High-Rate and Information-Lossless Space-Time Block Codes from Crossed-Product Algebras

A Thesis

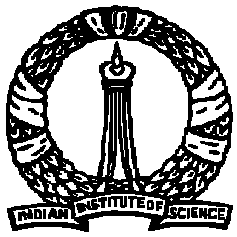
Submitted for the Degree of

Doctor of Philosophy

in the Faculty of Engineering

by

Shashidhar V



Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore
Bangalore – 560 012 (INDIA)

April 2004

Dedicated to

my parents, my wife,

my brother, my son

Abstract

It is well known that communication systems employing multiple transmit and multiple receive antennas provide high data rates along with increased reliability. It has been shown that coding across both spatial and temporal domains together, called Space-Time Coding (STC), achieves, a diversity order equal to the product of the number of transmit and receive antennas. Space-Time Block Codes (STBC) achieving the maximum diversity are called full-diversity STBCs. An STBC is called information-lossless, if the structure of it is such that the maximum mutual information of the resulting equivalent channel is equal to the capacity of the channel.

This thesis deals with high-rate and information-lossless STBCs obtained from certain matrix algebras called Crossed-Product Algebras. First we give constructions of high-rate STBCs using both commutative and non-commutative matrix algebras obtained from appropriate representations of extensions of the field of rational numbers. In the case of commutative algebras, we restrict ourselves to fields and call the STBCs obtained from them as STBCs from field extensions. In the case of non-commutative algebras, we consider only the class of crossed-product algebras.

For the case of field extensions, We first construct high-rate, full-diversity STBCs for arbitrary number of transmit antennas, over arbitrary apriori specified signal sets. Then we obtain a closed form expression for the coding gain of these STBCs and give a tight lower bound on the coding gain of some of these STBCs. This lower bound in certain cases indicates that some of the STBCs from field extensions are optimal in the sense of coding gain. We then show that the STBCs from field extensions are information-lossy. However, we also show that the finite-signal-set capacity of the STBCs from field extensions can be improved by increasing the symbol rate of the STBCs. The simulation results presented show that our high-rate STBCs perform better than the rate-1 STBCs in terms of the bit error rate performance.

Then we proceed to present a construction of high-rate STBCs from crossed-product algebras. After giving a sufficient condition on the crossed-product algebras under which

the resulting STBCs are information-lossless, we identify few classes of crossed-product algebras that satisfy this sufficient condition and also some classes of crossed-product algebras which are division algebras which lead to full-diversity STBCs. We present simulation results to show that the STBCs from crossed-product algebras perform better than the well-known codes in terms of the bit error rate.

Finally, we introduce the notion of asymptotic-information-lossless (AILL) designs and give a necessary and sufficient condition under which a linear design is an AILL design. Analogous to the condition that a design has to be a full-rank design to achieve the point corresponding to the maximum diversity of the optimal diversity-multiplexing tradeoff, we show that a design has to be AILL to achieve the point corresponding to the maximum multiplexing gain of the optimal diversity-multiplexing tradeoff. Using the notion of AILL designs, we give a lower bound on the diversity-multiplexing tradeoff achieved by the STBCs from both field extensions and division algebras. The lower bound for STBCs obtained from division algebras indicates that they achieve the two extreme points, i.e., zero multiplexing gain and zero diversity gain, of the optimal diversity-multiplexing tradeoff. Also, we show by simulation results that STBCs from division algebras achieves all the points on the optimal diversity-multiplexing tradeoff for n transmit and n receive antennas, where $n = 2, 3, 4$.

Acknowledgments

I would like to express my deep sense of gratitude to my supervisor *Prof. B. Sundar Rajan* for the constant encouragement given during the period of my research and broadening my research interests. I am also thankful to him for his personal interest in my career. This work would not have taken this shape without his support. I wish I had learned lot more from him than I did in the last five years.

My sincere thanks to Prof. Bharat Sethuraman, for his suggestions regarding various aspects of mathematical tools used in this thesis. I also thank Prof. Patil and Prof. Pradeep of Mathematics department for the courses they taught on algebra. I would also like to thank Prof. Vijay Kumar of our department for his valuable discussions on diversity-multiplexing tradeoff and other space-time coding techniques.

I thank Indian Institute of Science, for providing me with financial assistance during my research career. Indian Institute of Science and Department of ECE in particular, have given me a truly wonderful academic atmosphere and facilities for pursuing my research. I thank all the successive chairmen, the faculty members, the students and the office staff of the department for their co-operation during my stay in the department.

I am very fortunate to have a huge number of friends during my stay at IISc. Among them, I would like to mention few and thank them in particular. I thank Malli, Bikash, Amar, Ravi, Gowri, Suman, Nistala, Vinay, Madhu, Kottada, Phani, Sayee, Abhishek, Sastry, Murali for their joyful company during my stay in the hostel at IISc. I thank Anant and Malli for long discussions on various topics like puzzle solving, philosophy, communication theory, culture, traditions, geography, history, science, movies etc. I would specially like to mention and thank my lab mates with whom I had a memorable time: Kiran, Zafar, Bikash, Viswa, Sripati, Anshoo, Sury, Rahul, Jaggu, Vara, Anirbang, Nitin, Subru, Profie, Nandakishore, Chakri, Arun, Sanal, Manoj, Harmeet, Kaushik and Diptendu.

Finally, I am very thankful to my parents, my brother, my wife and my son whose constant support kept me in high spirits always. This thesis is dedicated to them as a token of love and affection, that I always shared with them.

Contents

Abstract **ii**

Acknowledgments **iv**

1 Introduction **1**

1.1 The System Model 2

1.2 Capacity and Outage Probability 4

1.3 Performance Analysis and Signal Design Criteria 5

1.4 State of the Art 10

1.4.1 STBCs from Orthogonal Designs 10

1.4.2 STBCs from quasi-orthogonal designs 12

1.4.3 Algebraic Space-Time Block Codes 12

1.4.4 Linear Dispersion Codes 13

1.4.5 Other constructions 13

1.5 Motivation 14

1.6 Organization of Thesis 14

2 Rate-1, Full-rank STBCs from Division Algebras **16**

2.1 STBCs from Division algebras 16

2.2 STBCs from Field Extensions 17

2.2.1 Rate-optimal codes over rotationally invariant Signal Sets 21

2.2.2 Rate 1 codes over signal sets derived from symmetric m-PSK signal sets for arbitrary number of antennas 24

2.2.3 Construction of STBCs using non-cyclotomic field extensions 26
2.3 STBCs from non-commutative division algebras 28
2.3.1 Codes From The Left Regular Representation of Division Algebras . 29
2.3.2 Cyclic Division Algebras 30
2.3.3 Rate-1 STBCs over SPSK signal sets 36

3 High-Rate, Full-Diversity STBCs from Field Extensions 38
3.1 Rate-1 STBCs over arbitrary finite subsets of $\mathbb{Q}(\omega_m)$ for arbitrary number of antennas 39
3.2 High-rate (> 1) codes from cyclotomic field extensions 41
3.3 Coding gain of STBCs from Field Extensions 44
3.3.1 Lower bounds on the coding gain 47
3.4 Capacity of STBC's from cyclotomic extensions 49
3.5 Finite-Signal-Set Capacities of STBCs from Field Extensions 52
3.6 Decoding and Simulation Results 57
3.7 Summary 61

4 Information-Lossless Designs from Crossed-Product Algebras 63
4.1 Introduction 63
4.2 Crossed-Product Algebras 67
4.3 STBCs from Crossed-Product Algebras 72
4.4 Mutual Information 81
4.5 Full-rank STBCs from Crossed-Product Division Algebras 87
4.5.1 Cyclic division algebras 88
4.5.2 STBCs from tensor-product division algebras 96
4.5.3 Rates beyond n symbols per channel use 104
4.5.4 Mutual Information 105
4.6 Decoding and Simulation Results 108
4.6.1 Capacity approaching codes 109
4.7 Summary 112

5 Asymptotic-Information-Lossless Designs and Diversity-Multiplexing Tradeoff **114**

5.1 Introduction and Preliminaries 115

5.2 Asymptotic-Information-Lossless Designs 120

5.3 Diversity-Multiplexing Tradeoff of Designs from Field Extensions 132

5.4 Diversity-Multiplexing Tradeoff of Designs from Division Algebras 134

5.5 Simulations 138

5.6 Summary 140

6 Conclusions **142**

6.1 Summary of the results 142

6.2 Directions for further research 143

A Preliminaries and Basics of Algebra **146**

A.1 Ring homomorphisms 146

A.2 Algebraic and transcendental extensions of fields 147

A.3 Tensor products 149

Bibliography **150**

List of Figures

1.1 System model 2

1.2 Outage probability as a function of the number of transmit and receive antennas, and SNR. 6

1.3 Achievable data rates with outage probability 5×10^{-2}, as a function of the number of transmit and receive antennas, and SNR. 7

2.1 Asymmetric 8-PSK signal set matched to a dihedral group with 8 elements 26

3.1 Comparison of mutual informations of STBCs from field extensions and the capacity of the channel. 52

3.2 Comparison of mutual informations achieved by Alamouti code and STBCs from field extensions 53

3.3 Capacity of 2 Tx and 1 Rx system 56

3.4 Capacity of 2 Tx and 2 Rx system 57

3.5 Constellation $S + e^{2.5j}S$, for $S = 4$-QAM. 59

3.6 Comparison of STBCs from field extensions with LD codes for 2-Tx and 2-Rx with 4 bits per channel use. 60

3.7 Comparison of STBCs from field extensions with LD codes for 2-Tx and 2-Rx with 8 bits per channel use. 61

4.1 Embedding of a crossed-product algebra into the set of $n \times n$ matrices over K. 73

4.2 Comparison of capacities for various values of $|t|$ and $|\delta|$. The plain solid curve is the capacity of the channel too. Also, $\mathbf{R_f} \neq \mathbf{R_{f'}}$ in the cases where $|t| \neq 1$ or $|\delta| \neq 1$ 87
4.3 Comparison of capacities for various values of $|t|$. The plain solid curve is the capacity of the channel too. 88
4.4 Comparison of capacities of type-I and type-II STBCs from Brauer division algebras. The plain solid curve is the capacity of the channel for 2-transmit and 2-receive antennas. And the plain dashed curve is the capacity of the channel for 4-transmit and 4-receive antennas. 106
4.5 Comparison of STBCs with 2 transmit and 2 receive antennas 110
4.6 Comparison of STBCs with 3 transmit and 3 receive antennas 111
4.7 Comparison of STBCs with 4 transmit and 4 receive antennas 112
4.8 Comparison of STBCs with 4 transmit and 4 receive antennas 113

5.1 Optimal diversity-multiplexing tradeoff for some specific cases 118
5.2 The diversity-multiplexing tradeoff achieved by Alamouti scheme (a) 1 receive antenna, (b) 2 receive antennas. 119
5.3 The diversity-multiplexing tradeoff achieved by BLAST schemes for 4 transmit and 4 receive antennas (a) V-BLAST, (b) D-BLAST. 120
5.4 Capacities of the actual channel and the design in Example 5.2.2 for 1 and 2 receive antennas. 125
5.5 Various ILL and AILL designs for $n_t = 2$ transmit antennas. CPA designs means the designs from crossed-product algebras [41] 126
5.6 Various ILL and AILL designs for $n_t \geq 3$ transmit antennas. CPA designs means the designs from crossed-product algebras [41] 127
5.7 Diversity-multiplexing tradeoff achieved by design from field extensions for 2 transmit and 1,2 receive antennas 134
5.8 Diversity-multiplexing tradeoff achieved by design from field extensions for 3 transmit and 1,3 receive antennas 135

5.9 Diversity-multiplexing tradeoff achieved by design from division algebras for (a) 2 transmit and 2 receive antennas, (b) 3 transmit and 3 receive antennas. 137
5.10 Error probability curves (solid) and outage probability curves (dashed)for 2 transmit and 2 receive antennas. 139
5.11 Error probability curves (solid) and outage probability curves (dashed)for 3 transmit and 3 receive antennas. 140
5.12 Error probability curves (solid) and outage probability curves (dashed)for 4 transmit and 4 receive antennas. 141

Chapter 1

Introduction

In a multipath wireless environment, due to the severe attenuation of the transmitted signal, it becomes very difficult for the receiver to detect the transmitted signal. One way of overcoming this difficulty is to introduce multiple replicas of the transmitted signal at the receiver. The chances that at least one replicated signal is received by the receiver with a low attenuation are very high and hence the receiver can detect the transmitted signal. This method of providing multiple replicas of transmitted signal to the receiver is called as *diversity*. There are mainly three forms of diversity:

(i) Time diversity - several replicas of the information signal are transmitted at different time instants. The disadvantage of this diversity is that there is reduction in the transmission rate.

(ii) Frequency diversity - if the channel is frequency selective, then the information is transmitted over several frequencies. The disadvantage of this method is that it occupies more bandwidth.

(iii) Space diversity (also known as antenna diversity) - spatially separated antennas are used to provide the receiver with replicas of the transmitted signal. This technique does not need extra bandwidth and there is no loss in the data rate.

Till early 1990s receive antenna diversity was extensively studied and more recently transmit antenna diversity has gained more importance because of the fact that it is easier and more cost effective to use multiple antennas at the transmitter (base station) to achieve

diversity for down-link (base station to the mobile) than to use multiple antennas at the receiver (mobile). Communication systems employing multiple transmit and receive antennas are called Multiple Input Multiple Output (MIMO) communication systems. In this thesis, we deal with construction of signal sets/codes for MIMO communication systems that provide maximum diversity and at the same time support high data rates.

1.1 The System Model

In this section, we derive the system model based upon several assumptions. Figure 1.1 shows a communication system with n_t transmit and n_r receive antennas. For every channel use, n_t complex symbols are transmitted using the n_t transmit antennas simultaneously. The channel is assumed to be flat, Rayleigh and quasi-static fading with additive white Gaussian noise at the input of each receive antenna.

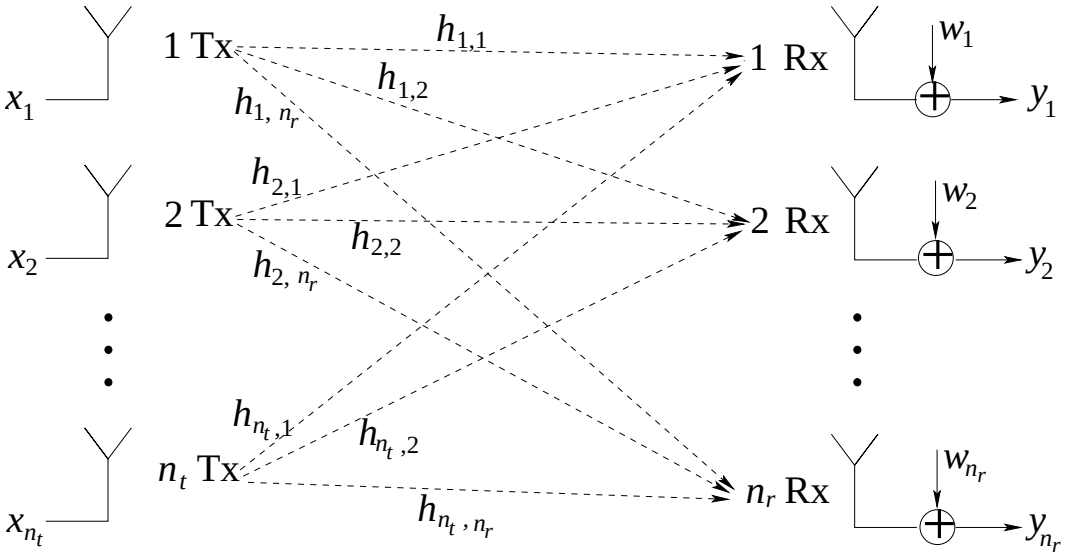


Figure 1.1: System model

Since we assumed the channel to be frequency-flat, we can model each wireless link between a pair of transmit and receive antennas as a complex scaling with the gain given by a complex number $h_{i,j}$. Note that this assumption is valid when the signal bandwidth is very narrow so that the entire signal frequency spectrum goes through a common fading. The assumption of Rayleigh fading on the channel means that the channel coefficients $h_{i,j}$

are independent and identically distributed (iid) with zero mean, unit variance circularly symmetric complex Gaussian $\mathcal{CN}(0,1)$. This assumption is valid only if the antennas are well separated and the environment has large number of scatters. Thus, for a given environment, there is a limit on the number of antennas that we can use, such that there is no correlation between the channel coefficients $h_{i,j}$. The channel is modeled as quasi-static fading channel, i.e., the channel remains fixed for a certain number of channel uses, called the '*coherence time of the channel*' and then changes to something independent for the next coherence time of the channel. At the receiver, all the faded signals from the transmitter are added together along with an iid additive white complex Gaussian noise with zero mean and variance per real dimension 1/2.

Throughout the thesis, we assume the number of channel uses used to transmit a codeword, denoted by l is less than the coherence time of the channel. With this assumption, every codeword transmitted experiences only one channel realization. With all the above assumptions, the received $n_r \times l$ signal matrix $\mathbf{Y}$ is

$$\mathbf{Y} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\mathbf{H}\mathbf{X} + \mathbf{W} \tag{1.1}$$

where $\mathbf{H}$ is the $n_r \times n_t$ channel matrix, $\mathbf{X}$ is the $n_r \times l$ transmitted signal matrix and $\mathbf{W}$ is the additive white Gaussian noise. The matrix $\mathbf{X}$ is such that the average power used to transmit it is $n_t l$, i.e.,

$$\mathcal{E}\left[tr\left(\mathbf{X}\mathbf{X}^H\right)\right] = n_t l.$$

The above condition makes the average received signal-to-noise power ratio (SNR) at each receive antennas equal to SNR.

1.2 Capacity and Outage Probability

First, let us assume that the transmitted n_t-length vectors are independent across the channel uses, i.e., there is no coding across time. Then, we have the received vector

$$\mathbf{y} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\mathbf{H}\mathbf{x} + \mathbf{w}.$$

For a given realization of $\mathbf{H}$, the channel capacity, i.e., the maximum rate at which we can achieve reliable communication, is [1, 2]

$$C(n_t, n_r, \mathsf{SNR}, \mathbf{H}) = \log_2 \left[\det \left(I_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^H \right) \right]. \tag{1.2}$$

The input distribution is assumed to be circularly symmetric complex Gaussian random vector with each entry zero mean and unit variance. Since, the transmitter has no knowledge of the channel, this distribution on the input vectors maximizes the mutual information between the received and transmitted vectors. However, if the transmitter knows the channel, the distribution on input which maximizes the mutual information could be different.

Notice that the capacity of the channel is a random variable. Thus, taking expectation of (1.2) over the channel realizations $\mathbf{H}$, we obtain the ergodic or mean capacity of the channel given by

$$C(n_t, n_r, \mathsf{SNR}) = \mathcal{E}_{\mathbf{H}} \left[\log_2 \left[\det \left(I_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^H \right) \right] \right]. \tag{1.3}$$

Since, the transmitter does not know the channel and hence cannot adjust its transmission rate accordingly, we assume that the transmission rate is fixed to R bits per channel use. Thus, when the channel capacity, which is a random variable, is less than the transmission rate R, the probability of error is bounded away from zero even for the best codes, i.e., we can not have a reliable communication. We call these events of the channel realizations for which the channel capacity falls below the transmission rate as outage events and the

probability that an outage occurs is called the outage probability, given by

$$P_{out}(R, \mathsf{SNR}) = P\left(C(n_t, n_r, \mathsf{SNR}) < R\right). \tag{1.4}$$

The number of transmit and receive antennas is understood according to the context and hence, we do not use them in the notation of outage probability. Thus, when the coding is done over only one channel realization, the error probability of the particular code is lower bounded by the outage probability. Figure 1.2 shows the outage probabilities for a date rate of 2 bits per channel use for n transmit and n receive antennas, where $n = 2, 3, 4$. Notice that as the SNR increases, the slope of the outage probability curve tends to 4 for 2 transmit and 2 receive antennas, 9 for 3 transmit and 3 receive antennas, and 16 for 4 transmit and 4 receive antennas. It has been shown recently [50] that the slope of the outage probability curve for n_t transmit and n_r receive antennas, at high SNRs is equal to $n_t n_r$. We will discuss more about this in Chapter 5. Figure 1.3 shows the achievable data rates as a function of SNR when the outage probability is 5%, i.e., 5×10^{-2} for n transmit and n receive antennas, $n = 2, 3, 4$. It is clear from the curves that to double the achievable data rate we, either, have to double the number of transmit and receive antennas or double the SNR dB level.

1.3 Performance Analysis and Signal Design Criteria

Signal design for taping the promised capacity discussed in the previous section is called Space-Time Coding (STC). There are two ways of space-time coding: (i) Space-Time Block Codes (STBCs) and (ii) Space-Time Trellis Codes (STTCs). Though, it was STTCs which were constructed first, STBCs gained more popularity because of the availability of good decoding algorithms. Throughout the thesis, we deal with STBCs only.

Definition 1.3.1 *A $n_t \times l$ space-time block code (STBC) for n_t transmit antennas is a finite set of $n_t \times l$ matrices with entries from the complex field $\mathbb{C}$, where l is a positive integer such that the coherence time of the channel is an integral multiple of l.*

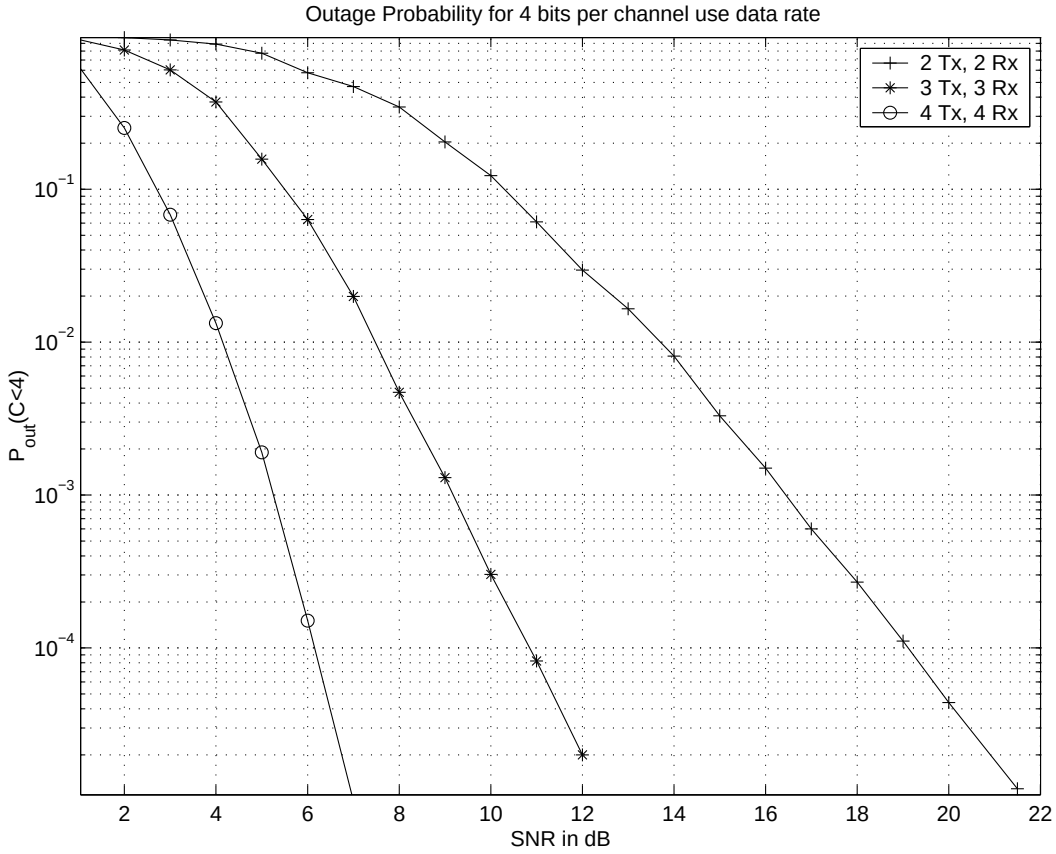


Figure 1.2: Outage probability as a function of the number of transmit and receive antennas, and SNR.

