\mathbf{u} = (u_0(z), u_1(z), u_2(z), \ldots, u_{n-1}(z))^T = \Theta\mathbf{s} \tag{3.30}$$

Take the rotated vector and form a diagonal matrix $\mathrm{diag}(u_0(z), u_1(z), \ldots, u_{n-1}(z))^T$. Replace z by a transcendental number of the form $e^{j\lambda}$ where λ is algebraic. This would ensure that the code would have full diversity. This is the codeword for a code with rate R. We shall propose the following upper bound for these codes.

Let the constellation $\mathcal{S}$ have an average energy $\mathcal{E}_s$. That is $E(|s|^2)_{s\in\mathcal{S}} = \mathcal{E}_s$. Also assume that the constellation is zero mean, ie., $E(s)_{s\in\mathcal{S}} = 0$. Then

$$E(|s_i(z)|^2) \quad = \quad E(\sum_{k=0}^{R-1} |s_{i,k} z^k|^2)$$

$$\begin{aligned}(|z|=1) \Rightarrow \quad &= E(\sum_{k=0}^{R-1} |s_{i,k}|^2) \\ &= R \cdot \mathcal{E}_s \end{aligned} \tag{3.31}$$

For fair comparison, we should normalize the power by $\sqrt{\mathcal{E}_s}$ and then do the analysis so that $E(||\mathbf{s}||^2) = R \cdot n$.

Theorem 3.5 (Upper bound on coding gain) *Consider a constellation $\mathcal{S} \subset \mathbb{Z}[j]$, normalized by $\sqrt{\mathcal{E}_s}$. Consider all rotation matrices which have the property $E(||\Theta\mathbf{s}||^2) = E(||\mathbf{s}||^2) = Rn$. Then the coding gain is upper bounded as follows*

$$\textit{Coding Gain} \quad \Delta \leq \frac{d_s^2}{n\mathcal{E}_s} \tag{3.32}$$

where $d_s = \min_{i \neq j} |s_i(z) - s_j(z)|$, the minimum distance between any two polynomial symbols.

*Proof:*Let Θ satisfy the power constraint $E(||\Theta\mathbf{s}||^2) = E(||\mathbf{s}||^2) = Rn$. After normalization, $E(|s_i(z)|^2) = R$. We know that $E(||\mathbf{s}||^2) = E(\mathbf{s}^*\mathbf{s})$. We can also say $E(s_i(z) \cdot s_i(z)^*) = R.I_n$, where I_n is the identity matrix of order n. Thus

$$\begin{aligned} R \cdot n = E(||\Theta\mathbf{s}||^2) = E(\mathbf{s}^*\Theta^*\Theta\mathbf{s}) &= E(\mathrm{tr}[\mathbf{s}\mathbf{s}^*\Theta^*\Theta]) \\ &= \mathrm{tr}[E(\mathbf{s}\mathbf{s}^*\Theta^*\Theta)] \\ &= \mathrm{tr}[E(\mathbf{s}\mathbf{s}^*)\Theta^*\Theta] \\ &= \mathrm{tr}[R \cdot \Theta^*\Theta] \\ &= R \cdot \mathrm{tr}[\Theta^*\Theta] \end{aligned} \tag{3.33}$$

$$\text{Thus} \quad \mathrm{tr}[\Theta^*\Theta] = n \tag{3.34}$$

By definition of the trace of a matrix and the non-negativity of the diagonal entries of $\Theta^*\Theta$, there exists at least one column of Θ with its Euclidean norm≤ 1. Without loss of generality, we can assume that the Euclidean norm of the pth column is ≤ 1, and let $\{\mathbf{s}, \tilde{\mathbf{s}}\}$ be a particular pair with $\mathbf{s} - \tilde{\mathbf{s}} = d_s\mathbf{e}_p/\sqrt{\mathcal{E}_s}$, where $\mathbf{e}_p$ is the pth column of the identity

matrix. Using that $||\theta_p||^2 = \sum_{m=1}^{n} |\theta_{mp}|^2 \leq 1$ (where θ_p is the pth column and θ_{mp} is the (m,p)th element of Θ), and the *AM-GM inequality*, the product distance of $\mathbf{s} - \tilde{\mathbf{s}}$ can be calculated as follows.

$$\begin{aligned} \prod_{m=1}^{n} |\theta_m^T(\mathbf{s}-\tilde{\mathbf{s}})|^2 &= \left(\frac{d_s^2}{\mathcal{E}_s}\right)^n \prod_{m=1}^{n} |\theta_{mp}|^2 \\ \text{(AM-GM ineq.)} \Rightarrow &\leq \left(\frac{d_s^2}{\mathcal{E}_s}\right)^n \left(\frac{\sum_{m=1}^{n} |\theta_{mp}|^2}{n}\right)^n \\ &\leq \left(\frac{d_s^2}{n\mathcal{E}_s}\right)^n \end{aligned} \tag{3.35}$$

Since the coding gain is the minimum taken over all pairs of matrix codewords, it would be less than a special case. Thus the coding gain would be upper bounded by

$$\text{Coding Gain} \quad \Delta \leq \frac{d_s^2}{n\mathcal{E}_s}.$$

□

Example 3.14 (High-Rate Codes : Upper bound for Coding Gain) *Consider a rate $R = 3$ symbols PCU high-rate code for $n = 4$ transmit antennas. Thus* $\mathbf{s}$ *is given as follows.*

$$\mathbf{s} = \begin{bmatrix} s_{00} + s_{01}z + s_{02}z^2 \\ s_{10} + s_{11}z + s_{12}z^2 \\ s_{20} + s_{21}z + s_{22}z^2 \\ s_{30} + s_{31}z + s_{32}z^2 \end{bmatrix} \tag{3.36}$$

where z is a transcendental number of the form $e^{j\lambda}$, where λ is algebraic. This vector $\mathbf{s}$ *is rotated by a rotation matrix Θ, which would give $\mathbf{u} = \Theta\mathbf{s}$. Θ would extend the field to a higher algebraic dimension. The transmitted code will be power normalized/distributed version of the diagonal matrix $D = diag(\mathbf{u})$. Let the points s_{ij} come from a constellation $\mathcal{S} \subset \mathbb{Z}[j]$. Then we can use the above theorem, since the code has been power normalized.*

The coding gain of this code is upper bounded by the above theorem as follows.

$$\Delta \leq \frac{d_s^2}{4\mathcal{E}_s} \tag{3.37}$$

where d_s is the minimum Euclidean distance between all points $s_i(z)$ in the expanded constellation given by $d_s = \min_{i \neq j} |s_i(z) - s_j(z)|$.

One can also use the above theorem to upper bound for the coding gain for the rate $R = 2$ symbols PCU code from field extensions described in Example 2.12 also. We get $\Delta \leq \frac{d_s^2}{3\mathcal{E}_s}$, where d_s is similarly defined.

We can see that when diagonalized, the High-Rate Codes in [16, 19] and Section 2.7.5, would give a diagonal matrix of the above form. This can be seen by analysis similar to that done in Section 3.2. But for them, this bound is rather loose, for we can get a closer upper bound by taking some trivial cases. In this section, we have derived an upper bound for a more general class of codes than the high-rate codes from field extensions described in Section 2.7.5. It might be an interesting problem to investigate into the special case of high-rate codes from field extensions alone.

Chapter 4

High-Rate Codes from Field Extensions vs. TAST

In this chapter, we try to study the difference between the structures of two types of STBC's namely High-Rate codes (Codes from Division Algebras) and Threaded Algebraic Space-Time Codes (a generalization of DAST).

4.1 DAST, STCR & Rate 1 Codes from Division Algebras

In [21] (also explained here in Section 2.6.1), the proposed Diagonal Algebraic Space-Time(DAST) code uses rotation matrices for creating constellations of full-modulation diversity. Each codeword matrix corresponds to a point in the rotated constellation. The full diversity of the STBC come from the rotation matrices that are used. These have been obtained from [22, 24] wherein irreducible polynomials are used to construct rotations which assure certain diversity. The diagonal matrix codewords are multiplied by *Walsh Hadamard matrices* to improve the peak-average ratio of the code.

The rate 1 codes from field extensions [16, 17, 18] have been analysed in Section 3.2 as a part of the calculation of coding gain. It has been found that this code, when diagonalized, gives, a diagonal matrix with a structure similar to that of DAST. By equation (3.8) we

can see the diagonalized version of the rate 1 code from field extension. We can clearly see that this diagonal matrix has been obtained by rotating the code vector by a rotational matrix Θ given by

$$\Theta = \begin{bmatrix} 1 & \alpha_0 & \alpha_0^2 & \dots & \alpha_0^{n-1} \\ 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n-1} & \alpha_{n-1}^2 & \dots & \alpha_{n-1}^{n-1} \end{bmatrix} \tag{4.1}$$

where $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ are the roots of the irreducible polynomial over which the code is constructed.

The above Θ matrix is exactly the same proposed as the Space-Time Constellation Rotating(STCR) Codes in [25] (explained in Section 2.6.2 here). But in [25], codes were proposed only for a restricted number of transmit antennas because only codes were constructed only for some specific polynomials. Hence we can see that the STCR codes, are clearly a subclass of the rate 1 codes from field extensions.

From Section 3.2 and equation (4.1) above, we can see that the codes from DAST are a subset of those from field extensions, like the STCR codes. This is because, DAST provides codes only for restricted number of transmit antennas. The approach in DAST [21] is different from that in STCR, but both of them use some specific polynomials. Hence rotation matrices obtained in DAST are only some special cases of the general theory developed as codes from field extensions. In [16, 17, 18], a generalized theory has been proposed, which covers all the codes mentioned in DAST.

4.2 High-Rate Codes vs. TAST

The High-Rate Codes over Field Extensions were proposed in [16, 19] (explained in Section 2.7.5 here). Here the theory of Rate 1 codes over Field Extensions were extended to obtain codes of arbitrary rate $R > 1$ symbols per channel use and arbitrary number of antennas. The Threaded Algebraic Space-Time(TAST) Codes [28] (Section 2.6.3 here) were a generalization of DAST and proposed a rate increase to $R \leq n$, where n is the number of transmit antennas.

By doing an analysis similar to that done for Rate 1 codes done in Section 3.2, we can get the diagonalization decomposition for the High-Rate codes, the corresponding diagonal matrix $D_s = \text{diag}(\mathbf{v})$ where $\mathbf{v}$ was given by

$$\mathbf{v} = \begin{bmatrix} s_0(z) + s_1(z)\alpha_0 + s_2(z)\alpha_0^2 + \ldots + s_{n-1}(z)\alpha_0^{n-1} \\ s_0(z) + s_1(z)\alpha_1 + s_2(z)\alpha_1^2 + \ldots + s_{n-1}(z)\alpha_1^{n-1} \\ \vdots \\ s_0(z) + s_1(z)\alpha_{n-1} + s_2(z)\alpha_{n-1}^2 + \ldots + s_{n-1}(z)\alpha_{n-1}^{n-1} \end{bmatrix} = \Theta \cdot \mathbf{s} \tag{4.2}$$

where Θ and $\mathbf{s}$ are given by

$$\Theta = \begin{bmatrix} 1 & \alpha_0 & \alpha_0^2 & \ldots & \alpha_0^{n-1} \\ 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n-1} & \alpha_{n-1}^2 & \ldots & \alpha_{n-1}^{n-1} \end{bmatrix} \text{ and } \mathbf{s} = \begin{bmatrix} s_0(z) \\ s_1(z) \\ \vdots \\ s_{n-1}(z) \end{bmatrix}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are the roots of the irreducible polynomial over which the code is constructed and $s_j(z) = \sum_{i=0}^{R-1} s_{ij} z^i$, where s_{ij} are the symbols to be sent.

The DAST codes have a form consisting of a diagonal matrix, by definition itself. But when it comes to analysing TAST (see matrix in equation (2.23)), wherein you have more than one thread of coded symbols, diagonalization becomes difficult. We attempted to find any algebraic structure in the TAST codes apart from the known thread structure by definition.