Towards deriving the performance of an STBC in terms of the pair-wise error probability (PEP), let $\mathcal{C}$ be an $n_t \times l$ STBC. Assume that there are only two codewords $\mathbf{X}$ and $\mathbf{X}'$ in $\mathcal{C}$, and $\mathbf{X}$ is transmitted. With maximum likelihood decoding at the receiver, the conditional probability that the received matrix $\mathbf{Y}$ is decoded as $\mathbf{X}'$ is

$$P\left(\mathbf{X} \rightarrow \mathbf{X}'/\mathbf{H}\right) \leq e^{-\frac{\left(\|\mathbf{H}(\mathbf{X}-\mathbf{X})'\|/2\right)^2 \mathsf{SNR}}{n_t}} = e^{-\frac{(\|\mathbf{H}\mathbf{\Delta}\|/2)^2 \mathsf{SNR}}{n_t}}$$

where $\Delta = \mathbf{X} - \mathbf{X}'$. Averaging the above expression over all the channel realizations, the PEP between $\mathbf{X}$ and $\mathbf{X}'$ is [3, 4]

$$P\left(\mathbf{X} \rightarrow \mathbf{X}'\right) \leq \left(\prod_{i=1}^{\Lambda} \frac{1}{1+\lambda_i^2 \mathsf{SNR}}\right)^{n_r}$$

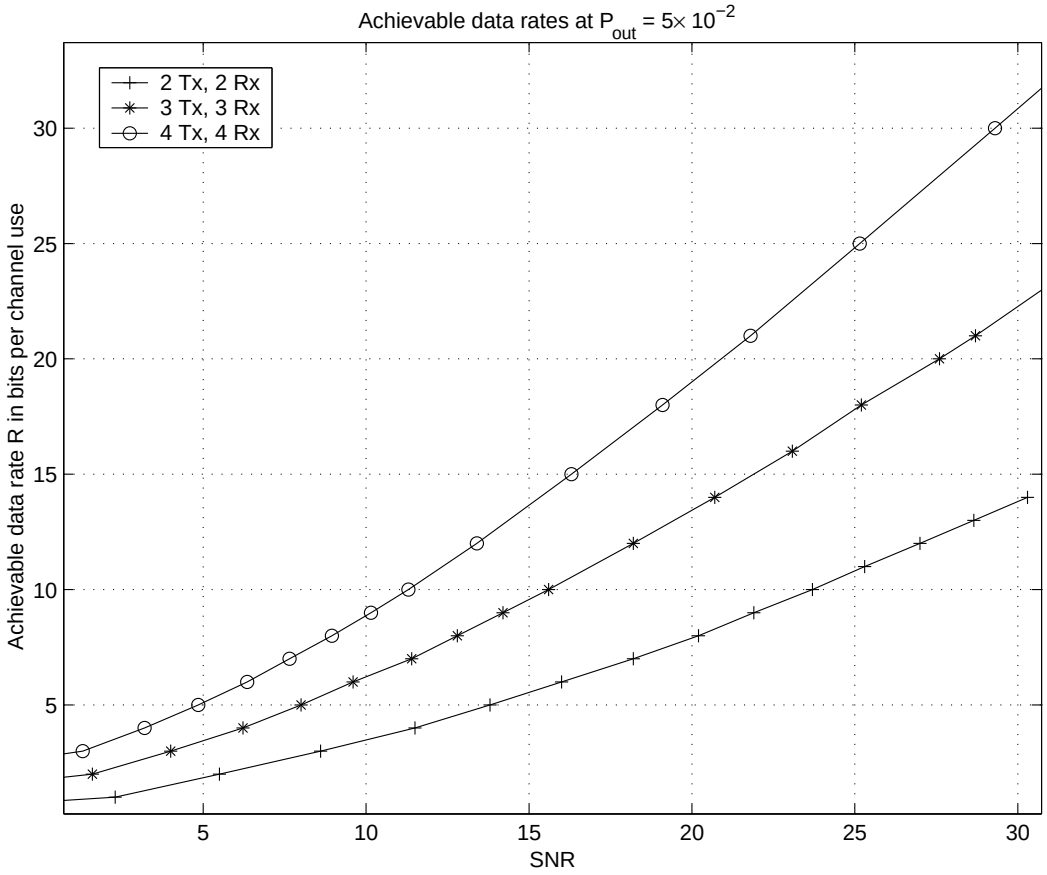


Figure 1.3: Achievable data rates with outage probability 5×10^{-2}, as a function of the number of transmit and receive antennas, and SNR.

where λ_i, $i = 1, 2, \ldots, \Lambda$ are the non-zero singular values of Δ. At sufficiently high SNRs, the above PEP expression can be approximated as

$$P\left(\mathbf{X} \to \mathbf{X}'\right) \leq \left(\prod_{i=1}^{\Lambda} \lambda_i^2\right)^{-n_r} \mathsf{SNR}^{-n_r \Lambda}.$$

Since at high SNRs, the overall performance, i.e., the actual codeword error probability is dominated by the worst case PEP, we should design our code such that the worst case PEP is minimized. The following are the three design criteria based on the PEP:

- As SNR increases, the PEP is dominated by the the term $\mathsf{SNR}^{-n_r \Lambda}$. The negative of the SNR exponent $n_r \Lambda$, called the **diversity gain of the code** $\mathcal{C}$, indicates the slope of the fall in the error probability with SNR. So, to obtain a good performance,

the code should be designed such that for every pair of codewords $\mathbf{X}, \mathbf{X}'$, the term $n_r\Lambda$ is maximized, i.e., the rank of the matrix $\Delta = \mathbf{X} - \mathbf{X}'$ is maximized. Since, the difference matrix Δ is a $n_t \times l$ matrix, the value of l should be at least n_r, so that the maximum diversity gain $n_t n_r$ can be achieved. Once we have $l \geq n_t$, we should design our code such that the difference matrix Δ for every pair of codewords, is a full-rank matrix and thus obtain a diversity gain of $n_t n_r$. We call the code $\mathcal{C}$ a full-rank STBC or a full-diversity STBC if $\Lambda = n_t$.

- Once we have designed our code such that it achieves a diversity gain of Λn_t, the coefficient of $\mathsf{SNR}^{-n_r\Lambda}$ has to be minimized to reduce the worst case PEP. Hence, the term $\min_{\Delta\neq 0}\left(\prod_{i=0}^{\Lambda}\lambda_i^2\right)^{1/\Lambda}$, called the **coding gain of the code** $\mathcal{C}$, has to be maximized. When the code is a full-rank STBC, the coding gain is given by $\min_{\Delta\neq 0}\det|\Delta|^{2/n_t}$.

- The actual error probability is approximately equal to the PEP multiplied with a positive integer κ, where κ is the average number of the codeword matrices $\mathbf{X}'$ such that $|\det(\Delta)|^{2/n_t}$ is equal to the coding gain of the code. The codeword matrices $\mathbf{X}'$ are called the nearest neighbors of the codeword matrix $\mathbf{X}$. Thus, to minimize the overall performance, we should minimize the average number of nearest neighbors for every codeword.

Among the above three design criteria, the first criteria is the most important one as it indicates the slope of the fall in error probability with SNR. Thus, our main aim is to construct full-rank STBCs for a given number of transmit antennas n_t.

In general, an STBC is described in terms of a matrix called **design** defined below:

Definition 1.3.2 *A rate-k/l, $n\times l$ design is an $n\times l$ matrix with entries that are complex linear combinations of k complex variables and their complex conjugates. We obtain an STBC for n transmit antennas by allowing these k variables to take values from a finite subset S of the complex field $\mathbb{C}$. We call such an STBC as* **an STBC over the signal set** *S. In particular, if all the entries, which are complex linear combinations of the k*

variables, take values from the signal set S itself, we call the resulting STBC **an STBC completely over** S.

Thus, a design and a signal set jointly describe an STBC. The rate of the design corresponds to the symbol rate of the STBC in symbols from the signal set per channel use. For example, the well-known Alamouti code [5] is an STBC based on the design

$$\begin{bmatrix} x_0 & x_1 \\ -x_1^* & x_0^* \end{bmatrix}$$

where x_0, x_1 are the complex variables. By restricting x_0, x_1 to take values from a given complex signal set we obtain the Alamouti code over the given signal set. If the signal set is symmetric with respect to both the real and the imaginary axes, then the resulting Alamouti code is completely over that signal set. Otherwise, it is not completely over the signal set. For instance, if x_0 and x_1 in the Alamouti code take values from a symmetric 3-PSK signal set S then the code is over S but not completely over S. It is completely over S' where S' denotes the symmetric 6-PSK signal that is the union of S and $-S$.

It has been shown in [3] that the symbol rate of $n \times n$ STBC is upper bounded as

$$R_s \leq n - d + 1$$

where R_s and d denote the symbol rate and the diversity gain of the STBC respectively.

Definition 1.3.3 *An STBC completely over S with rate meeting the upper bound above is called a full-rate code. A minimal-delay full-rank, full-rate STBC completely over S is said to be rate-optimal over S.*

We use the term "rate-optimal" to highlight the fact that these codes need not be of largest coding gain among such codes.

1.4 State of the Art

In this section, we briefly review some of the well known STBCs like STBCs from orthogonal designs and quasi-orthogonal designs, diagonal algebraic STBCs, space-time constellation rotation codes, threaded algebraic STBCs and linear dispersion codes.

1.4.1 STBCs from Orthogonal Designs

An $n \times l$ $(n \leq l)$ Real Orthogonal Design (ROD) is an $n \times l$ matrix Θ with entries $\pm x_0,\ \pm x_1, \ldots,\ \pm x_{k-1}$, where x_i are real variables, such that

$$\Theta^T \Theta = (x_0^2 + x_1^2 + \cdots + x_{k-1}^2) I_n$$

where I_n denotes the $n \times n$ identity matrix. Similarly an $n \times l$ Complex Orthogonal Design (COD) is an $n \times l$ matrix Θ with entries $\pm x_0,\ \pm x_0^*, \pm x_1, \pm x_1^*, \ldots, \pm x_{k-1}, \pm x_{k-1}^*$, such that

$$\Theta^H \Theta = (|x_0|^2 + |x_1|^2 + \cdots + |x_{k-1}|^2) I_n.$$

Example 1.4.1 *(a) RODs: For $n = 2$ transmit antennas, we have the following ROD:*

$$\begin{bmatrix} x_0 & x_1 \\ -x_1 & x_0 \end{bmatrix}.$$

For $n = 3$ transmit antennas, the following is one of the known RODs:

$$\begin{bmatrix} x_0 & -x_1 & -x_2 & -x_3 \\ x_1 & x_0 & x_3 & -x_2 \\ x_2 & -x_3 & x_0 & x_1 \end{bmatrix}.$$

(b) CODs: For $n = 2$, we have the well known Alamouti code

$$\begin{bmatrix} x_0 & x_1 \\ -x_1^* & x_0^* \end{bmatrix}$$

and for $n = 4$ transmit antennas, the following is one of the known CODs:

$$\begin{bmatrix} x_0 & x_1 & x_3 & 0 \\ -x_1^* & x_0^* & 0 & -x_3 \\ -x_2^* & x_2^* & x_0^* & x_1 \\ 0 & x_2^* & -x_1^* & x_0 \end{bmatrix}.$$

In [6], both RODs and CODs, and their generalizations have been used to obtain full-diversity STBCs over arbitrary finite subsets of the complex field. If $\mathbf{X}$ is a codeword of an STBC $\mathcal{C}$ obtained from an orthogonal design, and if $\mathbf{Y}$ is the received matrix when the codeword $\mathbf{X}$ is transmitted, then the ML estimate is given as

$$\widehat{\mathbf{X}} = arg \min_{\mathbf{X} \in \mathcal{C}} trace \left\{ \left(\mathbf{Y} - \sqrt{\frac{\mathsf{SNR}}{n_t}} \mathbf{HX} \right) \left(\mathbf{Y} - \sqrt{\frac{\mathsf{SNR}}{n_t}} \mathbf{HX} \right)^H \right\}.$$

But, since $\mathbf{X}\mathbf{X}^H$ is a scaled identity matrix, the above expression can be written as

$$\widehat{\mathbf{X}} = arg \min_{\mathbf{X} \in \mathcal{C}} trace \left\{ \sqrt{\frac{\mathsf{SNR}}{n_t}} \left(|x_0|^2 + |x_1|^2 + \cdots + |x_{k-1}|^2 \right) \mathbf{H}\mathbf{H}^H - \mathbf{H}\mathbf{X}\mathbf{Y}^H - \mathbf{Y}(\mathbf{H}\mathbf{X})^H \right\}.$$

Clearly, the LHS of the above expression can be broken into several terms each of which depend only on one of the k variables and thus the decoding complexity is linear in the size of the signal set. This property of the orthogonal designs has been termed as single-symbol decoding in [7]. However, the main disadvantage of the STBCs from orthogonal designs is that their symbol rates are upper bounded by 1 [13]. It was also shown that for arbitrary complex constellations, the only possible orthogonal design for 2 transmit antennas is the Alamouti code. Orthogonal designs were also dealt with in [8] using amicable designs. In [9], it has been shown that orthogonal designs maximize the SNR at the receiver. Orthogonal designs have also been constructed in [10] using Clifford algebras. In the same paper, an upper bound on the symbol rates of the orthogonal designs was obtained. Some specific orthogonal designs were constructed in [11]. In [12], all the STBCs admitting the single-symbol decoding were characterized and a class of designs called Co-ordinate

Interleaved designs were constructed that admit the single-symbol decoding.

1.4.2 STBCs from quasi-orthogonal designs

Since the rates of orthogonal designs were upper bounded by 1, there was a search for designs which can have better rate with small sacrifices in the decoding complexity and transmit diversity. A scheme that trades off diversity for simpler ML decoding (double-symbol decoding) was presented in [14] for four and eight antennas, using quasi-orthogonal designs (QODs).

Example 1.4.2 *The following was the QOD proposed by Jafarkhani in [14] for* 4 *transmit antennas:*

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ -x_1^* & x_0^* & -x_3^* & x_2^* \\ -x_2^* & -x_3^* & x_0^* & x_1^* \\ x_3 & -x_2 & -x_1 & x_0 \end{bmatrix}.$$

The diversity of the above design is 2*, but the decoding of the four symbols* x_0, x_1, x_2, x_3 *can be decoupled into decoding of pairs* x_0, x_3 *and* x_1, x_2*.*

While the symbol rates are better than that of orthogonal designs, the decoding complexity is equal to square of that of orthogonal designs, and the diversity gain achieved by QODs is equal to half the number of transmit antennas. In [15–17], several modifications to the STBCs from QODs have been proposed to retain the full diversity.

1.4.3 Algebraic Space-Time Block Codes

Using the concept of constellation rotation, Damen *et al.* in [18] have proposed Diagonal Algebraic Space-Time Block Codes (DAST) which have a rate equal to 1 symbol per channel use and achieve full diversity. The signal sets considered were finite subsets carved from the integer lattice $\mathbb{Z}[j]$.

In [20], Xin *et al.* have proposed STBCs similar to that of DAST, based on certain algebraic extensions of the rational number field $\mathbb{Q}$. In [21], El Gamal and Damen extended

the idea of DAST to more general system called Threaded Algebraic STBCs (TAST). The concept of layering is used here to obtain rates up to n_t symbols per channel use without reducing the diversity gain of the system. Damen constructed a code for 2 transmit antennas, which is a specific example of TAST codes. The code, however, has the added property that the code achieves capacity for any number of receive antennas. We will deal with this specific code in more detail in Chapter 4.

1.4.4 Linear Dispersion Codes

Hassibi and Hochwald [23] introduced codes that are linear in space and time called "Linear Dispersion Codes" (LD codes) which absorb STBCs from orthogonal designs as a special case. The construction of these LD codes is done by optimizing the maximum mutual information between the input to the encoder and the input to the receiver. But these codes maximize the mutual information only when the number of receive antennas is greater than or equal to the number of transmit antennas, i.e., $n_r \geq n_t$. In the remaining cases, there is about 5% loss in the mutual information at 10 dB SNR. The LD codes do not achieve the full diversity, as the basis of construction was mutual information and not the diversity. The ML decoding complexity of these codes is exponential but due to their linear structure, low complexity decoding algorithms like 'successive nulling and canceling', ' square-root' and 'sphere decoding' can be used [23].

1.4.5 Other constructions

Constructions of STBCs specific to PSK and QAM modulation have been studied in [24] and [25] respectively. Design of STBCs using groups and representation theory of groups have been reported in [26–29] and using unitary matrices STBCs have been studied in [30–33].

In the next chapter, we survey the construction of STBCs from division algebras [39] in detail, as we use the same basic principle in this thesis for constructing our codes.

1.5 Motivation

Most of the full-diversity STBCs constructed so far have symbol rate upper bounded by 1. There have been very few constructions, like TAST, where the symbol rate is more than one, but still upper bounded by n_t, the number of transmit antennas. Also, these specific constructions were limited to QAM constellations only. So, it is natural to ask whether it is possible to obtain capacity approaching, high-rate, full-diversity STBCs over arbitrary signal sets, with high symbol rates. It is in this context, that we explore the possibility of constructing such STBCs over arbitrary but apriori specified signal sets.

1.6 Organization of Thesis

In Chapter 2, we give the general principle of construction of STBCs from division algebras and present in detail the construction of rate-1, full-diversity STBCs using field extensions and non-commutative division algebras [39].

In Chapter 3, we give a construction of high-rate, full-diversity STBCs using the embeddings of both algebraic and transcendental extensions of the field of rational numbers $\mathbb{Q}$ into the matrix algebras. We then, obtain the expression for the coding gain for these high-rate STBCs and compare with the well known STBCs. Also, we give a detailed analysis of the mutual information of these STBCs and show that they are *information-lossy* (defined in Chapter 2). We then, present the finite-signal-set capacity of these STBCs and show that the capacity can be increased by increasing the rate of these STBCs. We conclude this chapter by presenting some simulations for bit error rate (BER) performance of these STBCs.

In Chapter 4, we give a general construction of high-rate STBCs from crossed-product algebras and show that several well known STBCs are special cases of these STBCs. We also give a sufficient condition under which these STBCs are information-lossless and identify some classes of STBCs which satisfy the sufficient condition. We also identify some classes of crossed-product algebras from which the STBCs obtained are full-diversity STBCs. We obtain an expression for the coding gain of a specific class of these STBCs.

We conclude this chapter with simulations results comparing the BER performance of these STBCs with that of some well known STBCs.

In Chapter 5, we give a brief introduction to the recently found [50] tradeoff between the diversity and multiplexing gain of any given scheme or design. We then introduce a class of STBCs namely, Asymptotically-Information-Lossless (AILL) scheme and show that it is necessary for a scheme to achieve the optimal diversity-multiplexing tradeoff. We then give a necessary and sufficient condition under which a scheme is AILL. Also, we briefly review the diversity-multiplexing tradeoff of several well known schemes. We then obtain lower bounds on the diversity-multiplexing tradeoff achieved by the schemes from field extensions and crossed-product algebras. We will conclude the chapter with some simulation results which indicate that the schemes from crossed-product algebras for n transmit and n receive antennas achieve the optimal diversity-multiplexing tradeoff, where $n = 2, 3, 4$.

In Chapter 6, we conclude the thesis by presenting some directions for further research on this topic.

In Appendix A, we give basic preliminaries of the algebraic tools used in this thesis.

Chapter 2

Rate-1, Full-rank STBCs from Division Algebras

In this chapter, we present the construction of STBCs from division algebras [34–36, 39]. In Section 2.1, we give the general principle which will be used to construct STBCs throughout the thesis. Construction of rate-1 STBCs over symmetric PSK signal sets and QAM signal sets, using field extensions is given in Section 2.2. In Section 2.3, we present the construction of rate-1, full-diversity STBCs using non-commutative division algebras.

2.1 STBCs from Division algebras

In this section we present the basic principle used to construct STBCs using division algebras. To avoid notational complexity, we assume that the number of transmit antennas $n_t = n$ throughout this section.

A division ring is a ring in which every nonzero element has a multiplicative inverse. Since every division ring is a vector space over its center, the term "division algebra" is used instead of division ring. A commutative division algebra, of course, is just a field. And non-commutative division algebras do exist. For example, the set $\mathbb{H}$ of quaternions

over the real field $\mathbb{R}$ given by

$$\mathbb{H} = \{a + ib + jc + kd | a, b, c, d \in \mathbb{R}\},$$

where $i^2 = j^2 = k^2 = -1$ and $ij = k$, is a non-commutative division algebra. It is easy to check that $ij = -ji$ and any non-zero element $a + ib + jc + kd$ has an inverse equal to $\frac{a-ib-jc-kd}{a^2+b^2+c^2+d^2}$.

The following proposition gives a very broad principle that is used to construct full-rank minimal-delay codes from division algebras in this thesis:

Proposition 2.1.1 *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 finite 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.*

Proof: Since every element in D is invertible, D has no nontrivial two-sided ideals, so the kernel of f is either all of D or else, f is an injective map. Since f does not map the unit element of D to zero, f must necessarily be an injection, and therefore, the image $f(D)$ (which is a subring of $M_n(F)$) must be isomorphic to D, i.e., $f(D)$ is an *embedding* of D in $M_n(F)$. Now let $E \subset f(D)$ be any subset of the image of f. If $\mathbf{M}_1 = f(d_1)$ and $\mathbf{M}_2 = f(d_2)$ are two distinct elements in E, then $\mathbf{M}_1 - \mathbf{M}_2 = f(d_1) - f(d_2) = f(d_1 - d_2)$. Since $\mathbf{M}_1$ and $\mathbf{M}_2$ are distinct and f is injective, $d_1 - d_2 \neq 0$, so it has a multiplicative inverse in D. Since D is isomorphic to its image $f(D)$, $f(d_1 - d_2) = \mathbf{M}_1 - \mathbf{M}_2$ must also be invertible in $f(D) \subset M_n(F)$. Hence, $\mathbf{M}_1 - \mathbf{M}_2$ must be of full-rank, and our subset E must therefore have the property that the difference of any two elements in E will be of full-rank. ■

2.2 STBCs from Field Extensions

We will recall some well-known facts (see (§7.3, [69]) for instance) about embedding field extensions into matrix algebras in this section. Let K and F be fields, with $F \subset K$, and

$[K : F] = n$, i.e., K is of dimension n over F. In our application to space-time codes, F will be a suitable extension field of $\mathbb{Q}$ determined by the signal set S over which we want to construct the code and K a subfield of $\mathbb{C}$, (i.e., $\mathbb{Q} \subset F \subset K \subset \mathbb{C}$) but in this section, F can be arbitrary. Recall that K can be viewed as an n-dimensional vector space over F, and that we have a natural map L from K to $End_F(K)$, which is the set of F-linear transforms of the vector space K. This map is given by $k \mapsto \lambda_k$, where λ_k is the map on the F-vector space K that sends any $u \in K$ to the element ku. (That is, λ_k is simply left multiplication by k.) As in the discussion in the introduction of this section, L maps K isomorphically into $End_F(K)$, that is, K embeds in $M_n(F)$. This particular method of embedding K into $M_n(F)$ is known as the *regular representation of K 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 for any k as follows: for any given basis element u_i $(1 \leq i \leq n)$, and for any j $(1 \leq j \leq n)$, let $u_i u_j = \sum_{l=1}^{n} c_{ij,l} u_l$. Then, the j-th column of λ_{u_i} is simply the coefficients $c_{ij,l}$ above, $1 \leq l \leq n$. Here, we use the convention that the vectors on which a matrix acts are written on the right of the matrix as a column vector. Once the matrix corresponding to each λ_{u_i}, call it $\mathbf{M}_i$, is obtained in this manner, the matrix corresponding to a general λ_k, with $k = \sum_{i=1}^{n} f_i u_i$ is just the linear combination $\sum_{i=1}^{n} f_i \mathbf{M}_i$. When K is generated over F by a primitive element α (this is always the case in characteristic zero, the case we will consider throughout the thesis), the matrices in the particular basis $\mathcal{B} = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ are easier to write down. Suppose that the minimal polynomial of α over F is $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then the matrix corresponding to λ_α is simply its companion matrix $\mathbf{M}$ given by

$$\mathbf{M} = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & 0 & \vdots \\ 0 & 0 & 0 & 1 & -a_{n-1} \end{bmatrix}, \tag{2.1}$$

and the matrices corresponding to the other powers α^i can be computed directly as the

i-th power of $\mathbf{M}$ and the general element $k = f_0 + f_1\alpha + \ldots f_{n-1}\alpha^{n-1}$ will be mapped to the matrix $f_0 I_n + f_1\mathbf{M} + f_2\mathbf{M}^2 + \cdots + f_{n-1}\mathbf{M}^{n-1}$. We thus have:

Proposition 2.2.1 *Let $K = F(\alpha)$ be an extension of the field F of degree n, and suppose that the minimal polynomial of α over F is $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Let $\mathbf{M}$ be the matrix in $M_n(F)$ defined in (2.1). Then the set of all matrices of the form $f_0\mathbf{I}_n + f_1\mathbf{M} + f_2\mathbf{M}^2 + \cdots + f_{n-1}\mathbf{M}^{n-1}$, with f_0, f_1, ..., f_{n-1} coming from F is an embedding of K into $M_n(F)$. 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.*

Proof: The last statement follows from Proposition 2.1.1 above. ■

When the minimal polynomial of α has the special form $x^n - \gamma$ for some $\gamma \in F^*$ (non-zero elements of F), the form of the matrices simplify considerably. The matrix corresponding to α is then same as (2.1) with $-a_0 = \gamma$, $a_1 = a_2 = \cdots = a_{n-1} = 0$ and the matrix corresponding to λ_k, where $k = f_0 + f_1\alpha + \cdots + f_{n-1}\alpha^{n-1}$, is

$$\begin{bmatrix} f_0 & \gamma f_{n-1} & \gamma f_{n-2} & \ldots & \gamma f_2 & \gamma f_1 \\ f_1 & f_0 & \gamma f_{n-1} & \ldots & \gamma f_3 & \gamma f_2 \\ f_2 & f_1 & f_0 & \ldots & \gamma f_4 & \gamma f_3 \\ f_3 & f_2 & f_1 & \ldots & \gamma f_5 & \gamma f_4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f_{n-1} & f_{n-2} & f_{n-3} & \ldots & f_1 & f_0 \end{bmatrix}. \tag{2.2}$$

These observations essentially prove the following special case of Proposition 2.2.1 above:

Proposition 2.2.2 *Let F be a field, and let γ be a nonzero element of F. Suppose that the polynomial $x^n - \gamma$ ($n \geq 2$) is irreducible in $F[x]$. Then, the set of all matrices of the form (2.2) above, with f_0, f_1, ..., f_{n-1} coming from 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 of any two in it will have full-rank.*

Proof: Let α be some n-th root of γ in some algebraic closure of F. Then the field $K = F(\alpha)$ has degree n over F, since the polynomial $x^n - \gamma$ is irreducible in $F[x]$. The

discussions above then shows that the set of matrices of the form (2.2) above is isomorphic to K under the map L. The last statement follows from Proposition 2.1.1 above. ■

Remark 2.2.1 *It is essential in the proposition above that the elements f_i all come from F. For instance, with $F = \mathbb{Q}$ and $\gamma = n = 2$, we find from the proposition that the set of matrices of the form $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$ with a and b coming from $\mathbb{Q}$ is isomorphic to $\mathbb{Q}(\sqrt{2})$. However, if a and b are allowed to be arbitrary complex numbers, the set of such matrices is no longer a field. For instance, taking $a = \sqrt{2}$ and $b = 1$, we get a nonzero matrix that is not invertible, so the set of all such matrices with arbitrary complex (or even real) entries cannot be a field.*

Let S be the finite subset of the nonzero complex numbers that we wish to use as our signal set, and say $|S| = m$. Write F for the field generated by all the elements of S over $\mathbb{Q}$. For instance, if $S = \{1, j, -1, -j\}$, then F is just the field obtained by adjoining the elements 1, j, -1, and $-j$ to $\mathbb{Q}$ or in other words, F is just $\mathbb{Q}(j)$. Let K be a field extension of F of degree n. Then, by the primitive element theorem, $K = F(\alpha)$, for some element $\alpha \in K$ whose minimal polynomial is $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ for suitable $a_i \in F$. We have the following sequence of field extensions:

$$\mathbb{Q} \subset \mathbb{Q}(S) = F \subset \mathbb{Q}(S, \alpha) = F(\alpha) = K.$$

Consider all matrices of the form $f_0\mathbf{I}_n + f_1\mathbf{M} + f_2\mathbf{M}^2 + \cdots + f_{n-1}\mathbf{M}^{n-1}$, where the f_0, f_1, ..., f_{n-1} come from the signal set S, and where $\mathbf{M}$ is the matrix in $M_n(F)$ defined in (2.1). This is a finite set of matrices of cardinality m^n, which, by Proposition 2.2.1 is a full-rank minimal-delay STBC over S. This construction becomes simpler if we know that there is an element $\gamma \in F^*$ that has the property that the polynomial $x^n - \gamma$ is irreducible in $F[x]$. (Note that γ need not be in S.) This time, we consider matrices of the form (2.2), with the f_i constrained to be in S. We get a finite set of matrices of size m^n, which, by Proposition 2.2.2 is again a full-rank minimal-delay code, and this code is over S and the entries of the codeword matrices are from the set $S \cup \gamma S$. However, suppose that the

set S and the element γ have the property that $\gamma s \in S$ for all elements $s \in S$. Then, all elements of the transmitted matrices will actually have their entries in S. Then S is *invariant under multiplication by* γ and the resulting code is completely over S. In many of our examples below, we will choose S and γ so that S is invariant under multiplication by γ. It is easily verified that a property that the element γ must have if our signal set S is to be invariant under multiplication by γ is:

Lemma 2.2.1 *Let S be a finite subset of the nonzero complex numbers, and let γ be some nonzero complex number. If S is invariant under multiplication by γ, then γ must be a root of unity.*

2.2.1 Rate-optimal codes over rotationally invariant Signal Sets

We first present the construction of rate-optimal STBCs over symmetric m-PSK signal set. The number of transmit antennas n is allowed to be any integer that has the property that the primes that appear in the factorization of n is some subset of the primes that appear in the factorization of m. For example, with 6-PSK signal set one can use 2^i antennas, or 3^j antennas, or 2^i3^j antennas, with i and j being arbitrary.

Given the integer $m \geq 2$ for which an m-PSK code has to be constructed, let ω_m denote $e^{2\pi j/m}$, which is a primitive m-th root of unity. Recall that the m-th cyclotomic field is the field generated by ω_m over $\mathbb{Q}$; $\mathbb{Q}(\omega_m)$ is of degree $\phi(m)$ over $\mathbb{Q}$, where $\phi(m)$ is the Euler totient function of m, that is, $\phi(m)$ is the number of integers i with $1 \leq i \leq m$ that are relatively prime to m. We denote the m-PSK signal set by S_m, that is, $S_m = \{\omega_m^i,\ 0 \leq i < m\}$. Now let n be any integer such that the primes that appear in the prime factorization of n is some subset of $\{p_1, \ldots, p_k\}$, which is the set of primes that appear in the factorization of m. We first prove:

Proposition 2.2.3 *Let n and m be as above and let l be any integer such that l and m are relatively prime. Then, any of the polynomials $x^n - \omega_m^l$, with ω_m as in the discussion above, is irreducible in $\mathbb{Q}(\omega_m)$.*

Proof: Let $\omega_{mn} = e^{2\pi j/mn}$. This is a primitive mn-th root of unity. The element ω_{mn}^l is

a root of $x^n - \omega_m^l$. The minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$ therefore divides $x^n - \omega_m^l$ in $\mathbb{Q}(\omega_m)[x]$. It is therefore sufficient to show that the minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$ is of degree n: this will show that $x^n - \omega_m^l$ must be the minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$, and this will then force $x^n - \omega_m^l$ to be irreducible in $\mathbb{Q}(\omega_m)[x]$. Note that ω_{mn}^l is also a primitive nm-th root of unity. Since $(\omega_{mn}^l)^n = \omega_m^l$, we have the natural containment of cyclotomic fields $\mathbb{Q} \subset \mathbb{Q}(\omega_m^l) \subset \mathbb{Q}(\omega_{mn}^l)$. Since ω_m^l is a primitive l-th root of unity, $\mathbb{Q}(\omega_m^l) = \mathbb{Q}(\omega_m)$. Similarly, $\mathbb{Q}(\omega_{mn}^l) = \mathbb{Q}(\omega_{mn})$, so our containment of fields reads $\mathbb{Q} \subset \mathbb{Q}(\omega_m) \subset \mathbb{Q}(\omega_{mn})$. The degree of $\mathbb{Q}(\omega_{mn})$ over $\mathbb{Q}$ is $\phi(mn)$, while the degree of $\mathbb{Q}(\omega_m)$ over $\mathbb{Q}$ is $\phi(m)$, so because degrees multiply in towers of field extensions, we find that the degree of $\mathbb{Q}(\omega_{mn})$ over $\mathbb{Q}(\omega_m)$ is $\phi(mn)/\phi(m)$.

It is therefore sufficient to prove that $\phi(mn) = n\phi(m)$. This will show that the degree of $\mathbb{Q}(\omega_{mn})$ over $\mathbb{Q}(\omega_m)$ is n, and since $\mathbb{Q}(\omega_{mn})$ $(= \mathbb{Q}(\omega_{mn}^l))$ is generated over $\mathbb{Q}(\omega_m)$ by ω_{mn}^l, this will show that the minimal polynomial of ω_{mn}^l over $\mathbb{Q}(\omega_m)$ is of degree n, as desired. We once again invoke the hypothesis that the primes belonging to the factorization of n appear from the set $\{p_1, \ldots, p_k\}$ (the result $\phi(mn) = n\phi(m)$ would be false without this hypothesis). Suppose that $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (some of the β_i could possibly be zero). Then $\phi(mn) = \phi(p_1^{\alpha_1+\beta_1} \cdots p_k^{\alpha_k+\beta_k}) = p_1^{\alpha_1+\beta_1-1}(p_1 - 1) \cdots p_k^{\alpha_k+\beta_k-1}(p_k - 1) = p_1^{\beta_1} \cdots p_k^{\beta_k} p_1^{\alpha_1-1}(p_1 - 1) \cdots p_k^{\alpha_k-1}(p_k - 1) = n\phi(m)$, as desired. ■

Now we construct the code on the signal set $S_m = \{\omega_m^i,\ 0 \leq i < m\}$ using matrices of the form (2.2) with the elements of S_m substituted for the f_i and with $\gamma = \omega_m^l$. This is our m-PSK code for n antennas. We get one such code for each l, $1 \leq l < n$, for which l and n are relatively prime. Note that under this construction, since multiplication by ω_m^l takes an m-th root of unity to another m-th root of unity, the entries of the matrices transmitted will all be in S_m, i.e., the code is completely over S_m. Moreover, the number of such matrices is $|S_m|^n$ and hence the rate is 1 symbol per channel use, resulting in rate-optimal codes.

Example 2.2.1 *Let us consider the* 4 *element set* $S_4 = \{1, j, -1, -j\}$. *(This set is invariant under multiplication by* j*.) Note that* j *is a primitive* 4*-th root of unity. By Proposition 2.2.3 above, the polynomial* $x^2 - j$ *is irreducible over* $\mathbb{Q}(j)$. *We thus get the*

following set of 16 2×2 *matrices with entries from* S_4 *for our code:*

$$\begin{bmatrix} 1 & j \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ j & 1 \end{bmatrix}, \begin{bmatrix} 1 & -j \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -j & 1 \end{bmatrix}, \begin{bmatrix} j & j \\ 1 & j \end{bmatrix}, \begin{bmatrix} j & -1 \\ j & j \end{bmatrix},$$
$$\begin{bmatrix} j & -j \\ -1 & j \end{bmatrix}, \begin{bmatrix} j & 1 \\ -j & j \end{bmatrix}, \begin{bmatrix} -1 & j \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -1 \\ j & -1 \end{bmatrix}, \begin{bmatrix} -1 & -j \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -j & -1 \end{bmatrix},$$
$$\begin{bmatrix} -j & j \\ 1 & -j \end{bmatrix}, \begin{bmatrix} -j & -1 \\ j & -j \end{bmatrix}, \begin{bmatrix} -j & -j \\ -1 & -j \end{bmatrix}, \begin{bmatrix} -j & 1 \\ -j & -j \end{bmatrix}.$$

The Alamouti code, which is a 2×2 complex orthogonal design of size 2 over S_4, and Example 2.2.1 give codes with identical parameters. In the following two examples we obtain codes with parameters that are not obtainable by orthogonal designs.

Example 2.2.2 *Let us consider the* 6*-PSK signal set* $S_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$ *where* $\omega = e^{\frac{j2\pi}{6}}$ *is a primitive* 6*-th root of unity. (This set is invariant under multiplication by* ω*.) By Proposition 2.2.3 above, the polynomial* $x^2 - \omega$ *and* $x^3 - \omega$ *are irreducible over* $\mathbb{Q}(\omega)$*. With* $x^2 - \omega$ *we get* 36 2×2 *codewords given by* $\begin{bmatrix} a & \omega b \\ b & a \end{bmatrix}$ *where* $a, b \in S_6$*, and with* $x^3 - \omega$ *we get* 216 3×3 *codewords given by* $\begin{bmatrix} a & \omega b & \omega c \\ b & a & \omega b \\ c & b & a \end{bmatrix}$ *where* $a, b, c \in S_6$*.*

Instead of codes from m-PSK signal sets, which are invariant under rotation by ω_m, we will now consider the codes over any signal set invariant under rotation of $2\pi/k$, that is, invariant under multiplication by $\omega_k = e^{2\pi/k}$. One would start from a set that is a subset of $\mathbb{Q}(\omega_k)$ and then construct codes for n antennas using the extension given by the n-th root of ω_k. (Of course, n has to satisfy the condition that the prime factorization of n should only involve primes that appear in the prime factorization of k.) For instance, when $k = 3$ (so our angle of rotation is 120°), we can let S_1 be any finite set of nonzero complex numbers contained in the cyclotomic extension $\mathbb{Q}(\omega_3)$, and let $S = S_1 \cup \omega_3 S_1 \cup \omega_3^2 S_1$. Then S is invariant under multiplication by ω_3, and we can construct a code on S for n transmit antennas, where n is any power of 3, using matrices of the form (2.2) with $\gamma = \omega_3$. The following example gives a code over signal sets invariant under 90° rotation.

Example 2.2.3 *Let $a \geq b > 2$ be odd integers, and let S consist of the union of the two sets $S_1 = \{(a-2k)+j(b-2l) | 0 \leq k \leq a,\ 0 \leq l \leq b\}$ and $S_2 = jS_1 = \{-(b-2l)+j(a-2k) | 0 \leq k \leq a,\ 0 \leq l \leq 2b\}$. Note that both S_1 and S_2 are invariant under multiplication by -1. When $a = b$, we have a square constellation. When $a > b$, S is a cross constellation. In both cases, we can obtain our codes from this signal set S for any n a power of 2 by taking matrices of the form (2.2) with $\gamma = j$, and with the elements f_i chosen from S. Of course, we can construct our codes on just the set S_1 using this same procedure. The entries of the matrices will then come from $S_1 \cup S_2$.*

As an another specific example, let us take $S = \{1, \omega_3, \omega_3^2, -1, -\omega_3, -\omega_3^2, \omega_3 - \omega_3^2, -1 + \omega_3^2, 1 - \omega_3\}$. Note that $S = \omega_3 S = \omega_3^2 S$, so S is already invariant under rotation by 120°. We can use this set to construct codes for transmission on $n = 3^l$ antennas for arbitrary l as described above.

2.2.2 Rate 1 codes over signal sets derived from symmetric m-PSK signal sets for arbitrary number of antennas

In the previous subsection for a given m the number of antennas n is restricted to have only those primes that are in m also *only* if we need rate-optimal codes. If rate-optimality is not a constraint then over any finite subset (including S_m) of subfields of $\mathbb{C}$, full-rank STBCs can be constructed for arbitrary number of antennas, using the following proposition:

Proposition 2.2.4 *Let F be a field of characteristic zero, and let z be an indeterminate. Also, let $F(z)$ be the rational function field over F in the indeterminate z, that is, it is the set of quotients of polynomials in z with entries from F. Then, for any integer $n \geq 1$, the polynomial $x^n - z$ is irreducible in the ring $F(z)[x]$.*

Proof: It is sufficient to prove that $x^n - z$ is irreducible in $F(\omega_n, z)[x]$, where ω_n is a primitive n-th root of unity. (Note that the assumption about the characteristic guarantees the existence of a primitive n-th root of unity.) If we let ζ denote an n-th root of z (in some algebraic closure of $F(\omega_n, z)$), then $x^n - z$ factors as $\Pi_{i=0}^{n-1}(x - \omega_n^i \zeta)$ over the field $F(\omega_n, z, \zeta) = F(\omega_n, \zeta)$. So, if f is some irreducible factor of $x^n - z$ in $F(\omega_n, z)[x]$,

say of degree $k < n$, then over $F(\omega_n, \zeta)$, f must equal the product of some k of these linear factors $(x - \omega_n^i \zeta)$. Studying the constant term of this product, we find that ζ^k is in $F(\omega_n, z)$, or, taking n-th powers, that z^k is an n-th power in $F(\omega_n, z)$. But it is easy to see that when $k < n$, this is impossible: if we were to write $z^k = (g(z)/h(z))^n$, where g and h are polynomials in z with coefficients in $F(\omega_n)$, then, $h(z)^n z^k$ should equal $g(z)^n$. Comparing the highest degree (in z) on both sides gives us the contradiction. Hence, k must equal n, that is, $x^n - z$ must be irreducible in $F(\omega_n, z)[x]$. ■

We will use this proposition as follows. Let S_m be the set of m-th roots of unity, and let us pretend that we are working over the field $\mathbb{Q}(\omega_m, z)$, where z is any transcendental number, for instance, e, or π, or e^{ju}, for any algebraic real number u, even $u = 1$. Then over that field, the polynomial $x^n - z$ is irreducible, since the transcendental element z acts just as an indeterminate over $\mathbb{Q}(\omega_m)$. (It follows from the well known fact that if z is transcendental over $\mathbb{Q}$, it remains transcendental over an algebraic extension of $\mathbb{Q}$ such as $\mathbb{Q}(\omega_m)$.) We may then consider the various $n \times n$ matrices of the form (2.2), with $\gamma = z$.

Note that there is no limitation under this scheme on n: the number of antennas can therefore be arbitrary. Also note that if we take z to be of the form $e^{ju} = \cos(u) + j \sin(u)$ for some real algebraic number, for example, $u = 1$, then the entries will consist of the original m equally spaced points on the unit circle, and a copy of these points multiplied by e^{ju}, that is, rotated counter clockwise by u radians.

In the following example we construct a code over such a signal set with 8 elements shown in Figure 2.1.

Example 2.2.4 *In Example 2.2.1 the codewords are* $\begin{bmatrix} f_0 & \gamma f_1 \\ f_1 & f_0 \end{bmatrix}$ *where* γ *was chosen to be* j *corresponding to the irreducible polynomial* $x^2 - j$ *and* $f_0, f_1 \in S = \{1, -1, j, -j\}$. *Now for some* θ *that is a real algebraic number we can take the irreducible polynomial* $x^3 - e^{j\theta}$, *use the same* S, *and construct code for* 3 *antennas (note that* 3 *is a prime not appearing in the prime power factorization of* 4*). We obtain the full-rank code over the asymmetric 8-PSK signal set shown in Figure 2.1, for* 3 *antennas containing the 64*

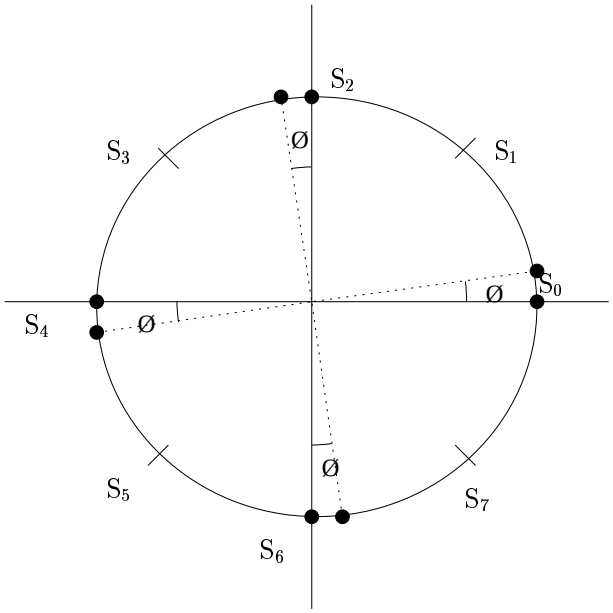


Figure 2.1: Asymmetric 8-PSK signal set matched to a dihedral group with 8 elements

codewords given by $\begin{bmatrix} a & ce^{j\theta} & be^{j\theta} \\ b & a & ce^{j\theta} \\ c & b & a \end{bmatrix}$ *where* $a, b, c \in S$*, using Proposition 2.2.4.*

On the other hand, when the transcendental element z is real, the entries will be the original m equally spaced points on the unit circle, and these same points shifted radially to the circle at radius $|z|$. Note too that by choosing different real transcendentals (for example, αe for any nonzero rational number α), we can get different radius for the second circle.

2.2.3 Construction of STBCs using non-cyclotomic field extensions

All our examples in the previous three subsections have arisen from application of Proposition 2.2.2, where the minimal polynomial of the element α was of the form $x^n - \gamma$. For the sake of completeness, we will give an example in this section of a code constructed by applying Proposition 2.2.1, that is, where the minimal polynomial has other terms besides the constant term and the highest degree term. Of course, the entries of the

matrices involved, in this general situation, will be linear combinations of the elements of the signal set.

First, a well-known result that will help us construct irreducible polynomials over fields other than the rationals:

Lemma 2.2.2 *Let $f(x)$ 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, $f(x)$ remains irreducible over F.*

Proof: This is standard. If α is a root of $f(x)$, then $\mathbb{Q}(\alpha)$ is an extension of $\mathbb{Q}$ of degree n. The field $F(\alpha)$ contains $\mathbb{Q}(\alpha)$, so $[F(\alpha) : \mathbb{Q}]$ is divisible by $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Similarly, $F(\alpha)$ contains F, so $[F(\alpha) : \mathbb{Q}]$ is divisible by $[F : \mathbb{Q}] = m$. Since n and m are relatively prime, $[F(\alpha) : \mathbb{Q}]$ is divisible by nm, and hence, $[F(\alpha) : F] = [F(\alpha) : \mathbb{Q}]/[F : \mathbb{Q}]$ is divisible by $nm/m = n$. On the other hand, the minimal polynomial of α over F divides $f(x)$, so the degree of this minimal polynomial is at most n. It follows that $[F(\alpha) : F]$ is exactly n, and that $f(x)$ is the minimal polynomial of α over F, and in particular, that $f(x)$ remains irreducible over F. ■

We now give a class of codes constructed from minimal polynomials that are one step more complicated than those of the form $x^n - \gamma$: Let $f(x)$ be of the form $x^n - px - p$, for some prime p. By Eisenstein's Criterion (§2.16, [69]), $f(x)$ is irreducible over the rationals. Let m be any integer such that $\phi(m)$ and n are relatively prime. Let ω_m be a primitive m-th root of unity, and consider $\mathbb{Q}(\omega_m)$, the m-th cyclotomic field. This is of degree $\phi(m)$ over the rationals, so, by the lemma above and the assumption about n and $\phi(m)$, $f(x)$ remains irreducible over $\mathbb{Q}(\omega_m)$. Hence, if M is the matrix (2.1) (with $a_0 = a_1 = p$, and $a_2 = \cdots = a_{n-1} = 0$), then, for S equal to the m-th roots of unity, the set of all matrices of the form $s_0 + s_1\mathbf{M} + s_2\mathbf{M}^2 + \cdots + s_{n-1}\mathbf{M}^{n-1}$, where the s_i are allowed to be arbitrary members of S, is an rate-optimal code of size m^n.

Example 2.2.5 *Consider $f(x) = x^3 - 2x - 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Let us work over $\mathbb{Q}(j)$, a field extension of $\mathbb{Q}$ of degree 2 (note that 2 and 3*

are relatively prime). Then, our code consists of all 3×3 *matrices of the form*

$$\begin{bmatrix} s_0 & 2s_2 & 2s_1 \\ s_1 & s_0 + 2s_2 & 2s_1 + 2s_2 \\ s_2 & s_1 & s_0 + 2s_2 \end{bmatrix}$$

where the s_i *are arbitrary members of the set* $\{1, j, -1, -j\}$*. Of course, the same set of matrices above also forms a code if the* s_i *are allowed to come from the set of* 2^r*-th roots of unity, for any* $r \geq 2$*, since the* 2^r*-th cyclotomic field has degree* 2^{r-1}*, which is relatively prime to* 3*.*

2.3 STBCs from non-commutative division algebras

In this section we begin the STBC construction using embeddings of non-commutative division algebras in matrix rings. First we present the basic structural properties of division algebras in the following subsection. Then we discuss the left regular representation of division algebras which is the counterpart of Subsection 2.2 for the case of field extensions.

Given a division algebra D, its *center* $Z(D)$ is the set $\{x \in D | xd = dx \forall d \in D\}$. It is easy to see that $Z(D)$ is a field; D therefore has a natural structure as a $Z(D)$ vector space. In this thesis, we will only consider division algebras that are finite dimensional as a vector space over their center. (Such algebras are referred to as *finite dimensional division algebras*.) Good references for division algebras are [53–55, 69].

If F is any field, by an *F division algebra*, or a *division algebra over F*, we will mean a division algebra D whose center is precisely F. It is well known that the dimension $[D : F]$ is always a perfect square. If $[D : F] = n^2$, the square root of the dimension, n, is known as the *degree* or the *index* of the division algebra.