As an example, we can consider the two matrices as given below

$$A = \begin{pmatrix} 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \\ 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix} \tag{4.3}$$

We can see that both of them are the same vector $\mathbf{v} = (1, 2, 3, 4)^T$ put on different threads (as defined by equation (2.20)). We shall try to see what form they take, when

diagonalized. These matrices are diagonalized as $A = P_A^{-1} D_A P_A$ and $B = P_B^{-1} D_B P_B$, where D_A and D_B are the diagonal matrices given by

$$D_A = \text{diag}\begin{pmatrix} -2.213 & 2.213j & -2.213j & 2.213 \end{pmatrix} \tag{4.4}$$

$$D_B = \text{diag}\begin{pmatrix} 1.732 & -1.732 & 2.828 & -2.828 \end{pmatrix} \tag{4.5}$$

Both A and B are the same vector sent on different threads. But when diagonalized, we can see that the resultant diagonal matrices D_A and D_B do not have any relation with each other. Also they do not have any apparent relation with the original vector $\mathbf{v} = (1, 2, 3, 4)^T$. Moreover, the computation shows that the diagonalizing matrices P_A and P_B are also different. This means that there is no way to diagonalize the TAST code simultaneously so that the information in the separate threads remain nicely separated. This was not the case with the High-Rate code based on field extensions wherein the diagonalization (see equation (4.2)) gave a nicely separated matrix from which each information symbol can be easily seen. We can see that the TAST matrices diagonalize without any apparent structure.

From the above arguments, we shall conclude that there is no connection between the TAST codes and the High-Rate codes obtained from field extensions, in general.

4.3 Remarks

We analysed the TAST codes and the High-Rate codes from field extensions to check for any relations between the two. This investigation was motivated by the fact that the rate 1 cases of these two codes, DAST and Rate 1 codes over field extensions, when analysed, were found to be very much the same in their structure. The DAST and STCR codes were clearly seen to be a subclass of the Rate 1 codes mentioned in [16, 17, 18].

Further investigation with TAST and High-Rate codes did not give any signs of similarity between the two. Hence we conclude that these codes are not the same in general, except for their rate 1 cases. This is illustrated as a Venn Diagram in the Figure 4.1 shown.

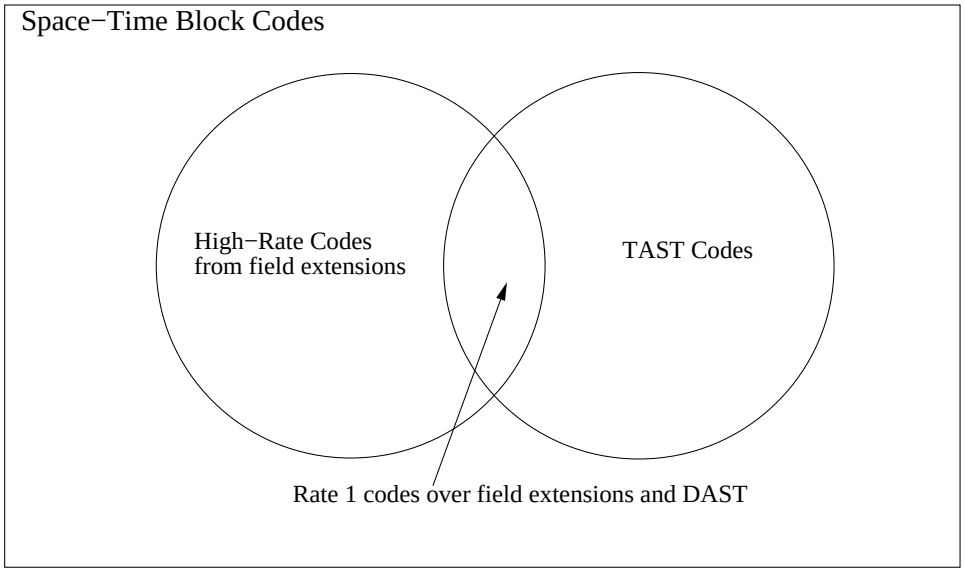


Figure 4.1: Relation of TAST and High-Rate codes over field extensions

Chapter 5

PAPR for DAST-like codes

In this chapter we investigate the feasibility of some Generalized transform matrices for power unifying the codes like DAST and hence minimizing the Peak-to-Average Power Ratio (PAPR).

DAST codes, explained in [21], use a matrix as a part of the code construction, mainly to distribute the power. This matrix would be used to transform a diagonal matrix to get the codeword matrix which would be transmitted. It has been shown in [21] that this matrix has to be unitary to maintain the diversity and other code properties. Hadamard matrices have been used for this purpose in [21]. The unitary condition motivates us to try out the viability of certain other known transform matrices and to see any improvement in the PAPR.

5.1 Generalized Reverse Jacket Transform

In [32], Moon Ho Lee *et al.* discussed about some generalizations of the Walsh Hadamard transforms. They proposed *Generalized Reverse Jacket Transform* which unified the Walsh Hadamard Transform (WHT), center-weighted Hadamard Transform (CWHT) and complex reverse-jacket transform (CRJT).

These transforms are defined and explained in [32]. The matrix form of all these transforms are also given. As an example, the Generalized Reverse Jacket Transform for

$n = 12$ is reproduced here from [32].

$$G = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & w\alpha & w\alpha & w\alpha^2 & w\alpha^2 & w\alpha^5 & w\alpha^5 & w\alpha^4 & w\alpha^4 & -1 & -1 \\
1 & -1 & w\alpha & -w\alpha & w\alpha^2 & -w\alpha^2 & w\alpha^5 & -w\alpha^5 & w\alpha^4 & -w\alpha^4 & -1 & 1 \\
1 & 1 & w\alpha^2 & w\alpha^2 & w\alpha^4 & w\alpha^4 & w\alpha^4 & w\alpha^4 & w\alpha^2 & w\alpha^2 & 1 & 1 \\
1 & -1 & w\alpha^2 & -w\alpha^2 & w\alpha^4 & -w\alpha^4 & w\alpha^4 & -w\alpha^4 & w\alpha^2 & -w\alpha^2 & 1 & -1 \\
1 & 1 & w\alpha^5 & w\alpha^5 & w\alpha^4 & w\alpha^4 & w\alpha & w\alpha & w\alpha^2 & w\alpha^2 & -1 & -1 \\
1 & -1 & w\alpha^5 & -w\alpha^5 & w\alpha^4 & -w\alpha^4 & w\alpha & -w\alpha & w\alpha^2 & -w\alpha^2 & -1 & 1 \\
1 & 1 & w\alpha^4 & w\alpha^4 & w\alpha^2 & w\alpha^2 & w\alpha^2 & w\alpha^2 & w\alpha^4 & w\alpha^4 & 1 & 1 \\
1 & -1 & w\alpha^4 & -w\alpha^4 & w\alpha^2 & -w\alpha^2 & w\alpha^2 & -w\alpha^2 & w\alpha^4 & -w\alpha^4 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1
\end{bmatrix} \tag{5.1}$$

where $\alpha = e^{j\frac{\pi}{3}}$ and $w \in \mathbb{R}$ is the weight. From [32], it is known that GRJT gives Walsh Hadamard Transform, when $\alpha = w = 1$.

5.2 Peak-to-Average Power Ratio (PAPR) of DAST codes

The Peak-to-Average Power Ratio (PAPR) of an STBC can be defined as follows. Let $B = [b_{ij}]$ be an $n \times n$ code matrix consisting of complex entries. Then

$$\text{PAPR} \triangleq \frac{\max_{1 \le i,j \le n} |b_{ij}|^2}{\sum_{1 \le i,j \le n} |b_{ij}|^2 / n^2} \tag{5.2}$$

From equation (2.18), we can see the DAST matrix which would be transmitted (for $n = 4$ antennas). We can see that all the elements there are the rotated elements multiplied by ± 1. Here, we would like to get a better PAPR performance for the DAST codes by keeping the code structure the same. In other words, we search for a unitary matrix, to

replace the $\mathcal{H}_n$ in equation (2.15), which would improve the PAPR performance.

From the structure of the Generalized Transforms and the Diagonal codes, we can see that pre-multiplying the diagonal matrix by a unitary matrix is equivalent to scaling each column of the unitary matrix by the corresponding elements of the diagonal matrix. Thus, we see that, the PAPR, would be the same even if we use matrices with different roots of unity. Any matrix, consisting of only complex numbers with magnitude 1, used in place of the Hadamard matrix in equation (2.15), would give the same PAPR. We can state that as follows.

Result 5.1 (Effect of unweighted transforms on PAPR) *The PAPR of DAST codes will be same, even when the $\mathcal{H}_n$ of equation (2.15) is replaced with matrices having complex entries of magnitude 1.*

Example 5.1 (Unweighted Transforms) *Consider a DAST code with a rotated vector given by $\mathbf{x} = (x_0, x_1, x_2, x_3)^T$ and let the corresponding diagonal matrix be $D = diag(\mathbf{x})$. Now when using the Hadamard matrix $\mathcal{H}_4$ to power distribute it, we get $\mathcal{H}_4 D$ and when we use Complex Reverse-Jacket Transform C_4, we get $C_4 D$. Let us call the power unified matrices, $\mathcal{H}_4 D = A$ and $C_4 D = B$. A and B are given by*

$$A = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & -x_2 & x_3 & -x_4 \\ x_1 & x_2 & -x_3 & -x_4 \\ x_1 & -x_2 & -x_3 & x_4 \end{bmatrix} \quad and \quad B = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & -x_2 j & x_3 j & -x_4 \\ x_1 & x_2 j & -x_3 j & -x_4 \\ x_1 & -x_2 & -x_3 & x_4 \end{bmatrix} \tag{5.3}$$

If we denote each element of A by a_{ij} and that of B by b_{ij}, we can easily see that $|a_{ij}| = |b_{ij}$, from the above matrices. This, in fact, is true for any transform matrix containing only elements of magnitude 1.

Thus the only remaining point of interest is when the GRJT are used with a weight $w \neq 1$. Thinking on similar lines to the above result, we can see that in analyses pertaining to PAPR of DAST-like codes, we just need to consider the magnitude of the entries involved in the transform matrix.

5.3 Effect of the weight w on PAPR

In this section, we shall inspect the effect of weighted transforms on the PAPR of DAST-like codes. We shall examine the same, taking a particular case, ie., square matrices with $n = 4$. We use the Center Weighted Hadamard Transform (CWHT) W_4 [32] for $n = 4$. Assume we have a rotated vector and it has been put in the diagonal to give a matrix D. Let the matrices be given as follows.

$$W_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -w & w & -1 \\ 1 & w & -w & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \text{ and } D = \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix} \tag{5.4}$$

where $\mathbf{x} = (x_1, x_2, x_3, x_4)^T$ is the rotated symbol vector given by equation (2.14). Notice that when the weight $w = 1$, we get the Walsh Hadamard Transform. We can see that $W_4 D$ is given by

$$W_4 D = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & -wx_2 & wx_3 & -x_4 \\ x_1 & wx_2 & -wx_3 & -x_4 \\ x_1 & -x_2 & -x_3 & x_4 \end{bmatrix} \tag{5.5}$$

We study the usefulness of the above assuming $w > 1$. We can easily see that the peak magnitude increases by w when $\max\{|x_1|, |x_2|, |x_3|, |x_4|\}$ is $|x_2|$ or $|x_3|$. Also the average, though it increases, does so by a smaller scale. So PAPR does not improve. Since the original signal set is rotated to get the vector $\mathbf{x}$ and considering the fact that there are four independent symbols chosen, we cannot control which one of the components of $\mathbf{x}$ is maximum beforehand. So we cannot use the weighted transform matrix and be sure of any improvement in PAPR.

In the case where $w < 1$, we can similarly see that the PAPR does not improve when $\max\{|x_1|, |x_2|, |x_3|, |x_4|\}$ is $|x_1|$ or $|x_4|$. Then also we cannot be sure of any improvement in PAPR. We can state this as follows.

Result 5.2 (Effect of wieght w) *When weighted transforms are used, no assurance can be made concerning the improvement in the PAPR of DAST-like codes with respect to the case when Walsh Hadamard Transforms are used.*

Example 5.2 (Effect of weight w) *We shall consider a case, when we use Center-Weighted Hadamard Transform (CWHT) with weight $w = 2$. As a special case of equation (5.5), we get the power distributed matrix as follows.*

$$W_4 D = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & -2x_2 & 2x_3 & -x_4 \\ x_1 & 2x_2 & -2x_3 & -x_4 \\ x_1 & -x_2 & -x_3 & x_4 \end{bmatrix} \tag{5.6}$$

Let us take a case when $(x_1, x_2, x_3, x_4) = (18, 10, 7, 3)$ (As the rotated vector depends on four input symbols which can be chosen independently, we can reasonably assume that the elements of the rotated vector would be in any order possible). In this case the power distribution using Hadamard matrix gives a matrix with Peak-to-Average Power Ratio (PAPR) 2.688. When we use CWHT, we get a PAPR of 2.268. This means that we do not get any improvement.