The Hamilton's Quaternions denoted by $\mathbb{H}$ is the four dimensional vector space over the field of real numbers $\mathbb{R}$ with basis $\{1, \hat{i}, \hat{j}, \hat{k}\}$, with multiplication given by $\hat{i}^2 = \hat{j}^2 = -1$ and $\hat{i}\hat{j} = k = -\hat{j}\hat{i}$. That is, $\mathbb{H}$ is the set of all expressions of the form $\{a(= a \cdot 1) + b\hat{i} + c\hat{j} + d\hat{k} \mid a, b, c, d \in \mathbb{R}\}$. The real numbers are identified with quaternions in which the

coefficients of $\hat{i}$, $\hat{j}$, and $\hat{k}$ are all zero. One can check that the multiplicative inverse of the nonzero quaternion $x = a+b\hat{i}+c\hat{j}+d\hat{k}$ is the quaternion $(a/z)-(b/z)\hat{i}-(c/z)\hat{j}-(d/z)\hat{k}$, where $z = a^2+b^2+c^2+k^2$. Thus, as every nonzero element has a multiplicative inverse, $\mathbb{H}$ is indeed a division algebra. Clearly, the center of $\mathbb{H}$ is just the set $\{a(= a\cdot 1)+0\hat{i}+0\hat{j}+0\hat{k}\}$, that is, under the identification described above, the center of $\mathbb{H}$ is just $\mathbb{R}$. Notice that $\mathbb{H}$ is four $(= 2^2)$ dimensional over its center $\mathbb{R}$, that is, $\mathbb{H}$ is of degree (or "index") 2.

By a *subfield* of a division algebra, we will mean a field K, such that $F \subseteq K \subseteq D$. Note that D can have other subfields K such that $F \not\subseteq K$, but we will not consider such subfields. If K is a subfield of D, then K is a subspace of the F-vector space D, and $[K : F]$ divides $[D : F] = n^2$. It is known that the maximum possible value of $[K : F]$ is n; such a subfield is called a *maximal subfield* of D. It is known that maximal subfields exist in profusion. If E is any subfield of D, then viewing D as an E-space, we can obtain an embedding of D into $M_{n_e}(E)$ where n_e is $[D : E]$. In particular, we give, in the following subsections embeddings of D into $M_{n^2}(F)$ and $M_n(K)$.

2.3.1 Codes From The Left Regular Representation of Division Algebras

Given an F division algebra D of degree n, D is naturally an F-vector space of dimension n^2. We thus have a map $L\colon D \rightarrow End_F(D)$, where $End_F(D)$ is the set of F linear transforms of the vector space D. This map is given by left multiplication: it takes any $d \in D$ to λ_d, where λ_d is *left* multiplication by d, that is, $\lambda_d(e) = de$ for all $e \in D$. It is easy to check that λ_d is indeed an F-linear transform of D, that is, $\lambda_d(f_1e_1 + f_2e_2) = f_1\lambda_d(e_1) + f_2\lambda_d(e_2)$. (Notice that it is crucial that F be the center of D, otherwise, the map λ_d will not be F linear, that is, $\lambda_d(fe)$ will not equal $f\lambda_d(e)$!) One also checks that L is a ring homomorphism from D to $End_F(D)$, that is, $\lambda_{d_1+d_2} = \lambda_{d_1} + \lambda_{d_2}$, $\lambda_{d_1d_2} = \lambda_{d_1}\lambda_{d_2}$, and $\lambda_1 = 1$. Since D has no two sided ideals, L is an injection, and on choosing a basis for D as an F vector space, we will get an embedding of D in $M_{n^2}(F)$. Notice that the size of the matrices involved is n^2 and not n. (An analogous game can be played with right multiplication maps ρ_d, but there we would have $\rho_{d_1d_2} = \rho_{d_2}\rho_{d_1}$, and thus we would have

a ring *anti-homomorphism* from D to $End_F(D)$. We will not pursue this further here.)

Exactly as in the field case in Subsection 2.2, we write down the matrix corresponding to λ_d with respect to a given basis $\mathcal{B} = \{u_1, u_2, \ldots, u_{n^2}\}$ as follows: For any given basis element u_i $(1 \leq i \leq n^2)$, and for any j $(1 \leq j \leq n^2)$, let $u_i u_j = \sum_{l=1}^{n^2} c_{ij,l} u_l$. Then, the j-th column of λ_{u_i} is simply the coefficients $c_{ij,l}$ above, $1 \leq l \leq n^2$. (Here, we use the convention that the vectors on which a matrix acts are written on the right of the matrix as a column vector, so the j-th column of the matrix just represents the image of the j-th standard basis vector under the action of the matrix.) Once the matrix corresponding to each λ_{u_i}, call it M_i, is obtained in this manner, the matrix corresponding to a general λ_d, with $d = \sum_{i=1}^{n^2} f_i u_i$ is just the linear combination $\sum_{i=1}^{n^2} f_i M_i$.

Example 2.3.1 *Let us consider the left regular representation of* $\mathbb{H}$ *with respect to the basis* $\{1, \hat{i}, \hat{j}, \hat{k}\}$. *The defining relations* $\hat{i}^2 = \hat{j}^2 = -1$, $\hat{i}\hat{j} = \hat{k} = -\hat{i}\hat{j}$, *etc. show that for* $x = a + b\hat{i} + c\hat{j} + d\hat{k}$, *the matrix corresponding to* λ_x *is* $\begin{bmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{bmatrix}$ *which is precisely the 4 dimensional orthogonal real design of the paper [6, §III-A] of Tarokh, et. al.*

In the sections ahead, we will construct other division algebras besides the quaternions, and we can apply the left regular representation to these algebras to get codes of size m^{n^2} for n transmit antennas, where m is the size of the signal set, and n is the index of the division algebra.

2.3.2 Cyclic Division Algebras

A *cyclic division algebra* D over the field F is a division algebra that has a maximal subfield K that is Galois over F, with $Gal(K/F)$ being cyclic.

Example 2.3.2 *Hamilton's quaternions* $\mathbb{H}$ *is a cyclic division algebra! For, notice that the subset* $\{a + 0\hat{i} + c\hat{j} + 0\hat{k} \mid a, b \in \mathbb{R}\}$ *is isomorphic to the complex numbers* $\mathbb{C}$. *Let us*

identify the complex numbers with this subset and write (by abuse of notation) $\mathbb{C}$ *for this subset. Notice that* $\mathbb{C}$ *is of dimension* 2 *over the center* $\mathbb{R}$*, that is,* $\mathbb{C}$ *is a maximal subfield of* $\mathbb{H}$*. Now notice that* $\mathbb{C}/\mathbb{R}$ *is indeed a Galois extension, whose Galois group is* $\{1, \sigma\}$*, where* σ *stands for complex conjugation. This is of course a cyclic group! Thus,* $\mathbb{H}$ *is a cyclic division algebra.*

Now, given a cyclic division algebra D with center F, of index n, and with maximal cyclic subfield K/F, let $Gal(K/F)$ be generated by σ. Then $\sigma^n = 1$, of course. D is naturally a *right* vector space over K, with the product of the (scalar) $k \in K$ on the vector $d \in D$ defined to be dk. (Note the definition: the action of scalars is defined via multiplication on the right—if one were to define the action of scalars via multiplication from the left, one would get a different K vector space structure on D.) It is well known that we have the following decomposition of D as right K spaces:

$$D = K \oplus zK \oplus z^2K \oplus \cdots \oplus z^{n-1}K, \tag{2.3}$$

where z is some element of D that satisfies the relations

$$kz = z\sigma(k)\ \forall k \in K \tag{2.4}$$

$$z^n = \delta, \text{ for some } \delta \in F^* \tag{2.5}$$

where F^* is the set F excluding the zero element and z^iK stands for the set of all elements of the form z^ik for $k \in K$. (Note that the element δ above is actually in F, the center.)

Equations (2.3) and (2.4) above provide a very convenient handle into the division algebra: all the non-commutativity is concentrated just in the way in which the element z interacts with elements of K: pulling z from the right of $k \in K$ to the left just induces σ on k. Also, the field generated by the element z over F is of a particularly nice kind: it is given by just adjoining an n-th root of the element δ. It is the existence of such a decomposition that makes cyclic division algebras a very manageable class of division algebras.

The division algebra D, with its decomposition above, is often written as $(K/F, \sigma, \delta)$.

Example 2.3.3 *One sees easily that in the case of* $\mathbb{H}$*, one can regroup the* $\mathbb{R}$ *space decomposition* $\mathbb{H} = \{a + b\hat{i} + c\hat{j} + d\hat{k} \mid a, b, c, d \in \mathbb{R}\}$ *as* $\mathbb{H} = \mathbb{C} \oplus i\mathbb{C}$*, where, as in Example 2.3.2, we have identified* $\mathbb{C}$ *with the subset* $\{a + 0\hat{i} + c\hat{j} + 0\hat{k}\}$ *of* $\mathbb{H}$*. This gives the decomposition of* $\mathbb{H}$ *as a right* $\mathbb{C}$ *vector space, with the element* $\hat{i}$ *playing the role of "z" above. Moreover, since* $\hat{i}^2 = -1$*, the element* δ *above is* -1 *in this example.*

Let D be a cyclic division algebra over F of index n, with maximal cyclic subfield K. As we have seen above, D is a right K space, of dimension n (each summand z^iK in Equation (2.3) above is a one-dimensional K space, and there are n such). To emphasize the right K structure, let us write D_K for D viewed as a right K vector space. Now note that D acts on D_K by multiplication on the *left* as follows: given $d \in D$, it sends an arbitrary $e \in D_K$ to de. Since this action is from the left, while the scalar action of K on D_K is from the right, these two actions commute. That is, $d(ek) = (de)k$, something that is, of course obvious, but crucial. Let us write λ_d for the map from D_K to D_K that sends $e \in D$ to de. Then, the fact that the action of λ_d and that of the scalars commute means that λ_d is a K-linear transform of D_K. In other words, we have a map $f\colon D \to End_K(D_K)$ that sends d to λ_d. One checks that this is a ring homomorphism, that is $\lambda_{d_1+d_2} = \lambda_{d_1} + \lambda_{d_2}$, and $\lambda_{d_1 d_2} = \lambda_{d_1}\lambda_{d_2}$. (For this second relation, note that $\lambda_{d_1 d_2}(e) = (d_1 d_2)e = d_1(d_2 e) = \lambda_{d_1}(\lambda_{d_2}(e))$.)

We thus have an embedding of D into $End_K(D_K)$, which, once one chooses a K basis for D_K, translates into the embedding of D into $M_n(K)$ that is needed for Proposition 2.1.1. A natural basis, of course, is given by the decomposition in Equation (2.3) above: we choose the basis $\{1, z, z^2, \ldots, z^{n-1}\}$. A typical element $d = k_0 + zk_1 + \cdots + z^{n-1}k_{n-1}$ sends 1 to $d = k_0 + zk_1 + \ldots z^{n-1}k_{n-1}$, so the first column of the matrix corresponding to λ_d in this basis reads k_0, k_1, $\ldots$, k_{n-1}. For the second column, note that $dz = (k_0 + zk_1 + \ldots z^{n-1}k_{n-1})z = k_0 z + zk_1 z + \ldots z^{n-1}k_{n-1}z = z\sigma(k_0) + z^2\sigma(k_1) + \ldots z^{n-1}\sigma(k_{n-2}) + \delta\sigma(k_{n-1})$, where we've used the relations in Equation (2.4) to pull z from the right to the left. So, the second column reads $\delta\sigma(k_{n-1}), \sigma(k_0), \sigma(k_1), \ldots, \sigma(k_{n-2})$. Similarly, $dz^2 = (k_0 + zk_1 + \ldots z^{n-1}k_{n-1})z^2 = z^2\sigma^2(k_0) + z^3\sigma^2(k_1) + \cdots \delta\sigma^2(k_{n-2}) + z\delta\sigma^2(k_{n-1})$.

Proceeding thus, we find that the matrix corresponding to λ_d is the following:

$$\begin{bmatrix} k_0 & \delta\sigma(k_{n-1}) & \delta\sigma^2(k_{n-2}) & \dots & \delta\sigma^{n-2}(k_2 & \delta\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \delta\sigma^2(k_{n-1}) & \dots & \delta\sigma^{n-2}(k_3) & \delta\sigma^{n-1}(k_2) \\ k_2 & \sigma(k_1) & \sigma^2(k_0) & \dots & \delta\sigma^{n-2}(k_4) & \delta\sigma^{n-1}(k_3) \\ k_3 & \sigma(k_2) & \sigma^2(k_1) & \dots & \delta\sigma^{n-2}(k_5) & \delta\sigma^{n-1}(k_4) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ k_{n-1} & \sigma(k_{n-2}) & \sigma^2(k_{n-3}) & \dots & \sigma^{n-2}(k_1) & \sigma^{n-1}(k_0) \end{bmatrix} \tag{2.6}$$

We thus have the following corollary to Proposition 2.1.1:

Corollary 2.3.1 *Let F be a subfield of the complex numbers, and let D be a cyclic division algebra over F of index n. Let K be a maximal cyclic subfield of D. Let δ be defined by the cyclic decomposition given in Equations (2.3) and (2.4). Then, any finite subset E of matrices of the form (2.6) above, with the k_i coming from K, will have the property that the difference of any two elements in E will be of full-rank.*

Let us go back to the examples of the quaternions: we saw above in Example 2.3.2 that $\mathbb{H}$ is cyclic: the subfield $\mathbb{C}$ (under the identification described in that example) is a cyclic extension of $\mathbb{R}$, with Galois group generated by complex conjugation. Let us write k^* for the complex conjugate of $k \in \mathbb{C}$. In Example 2.3.3, we saw that we have the decomposition $\mathbb{H} = \mathbb{C} \oplus i\mathbb{C}$, as a right $\mathbb{C}$ space, with the role of the element "z" of the discussion above played by the quaternion $\hat{i}$. We also saw that since $\hat{i}^2 = -1$, the element δ of the discussion above is just -1. Thus, by Corollary 2.3.1 above, any finite set of matrices of the form $\begin{bmatrix} k_0 & -k_1^* \\ k_1 & k_0^* \end{bmatrix}$ is a full rank minimum delay code. But these are precisely Alamouti's matrices!

Alamouti's construction has a certain uniqueness from the point of view of division algebras. (Of course, in [6], the authors have also studied the uniqueness of these codes from the point of view of orthogonal designs.) One has the following: Hamilton's quaternions $\mathbb{H}$ is the only (non-commutative) division algebra which has $\mathbb{C}$ as a maximal subfield.

This arises from two well known facts: first, the only subfield F (up to a suitable isomorphism) of $\mathbb{C}$ such that $[\mathbb{C} : F]$ is finite is the $\mathbb{R}$ (a theorem of Artin and Schreier, see [70, Theorem 11.14], and second, the only non-commutative (and associative) division algebra over the $\mathbb{R}$ is the quaternions (a theorem of Frobenius, see [55, Chapter 13, Corollary C] for instance). Thus, the only possible set of matrices of the form (2.6) in which the k_i are allowed to be arbitrary complex numbers that forms a division algebra is the one corresponding to the quaternions: matrices of the form (2.3.2) where $n = 2$, $\delta = -1$ and σ given by complex conjugation.

Note that we will come up with several examples below where we will embed suitable division algebras D into $M_n(\mathbb{C})$ for various values of n other than $n = 2$ and thus obtain space time codes for more than 2 transmit antennas. The key distinction is that these division algebras will not have $\mathbb{C}$ as a maximal subfield, and therefore, the entries of the corresponding matrices will not be allowed to take on arbitrary complex values (in contrast with Alamouti's example).

To apply the general machinery of Corollary 2.3.1 above for constructing space time codes, we need to generate concrete division algebras over suitable subfields of $\mathbb{C}$. A natural candidate for this is the following technique: Let us take a known cyclic Galois extension K/F, whose Galois group is generated by some σ. Suppose that $[K : F] = n$, so that $\sigma^n = 1$. Let us pick a nonzero element $\delta \in F^*$, and let us construct abstractly the algebra

$$(K/F, \sigma, \delta) = K \oplus zK + \oplus z^2K + \cdots + \oplus z^{n-1}K,$$

where z is some symbol that satisfies the two relations given in Equation 2.4, namely, $kz = z\sigma(k)$ for all $k \in K$, and $z^n = \delta$. It would be tempting to assume that this technique would automatically give us a division algebra, but unfortunately, this is not true. What is known is that we get an algebra whose center is F, and which is *simple,* that is, it has no nontrivial two sided ideals. Not every nonzero element in this algebra need be invertible, however. Fortunately, we have the following *sufficient* criterion to help us ([55, Chapter 15, Corollary d], or [70, Theorem 8.14]):

Proposition 2.3.1 *In the construction above,*

$$A = (K/F, \sigma, \delta)$$

is a division algebra if the smallest positive integer t such that δ^t is the norm of some element in K^* is n. (The norm of an element $k \in K^*$ is the product $k\sigma(k)\sigma^2(k)\ldots\sigma^{n-1}(k)$; this is clearly invariant under σ and is hence in F. Note that for any $a \in F^*$, the norm of a is just a^n, and hence, δ^n is the norm of δ. Thus, n is an upper bound for the integer t of the proposition above, and the content of the proposition is that if t is the maximum it can be, then A is definitely a division algebra.)

We can use Proposition 2.3.1 to construct cyclic division algebras very easily over fields of the form $F(\delta)$, where F is a suitable algebraic number field (for instance, when F is a finite extension of $\mathbb{Q}$), and where δ is some transcendental number, for example, e, or π, or $e^{ju} = \cos(u) + j\sin(u)$ for any real algebraic number u. (The fact that e^{ju} is transcendental for any real algebraic number u follows from the Lindemann-Weierstrass Theorem ([69, pp. 277, vol. 1], see Chapter 4 for the statement of the theorem); Suppose that F has a cyclic extension K of degree n, whose Galois group is generated by some σ. We have the following:

Proposition 2.3.2 *With F, K, n, z, and σ as above, the algebra*

$$(K(\delta)/(F(\delta), \sigma, \delta)$$

is a division algebra.

Corollary 2.3.2 *Continuing with the notation of Proposition 2.3.2, any finite subset E of matrices of the form (2.6) above, with the k_i coming from K, will have the property that the difference of any two matrices in E will be of full rank.*

Proof: This follows from Corollary 2.3.1. ■

In the following subsection we will construct STBCs over certain SPSK signal sets by way of illustration of Proposition 2.3.2.

2.3.3 Rate-1 STBCs over SPSK signal sets

Let $m = p^\alpha$, where p is an *odd* prime, and let $n = p^\beta$, for any $\alpha > 0$ and $\beta > 0$. Let ω_m be a primitive m-th root of unity, and let $F = \mathbb{Q}(\omega_m)$. As we saw in Proposition (2.2.3) above, the polynomial $x^n - \omega_m$ is irreducible in $F[x]$. If ω_{mn} is a primitive mn-th root of unity which is a root of this polynomial, then $K = \mathbb{Q}(\omega_{mn})$ is of degree n over F. Moreover, K/F is actually a cyclic Galois extension. This follows from two well know facts: The Galois group of $\mathbb{Q}(\omega_k)/\mathbb{Q}$, where ω_k is a primitive k-th root of unity for some k, is isomorphic to the group of units of the ring $\mathbb{Z}/k\mathbb{Z}$, and when k is a power of an odd prime (in our case, $p^{\alpha+\beta}$), the group of units of $\mathbb{Z}/k\mathbb{Z}$ is a cyclic group. Hence, the Galois group of K/F, which is a subgroup of the Galois group of $K/\mathbb{Q}$, is also cyclic.

We may use this field extension K/F to construct our codes: for instance, our signal set could be the set of mn-th roots of unity, which would be mn equally spaced points on the circle. For the Galois action on K, note that we have an isomorphism between the group of units of the ring $\mathbb{Z}/mn\mathbb{Z}$ and $Gal(K/\mathbb{Q})$ given as follows: one fixes a generator $[l]$ of the group of units of the ring $\mathbb{Z}/mn\mathbb{Z}$ $(0 < l < n)$, and one considers the map that sends ω_{mn} to ω_{mn}^l. One shows that this map is indeed in the Galois group of $K/\mathbb{Q}$, and in fact, generates the group. Now, since the group $\mathbb{Z}/mn\mathbb{Z}^*$ is cyclic, we find that the Galois group of K/F is the unique cyclic subgroup of this group of order n, and this is generated by $[l]^{\phi(nm)/n} = [l]^{\phi(m)}$. (Note that because m and n are both powers of the same prime, $\phi(nm) = n\phi(m)$.) Hence, once we fix a generator $[l]$ of $\mathbb{Z}/mn\mathbb{Z}^*$, our map σ is the one that sends ω_{mn} to $\omega_{mn}^{l^{\phi(m)}} = \omega_{mn}^{l^{p^{\alpha-1}(p-1)}}$.

When $n \leq m$ (so that ω_n is already contained in F) the map σ is a little easier to describe. It is easy to see that $1 + m$ has order exactly n in $\mathbb{Z}/mn\mathbb{Z}^*$ (one observes using the binomial theorem and the fact that $n = p^\beta \leq m = p^\alpha$ that $(1 + m)^t = 1 + tm$ in $\mathbb{Z}/mn\mathbb{Z}$). Hence, our map σ is the one that sends ω_{mn} to $\omega_{mn}^{1+m} = \omega_n\omega_{mn}$.

Example 2.3.4 *Suppose that $m = 3^2 = 9$, and $n = 3$. Then, $mn = 27$, so our signal set is 27-PSK. Take $\omega_9 == e^{2\pi j/9}$, a primitive 9-th root of unity. The number $e^{2\pi j/27}$ is a primitive 27th root of unity, and satisfies $(e^{2\pi j/27})^3 = e^{2\pi j/9}$. We may take $e^{2\pi j/27}$ to be*

our ω_{27}*. Note that* $(e^{2\pi j/27})^9 = e^{2\pi j/3}$*, a primitive* 3*rd root of unity. Our map* σ *therefore sends* ω_{27} *to* $\omega_{27}^{1+9} = e^{2\pi j/3}\omega_{27} = e^{20\pi j/27}$*, and in general,* ω_{27}^k *to* $e^{20k\pi j/27}$*. So, the set of* 3×3 *matrices*

$$\begin{pmatrix} \omega_{27}^k & \delta \cdot \sigma(\omega_{27})^m & \delta \cdot \sigma^2(\omega_{27})^l \\ \omega_{27}^l & \sigma(\omega_{27})^k & \delta \cdot \sigma^2(\omega_{27})^m \\ \omega_{27}^m & \sigma(\omega_{27})^l & \sigma^2(\omega_{27})^k \end{pmatrix}$$

where δ *is any transcendental number, where* k*,* l*, and* m *can be any of* $\{0, 1, 2, \ldots, 26\}$*, forms a full rank minimum delay space time code.*

In Chapter 4, we will discuss as a special case more about cyclic division algebras and STBCs from them.

Chapter 3

High-Rate, Full-Diversity STBCs from Field Extensions

First, we briefly summarize the constructions of STBCs from field extensions discussed in the previous chapters as follows:

- Rate-optimal codes over rotationally invariant signal sets are constructed using algebraic extensions of the field $\mathbb{Q}$. This includes the case when the signal set is a finite subset of the field $\mathbb{Q}(\omega_m)$ (which includes symmetric m-PSK signal set) and n, the number of transmit antennas, is such that the set of prime factors of n are subset of the set of prime factors of m. Thus, if the signal set is a QAM signal set or an m-PSK signal set, where $m = 2^b$, then we can construct STBCs for $n = 2^a$ transmit antennas only.

- Rate-1 codes over signal sets derived from symmetric m-PSK signal sets, for arbitrary number of transmit antennas have been constructed using transcendental extensions of the field $\mathbb{Q}$. The disadvantage of these codes is that it is very difficult to get the value or a lower bound on the value of coding gain.

- Rate-1 codes over finite subsets of $\mathbb{Q}(\omega_m)$ for n transmit antennas were constructed using non-cyclotomic field extensions, where n and m are such that $(n, \phi(m)) = 1$.

[1]Part of the results presented in this chapter are available in publications [37–39].

Since $\phi(m)$ is even for $m \geq 3$, the number of transmit antennas n can not take values from the set of positive even integers.

In this chapter,

- We obtain rate-1 codes over m-PSK signal sets for arbitrary number of transmit antennas, using algebraic extensions (Section 3.1).
- We construct high-rate, full-rank STBCs over arbitrary finite subsets of $\mathbb{Q}(\omega_m)$ for arbitrary number of transmit antennas, using both algebraic and transcendental extensions of the field $\mathbb{Q}$ (Section 3.2).
- We give an expression for the coding gain of the STBCs from field extensions for arbitrary number of transmit antennas (Section 3.3).
- We obtain lower bounds on the value of coding gain for some STBCs from field extensions (Subsection 3.3.1).
- We analyze the mutual information of the STBCs from field extensions, when the input is a continuous Gaussian random variable (Section 3.4). Also, we show that the finite-signal-set capacity of the STBCs improves with increase in the symbol rate of the STBC (Section 3.5).
- Finally, we present simulation results to show that high-rate, full-rank STBCs from field extensions perform better than the rate-1, full-rank STBCs (Section 3.6).

3.1 Rate-1 STBCs over arbitrary finite subsets of $\mathbb{Q}(\omega_m)$ for arbitrary number of antennas

In the previous chapter, we have seen that when the number of transmit antennas n and the size of PSK signal set m are such that the set of prime factors of n is a subset of prime factors of m, then we can construct a rate-1, full-rank STBC over m-PSK signal set for n transmit antennas. To obtain a rate-1, full-rank STBC for arbitrary number of

transmit antennas, we used the transcendental extensions of the rational field $\mathbb{Q}$. It will be shown in Section 3.3, that it is very difficult to obtain the exact value of coding gain or a lower bound on it for STBCs obtained using the transcendental extensions. In this section, we will use algebraic extensions of $\mathbb{Q}$ and obtain rate-1, full-rank STBCs over apriori specified PSK signal set for arbitrary number of transmit antennas.