When the rotated vector is $(x_1, x_2, x_3, x_4) = (10, 7, 18, 3)$, the PAPR obtained are as follows. The Hadamard transform distributes the power giving a PAPR of 2.688. The CWHT results in a codeword matrix, having PAPR of 4.977. Here we get an improvement.

A simple permutation in the rotated vector causes improvement/degradation of the PAPR. Hence we cannot assure of any improvement in PAPR due to weighted transforms. The case is similar when we use other weights $w > 1$ and $w < 1$ also.

Since we have seen that no assurance can be given on the improvement in PAPR, we can suggest that one can use the Walsh Hadamard Transform itself for the power distribution purposes during the construction of DAST-like codes. Since there is no scope for better PAPR, we can conclude that there is no need to go for more complex transforms.

Chapter 6

Conclusions

6.1 Summary of the thesis

In this thesis, we study the coding gain and other properties of the codes from field extensions [16]. A closed form expression for the coding gain is found out for a class of rate 1 codes from field extensions. An upper bound has been proposed for a class of codes that includes the High-Rate codes of [16]. The codes DAST [21] and STCR [25] have been shown to a subset of the codes over field extensions in [16]. The relationship between TAST codes [28] and the High-Rate codes in [16] have been studied. The feasibility of using certain generalized transforms for improving PAR performance of DAST-like codes were studied. Specifically, the contributions (new results) of this thesis are

- We provide a closed form expression for the coding gain for a sub-class of STBC's from field extensions [26].
- We provide an upper bound for the coding gain for a class of High-Rate STBC's which subsumes the High-Rate STBC's from field extensions.
- We show that DAST and Space-Time Constellation-Rotating(STCR) Codes are a subclass of the codes from field extensions [26].
- The Threaded Algebraic Space-Time(TAST) codes are shown to be *not* the same as High-Rate STBC's from field extensions.

- The Generalized Reverse Jacket Transform(GRJT) is shown *not* to provide any improvement in the PAPR of codes like DAST.

We shall now observe the scope for further work, which seems to be feasible in this area.

6.2 Scope for future work

Here we point out some areas in which further progress can be done.

- The coding gain has been found out for codes formed using monic polynomials over $\mathbb{Z}[j]$ only. It would be interesting to extend the result to polynomials over $\mathbb{Q}[j]$.
- The coding gain has been calculated for codes over QAM constellations where the symbols come from $\mathbb{Z}[j]$. Again, one could look into generalizing this to constellations coming from $\mathbb{Q}[j]$.
- The upper bound found for the High-Rate codes is seen to be a loose bound for some cases. Finding out tighter bounds can be attempted.
- The coding gain for the latter half of [16], ie., codes from division algebras, could be a problem to work on.
- In [20], a code for $n = 2$ transmit antennas was proposed which met channel capacity. It would be a nice problem to construct such codes for different values of n.
- Most of the codes considered here are decoded using Sphere Decoding. One could try to construct codes which admit decoding of lesser complexity.
- On the PAPR of DAST-like codes, we tried the feasibility of the Generalized transforms by one sided multiplication only. One could explore, by multiplying the diagonal matrix by transform matrices on both sides.

Appendix A

Mathematical Preliminaries

In this Appendix, we shall discuss certain definitions and results from algebra [33, 34], which would be helpful for the reader to appreciate parts of this thesis. Here, we describe the basic algebraic structures such as abelian groups, rings and fields. Then we explain the concept of homomorphisms, endomorphisms etc. followed by the basics of field extensions.

Definition A.1 (Abelian Group) *A non-empty set of elements G is said to form an* abelian group *if in G there is defined a binary operation, denoted by '$\cdot$', such that*

1. (Closure Property) *$a, b \in G$ implies that $a \cdot b \in G$.*
2. (Commutative Law) *For $a, b \in G$, $a \cdot b = b \cdot a$.*
3. (Associative Law) *For $a, b, c \in G$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*
4. (Existence of Identity) *There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$, for all $a \in G$.*
5. (Existence of Inverse) *For every $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$, where e is the identity element.*

Note that there exists *non-abelian groups* also, for which all the above properties except the Commutative Law are satisfied.

The number of elements in a group G is called the *order* of the group G and is denoted by $o(G)$. We say G is a *finite group* when $o(G)$ is finite.

Example A.1 (Abelian Groups) *Consider* $G = \{0, 1, 2, 3, 4, 5\}$ *and* $a \cdot b$ *for* $a, b \in G$ *defined as* $a \cdot b \equiv a + b \pmod 6$. *We can see that closure, commutativity and associativity are easily satisfied. Also* 0 *is the identity element. For any element* $a \in G$, *we have an inverse* $-a \pmod 6$ *also. Hence* G *is an finite Abelian Group.*

The set of integers $\mathbb{Z}$ *is an Abelian Group, the operation defined as follows. For* $a, b \in \mathbb{Z}$, $a \cdot b = a + b$. 0 *is the identity element and* $-a$ *is the inverse of* a.

Definition A.2 (Associative Ring) *A non-empty set* R *is said to be an* associative ring, *if in* R *there are defined two operations, denoted by* $+$ *and* $\cdot$ *respectively, such that for all* $a, b, c \in R$

1. (Abelian Group under $+$) *The set* R *forms an Abelian Group under the operation* $+$, *which is called addition.*

2. (Closed under $\cdot$) $a \cdot b$ *is in* R.

3. (Associative Law for $\cdot$) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

4. (Distribution of $\cdot$ over $+$) $a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(b + c) \cdot a = b \cdot a + c \cdot a$.

The additive identity, in a ring R is denoted by 0 and is referred to as zero element, usually. The operation $\cdot$ is called multiplication, in general. Note that we can have *non-associative rings* which satisfy all the above except for the associative law for multiplication. If multiplication in R is commutative, ie., $a \cdot b = b \cdot a$ for every $a, b \in R$, R is called a *commutative ring.*

The ring axioms do not necessitate the existence of a *multiplicative identity*, ie., an element $1 \in R$ such that for all $a \in R$, $a \cdot 1 = 1 \cdot a = a$. Rings with such an element are called *rings with identity.* In general, a 'ring' means associative ring with identity.