Suppose we need to construct codes over symmetric M-PSK for n antennas then choose m such that it contains all the primes of both M and n. Now $\mathbb{Q}(\omega_m)$ contains S_M, the M-PSK signal set, and the conditions of Proposition 2.2.3 are satisfied. Hence we obtain the code as

$$\mathcal{C} = \left\{ \begin{pmatrix} f_0 & \gamma f_{n-1} & \cdots & \gamma f_1 \\ f_1 & f_0 & \cdots & \gamma f_2 \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1} & f_{n-2} & \cdots & f_0 \end{pmatrix} \mid f_i \in S_M \subset \mathbb{Q}(\omega_m), i = 0, 1, \ldots, n-1 \right\} \tag{3.1}$$

where $\gamma = \omega_m^l$ with $(m, l) = 1$, which is a full-rank rate-one code over S_M. Clearly, the code is **not** completely over S_M when m contains a prime that is not in M, in which case the code is not rate-optimal.

It is important to notice that for S any finite subset of $\mathbb{Q}(\omega_m)$ the code given by (3.1) with S_M replaced by S is a full-rank, rate-one code over S. In particular, if m is a multiple of 4 then $\mathbb{Q}(\omega_m)$ contains the entire lattice $\mathbb{Q}(j)$ and by choosing S to be any lattice constellation we get full-rank rate-one code over that lattice constellation. The following examples illustrate these observations.

Example 3.1.1 *Let us construct a STBC for $n = 2$. Then, the allowed values of m are $x2^y$, where x and y are any positive integers. By the above corollary, $x^2 - \omega_m^l$ is irreducible over $\mathbb{Q}(\omega_m)$, where $(l, m) = 1$. Let the signal set be 4-PSK signal set. So, m should be such that $\mathbb{Q}(\omega_m)$ contains the 4-PSK signal set (for example, $m = 4$). Then, the STBC we obtain is,*

$$\mathcal{C} = \left\{ \begin{pmatrix} f_0 & \omega_m^l f_1 \\ f_1 & f_0 \end{pmatrix} \mid f_0, f_1 \in \{1, -1, j, -j\} \right\}.$$

The size of $\mathcal{C}$ is 16 and the rate of the code is 1. If we choose $m = 4$, then $l = 1$ or 3 and hence $\omega_m^l = j$ or $-j$. If we choose some other M-PSK signal set, the value of m should be chosen appropriately, i.e., m should be chosen such that the M-PSK signal set is a subset of $\mathbb{Q}(\omega_m)$. which implies, m should be a multiple of M.

From the above example, it is clear that the value of m, though independent to a large extent, should be a multiple of the size of the PSK signal set over which the STBC is being constructed. However, if the signal set chosen is a QAM signal set, then m should be $4x$, where x is any positive integer and depends only on n, as any QAM signal set is a finite subset of $\mathbb{Q}(\omega_{4x})$, for any x.

Example 3.1.2 *Suppose we need STBCs over the 6-PSK signal set $S_6 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5\}$, for five antennas (n=5). Then, we can choose $m = 30$, then we get the code given by (3.1) where $n = 5$, γ is a primitive 30-th root of unity and $f_i, i = 0, 1, 2, 3, 4 \in S_6$. Notice that this code is not rate-optimal since γ is not in S_6. Now, we wish to have code over a lattice constellation, say 16-QAM, then our choice of $m = 30$ is not sufficient since it is not a multiple of 4 and hence $\mathbb{Q}(\omega_m)$ does not contain the 16-QAM. The choice $m = 60$ will include the entire lattice in $\mathbb{Q}(\omega_m)$ (where now γ is a 60-th primitive root of unity) and hence this code is of full-rank rate-one STBC over any lattice constellations from which $f_i, i = 0, 1, 2, 3, 4$ come from.*

3.2 High-rate (> 1) codes from cyclotomic field extensions

Consider a rate-one code for n antennas over $\mathbb{Q}(\omega_m)$ and let $\mathbb{Q}(\omega_l) \subset \mathbb{Q}(\omega_m)$, where l divides m. Then, every element of $\mathbb{Q}(\omega_m)$ can be written as $\sum_{b \in B} l_b b$, where B is the basis of the field $\mathbb{Q}(\omega_m)$ seen as vector space over $\mathbb{Q}(\omega_l)$ and $l_b \in \mathbb{Q}(\omega_l)$. In (3.1), replacing f_i

with $\sum_{b\in B} f_{i,b}b$, we have a code $\mathcal{C}$

$$\mathcal{C} = \left\{ \begin{pmatrix} \sum_{b\in B} f_{0,b}b & \gamma\sum_{b\in B} f_{n-1,b}b & \cdots & \gamma\sum_{b\in B} f_{1,b}b \\ \sum_{b\in B} f_{1,b}b & \sum_{b\in B} f_{0,b}b & \cdots & \gamma\sum_{b\in B} f_{2,b}b \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{b\in B} f_{n-1,b}b & \sum_{b\in B} f_{n-2,b}b & \cdots & \sum_{b\in B} f_{0,b}b \end{pmatrix} \mid f_{i,b} \in \mathbb{Q}(\omega_l), i \in [0, n-1] \right\} \quad (3.2)$$

Clearly, $\mathcal{C}$ is a rate-$|B|$ code over any finite subset of $\mathbb{Q}(\omega_l)$. For example if $m = 8$ and $l = 4$, we get 2×2, rate 2, full-rank STBC's over any finite subset of $\mathbb{Q}(\omega_4)$, i.e., over lattice constellations. Thus, if we want a rate $R > 1$, (R-an integer) $n \times n$, full-rank STBC over the signal set S_M, then we do the following:

- Choose m such that it has all primes of R and M divides m. Then, using the irreducible polynomial $x^R - \omega_m$, extend the field $\mathbb{Q}(\omega_m)$ to the field $\mathbb{Q}(\omega_{mR})$.
- Construct the $n \times n$ full-rank STBC over $\mathbb{Q}(\omega_{mR})$ using the constructions given in the previous section, i.e., construct a $n \times n$ full-rank rate-one STBC over any finite subset of $\mathbb{Q}(\omega_{mR})$.
- Replace each entry of the codeword matrices with a linear combination of the basis of $\mathbb{Q}(\omega_{mR})$ over $\mathbb{Q}(\omega_m)$. Thus, we have a rate R, full-rank code over S_M given by

$$\mathcal{C} = \left\{ \begin{pmatrix} \sum_{i=0}^{R-1} f_{0,i}\omega_{mR}^i & \gamma\sum_{i=0}^{R-1} f_{n-1,i}\omega_{mR}^i & \cdots & \gamma\sum_{i=0}^{R-1} f_{1,i}\omega_{mR}^i \\ \sum_{i=0}^{R-1} f_{1,i}\omega_{mR}^i & \sum_{i=0}^{R-1} f_{0,i}\omega_{mR}^i & \cdots & \gamma\sum_{i=0}^{R-1} f_{2,i}\omega_{mR}^i \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{R-1} f_{n-1,i}\omega_{mR}^i & \sum_{i=0}^{R-1} f_{n-2,i}\omega_{mR}^i & \cdots & \sum_{b\in B} f_{0,i}\omega_{mR}^i \end{pmatrix} \mid f_{k,i} \in S_M \right\} \quad (3.3)$$

  where γ is an m_R-th primitive root of unity and m_R is a positive integer such that it has all the primes of n.

Clearly, with the above constructions, the rate is upper bounded by the degree of the polynomial $x^R - \omega_m$ and also the value of γ depends on the value of R. In the rest of this subsection, we give another method of constructing STBC's with arbitrary rate, where γ is independent of the rate R and hence, as will be seen in the sequel, we can have better coding gain.

Consider the rational function field $\mathbb{Q}(\omega_m, z)$ over $\mathbb{Q}(\omega_m)$ in the indeterminate z. The elements of $\mathbb{Q}(\omega_m, z)$ are of the form $a(z)/b(z)$, where $a(z)$ and $b(z) \neq 0$ are polynomials over $\mathbb{Q}(\omega_m)$. Then, from Theorem 2.2.4 we have that $x^n - z$ is irreducible over $\mathbb{Q}(\omega_m, z)$. Hence we have the STBC obtained by using the polynomial $x^n - z$,

$$\mathcal{C} = \left\{ \begin{pmatrix} f_0(z) & zf_{n-1}(z) & \cdots & zf_1(z) \\ f_1(z) & f_0(z) & \cdots & zf_2(z) \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1}(z) & f_{n-2}(z) & \cdots & f_0(z) \end{pmatrix} \mid f_i(z) \in \mathbb{Q}(\omega_m)[z], i = 0, 1, \ldots, n-1 \right\} \tag{3.4}$$

Note that, in the above STBC the entries in the matrices are polynomials instead of the rational functions of polynomials. Now each of $f_i(z) = \sum_{k=0}^{R-1} f_{i,k} z^k$, where $f_{i,k} \in \mathbb{Q}(\omega_m)$. Here, R can be any integer and hence the rate which is equal to R is arbitrary (this is because we can have polynomials with any degree as the extension of $\mathbb{Q}$ to $\mathbb{Q}(z)$ is infinite dimensional). z can be any transcendental number. If θ is an algebraic number, then from [69] (§4.12), $e^{j\theta}$ is a transcendental number. Thus, we can take $e^{j\theta}$ as z in the above construction. The following example shows that we can achieve better performance in terms of coding gain with codes with rate larger than one.

Example 3.2.1 *Consider a rate 2,* 2×2 *full-rank STBC* $\mathcal{C}$ *over 4-PSK signal set.*

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} f_{0,0} + f_{0,1} z & f_{1,0} z + f_{1,1} z^2 \\ f_{1,0} + f_{1,1} z & f_{0,0} + f_{0,1} z \end{pmatrix} \right\}$$

where $f_{i,k} \in 4 - PSK$ *for* $i, k = 0, 1$. *The size of the code is 256 and hence the bit rate is 4 bits per channel use. The scaling factor* $1/\sqrt{2}$ *is used to make the average power per antenna per channel use equal to one. Coding gain of this code is at least equal to 0.136* ($z \approx e^{j0.52}$, *coding gain might be more than this for some other z). Now consider a rate 1,* 2×2 *full-rank STBC* $\mathcal{C}'$ *over M-PSK signal set. Then, to obtain bit rate 4 bits per channel use, M should be equal to 16. Coding gain of this rate-one code is 0.052 approximately. Clearly, the coding gain of the rate 2 code is about 2.5 times the coding gain of rate-one*

code.

Consider the rate 2 STBC over 4-PSK for 2 antennas, obtained from algebraic extensions. We have $m = 4$ and $R = 2$. So, $\gamma = \omega_8$. By manually computing the coding gain, it is found that coding gain of this code is at most 0.13, which is lesser than the coding gain obtained from transcendental extensions.

3.3 Coding gain of STBCs from Field Extensions

In this section we discuss the coding gain of STBCs obtained from both the cyclotomic and non-cyclotomic field extensions.

Let $A(\mathbf{c}, \mathbf{e})$ be the difference of the two codeword matrices $\mathbf{c}$, $\mathbf{e}$ in an STBC $\mathcal{C}$ and let $B(\mathbf{c}, \mathbf{e}) = A(\mathbf{c}, \mathbf{e})^* A(\mathbf{c}, \mathbf{e})$. Let $a_k, k = 0, 1, \ldots, v-1$ denote the v non-zero eigen values of $B(\mathbf{c}, \mathbf{e})$, where v is the rank of $A(\mathbf{c}, \mathbf{e})$. In our case $B(\mathbf{c}, \mathbf{e})$ have full-rank, $v = n$. Then, the coding gain of a STBC $\mathcal{C}$ is given by the minimum of $\mid \prod_{k=0}^{n-1} a_k \mid^{1/n}$ for all possible pairs $\mathbf{c}$ and $\mathbf{e}$ of codeword matrices of the code. That is,

$$G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \mid det(B(\mathbf{c}, \mathbf{c}')) \mid^{1/n} \tag{3.5}$$

Theorem 3.3.1 *If $\mathcal{C} = \{f_0 I + f_1 M + f_2 M^2 + \cdots + f_{n-1} M^{n-1} | f_i \in S \subset F\}$, where M is an (2.1), then coding gain is*

$$G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \left| N_{K/F} \left(\sum_{i=0}^{n-1} (f_i - f_i') \alpha^i \right) \right|^{2/n}$$

where $N_{K/F}(x)$ denotes the norm of the element x from K to F, $\mathbf{c} = \sum_{i=0}^{n-1} f_i M^i$ and $\mathbf{c}' = \sum_{i=0}^{n-1} f_i' M^i$.

Proof: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be the minimal polynomial of α over F. Let L be a normal closure of K/F and σ_i, $i = 0, 1, \ldots, n-1$ be the distinct $F-$ homomorphisms from K to L. Let $p(x)$ be the minimal polynomial of $k = \sum_{i=0}^{n-1} (f_i - f_i') \alpha^i$ over F of degree $m \leq n$. Then, it is easy to see that m divides n and that every root of

$p(x)$ is of the form $\sigma_i(k)$ for some $0 \leq i < n$. Thus, the polynomial $g(x) = \prod_{i=0}^{n-1}(x-\sigma_i(a))$ and the polynomial $p(x)$ have same roots. Since, $g(x) \in F[x]$, the only irreducible factor of $g(x)$ is $p(x)$ and hence we have $g(x) = p(x)^{n/m}$. Now, since the minimal polynomial of k divides the characteristic polynomial $\chi(x)$ of $\lambda_k = (f_0 - f_0')I + (f_1 - f_1')M + (f_2 - f_2')M^2 + \cdots + (f_{n-1} - f_{n-1}')M^{n-1}$, and share the same irreducible factors over F, $\chi(x)$ must have $p(x)$ as the only irreducible factor. Thus, $\chi(x) = p(x)^{n/m} = g(x)$ (since degree of $\chi(x)$ is n). And since determinant of λ_k is the coefficient of the constant term in the characteristic polynomial, we get

$$\det \lambda_k = \prod_{i=0}^{n-1} \sigma_i(k) = N_{K/F}(k).$$

Thus, the coding gain is $G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \mid N_{K/F}(k) \mid^{2/n}$. ■

The above theorem gives coding gain expression for STBCs obtained using arbitrary field extensions. When, the field extension is a cyclotomic extension, we have the following corollary to the above theorem.

Corollary 3.3.1 *If the code $\mathcal{C}$ is as in the (3.1), then*

$$G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \left| \prod_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} (f_i - f_i')\gamma_j^i \right) \right|^{2/n}$$

where γ_i for $i = 0, 1, \ldots, n-1$ are the n^{th} roots of γ, $\mathbf{c} = c([f_0, f_1, \ldots, f_{n-1}], \gamma)$ (the codeword matrix with $(i,1)$-th component as f_{i-1}) and $\mathbf{c}' = c([f_0', f_1', \ldots, f_{n-1}'], \gamma)$ (the codeword matrix with $(i,1)$-th component as f_{i-1}').

Proof: The F-homomorphisms of K into the normal closure of K/F are given as $\sigma_i : \gamma_0 \mapsto \gamma_i$ for all $i = 0, 1, 2, \ldots, n-1$, where γ_i are the n-th roots of γ. Thus, from Theorem 3.3.1, we have $G = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \left| N_{K/F}(\sum_{i=0}^{n-1}(f_i - f_i')\gamma_0^i) \right|^{2/n} = \min_{\mathbf{c},\mathbf{c}' \in \mathcal{C}} \left| \prod_{j=0}^{n-1} \sum_{i=0}^{n-1} (f_i - f_i')\gamma_j^i \right|^{2/n}$. ■

From the above theorem, if $\mathbf{c}$ and $\mathbf{c}'$ have $f_k = f_k'$ for all k except for some $k' \in [0, n-1]$

then we have the coding gain as (assuming γ lies on unit circle)

$$G \leq \left|\prod_{i=0}^{n-1}(f_{k'} - f'_{k'})\gamma_i^{k'}\right|^{2/n} \leq |\, f_{k'} - f'_{k'}\,|^2 .$$

Thus, the main factor which dominates the coding gain is the selection of S. From the above theorem the coding gain for the STBC in Example 2.2.1 is

$$G = \min_{\mathbf{c},\mathbf{c}'\in\mathcal{C}} \left|\prod_{i=0}^{n-1}\left(\sum_{k=0}^{n-1}(f_k - f'_k)\gamma_i^k\right)\right|^{2/n} = 2.$$

Now, let us see the how the coding gain depends on γ. Let m_{opt} be the smallest m such that the prime factors of n are a subset of the prime factors of m and the signal set, S_M is subset of $\mathbb{Q}(\omega_{m_{opt}})$. Therefore, $m_{opt} = xM$ for some integer x. Now let $m' \neq m_{opt}$ be another integer such that the prime factors of n are subset of the prime factors of m' and the signal set is subset of $\mathbb{Q}(\omega_{m'})$. Clearly, $m_{opt} < m'$. The codeword matrices have the entries of the form f_i and γf_i, where $f_i \in S$. If x is not equal to one, then it is easy to see that the minimum distance (which happens to be the distance between any $f_i \in S$ and γf_i) of the resulting signal set decreases if we add the points γS to the signal set. Now, if we let γ to be $\omega_{m_{opt}}$, then we claim that the decrease in the minimum distance is minimum possible. This can be seen in the following way : as m increases from m_{opt}, the point $\omega_m f_i$ gets closer to the point f_i and hence the minimum distance decreases more as m increases. Though, the minimum distance is not the coding gain of the STBC, it is intuitive enough to choose γ which keeps the minimum distance of the $S \cup \gamma S$ as maximum as possible. For instance, in Example 2.2.1 we have $m_{opt} = 4$ and the corresponding coding gain is 2. However, if we let $m = 8$ (or 12), the coding gain falls down to 1.53 (or 1.0). The same holds true for QAM constellations too.

In codes with rate larger than one obtained from transcendental extensions, the degree n of the irreducible polynomial $x^n - z$ is independent of the signal set we choose and hence m should be chosen such that the signal set is invariant under the multiplication of ω_m so that the minimum distance of the signal set remains same. However, the entries of

the codeword matrices are polynomials in z (any transcendental number), and hence, the coding gain depends on z also. It is very difficult to see how the coding gain and z are related. In example 3.2.1, the coding gains as a function of z are as follows: $G(e^{j0.1}) = 0.001$, $G(e^{j0.3}) = 0.027$, $G(e^{j0.5}) = 0.121$, $G(e^{j0.52}) = 0.136$, $G(e^{j0.7}) = 0.019$, $G(e^{j0.9}) = 0.116$, $G(e^{j1.1}) = 0.093$, $G(e^{j1.3}) = 0.073$, $G(e^{j1.5}) = 0.005$, $G(e^{j1.7}) = 0.017$, $G(e^{j1.9}) = 0.107$, $G(e^{j2.1}) = 0.01$, $G(e^{j2.3}) = 0.014$, $G(e^{j2.7}) = 0.084$, $G(e^{j2.9}) = 0.015$ and $G(e^{j3.1}) = 0.0001$.

In general, it is very difficult to obtain the exact value of coding gain for any STBC. In such cases, a good lower bound on the coding gain will be helpful. In the following subsection, we will obtain lower bounds on the coding gains of some of the STBCs in our constructions.

3.3.1 Lower bounds on the coding gain

In this subsection, we obtain lower bounds on the coding for some special cases. We then show that under certain special cases, the lower bound matches with the maximum coding gain and hence the specific STBCs constructed are optimal in the sense of the coding gain.

Let n be the number of transmit antennas and S be the signal set over which we want to construct the STBCs. Then, let m be such that there exists a monic irreducible polynomial $f(x)$ of degree n over the field $F = \mathbb{Q}(S, \omega_m)$, with coefficients from $\mathbb{Z}[\omega_m]$. Let α be a root of the polynomial $f(x)$ and $K = F(\alpha)$ be a Galois extension of F. Then, clearly, the algebraic norm of any element

$$k = f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_{n-1}\alpha^{n-1}$$

where $f_i \in \mathbb{Z}[\omega_m]$, is

$$N_{K/F}(k) = \prod_{i=0}^{n-1} \left(f_0 + f_1\sigma_i(\alpha) + \cdots + f_{n-1}\sigma_i(\alpha^{n-1})\right)$$

where σ_i, $i = 0, 1, 2, \ldots, n-1$ are n distinct automorphisms of K fixing F. We then have the following lemma:

Lemma 3.3.1 *With the assumptions on F, K, k and $f(x)$, the algebraic norm $N_{K/F}$ of k belongs to the set $\mathbb{Z}[\omega_m]$.*

Suppose that the the signal set S is such that it is carved out from the set $\mathbb{Z}[\omega_m]$. Then, the coding gain of the STBC obtained using the minimal polynomial $f(x)$ and the signal set S is

$$G = \min_{k \neq k'} \left| N_{K/F}(k - k') \right|^{2/n}$$

where $k - k' = \sum_{i=0}^{n-1} (f_i - f_i') \, \omega_m$ takes values from the set $\mathbb{Z}[\omega_m]$. Thus, $G \in \mathbb{Z}[\omega_m]$. But the set $\mathbb{Z}[\omega_m]$ forms a lattice and hence a minimum Euclidean distance. Thus,

$$G \geq d^2_{\min} \text{ of the lattice } \mathbb{Z}[\omega_m].$$

Thus, we have proved the following proposition.

Proposition 3.3.1 *Let $\mathcal{C}$ be an STBC over a signal set S carved from $\mathbb{Z}[\omega_m]$, obtained using the polynomial $f(x) \in \mathbb{Z}[\omega_m][x]$. Then, the coding gain of the code $\mathcal{C}$ is lower bounded by the minimum squared Euclidean distance $d^2_{\min}$ of the lattice $\mathbb{Z}[\omega_m]$. In particular, if the signal set S has two neighboring points of $\mathbb{Z}[\omega_m]$ with distance between them equal to $d_{\min}$, then the coding gain is equal to $d^2_{\min}$.*

From the later half of the above proposition, it is clear that under the given conditions the STBCs from field extensions achieve the maximum coding gain and hence are optimal in the sense of coding gain.

Corollary 3.3.2 *Let S be a QAM constellation and $\mathcal{C}$ be an STBC over S, obtained using an irreducible polynomial over $\mathbb{Z}[j]$. Then, coding gain of the code $\mathcal{C}$ is equal to the minimum squared Euclidean distance of the QAM constellation S.*

Proof: Let f and f' be two points from the QAM constellation. Then, $f - f'$ belongs to the sublattice $2\mathbb{Z}[j]$ of the lattice $\mathbb{Z}[j]$. Thus, the norm of the element $k - k'$, where

$k = \sum_{i=0}^{n-1} f_i \alpha^i$ and $k' = \sum_{i=0}^{n-1} f'_i \alpha^i$, belongs to the sublattice $2\mathbb{Z}[j]$. Thus, the coding gain is lower bounded by the minimum squared Euclidean distance of the sublattice which is equal to 4. ■

3.4 Capacity of STBC's from cyclotomic extensions

In this section we study the maximum mutual information achieved by the STBCs obtained from cyclotomic field extensions. The analysis can be extended to the STBCs obtained from non-cyclotomic field extensions.

Let $\mathbf{x}$ be the transmitted vector using n_t transmit antennas and $\mathbf{y}$ be the received vector using n_r receive antennas. Then, we have

$$\mathbf{y} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\mathbf{H}\mathbf{x} + \mathbf{w} \tag{3.6}$$

where $\mathbf{y} \in \mathbb{C}^{n_r \times 1}$, $\mathbf{x} \in \mathbb{C}^{n_t \times 1}$, $\mathbf{H} \in \mathbb{C}^{n_r \times n_t}$ is the channel matrix, $\mathbf{w} \in \mathbb{C}^{n_r \times 1}$ is the additive white Gaussian noise. The entries in the channel matrix and the transmitted vector are assumed to have unit variance, i.e.,

$$\mathrm{E}tr(\mathbf{H}\mathbf{H}^H) = n_t n_r \text{ and } \mathcal{E}\{\mathbf{f}^*\mathbf{f}\} = n_t$$

When the channel is known at the receiver, the resulting channel capacity is [1]

$$C(n_t, n_r, \mathsf{SNR}) = \mathcal{E}\left\{\log\det\left(I_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^H\right)\right\} \tag{3.7}$$

If $\mathbf{X}$ is the transmitted codeword matrix, then

$$\mathbf{Y} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\mathbf{H}\mathbf{X} + \mathbf{W}$$

The transmitted signal matrix in our STBC constructions is as in (3.1). And if $\mathbf{H} =$

$(h_{i,j})_{i\in[0,n_r-1],j\in[0,n_t-1]}$, we have

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\hat{\mathbf{H}}[f_0\ f_1\ \cdots\ f_{n-1}]^T + \widehat{\mathbf{w}}$$

where $\widehat{\mathbf{y}} = vec(\mathbf{Y})$, $\widehat{\mathbf{w}} = vec(\mathbf{W})$ and

$$\hat{H} = \begin{pmatrix} c_0 = c([h_{0,0}, h_{0,1}, \ldots, h_{0,n_t-1}], \gamma) \\ c_1 = c([h_{1,0}, h_{1,1}, \ldots, h_{0,n_t-1}], \gamma) \\ \vdots \\ c_{r-1} = c([h_{n_r-1,0}, h_{n_r-1,1}, \ldots, h_{n_r-1,n_t-1}], \gamma) \end{pmatrix}$$

In the above equation, recall that c_j are $n \times n$ matrices as in (3.1), with $f_i = h_{i,j}$. It can be checked easily that eigen values $a_{i,k}$ of c_i are given by

$$a_{i,k} = \sum_{l=0}^{n-1} h_{l,i}\gamma_k^l, \text{ for } k = 0, 1, 2, \ldots, n-1$$

Then, the c_i can be written as $P_i\Lambda_i P_i^{-1}$, where P_i is the eigenvector matrix and Λ_i is the eigenvalue matrix. It can be easily seen that,

$$P_i = diag(1, \gamma_0, \gamma_0^2, \ldots, \gamma_0^{n-1})DFT_n \tag{3.8}$$

Now, the capacity, denoted by $C_\gamma(n_t, n_r, \mathsf{SNR})$, of these codes is given by replacing $\mathbf{H}$ with $\hat{H}$ and $R_f = I_{nr}$ in (3.7), which is

$$C_\gamma(n_t, n_r, \mathsf{SNR}) = \frac{1}{n_t}\mathrm{E}\log\det\left(I_{n_r n_t} + \frac{\mathsf{SNR}}{n_t}\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H\right) \tag{3.9}$$

where the normalizing factor $1/n_t$ in front of the expectation is for the n_t channels uses we have in our STBC. The term $\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H$ in the capacity expression is equal to $(c_i^* c_j)_{i,j\in[0,r-1]}$. Computing the determinant of $I_{n_t n_r} + \sqrt{\frac{\mathsf{SNR}}{n_t}}\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H$ is very difficult for any n_r number of receive antennas. So, let us see the case when we have only one receive antenna. Then, removing the subscript corresponding to the receive antennas in $\widehat{\mathbf{H}}$, we have $\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H =$

$P\Lambda P^{-1}P^{-1^H}\Lambda^H P^H$. From (3.8), we have $\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H = (1/n_t)P|\Lambda|^2P^H$. Thus,

$$\begin{aligned}\det\left(I_{n_t}+\sqrt{\frac{\mathsf{SNR}}{n_t}}\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H\right) &= \det\left(P^{-1}\left(I_{n_t}+\sqrt{\frac{\mathsf{SNR}}{n_t}}\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H\right)P\right)\\ &= \det\left(I_{n_t}+\sqrt{\frac{\mathsf{SNR}}{n_t}}|\Lambda|^2\right)\end{aligned}$$

Thus, the capacity is

$$\begin{aligned}C_\gamma(n_t,n_r=1,\mathsf{SNR}) &= \mathcal{E}\left\{\log\left(\prod_{k=0}^{n_t-1}\left(1+\left|\sum_{i=0}^{n_t-1}h_i\gamma_k^i\right|^2\right)\right)^{1/n_t}\right\}\\ &\leq \mathcal{E}\left\{\log\left(\prod_{k=0}^{n_t-1}\left(1+\sum_{i=0}^{n_T-1}|h_i|^2\right)\right)^{1/n_t}\right\}\\ &= C(n_t,n_r=1,\mathsf{SNR})\end{aligned}$$

Thus, the STBCs from field extensions do not maximize the mutual information. Now, let us see what the capacity is for rate more than one codes. In this case the transmitted signal matrix $\mathbf{X}$ is given as in either (3.3) or (3.4). Thus, assuming the signal points the constellation to be independent and to ensure unit power transmitted per antenna per channel use, we have $R_f = \frac{1}{R}I_{n_tR}$. Let $\hat{f} = [f_0(z)f_1(z)\ldots f_{n_t-1}(z)]^T$. Then, $R_{\hat{f}} = I_{n_t}$. Since, the covariance matrix is same in both the cases (rate-one and rate more than one), the capacity remains unchanged. Indeed, the capacity remains unchanged, as we have computed it for the input distribution to have $R_f = I_{n_t}$, and in both the cases the codeword matrices remain same in the sense of their structure.

We have plotted the capacity for the 2×2 code from cyclotomic extensions and the capacity for Alamouti's code as a function of SNR in Figure 3.1. From this plot it can be seen that the Alamouti code has more capacity (by about 1/2 a bit at 30dB SNR with one receive antenna). However, as number of receive antennas increase, one sees that the difference is coming down from the Figure 3.2. So, it seems asymptotically (as number of receive antennas tend to infinity), the capacities match in both the cases. Indeed, from the expression (. (3.9)) of capacity in our case, we can see that the cross product terms like

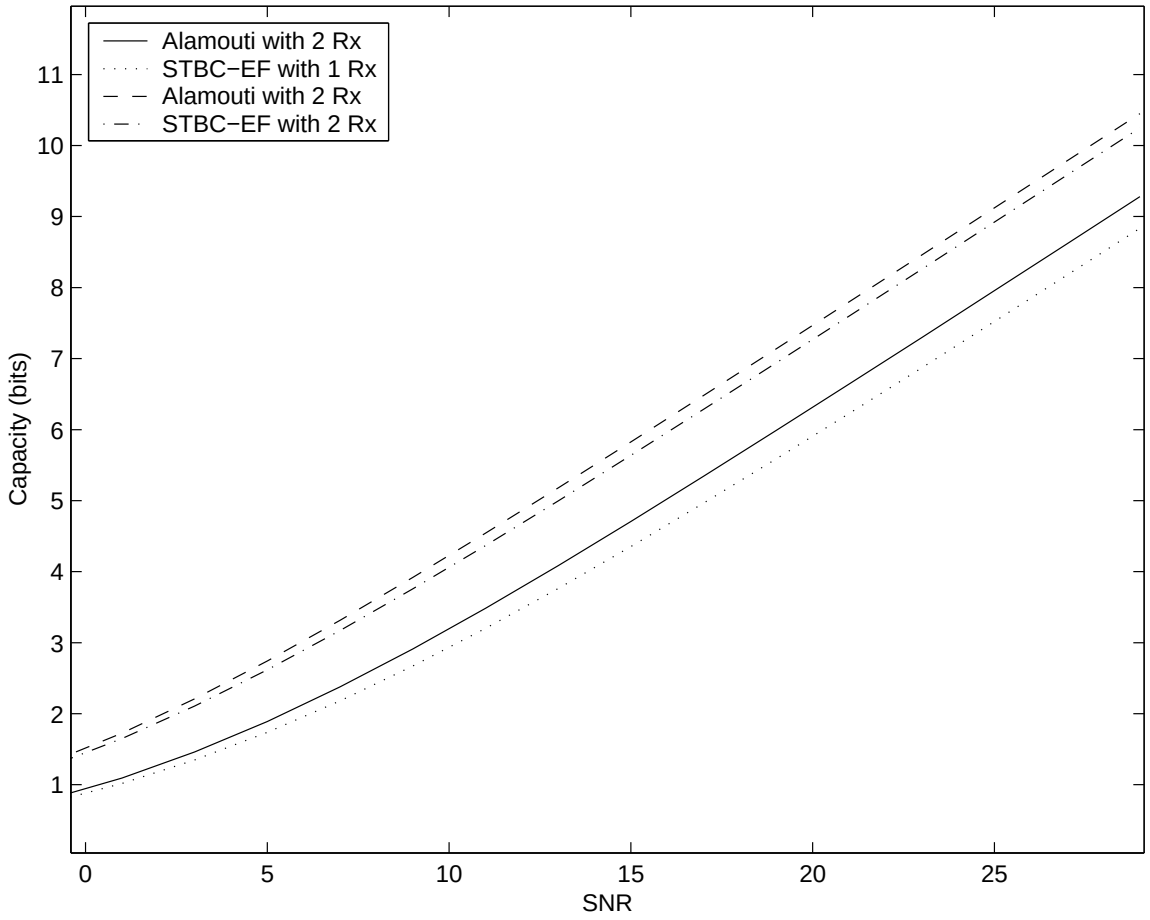


Figure 3.1: Comparison of mutual informations of STBCs from field extensions and the capacity of the channel.

$h_{i,j}h_{k\neq i,l\neq j}$ of $\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H$ vanish and the term $\sum_{i=0}^{1}\sum_{j=0}^{r-1}|h_{i,j}|^2$ remains. So the determinant of $I_{n_t n_r} + \frac{\mathsf{SNR}}{2}\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H$ turns out to be $(1 + \frac{\mathsf{SNR}}{2}\sum_{i=0}^{1}\sum_{j=0}^{n_r-1}|h_{i,j}|^2)^2$ as n_r tends to infinity. Thus, the capacity is $\mathcal{E}\left\{\log\left(1 + \frac{\rho}{2}\sum_{i=0}^{1}\sum_{j=0}^{r-1}|h_{i,j}|^2\right)\right\}$ as r tends to infinity, which is the same as the capacity achieved by Alamouti's code [23].

3.5 Finite-Signal-Set Capacities of STBCs from Field Extensions

In the previous section, we have shown that the capacity of the STBCs from field extensions remains same for any rate R. This is because, when we compute the capacity of the

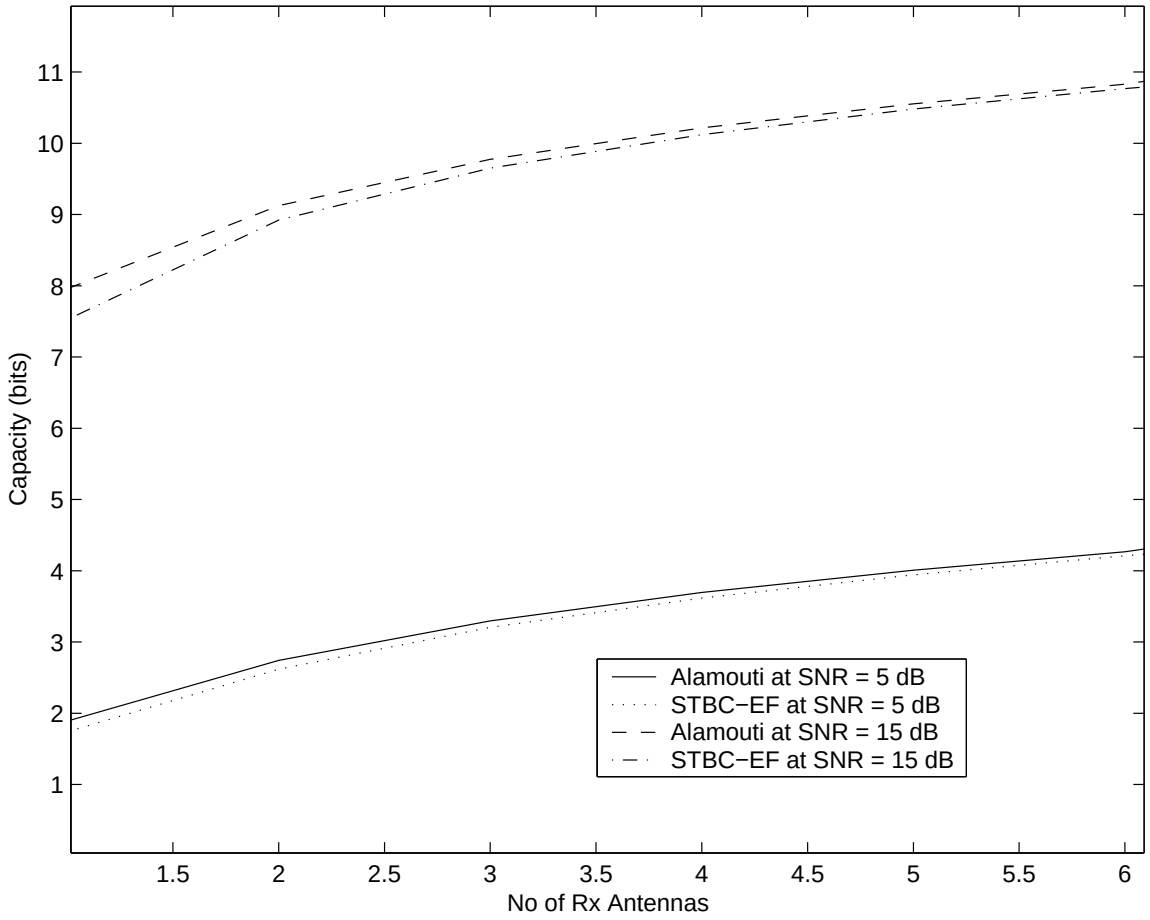


Figure 3.2: Comparison of mutual informations achieved by Alamouti code and STBCs from field extensions

channel for these STBCs we do not assume any **finite signal set,** but assume the signal space to be the entire complex space. However, if we restrict the signal space to be a finite subset of the complex space, we get different capacities. For instance, the capacities of 8 QAM and 8 PSK signal sets for a AWGN channel are different at low SNRs (approach the same value asymptotically) [45]. Similarly, in this section we obtain the capacities of some of our high-rate codes and show that they achieve the asymptotic value at an SNR lower than the rate-1 codes achieve, the asymptotic values being the same. Also, we compare the capacity of these high-rate codes with the capacity of V-BLAST for 2 transmit and 2 receive antennas.

From [46], the capacity of a continuous output discrete memoryless channel is

$$C = \max_{q(0),q(1),\cdots,q(N-1)} \sum_{k=0}^{N-1} q(k) \int_{-\infty}^{\infty} p(x/a_k) \log_2 \left\{ \frac{p(x/a_k)}{\sum_{i=0}^{N-1} q(i)p(x/a_i)} \right\} dz \tag{3.10}$$

where $a_0, a_1, \ldots, a_{N-1}$ are the discrete channel inputs, $q(k)$ denotes the *a priori* probability associated with a_k and x denotes the received symbol when a_k is transmitted, i.e., $x = a_k + w$, where w is Gaussian noise with zero mean and variance σ^2. And $p(./.)$ denotes the *a posteriori* distribution at the receiver. In our case, if the transmitted vector is $\mathbf{s}_i$ at i^{th} channel use and the channel matrix is H, we have for the i^{th} channel use,

$$\mathbf{x}_i = \sqrt{\frac{\rho}{n}} H\mathbf{s}_i + \mathbf{w}_i \tag{3.11}$$

where $\mathbf{x}_i$ is received vector, ρ is the SNR at each receive antenna and $\mathbf{w}_i$ is the noise vector whose components are independent zero mean complex Gaussian and of variance σ^2. If the number of transmit and receive antennas are n and t respectively, H is a $t \times n$ matrix with entries which are zero mean complex Gaussian and unit variance. It can be viewed as a AWGN channel with input $H\mathbf{s}$. Thus, our set $\{a_0, a_1, \ldots, a_{N-1}\}$ of discrete inputs in (3.10) will be

$$\{\mathbf{a}_k | k = 0, 1, \ldots, N-1\} = \left\{ \sqrt{\frac{\rho}{n}} H\mathbf{s} | \mathbf{s} \in S^n \right\} \tag{3.12}$$

where S denotes the input signal set. Notice that the $\mathbf{a}_k$'s are column vectors now and the value of N depends on the channel matrix. Assuming uniform distribution on the signal set S, the distributions q_k's of $\mathbf{a}_k$'s can be computed easily, since the signal set is a finite set. By substituting expectation for the integral term and $\mathbf{x} = \mathbf{a_k} + \mathbf{w}$ in (3.10), we have the following expression for the capacity for a given channel matrix H :

$$C(H) = \sum_{k=0}^{N-1} q(k) \mathrm{E} \left\{ \log_2 \left\{ \frac{p(\mathbf{w})}{\sum_{i=0}^{N-1} q(i)p(\mathbf{a_k} + \mathbf{w}/\mathbf{a_i})} \right\} \right\}. \tag{3.13}$$

Notice that the maximization with respect to $q(k)$ is removed, since we assume the signal

set to have uniform distribution. Substituting the Gaussian distributions for p's in the above equation, we have

$$C(H) = \sum_{k=0}^{N-1} q(k) \mathrm{E} \left\{ \log_2 \left\{ \frac{\sqrt{|\det L|} e^{-\frac{\mathbf{w}^* \mathbf{w}}{2\sigma^2}}}{\sigma \sum_{i=0}^{N-1} q(i) e^{-(\mathbf{a_k}+\mathbf{w}-\mathbf{a_i})^* L^{-1} (\mathbf{a_k}+\mathbf{w}-\mathbf{a_i})}} \right\} \right\} \tag{3.14}$$

where L is the covariance matrix of the vector $\mathbf{a_k} + \mathbf{w} - \mathbf{a_i}$. So, the capacity of the channel when the input is discrete is obtained by taking expectation of $C(H)$ over H. The expectations are evaluated by Monte Carlo averaging.

For our STBCs, if $\mathbf{F} = c([f_0, f_1, \ldots, f_{n-1}], \gamma)$ is the transmitted codeword matrix, then we have

$$\mathbf{X} = \sqrt{\frac{\rho}{n}} \mathbf{F} H + \mathbf{W} \tag{3.15}$$

where H is now a transpose of our channel matrix and similarly, $\mathbf{X}$ and $\mathbf{W}$ are $[\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_{n-1}}]^T$ and $[\mathbf{w_1}, \mathbf{w_2}, \ldots, \mathbf{w_{n-1}}]^T$ respectively. If $H = (h_{i,j})$, we have

$$\hat{\mathbf{X}} = \sqrt{\frac{\rho}{n}} \hat{H} [f_0 \ f_1 \ \cdots \ f_{n-1}]^T + \hat{\mathbf{V}} \tag{3.16}$$

where $\hat{\mathbf{X}} = vec(\mathbf{X})$, $\hat{\mathbf{V}} = vec(\mathbf{V})$ and

$$\hat{H} = \begin{pmatrix} c_0 = c([h_{0,0}, h_{1,0}, \ldots, h_{n-1,0}], \gamma) \\ c_1 = c([h_{0,1}, h_{1,1}, \ldots, h_{n-1,1}], \gamma) \\ \vdots \\ c_{r-1} = c([h_{0,r-1}, h_{1,r-1}, \ldots, h_{n-1,r-1}], \gamma) \end{pmatrix}.$$

So, to compute the capacity for our STBCs, we replace H in (3.11) by $\hat{H}$ and use the same formulation from there onwards. Hence, we have

$$C = \mathrm{E}C(H) = \frac{1}{n} \mathrm{E} \sum_{k=0}^{N-1} q(k) \mathrm{E} \left\{ \log_2 \left\{ \frac{\sqrt{|\det L|} e^{-\frac{\mathbf{w}^* \mathbf{w}}{2\sigma^2}}}{\sigma \sum_{i=0}^{N-1} q(i) e^{-(\mathbf{a_k}+\mathbf{w}-\mathbf{a_i})^* L^{-1} (\mathbf{a_k}+\mathbf{w}-\mathbf{a_i})}} \right\} \right\}. \tag{3.17}$$

The term $1/n$ on the RHS is because we send the same information for every n channel uses.

Figure 3.3 shows the capacity of 16 QAM signal set when we use a rate-1 STBC given in Example 3.1.1 and the capacity of 4 QAM signal set when we use a rate-2 STBC given in Example 3.2.1 for one receive antenna. Though the asymptotic values are same in both the cases, the rate-2 STBC achieves the asymptotic value at a lower SNR than the rate-1 code achieves. This motivates us to use high-rate codes instead of rate-1 codes.

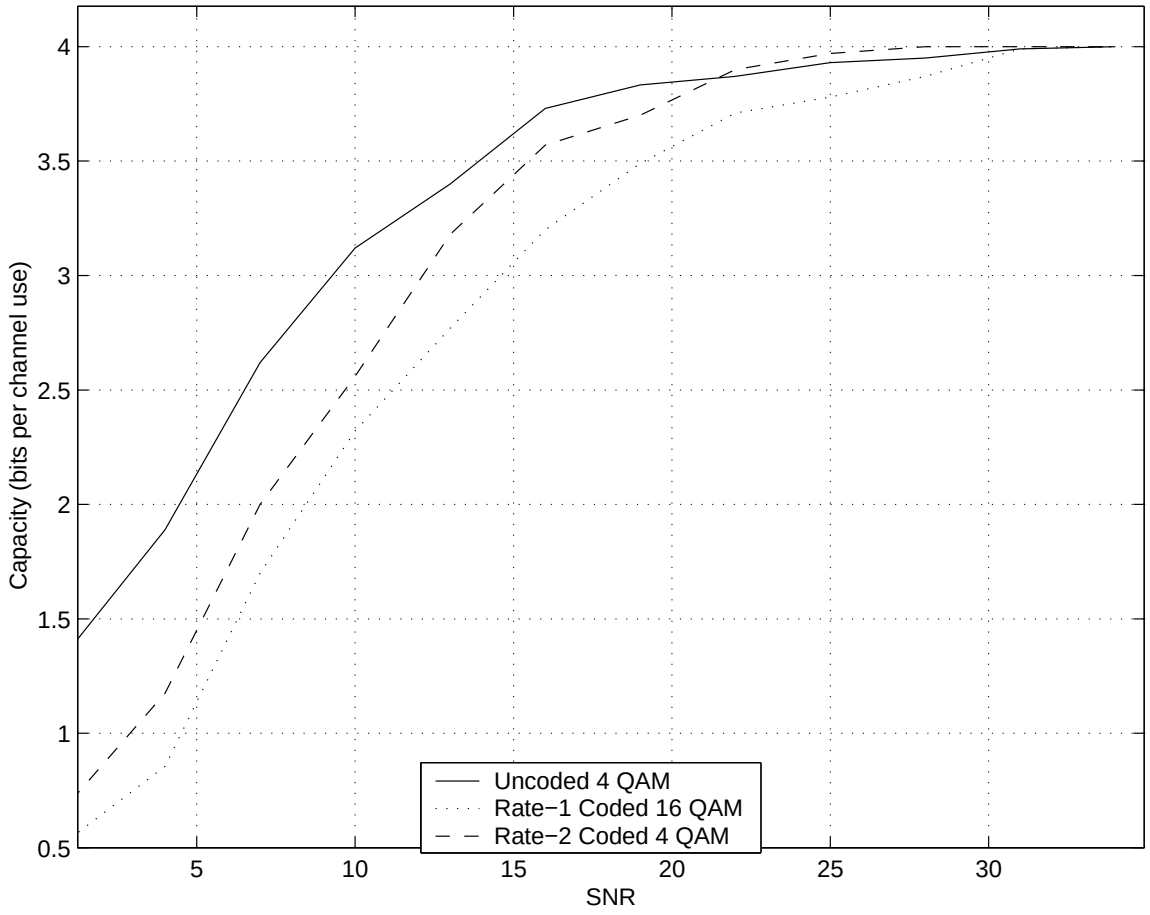


Figure 3.3: Capacity of 2 Tx and 1 Rx system

Figure 3.4 shows the capacity of 4 QAM signal set when we use a 2×2 V-BLAST system and the capacity of rate-2 code of Example 3.2.1 with 4 QAM signal set. Though the capacity of the rate-2 STBC is lower than the rate-2 V-BLAST at low SNRs, our STBC approaches asymptotic value at a lower SNR than V-BLAST achieves. Also, the capacity of rate-2 STBC is more than the capacity of rate-1 STBC. In Section 3.6 we show that by going to rate-2 STBC, we get an improvement of 3.5 dB SNR per bit at

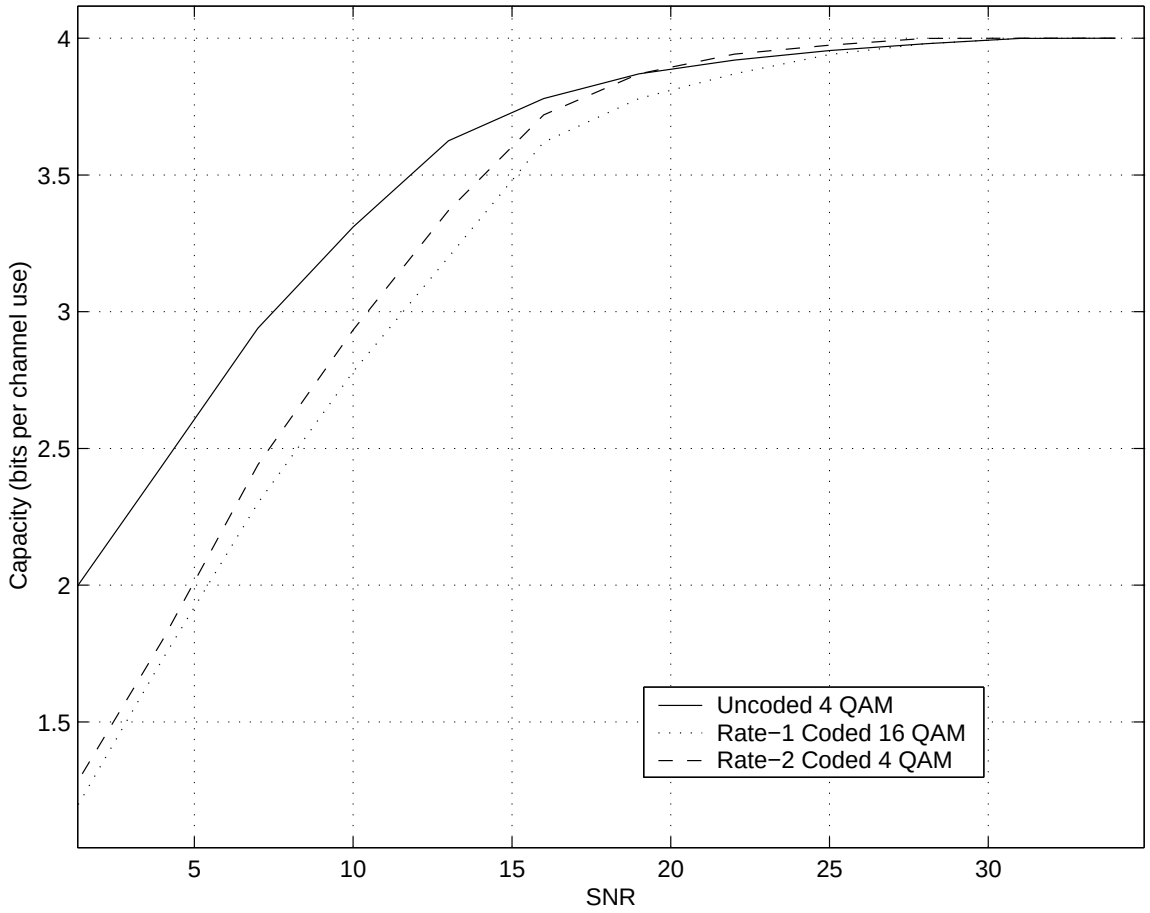


Figure 3.4: Capacity of 2 Tx and 2 Rx system

10^{-5} BER.