Example A.2 (Rings) *Consider* $\mathbb{Z}$, *the set of all integers, positive, negative and* 0. *Let* $\cdot$ *be the usual multiplication of integers and let* $+$ *be the usual addition. It is easy to see that* $\mathbb{Z}$ *is a commutative ring with identity.*

Consider $R = \{0, 1, 2, 3, 4, 5\}$*, the addition* $+$ *and multiplication* $\cdot$ *defined modulo* 6*. This is a commutative ring with identity. Notice that,* $3 \cdot 4 = 0$ *in* R*. It can happen in a ring that non-zero elements can be multiplied to get zero.*

Consider $R = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}$*. One can verify that* $+$ *and* $\cdot$ *being the usual addition and multiplication,* R *is a ring with identity* 1 *itself.*

Definition A.3 (Ring Homomorphism) *A mapping* ϕ *from the ring* R *into the ring* R' *is said to be a* homomorphism *if for all* $a, b \in R$ *and operations denoted by* $+$ *and* $\cdot$ *in both* R *and* R'*, the following hold.*

1. $\phi(a + b) = \phi(a) + \phi(b)$.

2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Do note that the operations, $+$ and $\cdot$ appearing on the left-hand sides of the above axioms correspond to those in R, whereas the $+$ and $\cdot$ on the right-hand sides correspond to those in R'.

Definition A.4 (Kernel) *If* ϕ *is a homomorphism of* R *into* R'*, then the* kernel *of* ϕ*,* $I(\phi)$ *is defined as the set of all elements* $a \in R$ *such that* $\phi(a) = 0$*, the zero-element (additive identity) of* R'*.*

Example A.3 (Ring Homomorphisms) *Let* R *and* R' *be any two rings. Define* $\phi(a) = 0$ *for all* $a \in R$*. This is trivially a homomorphism. The kernel* $I(\phi) = R$*. This* ϕ *is called zero-homomorphism.*

Consider a ring R *and let* $R = R'$*. Define* $\phi(x) = x$ *for all* $x \in R$*. This is clearly a homomorphism and kernel* $I(\phi) = \{0\}$*.*

Consider the ring $R = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}$ *from Example A.2. Define* $\phi : R \to R$ *as follows.* $\phi(a + b\sqrt{2}) = a - b\sqrt{2}$*. This* ϕ *is a homomorphism as well and its kernel is* $I(\phi) = \{0\}$*.*

A homomorphism ϕ of a ring R into itself is called an *endomorphism.* A homomorphism of R to R' is said to be an *isomorphism* if it is a one-to-one mapping. Two rings

are said to be *isomorphic* to each other if there exists an isomorphism of one *onto* the other.

Definition A.5 (Field) *A non-empty set F is said to be a* field *if in F, there are defined two operations, denoted by $+$ and $\cdot$ respectively, such that the following hold.*

1. (Abelian Group under $+$) *The set F forms an Abelian group under the operation $+$, which is called addition. The additive identity is denoted by 0 and called zero element.*

2. ($F\backslash\{0\}$ Abelian Group under $\cdot$) *The set $F\backslash\{0\}$, ie., the set of all elements in F but for the zero element, forms an Abelian group under the operation $\cdot$.*

3. (Distribution of $\cdot$ over $+$) *For all $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.*

In other words, a field is a commutative ring with multiplicative identity, in which every non-zero element has a multiplicative inverse. The multiplicative identity is usually denoted by 1. If F contains finite number of elements, we call F a *finite field.*

Example A.4 (Fields) *Consider the set $F = \{0, 1, 2, 3, 4, 5, 6\}$, with addition and multiplication defined modulo 7. This set F is a finite field with 7 elements. The additive identity is 0 and the multiplicative identity is 1. One can easily verify that F contains additive inverses for all elements and multiplicative inverses for all elements except 0.*

Consider the set of rational numbers $\mathbb{Q}$, with addition and multiplication as usual. This is a field with additive identity 0 and multiplicative identity 1. It is easy to verify the existence of inverses for all elements. Similarly, the set of all real numbers $\mathbb{R}$ and the set of all complex numbers $\mathbb{C}$ are also fields.

The set $\mathbb{Q}(j) = \{x + jy : x, y \in \mathbb{Q}\}$ is also a field, with usual addition and multiplication. It contains all the complex numbers, whose real and imaginary parts are rational. The existence of identities and inverses for all numbers can be verified easily.

Definition A.6 (Vector Space) *A non-empty set V is said to be a* vector space *over a field F if V is an Abelian group under an operation which we denote by $+$, and if for*

every $\alpha \in F, v \in V$ there is defined an element, written αv, in V such that the following hold

1. $\alpha(v + w) = \alpha v + \alpha w$.
2. $(\alpha + \beta)v = \alpha v + \beta v$.
3. $\alpha(\beta v) = (\alpha\beta)v$.
4. $1v = v$.

for all $\alpha, \beta \in F$ and $v, w \in V$ (where the 1 denotes the identity element of F under multiplication).

Note that in Axiom 1 above, the $+$ is that of the vector space V, whereas on the left hand side of Axiom 2, it is that of the base field F and on the right hand side, that of F.

Definition A.7 (Basis of a vector space) *Let V be a vector space over a field F. Then a set of vectors $\{v_1, v_2, \ldots, v_n\}$ which satisfy the following properties, is a basis of V over F.*

1. (Linear independence) *For $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$, $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = 0$ implies $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$.*
2. (Spanning property) *Any given vector $v \in F$ can be written as an F-linear combination of the basis set, ie., $v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$.*

It is known that the cardinality of any basis of a vector space V over F is the same. This number is called the *dimension* of V over F.

Example A.5 (Vector Spaces) *Consider $F = \mathbb{R}$, the real field and let $V = \{(x, y) : x, y \in \mathbb{R}\}$. One can easily see that V is a vector space over $\mathbb{R}$. It can be verified that the dimension of V over $\mathbb{R}$ is 2.*

Definition A.8 (Extension Field) *Let F be a field. A field K is said to be an* extension *of F, if K contains F. The* degree *of K over F is defined as the dimension of K seen as a vector space over F.*

The degree of K over F is denoted using $[K : F]$. When $[K : F]$ is finite, we say that K is a *finite extension* of F. From here on, we shall use K to denote an extension field of F, always.