3.6 Decoding and Simulation Results

Maximum Likelihood (ML) decoding of STBCs using exhaustive search is prohibitively complex as the decoding complexity increases exponentially with number of transmit antennas. Recently, Viterbo and Boutrous in [63] proposed sphere decoding which uses the algorithm to find the closest lattice point to a given point [62]. The algorithm uses the fact that the generator matrix of the lattice is of full column rank and searches the lattice points enclosed in a sphere of radius C_0 centered at the received point. At each time, a lattice point of Euclidean norm less than C_0 is found, and the radius of the sphere

is reduced to the norm of the newly found lattice point. We repeat this until we are left with a sphere with no lattice points in it. The lattice point whose norm was the radius of the last sphere, is the decoded lattice point, i.e., it is the closest lattice point to the received point. If the sphere we started with did not have any lattice points then we increase the radius and repeat the process. Damen *et al.* in [64], have shown that sphere decoding can be applied for multiple antenna systems if the perfect CSI is known at the receiver. It has been shown in [65] that sphere decoding achieves ML performance in a significantly reduced complexity which is roughly cubic in n at high SNRs. Though PSK constellations are not a subset of any lattice, we can still use the sphere decoder, known as complex sphere decoder, as shown by Hochwald and Brink in [61].

In the case of our STBCs, (3.16) can be written as

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n}}\widehat{\mathbf{H}}[f_0(z), f_1(z), \ldots, f_{n-1}(z)]^T + \widehat{\mathbf{w}} \tag{3.18}$$

where $f_0(z), f_1(z), \cdots, f_{n-1}(z)$ are $(R-1)^{th}$ degree polynomials in the indeterminate z. The above equation can be written as

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n}}\tilde{\mathbf{H}}\tilde{\mathbf{f}} + \widehat{\mathbf{w}} \tag{3.19}$$

where $\tilde{\mathbf{H}} = [\widehat{\mathbf{H}}\ z\widehat{\mathbf{H}} \cdots z^{R-1}\widehat{\mathbf{H}}]$ and $\tilde{\mathbf{f}} = [f_{0,0}, f_{1,0}, \ldots, f_{n-1,0}, f_{0,1}, \ldots, f_{0,R-1}, \ldots, f_{n-1,R-1}]^T$ where $f_{i,j}$ is j^{th} coefficient in $f_i(z)$. Now, when the rate R is equal to one, the equivalent channel matrix, $\tilde{\mathbf{H}}$, is of full column rank and hence we can use sphere decoding. However, if the rate R is greater than one, then the equivalent channel matrix is not of full column rank, and hence we cannot use sphere decoding. Instead, we can use the generalization of sphere decoding [18],where one works with a *projection* of this lattice onto $\mathbb{R}^{2n}$. Here, we take the worst case bounds for $2nR - 2n$ unknowns ($2n$ is the rank of equivalent channel matrix and we have $2nR$ unknowns) and use sphere decoding for the remaining $2n$ unknowns. The decoding complexity increases, but is still lower than the complexity of exhaustive-search ML detection. The complexity can be reduced by intelligently choosing values of these $2nR - 2n$ variables to get bounds on the remaining $2n$ variables. For

this, we adopt the method of Schnorr-Euchner lattice point search strategy [67]. In this strategy, the lattice point component nearest to the corresponding component in the received point is chosen to obtain further bounds. A similar strategy is adopted in [68].

An alternative way of decoding is as follows : clearly, the set

$$\Lambda' = (\sum_{j=0}^{R-1} z^j)\Lambda = \left\{ f_i(z) = \sum_{j=0}^{R-1} f_{i,j} z^j | f_{i,j} \in \Lambda \right\}$$

forms a lattice, where Λ is the lattice from which the constellation is chosen. For example, Figure 3.5 shows the constellation $S + e^{2.5j}S$ where S is a 4-QAM signal set. Here Λ'

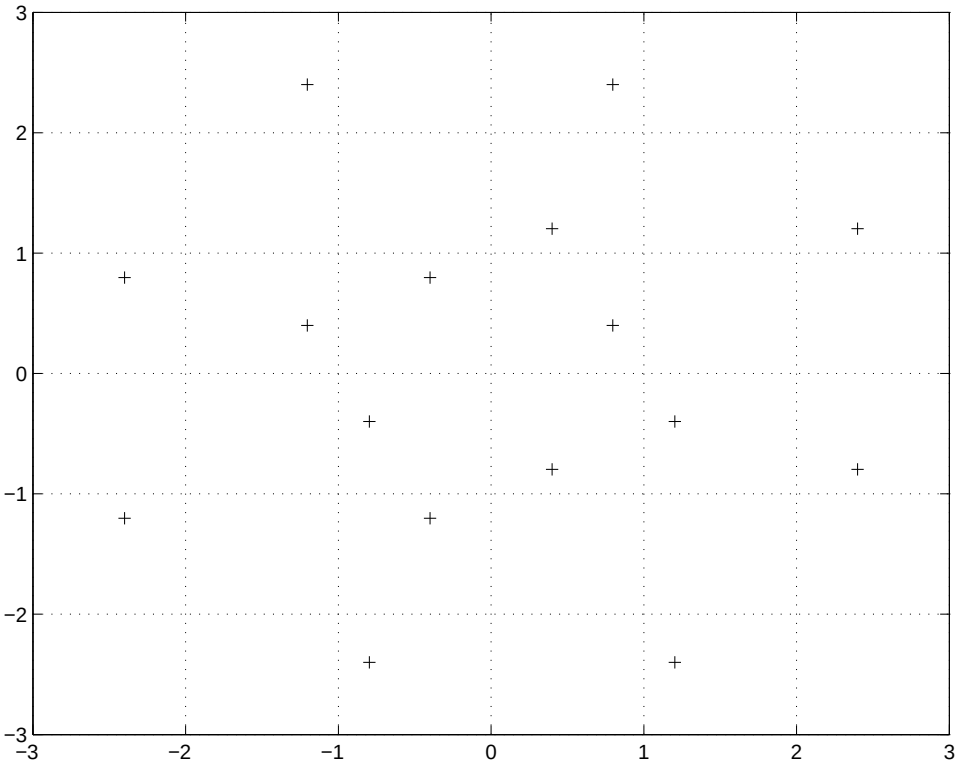


Figure 3.5: Constellation $S + e^{2.5j}S$, for $S =$ 4-QAM.

is the lattice containing the resultant signal set $S + e^{2.5j}S$. So, using SD with $\hat{H}$ as the equivalent channel matrix, we decode the received symbol to a nearest lattice point in the lattice Λ'. Then, we can decode to the individual symbols, $f_{i,j}$, using a look-up table. Since, every $R-$tuple of $f_{i,j}$'s uniquely determine a polynomial $f_i(z)$, it is still ML. The decoding complexity now depends on the lattice Λ' and hence z.

We now present the simulation results for space-time block codes constructed using field extensions. We have employed the sphere decoding algorithm [64] for our simulations. We use the rate-1 STBC $\begin{bmatrix} f_0 & jf_1 \\ f_1 & f_0 \end{bmatrix}$, with f_0, f_1 coming from 16-QAM signal set for 4 bits per channel use and from 256-QAM for 8 bits per channel use. And for rate-2 STBCs we used the one constructed in Example 3.2.1 with $f_{i,j}$ coming from 4-QAM for 4 bits per channel use and from 16-QAM for 8 bits per channel use. Figure 3.6 shows plots for 2 transmit and 2 receive antenna system with 4 bits per channel use. From the plot, it can be seen that the though the LD code performs at better than rate-1 code, the rate-2 code performs better than LD code at high SNRs. This is because, the LD codes are constructed to maximize the mutual information and not the diversity. And from

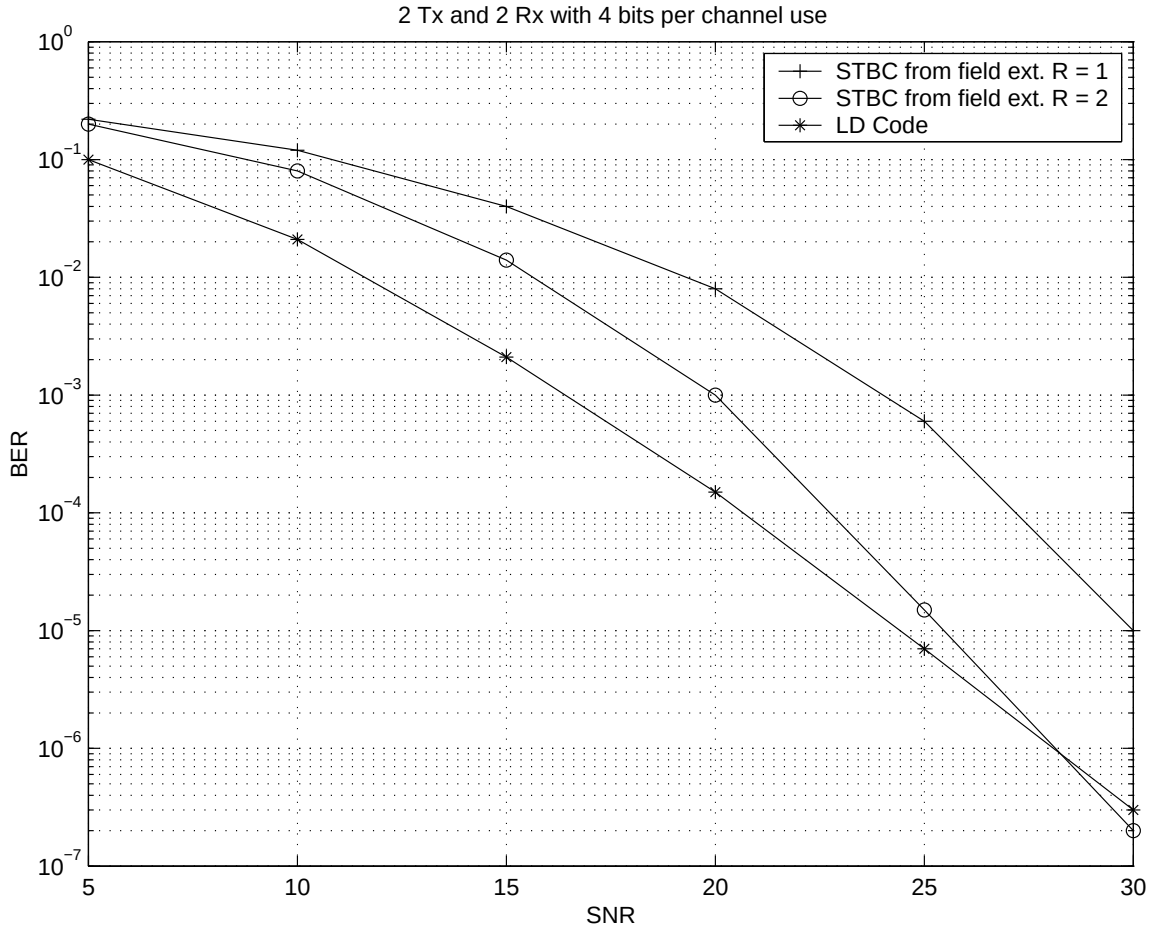


Figure 3.6: Comparison of STBCs from field extensions with LD codes for 2-Tx and 2-Rx with 4 bits per channel use.

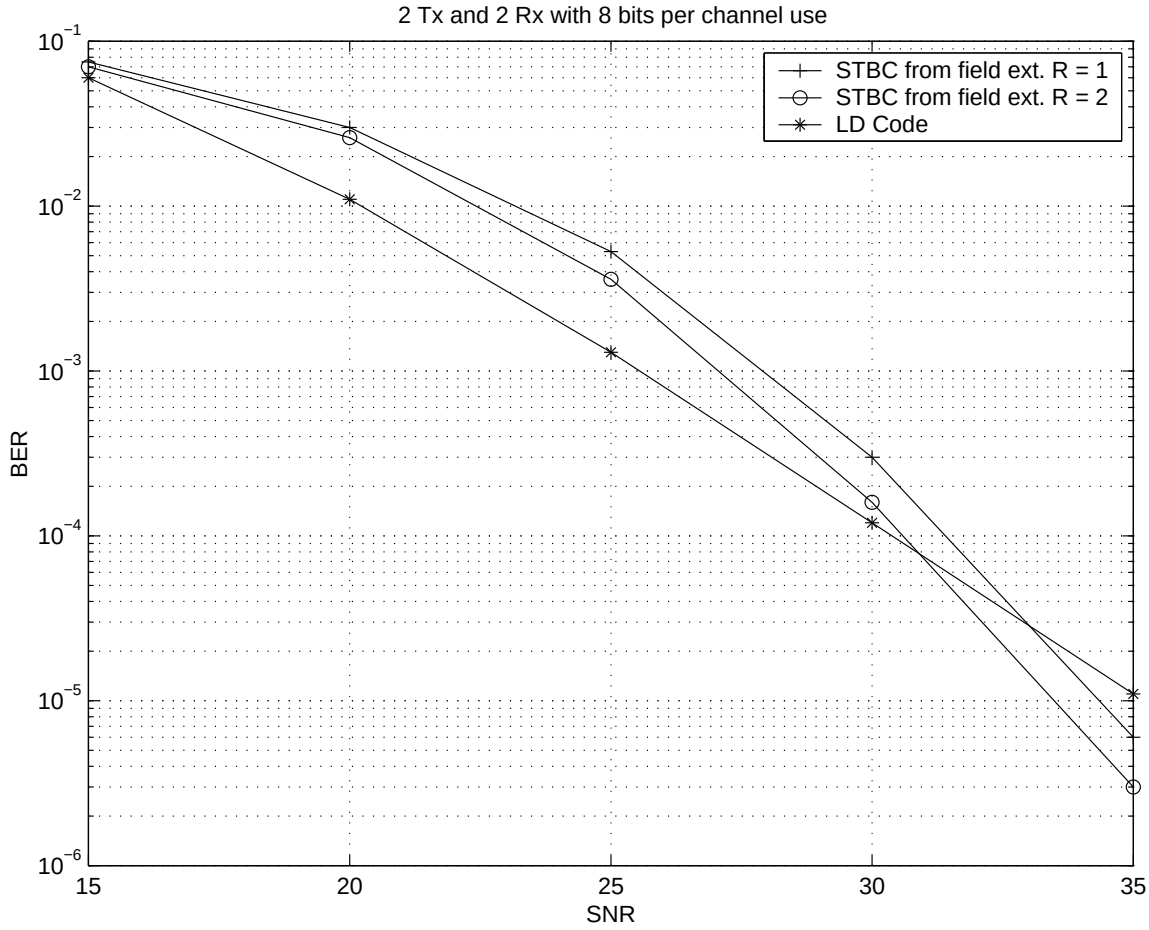


Figure 3.7: Comparison of STBCs from field extensions with LD codes for 2-Tx and 2-Rx with 8 bits per channel use.

Figure 3.7, it is clear that though the rate-1 code performs better than LD code only at very high SNRs, rate-2 code outperforms the LD code at medium and high SNRs. This motivates the use of high rate codes.

3.7 Summary

In this chapter, we have given constructions of rate-1, full-rank STBCs for arbitrary number of transmit antennas over arbitrary finite subsets of $\mathbb{Q}(\omega_m)$, using algebraic extensions of $\mathbb{Q}$. We also gave constructions of high rate (≥ 1), full-rank STBCs over arbitrary signal sets for arbitrary number of transmit antennas, using both algebraic and transcendental

extensions of $\mathbb{Q}$. We have obtained an expression for the coding gain of all these STBCs and gave a lower bound on it for some specific cases. We have also shown that the STBCs from field extensions do not maximize the mutual information. However, for one receive antenna, the loss in the mutual information is very less. We have also shown that the finite-signal-set capacity of the high-rate STBCs is better than that of the rate-1 STBCs. We have presented simulation results to show that high-rate STBCs perform better than rate-1 STBCs in terms of BER.

Chapter 4

Information-Lossless Designs from Crossed-Product Algebras

In this chapter, we obtain designs using crossed-product algebras (defined in Section 4.2) including division algebras and give a sufficient condition for the STBCs obtained using them to be information-lossless. We give some classes of crossed-product algebras, from which the STBCs obtained are information-lossless and also of full rank. The STBCs constructed in this chapter include the STBCs constructed in [39, 40, 44] as a special case. We present some simulation results for two, three and four transmit antennas to show that our STBCs perform better than some of the best known codes and also that these STBCs are very close to the capacity of the channel with QAM symbols as the input.

4.1 Introduction

In this section, we will first recall the expressions for the capacity of a Rayleigh fading channel for n_t transmit and n_r receive antennas and then define the term **Information-Lossless** (ILL) STBCs. Let $\mathbf{x} \in \mathbb{C}^{n_t \times 1}$ be the transmitted vector for one time instant and $\mathbf{y} \in \mathbb{C}^{n_r \times 1}$ be the received vector. If $\mathbf{H} \in \mathbb{C}^{n_r \times n_t}$ is the channel matrix whose entries are

[1]Part of the results presented in this chapter are available in publications [39–42].

iid with zero-mean, unit-variance, complex Gaussian, then we have

$$\mathbf{y} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\mathbf{H}\mathbf{x} + \mathbf{w} \tag{4.1}$$

where $\mathbf{w} \in \mathbb{C}^{r\times 1}$ is the additive noise vector whose entries are iid with zero-mean unit-variance, complex Gaussian. We assume that the vector $\mathbf{f}$ has entries with unit variance i.e., $\mathrm{E}(\mathbf{x}^H\mathbf{x}) = n_t$. The channel matrix $\mathbf{H}$ is assumed to be known at the receiver but not at the transmitter. Then, the resulting channel capacity is given by [1, 2]

$$C(n_t, n_r, \mathsf{SNR}) = \max_{\mathbf{R_x}\geq 0, tr(\mathbf{R_x})=n_t} \mathcal{E}\left\{\log_2\left(\det\left(\mathbf{I}_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{R}_\mathbf{x}\mathbf{H}^H\right)\right)\right\} \tag{4.2}$$

where $\mathbf{R_x}$ is the covariance matrix of the vector $\mathbf{x}$ and $\mathbf{I}_{n_r}$ is the $n_r \times n_r$ identity matrix. The capacity-achieving $\mathbf{x}$ is a zero-mean complex Gaussian vector with covariance matrix say $\mathbf{R_{x,opt}}$. Under the assumption that the distribution of $\mathbf{H}$ is rotationally invariant, the optimizing covariance matrix is $\mathbf{R_{x,opt}} = \mathbf{I}_{n_t}$. Thus,

$$C(n_t, n_r, \mathsf{SNR}) = \mathcal{E}_\mathbf{H}\left\{\log_2\left(\det\left(\mathbf{I}_{n_r} + \frac{\mathsf{SNR}}{n_t}\mathbf{H}\mathbf{H}^H\right)\right)\right\}. \tag{4.3}$$

The above expression gives channel capacity when we transmit independent vectors at every time instant i.e., there is no coding in time. However, if we use an $n_t \times l$ STBC, we transmit l vectors in l time instants which need not be independent of each other. So, if the transmitted $n_t \times l$ matrix over l time instants is $\mathbf{X}$, then we have

$$\mathbf{Y} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\mathbf{H}\mathbf{X} + \mathbf{W} \tag{4.4}$$

where $\mathbf{Y}$, $\mathbf{W}$ are the received $(r \times l)$ and additive noise $(r \times l)$ matrices. Let the STBC used in the above equation be of rate R symbols per channel use. Then, we have lR independent variables describing the matrix $\mathbf{X}$. Let us denote them by $f_1, f_2, \ldots, f_{lR}$ and

let $\mathbf{f} = [f_1, f_2, \ldots, f_{lR}]^T$. Suppose that we can rewrite (4.4) as

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\widehat{\mathbf{H}}\mathbf{f} + \widehat{\mathbf{w}} \tag{4.5}$$

where $\widehat{\mathbf{y}}$ and $\widehat{\mathbf{w}}$ are the matrices $\mathbf{Y}$ and $\mathbf{W}$, respectively, arranged in a single column, by serializing the columns. Notice that this can be done for any linear design. The size of the matrix $\widehat{\mathbf{H}}$ is $n_r l \times lR$. Then, the capacity of this new channel $\widehat{\mathbf{H}}$, known as *equivalent channel* is given by (4.3) with $n_t, n_r, \mathbf{H}$ replaced with $lR, ln_r, \widehat{\mathbf{H}}$ respectively (except for n_t in the term $\sqrt{\frac{\rho}{n}}$). So, by introducing coding, the maximum mutual information between the actual information vector $\mathbf{f}$ and the received matrix $\mathbf{X}$ (or $\widehat{\mathbf{x}}$) is given by

$$C_{STBC}(n_t, n_r, \mathsf{SNR}) = \frac{1}{l}\mathcal{E}_{\mathbf{H}}\left\{\log_2\left(\det\left(\mathbf{I}_{ln_r} + \frac{\mathsf{SNR}}{n_t}\widehat{\mathbf{H}}\widehat{\mathbf{H}}^H\right)\right)\right\} \tag{4.6}$$

where $C_{STBC}(n_t, n_r, \mathsf{SNR})$ denotes the maximum mutual information when the STBC is introduced. Clearly, this can at most be equal to $C(n_t, n_r, \mathsf{SNR})$.

Definition 4.1.1 *If the maximum mutual information when an STBC $\mathcal{C}$ is used for n_t transmit and n_r receive antennas, is equal to the capacity of the channel for n_t transmit and n_r transmit antennas given by $C(n_t, n_r, \mathsf{SNR})$, then $\mathcal{C}$ is called an* **information lossless STBC** *[22]. We call the design used to describe $\mathcal{C}$ as a capacity achieving design.*

Though, an STBC might be an information-lossless STBC, it may still be far from achieving the channel capacity. When we say an STBC is information-lossless, we only mean that there is no loss in the mutual information due to the structure of the design used to describe the STBC. Note that a trivial code (e.g. V-BLAST [49]), that is, there is no dependency between the entries of the codeword matrices, is an information lossless code. But, it is known that V-BLAST doesn't achieve capacity with simple ML decoding. Thus, "information-losslessness" is a necessary condition of an STBC to achieve capacity, but not a sufficient condition.

In [23], it is shown that the Alamouti code is the only rate-1, 2×2 design which achieves capacity, among all the orthogonal designs and that too only for one receive

antenna. In the same paper, a class of codes namely, Linear Dispersion (LD) codes were introduced and these STBCs were constructed by optimizing for the mutual information and the designs they construct achieve 90% of the channel capacity. In [22], a rate-2, 2×2 design based on number theory was proposed which achieves capacity for 2 transmit and arbitrary number of receive antennas. In [34–37, 39, 40], full-rank, arbitrary rate STBCs were constructed for arbitrary number of transmit antennas, over any finite subsets of any subfields of $\mathbb{C}$, using commutative and non-commutative (cyclic) division algebras and have given a class of information-lossless STBCs. In [44], STBCs over QAM signal sets are constructed using cyclic division algebras for 2, 3 and 4 transmit antennas.