Example A.6 (Extension Fields) *Consider the real field* $\mathbb{R}$ *and the complex field* $\mathbb{C}$. *Since* $\mathbb{R} \subset \mathbb{C}$, $\mathbb{C}$ *is an extension field of* $\mathbb{R}$. *Also the degree* $[\mathbb{C} : \mathbb{R}] = 2$.

We can see that the real field $\mathbb{R}$ *is an extension of the rational field* $\mathbb{Q}$. *Note that this is* not *a finite extension.*

Consider the field $\mathbb{Q}(j)$ *mentioned in the Example A.4.* $\mathbb{Q}(j)$ *is an extension of the rational field* $\mathbb{Q}$ *and the degree* $[\mathbb{Q}(j) : \mathbb{Q}] = 2$.

Let K *be an extension of* F. *Consider the smallest field containing a field* F, *and an element* a. *This field is denoted by* $F(a)$, *and is an extension of* F. $F(a)$ *is called the field obtained by* adjoining a *to* F.

Definition A.9 (Algebraic over F) *An element* $a \in K$ *is said to be* algebraic over F *if there exist elements* $\alpha_0, \alpha_1, \ldots, \alpha_n$ *in* F, *not all* 0, *such that* $\alpha_0 a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0$. *An element which is not algebraic over* F *is said to be* transcendental *over* F.

It is known that the element $a \in K$ is algebraic over F if and only if $F(a)$ (as in Example A.6) is a finite extension of F.

Definition A.10 (Algebraic of Degree n) *The element* $a \in K$ *is said to be* algebraic of degree n *over* F *if it satisfies a non-zero polynomial over* F *of degree* n *but no non-zero polynomial of lower degree.*

It is known that if an element $a \in K$ is algebraic of degree n over F, then the $[F(a) : F] = n$.

Example A.7 (Elements algebraic over F) *Consider the rational field* $\mathbb{Q}$. *The number* $\sqrt{2}$ *is irrational and is not in* $\mathbb{Q}$. *Consider the polynomial* $p(x) = x^2 - 2$. *This polynomial is over* $\mathbb{Q}$ *and* $\sqrt{2}$ *is a root of* $p(x)$. *So* $\sqrt{2}$ *is algebraic over* $\mathbb{Q}$ *and is of degree* 2 *over* $\mathbb{Q}$. *Similarly,* j *is algebraic of degree* 2 *over the rational field since it satisfies* $x^2 + 1 = 0$.

The element $\sqrt{2}+\sqrt{3}$ is algebraic over the field $\mathbb{Q}(j)$. This satisfies the polynomial $p(x) = x^4 - 10x^2 + 1$ and it does not satisfy any polynomial of smaller degree. Hence $\sqrt{2}+\sqrt{3}$ is algebraic of degree 4 over $\mathbb{Q}(j)$.

The numbers e and π do not satisfy any polynomial over the rational field $\mathbb{Q}$ and hence they are transcendental over $\mathbb{Q}$. However, notice that, $\sqrt{\pi}$ satisfies the polynomial $x^2 - \pi$, which is over the field $\mathbb{Q}(\pi)$ and hence is algebraic of degree 2 over $\mathbb{Q}(\pi)$.

A case of special interest is when we have the rational field $\mathbb{Q}$ in the place of F. A number is said to be an *algebraic number* if it is algebraic over the field of rational numbers. Trivially, all rational numbers are algebraic numbers. A number which is not an algebraic number is called a *transcendental number*. One can note that the set of all algebraic numbers in $\mathbb{C}$ form a field, called the field of algebraic numbers.

Definition A.11 (Algebraic Extension) *An extension K of F is called an* algebraic extension *of F if every element in K is algebraic over F. Extensions K of F, which are not algebraic, are called* transcendental extensions.

Example A.8 (Algebraic/Transcendental Extensions) *The field $\mathbb{Q}(\sqrt{2})$ is an algebraic extension of the rational field $\mathbb{Q}$. The field $\mathbb{Q}(j)$ is another algebraic extension of $\mathbb{Q}$.*

The extension $\mathbb{Q}(\pi)$ is a transcendental extension of $\mathbb{Q}$. Since $\mathbb{Q}(\pi)$ contains π which is not algebraic over $\mathbb{Q}$, it is not an algebraic extension.

Now we shall state a couple of theorems [33], the consequences of which have been used many a time in this thesis.

Theorem A.1 (Lindemann-Weierstrass) *If $u_1, u_2, \ldots, u_n$ are algebraic numbers, which are linearly independent over $\mathbb{Q}$, then the complex exponentials $e^{u_1}, e^{u_2}, \ldots, e^{u_n}$ are linearly independent over the field of algebraic numbers.*

(For definition of linear independence, check Axiom 1 of Definition A.7).

An interesting special case of the above theorem is when $n = 1$ and $u \neq 0$ is an algebraic number. From the theorem, one can infer that e^u has to be transcendental number.

Corollary A.2 *For any algebraic number $u \neq 0$, e^u is transcendental.*

The following theorem concerns the irreducibility of polynomials over $\mathbb{Z}[j]$.

Theorem A.3 (Eisenstein Criterion) *Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ be a polynomial with integer coefficients. If there exists a prime p such that p divides the coefficients $a_0, a_1, \ldots, a_{n-1}$, p does not divide a_n and p^2 does not divide a_0. Then $f(x)$ is irreducible over the rational field $\mathbb{Q}$.*

Example A.9 (Eisenstein Criterion) *Consider polynomials of the form $x^n - px - p$, where p is a prime number. Clearly, the prime p satisfies the conditions for the above theorem and hence the polynomial $x^n - px - p$ is irreducible over the rational field.*

Bibliography

[1] Vahid Tarokh, Nambi Seshadri and A.R.Calderbank, "Space-Time Codes for High Date Rate Wireless Communication: Performance Criterion and Code Construction", *IEEE Trans. Information Theory*, vol.44, pp.744-765, March 1998.

[2] Jiann-Ching Guey, Michael P.Fitz, Mark R.Bell and Wen-Yi Kuo, "Signal Design for Transmitter Diversity Wireless Communication Systems over Rayleigh Fading Channels", *IEEE Trans. Communications*, vol.47, pp.527-537, April 1999.

[3] Vahid Tarokh, Hamid Jafarkhani and A.R.Calderbank, "Space-Time Block Codes from Orthogonal Designs", *IEEE Trans. Information Theory*, vol.45, pp.1456-1467, July 1999.

[4] İ.Emre Telatar, "Capacity of Multi-antenna Gaussian Channels", *AT&T Bell Labs Technical Report*, June 1995.

[5] Gerard J.Foschini, Jr. and Michael J.Gans, "On Limits of Wireless Communications in a Fading Environment when using Multiple Antennas", *Wireless Personal Communication*, pp.311-335, March 1998.

[6] S.M.Alamouti, "A simple transmit diversity technique for Wireless Communications", *IEEE Journal on Selected Areas in Commn.*, vol.16, pp.1451-1458, October 1998.

[7] John G.Proakis, *Digital Communications*, Fourth edition, McGraw Hill International, 2001.

[8] W.C.Jakes, *Microwave Mobile Communications*, John Wiley & Sons, 1974.

[9] Sumeet Sandhu and Arogyaswami Paulraj, "Space-Time Block Codes: A Capacity Perspective", *IEEE Communications Letters*, vol.4, pp.384-386, December 2000.

[10] Hamid Jafarkhani, "A Quasi-Orthogonal Space-Time Block Code", *IEEE Trans. Communications*, vol.49, January 2001.

[11] Vahid Tarokh and Hamid Jafarkhani, "A Differential Detection Scheme for Transmit Diversity", *IEEE Journal on Selected Areas in Commn.*, vol.18, pp.1169-1174, July 2000.

[12] Babak Hassibi and Bertrand M. Hochwald, "High-Rate Codes that are linear in Space and Time", *IEEE Trans. Information Theory*, vol.48, pp.1804-1824, July 2002.

[13] Olav Tirkkonen and Ari Hottinen, "Square-Matrix Embeddable Space-Time Block Codes for Complex Signal Constellations", *IEEE Trans. Information Theory*, vol.48, pp.384-395, February 2002.

[14] Weifeng Su and Xiang-Gen Xia, "Quasi-Orthogonal Space-Time Block Codes with Full Diversity", *Proc. of IEEE GLOBECOM 2002*, November 2002.

[15] Naresh Sharma and Constantinos B.Papadias, "Improved Quasi-Orthogonal Codes through Constellation Rotation", *Proc. IEEE ICASSP 2002*, vol.4, pp.3968-3971, May 2002.

[16] B.A.Sethuraman, B.Sundar Rajan and V.Shashidhar, "Full-Diversity, High-Rate Space-Time Block Codes from Division Algebras", submitted to *IEEE Trans. Information Theory.*

[17] B.A.Sethuraman and B.Sundar Rajan, "Optimal STBC over PSK Signal Sets from Cyclotomic Field Extensions", *Proc. IEEE ICC 2002*, pp.1783-1787, May 2002.

[18] B.A.Sethuraman and B.Sundar Rajan, "STBC from Field Extensions of the Rational Field", *Proc. IEEE ISIT 2002*, p.274, July 2002.

[19] B.A.Sethuraman, B.Sundar Rajan and V.Shashidhar, "High-Rate, Full-Diversity STBCs from Field Extensions", submitted to *IEEE ISIT 2003*.

[20] Mohamed Oussama Damen, Ahmed Tewfik and Jean-Claude Belfiore, "A Construction of a Space-Time Code Based on Number Theory", *IEEE Trans. Information Theory*, vol.48, March 2002.

[21] Mohamed Oussama Damen, Karim Abed-Meraim and Jean-Claude Belfiore, "Diagonal Algebraic Space-Time Block Codes", *IEEE Trans. Information Theory*, vol.48, pp.628-636, March 2002.

[22] Joseph Boutros and Emanuele Viterbo, "Signal Space Diversity: A Power- and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel", *IEEE Trans. Information Theory*, vol.44, pp.1453-1467, July 1998.

[23] Joseph Boutros, Emanuele Viterbo, Catherine Rastello and Jean-Claude Belfiore, "Good Lattice Constellations for Both Rayleigh Fading and Gaussian Channels", *IEEE Trans. Information Theory*, vol.42, pp.502-518, March 1996.

[24] Xavier Giraud, Emmanuel Boutillon and Jean-Claude Belfiore, "Algebraic Tools to Build Modulation Schemes for Fading Channels", *IEEE Trans. Information Theory*, vol.43, pp.938-952, May 1997.

[25] Yan Xin, Zhengdao Wang and Georgios B.Giannakis, "Space-Time Constellation-Rotating Codes Maximizing Diversity and Coding Gains", *Proc. of IEEE GLOBECOM 2001*, vol.1, pp.455-459, November 2001.

[26] K.Subrahmanyam, R.Chandrasekharan and B.Sundar Rajan, "Lattice Code Decoding of STBCs from Field Extensions", submitted to *IEEE ISIT 2003*.

[27] V.Shashidhar, R.Chandrasekharan and B.Sundar Rajan, "Performance of High-Rate Full-Diversity STBC's from Field Extensions", submitted to *IEEE Trans. Signal Processing (Special Issue on Signal Processing for MIMO Wireless Communications)*.

[28] Hesham El Gamal and Mohamed Oussama Damen, "Universal Space-Time Coding", submitted to *IEEE Trans. Information Theory.*

[29] Gerard J.Foschini, "Layered Space-Time Architecture for Wireless Communication in a Fading Environment when using Multiple Antennas", *Bell Laboratories Technical Journal*, vol.1, no.2, pp.41-59, Autumn 1996.

[30] Hesham El Gamal and A.Roger Hammons Jr., "A new approach to Layered Space-Time Coding and Signal Processing", *IEEE Trans. Information Theory*, vol.47, pp.2321-2334, September 2001.

[31] Oussama Damen, Ammar Chkeif and Jean-Claude Belfiore, "Lattice Code Decoder for Space-Time Codes", *IEEE Communications Letters*, vol.4, pp.161-163, May 2000.

[32] Moon Ho Lee, B.Sundar Rajan and J.Y.Park, "A Generalized Reverse Jacket Transform", *IEEE Trans. Circuits and Systems*, vol.48, pp.684-690, July 2001.

[33] Nathan Jacobson, *Basic Algebra I*, Second edition, W.H.Freeman and Company, New York, 1985.

[34] I.N.Herstein, *Topics in Algebra*, Second edition, John Wiley & Sons, 1999.