Table 4.1 summarizes the important aspects of several well known STBCs along with that of the codes of this chapter.

Table 4.1: Comparison of various known square STBCs

STBC or the design	No. of transmit antennas	Rank	Rate	Capacity	Signal set (finite subset of)	Decoding
ODs [6, 10]	power of 2	full	≤ 1	achieves only for $n = 2, r = 1$	$\mathbb{C}$	single-symbol decodable
LDC [23]	arbitrary	full	≤ 1	achieves 90% of the possible	$\mathbb{Z}[j]$	sphere decodable
Damen *et al.* [22]	2	full	2	achieves for any r	$\mathbb{Z}[j]$	sphere decodable
DAST [18]	arbitrary	full	1	away from capacity	$\mathbb{Z}[j]$	sphere decodable
Sethuraman *et al.* [39, 40]	arbitrary	full	arbitrary	away from capacity	any subfield of $\mathbb{C}$	sphere decodable
TAST [21]	arbitrary	full	$\leq n$	close to capacity	$\mathbb{Z}[j]$	sphere decodable
Galliou *et al.* [43]	arbitrary	full	n	claim to maximize mutual information	$\mathbb{Z}[j]$	sphere decodable
Belfiore *et al.* [44]	2, 3 and 4	full	n	away from capacity	$\mathbb{Z}[j]$	sphere decodable
Proposed in this chapter	arbitrary	full	arbitrary	achieve capacity	any subfield of $\mathbb{C}$	sphere decodable

The remaining part of this chapter is organized as follows: In Section 4.2, we give a brief introduction to crossed-product central simple algebras. The main principle and construction of the STBCs from such algebras are given in Section 4.3. Also it is shown that the well known Alamouti code and quasi-orthogonal designs can be obtained from crossed-product algebras, which in general need not be of full-rank. In Section 4.4, we give a sufficient condition for our STBCs to be information-lossless and show that under certain conditions, the STBCs from cyclic algebras satisfy this sufficient condition, i.e., these STBCs are information-lossless. In Section 4.5, we restrict ourselves to those crossed-product algebras which are division algebras. We give some classes of division algebras using which construction of full-rank STBCs is illustrated with examples. In the same section, we show that the STBCs arising from these division algebras are information-lossless. Decoding of the codes obtained in this chapter is discussed in Section 4.6. Finally, in the same section, we present simulation results to show that our codes perform better than the best known codes and approach the capacity of the channel with QAM input. Throughout the chapter, we take the number of transmit antennas equal to $n_t = n$.

4.2 Crossed-Product Algebras

In this section we give a brief introduction to crossed-product algebras. Let F be a field. Then, an associative F-algebra A is called a F-central simple algebra if the center of A is F and A is a simple algebra i.e., A does not have non-trivial two-sided ideals. Clearly, any field has no non-trivial two sided ideals and hence are central simple algebras, the center being the field itself. In the following example we give another famous example of central simple algebras.

Example 4.2.1 *Consider the matrix algebra $M_n(F)$ of $n \times n$ matrices over a field F. Let I be a non-zero ideal of $M_n(F)$. If $\mathbf{U} \in M_n(F)$, then we have*

$$\mathbf{U} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} e_{i,j}u_{i,j} = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} e_{i,p}\mathbf{V}e_{q,j}v_{p,q}^{-1}u_{i,j}$$

where $e_{i,j}$ is the standard basis of $M_n(F)$ over F, i.e., $e_{i,j}$ is an $n \times n$ matrix with (i,j)-th as the only non-zero component, and $\mathbf{V}$ is a non-zero element, with $v_{p,q}$ as a non-zero component, of the ideal I. From the LHS of the above expression, the element $\mathbf{U}$ also belongs to the ideal I. Thus $I = M_n(F)$ and the algebra $M_n(F)$ is a simple algebra. It is easy to check that F is the center of this algebra and hence $M_n(F)$ is an F-central simple algebra.

Henceforth A will denote a central simple algebra. It is well known that the dimension $[A : F]$ of A over its center F is always a perfect square, say n^2 [54, 55]. The square root of $[A : F]$ is called the degree of A. The algebra A is a division algebra if every element of A is invertible in A. It is known that all division algebras are central simple algebras. By a subfield K of A, we mean $F \subset K \subset A$. Let K be a maximal subfield of A, i.e., $K \subset A$ and K is not contained in any other subfield of A. Also, let K be such that the centralizer of K in A is K itself. Then, K is called a strictly maximal subfield and it is well known that $[K : F] = n$, the degree of the algebra A. When A is a division algebra, then every maximal subfield is its own centralizer in A and thus $[K : F] = n$ for every maximal subfield K. We will always consider central simple algebras which have at least one strictly maximal subfield as a subfield of the complex field $\mathbb{C}$. In addition, let the extension K/F be a Galois extension and let $G = \{\sigma_0 = 1, \sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}$ be the Galois group ($\sigma_0 = 1$ is the identity map and the identity element of G) of K/F. Then, from [54][Noether-Skolem theorem], there exists a set $U_G = \{u_{\sigma_i} : \sigma_i \in G\} \subset A$ such that

$$\sigma_i(k) = u_{\sigma_i}^{-1} k u_{\sigma_i} \quad \forall \;\; k \in K \text{ and } \;\; \sigma_i \in G. \tag{4.7}$$

We can always normalize the set U_G such that $u_{\sigma_0} = 1$. It can be seen easily that the u_{σ_i} are linearly independent over K. Since $|U_G| = |G| = [K : F] = n$, U_G is a basis of A over K and called a Noether-Skolem basis. Thus, A can be seen as a right K-space of dimension n over K, i.e.,

$$A = \bigoplus_{\sigma_i \in G} u_{\sigma_i} K. \tag{4.8}$$

In the above form of A, addition and equality are component-wise. From (4.7), we have

$$\sigma_i(\sigma_j(k)) = u_{\sigma_i}^{-1} u_{\sigma_j}^{-1} k u_{\sigma_j} u_{\sigma_i} = (\sigma_j \sigma_i)(k) = u_{\sigma_j\sigma_i}^{-1} k u_{\sigma_j\sigma_i}.$$

From the above expression, $u_{\sigma_j\sigma_i}(u_{\sigma_j}u_{\sigma_i})^{-1}$ commutes with every element of K and hence belongs to the centralizer of K. Since, the centralizer of K is K itself, we have $u_{\sigma_j\sigma_i}\left(u_{\sigma_j}u_{\sigma_i}\right)^{-1} \in K$, i.e., $u_{\sigma_j}u_{\sigma_i} = u_{\sigma_j\sigma_i}\phi(\sigma_j,\sigma_i)$, where $\phi(\sigma_i,\sigma_j) = u_{\sigma_i\sigma_j}^{-1}u_{\sigma_i}u_{\sigma_j} \neq 0 \in K$. From the associativity of A, we have $u_{\sigma_h}(u_{\sigma_i}u_{\sigma_j}) = (u_{\sigma_h}u_{\sigma_i})u_{\sigma_j}$ which implies that

$$\phi(\sigma_h, \sigma_i\sigma_j)\phi(\sigma_i,\sigma_j) = \phi(\sigma_h\sigma_i,\sigma_j)\sigma_j(\phi(\sigma_h,\sigma_i)).$$

The above condition is called the cocycle condition and any map from $G \times G$ to $K\backslash\{0\}$ satisfying the cocycle condition is a cocycle. Thus, the map $\phi : G \times G \mapsto K\backslash\{0\}$ is a cocycle. With $u_{\sigma_0} = 1$, we have $\phi(\sigma_i,\sigma_0) = \phi(\sigma_0,\sigma_i) = \phi(\sigma_0,\sigma_0) = 1$ for all $\sigma_i \in G$.

Now, with the above development, it is easy to see that the multiplication between two elements of A, say $a = \sum_{i=0}^{n-1} u_{\sigma_i}k_{\sigma_i}$ and $a' = \sum_{j=0}^{n-1} u_{\sigma_j}k'_{\sigma_j}$, is

$$\left(\sum_{i=0}^{n-1} u_{\sigma_i}k_{\sigma_i}\right)\left(\sum_{j=0}^{n-1} u_{\sigma_j}k'_{\sigma_j}\right) = \sum_{l=0}^{n-1} u_{\sigma_l}k''_{\sigma_l}$$

where $k''_{\sigma_l} = \sum_{\sigma_i\sigma_j=\sigma_l}\phi(\sigma_i,\sigma_j)\sigma_j(k_{\sigma_i})k'_{\sigma_j}$. The algebra A with the decomposition as in (4.8) with addition and multiplication defined as above is called the *crossed product* of K and G with respect to ϕ and is denoted (K, G, ϕ).

Definition 4.2.1 *An F-central simple algebra A is called a crossed-product algebra if it can be written as a crossed product, i.e., if it has a strictly maximal subfield Galois over the center F.*

Example 4.2.2 *Consider the set of Hamiltonians, given by $\mathbb{H} = \{a+ib+jc+kd | a,b,c,d \in \mathbb{R}\}$, where $\mathbb{R}$ is the real field, $i^2 = j^2 = k^2 = -1$ and $ij = k$. Every element $h = a+ib+jc+kd \in \mathbb{H}$ has a unique inverse given by $(a-ib-jc-kd)/(a^2+b^2+c^2+d^2)$, and thus $\mathbb{H}$ is a division algebra and hence also a central simple algebra. The center of this algebra*

is the real field $\mathbb{R}$ *and* $[\mathbb{H} : \mathbb{R}] = 4$. *The sets* $\mathbb{C}_0 = \{a+ib|a, b \in \mathbb{R}\}, \mathbb{C}_1 = \{a+jc|a, c \in \mathbb{R}\}$ *and* $\mathbb{C}_2 = \{a + kd|a, d \in \mathbb{R}\}$ *are the maximal subfields of* $\mathbb{H}$. *Notice that each of the* $\mathbb{C}_i$*'s is an isomorphic copy of the complex field* $\mathbb{C}$. *Thus, we will identify one of them, say* $\mathbb{C}_1$ *with the complex field* $\mathbb{C}$. *It can be seen that* $[\mathbb{C} : R] = 2$ *and* $[\mathbb{H} : \mathbb{C}] = 2$. *With* $\mathbb{C}$ *as a maximal subfield,* $\{1, i\}$ *is a basis of* $\mathbb{H}$ *over* $\mathbb{C}$. *If* $\{\sigma_0 = 1, \sigma_1 = \sigma\}$ *is the Galois group of* $\mathbb{C}/\mathbb{R}$, *then it is easy to see that (*σ *is the complex conjugation)*

$$\sigma(c = r_1 + jr_2) = i^{-1}(r_1 + jr_2)i = -ir_1i - ijr_2i = r_1 - jr_2.$$

Thus, $U_G = \{u_{\sigma_0} = 1, u_{\sigma_1} = i\}$ *forms a Noether-Skolem basis of* $\mathbb{H}$ *over* $\mathbb{C}$. *Similarly, one can check that* $\{1, k\}$ *form a Noether-Skolem basis of* $\mathbb{H}$ *over* $\mathbb{C}$. *With* U_G *as a basis of* $\mathbb{H}$ *over* $\mathbb{C}$, *it is easy to see that* $\phi(\sigma_0, \sigma_0) = \phi(\sigma_1, \sigma_0) = \phi(\sigma_0, \sigma_1) = 1$ *and* $\phi(\sigma_1, \sigma_1) = -1$. *Thus,* $\mathbb{H}$ *is a crossed-product algebra.*

Suppose we have a Galois extension K of a field F with the Galois group G. Then, we can construct an F-central simple algebra which has K as a strictly maximal subfield as follows: Let ϕ be a map from $G \times G$ to K^* satisfying the cocycle condition $(\phi(\sigma, \tau\gamma)\phi(\tau, \gamma) = \phi(\sigma\tau, \gamma)\gamma(\phi(\sigma, \tau))$ for all $\sigma, \tau, \gamma \in G)$. Then consider the algebra

$$A = (K, G, \phi) = \bigoplus_{\sigma \in G} u_\sigma K$$

where equality and addition are component-wise and where u_σ are symbols such that (i) $\sigma(k) = u_\sigma^{-1} k u_\sigma$ and (ii) $u_\sigma u_\tau = u_{\sigma\tau}\phi(\sigma, \tau)$. It can be seen with simple computations that this algebra is a simple algebra with center F and hence an F-central simple algebra. And that this algebra is a crossed-product algebra is obvious from its construction.

In the next section, we construct some more crossed-product algebras and construct STBCs from these crossed-product algebras. But we shall first see a class of central simple algebras of which the set of Hamiltonians is a special case.

Example 4.2.3 *Let* $\mathbb{Q}$ *be the field of rational numbers and* F *be a subfield of the complex field. Consider a four dimensional* F*-space* $A = \{f_0 + y_1 f_1 + y_2 f_2 + y_3 f_3 | f_0, f_1, f_2, f_3 \in F\}$

with basis $y_0 = 1, y_1, y_2, y_3$. *With* 1 *as the multiplicative identity and multiplication of any two basis elements defined as follows, it is easy to check that the space* A *also forms a ring:*

$$y_1^2 = a, \quad y_2^2 = b, \quad y_1 y_2 = -y_2 y_1 = y_3$$

where a, b *are any two non-zero elements of* F. *Thus,* A *is an* F*-algebra and is called a generalized Quaternion algebra. It is easy to check that the center of this algebra is* F. *Now let us see whether* A *has any strictly maximal subfields. Clearly, if there exists one then it should be of degree 2 over* F, *as* A *is of degree 4 over* F. *So, it is sufficient to consider the degree 2 extensions of* F *contained in* A. *The set of elements of the form* $f_0 + y_1 f_1$ *forms a field, namely* $F(y_1)$. *Clearly,* $[F(y_1) : F] = 2$. *Also, the centralizer of* $F(y_1)$ *is* $F(y_1)$. *Thus,* $F(y_1)$ *is a strictly maximal subfield. Similarly,* $F(y_2)$ *and* $F(y_3)$ *are strictly maximal subfields of* A. *Also, it is easy to check that* $F(y_1)/F, F(y_2)/F$ *and* $F(y_3)/F$ *are all Galois extensions. Let* $K = F(y_1)$, *then the Galois group of* K/F *is* $G = \{\sigma_0 = 1, \sigma_1 = \sigma : y_1 \mapsto -y_1\}$. *Since* K/F *is Galois, there exists a Noether-Skolem basis of* A *over* K. *Since*

$$\sigma(f_0 + y_1 f_1) = (y_2)^{-1}(f_0 + y_1 f_1)y_2 = \frac{y_2}{b}(f_0 + y_1 f_1)y_2 = f_0 + \frac{y_2 y_1 y_2}{b} f_1 = f_0 - y_1 f_1,$$

we have $U_G = \{u_{\sigma_0} = 1, u_{\sigma_1} = y_2\}$ *as a basis of* A *over* K. *Also* $\phi(\sigma_0, \sigma_0) = \phi(\sigma_0, \sigma_1) = \phi(\sigma_1, \sigma_0) = 1$ *and* $\phi(\sigma_1, \sigma_1) = b$. *It would be interesting to see if this algebra is a division algebra too. It is clear that when* $a = b = -1$, *it is a division algebra (subset of Hamiltonians). We shall find for what other values of* a *and* b *this algebra is a division algebra. Any element* x *in* A *will be of the form* $x = f_0 + y_1 f_1 + y_2 f_2 + y_3 f_3$ *and we will denote the element* $f_0 - y_1 f_1 - y_2 f_2 - y_3 f_3$ *with* $\bar{x}$. *Clearly,* $x\bar{x} = f_0^2 - a f_1^2 - b f_2^2 + ab f_3^2 \in F$. *If* $x \neq 0$ *implies* $x\bar{x} \neq 0$, *then* $x\bar{x}(x\bar{x})^{-1} = x\,(\bar{x}(x\bar{x})^{-1}) = 1$ *which implies* $x^{-1} = \bar{x}(x\bar{x})^{-1}$ *and thus* x *is invertible. Suppose* a, b *are such that the equation* $d_0^2 = a d_1^2 + b d_2^2$ *does not have non-zero solution in* F. *Then* $x\bar{x} = 0$ *will imply that* $x = 0$. *Therefore,* $x\bar{x} \neq 0$ *if* $x \neq 0$. *Thus, with* a, b *as above, the algebra* A *is a division algebra. And if* $d_0^2 = a d_1^2 + b d_2^2$ *has a non-zero solution in* F, *then* A *is not a division algebra. With* $F = \mathbb{R}$ *and* $a = b = -1$,

we get the set of Hamiltonians.

4.3 STBCs from Crossed-Product Algebras

In the previous section, we have seen that if an algebra A has a strictly maximal subfield K which is Galois over the center F, then we can view A as a right K-space i.e., the action of scalar multiplication is given by right multiplication. In this section, we use this property and construct rate-n, full-rank STBCs.

Consider the map $L : A \mapsto End_K(A)$ given by $L(a) = \lambda_a$, where $\lambda_a(u) = au$ for all $u \in A$. Since, the scalar multiplication is via right and the action of λ_a gives left multiplication, these actions commute. That is $(\lambda_a(u))k = (au)k = a(uk) = \lambda_a(uk)$. This means, that λ_a is a K-linear transform of A. Clearly, L is a ring homomorphism from A to $End_K(A)$ i.e., $\lambda_{a+a'} = \lambda_a + \lambda_{a'}$ and $\lambda_{aa'} = \lambda_a\lambda_{a'}$ (this is because $\lambda_{aa'}(u) = (aa')u = a(a'u) = \lambda_a(\lambda_{a'}(u))$. Since A is a simple algebra, i.e., $\{0\}$ and A are the only ideals of A, L is injective. That is, $a - a' \neq 0 \Rightarrow \lambda_{a-a'}(u) = \lambda_a(u) - \lambda_{a'}(u) \neq 0$. If A is a division algebra, then, since $a - a'$ is invertible, say its inverse is a'', its image $\lambda_{a-a'}$ is also invertible (since $\lambda_{(a-a')a''}(u) = u$). Thus, the image of L is also a division algebra.

Now, since A is a right K-space, we can view the elements of $End_K(A)$ as matrices over K, with respect to a basis. We have seen in the previous section that the set U_G forms a basis for the algebra A over its maximal subfield K. With respect to this basis, we shall find the matrix representation of λ_a. For this, let $a = \sum_{\sigma_i \in G} u_{\sigma_i} k_{\sigma_i}$. To find the matrix representation of λ_a, it is sufficient to find the action of λ_a on each of the basis elements. Thus, $\lambda_a(u_{\sigma_j})$ is

$$\lambda_a(u_{\sigma_j}) = \sum_{\sigma_i \in G} u_{\sigma_i\sigma_j}\phi(\sigma_i, \sigma_j)\sigma_j(k_{\sigma_i}) = \sum_{\sigma_l \in G} u_{\sigma_l} k'_{\sigma_l}$$

where $k'_{\sigma_l} = \sum_{\sigma_i\sigma_j = \sigma_l} \phi(\sigma_i, \sigma_j)\sigma_j(k_{\sigma_i})$. Recall that $\phi(\sigma_i, \sigma_j) = u^{-1}_{\sigma_i\sigma_j} u_{\sigma_i} u_{\sigma_j} \in K$. From the above equation, if the rows and columns of the matrix of λ_a, denoted by $\mathbf{M}_a$, are indexed

with the elements of G, then the $(\sigma_i, \sigma_j)^{th}$ entry of $\mathbf{M}_a$ is $\phi(\sigma_i\sigma_j^{-1}, \sigma_j)\sigma_j\left(k_{\sigma_i\sigma_j^{-1}}\right)$, i.e.,

$$\mathbf{M}_a = \begin{bmatrix} k_{\sigma_0} & \delta_{0,1}\sigma_1(k_{\sigma_0\sigma_1^{-1}}) & \delta_{0,2}\sigma_2(k_{\sigma_0\sigma_2^{-1}}) & \cdots & \delta_{0,n-1}\sigma_{n-1}(k_{\sigma_0\sigma_{n-1}^{-1}}) \\ k_{\sigma_1} & \delta_{1,1}\sigma_1(k_{\sigma_1\sigma_1^{-1}}) & \delta_{1,2}\sigma_2(k_{\sigma_1\sigma_2^{-1}}) & \cdots & \delta_{1,n-1}\sigma_{n-1}(k_{\sigma_1\sigma_{n-1}^{-1}}) \\ k_{\sigma_2} & \delta_{2,1}\sigma_1(k_{\sigma_2\sigma_1^{-1}}) & \delta_{2,2}\sigma_2(k_{\sigma_2\sigma_2^{-1}}) & \cdots & \delta_{2,n-1}\sigma_{n-1}(k_{\sigma_2\sigma_{n-1}^{-1}}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{\sigma_{n-1}} & \delta_{n-1,1}\sigma_1(k_{\sigma_{n-1}\sigma_1^{-1}}) & \delta_{n-1,2}\sigma_2(k_{\sigma_{n-1}\sigma_2^{-1}}) & \cdots & \delta_{n-1,n-1}\sigma_{n-1}(k_{\sigma_{n-1}\sigma_{n-1}^{-1}}) \end{bmatrix} \tag{4.9}$$

where $\delta_{i,j} = \phi(\sigma_i\sigma_j^{-1}, \sigma_j)$. This implies, L is an embedding of the algebra A into $M_n(K)$, the set of $n \times n$ matrices over K, as shown in Figure 4.1. Thus, we have the following

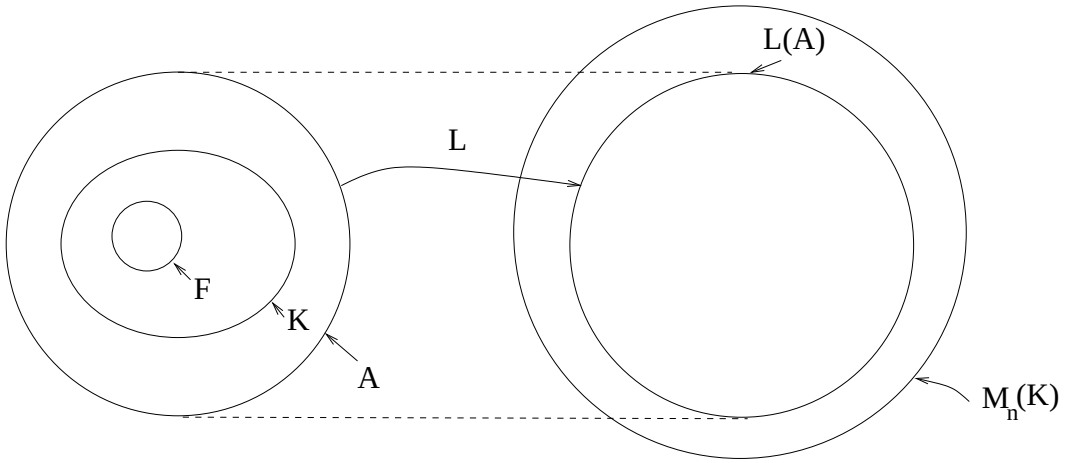


Figure 4.1: Embedding of a crossed-product algebra into the set of $n \times n$ matrices over K.

theorem:

Proposition 4.3.1 *With A, K, F, G and ϕ as above and in addition if A is a division algebra, then the set of matrices of the form as in (4.9) have the property that the difference of any two such matrices is invertible.*

From the above proposition it is clear that if K is a subfield of $\mathbb{C}$ and if we restrict k_i to some finite subset S of K, we will get a finite set of $n \times n$ matrices and the STBC defined by this set of matrices will be a rate-n STBC and it will be of full-rank if A is a division algebra. We normalize these matrices with a scaling factor such that the expected power

transmitted by every transmit antenna is unity per channel use. In the above case, the normalizing factor will be $n/\sqrt{\left(n+\sum_{i=0}^{n-1}\sum_{j=1}^{n-1}|\delta_{i,j}|^2\right)}$ (under the assumption that k_i have unit variance).

Example 4.3.1 *Consider the set $\mathbb{H}$ of Hamiltonians of Example 4.2.2. We have seen that $\mathbb{H}$ is a division algebra with $\mathbb{R}$ as its center and $\mathbb{C}$ as a maximal subfield and hence a crossed-product algebra. With $U_G = \{u_{\sigma_0} = 1, u_{\sigma_1} = i\}$ as one of the possible bases, the cocycle with respect to this basis is $\phi(\sigma_0, \sigma_0) = \phi(\sigma_1, \sigma_0) = \phi(\sigma_0, \sigma_1) = 1$ and $\phi(\sigma_1, \sigma_1) = -1$. And the matrix representation of the map λ_d, where $d = c_{\sigma_0} + ic_{\sigma_1}$, is*

$$\mathbf{M}_d = \begin{bmatrix} c_{\sigma_0} & -c^*_{\sigma_1} \\ c_{\sigma_1} & c^*_{\sigma_0} \end{bmatrix}.$$

The STBC defined with the above matrix is nothing but the well known Alamouti code.

Example 4.3.2 (Example 4.2.3 continued) *Recall that the crossed-product algebra $A(a,b) = F \oplus y_1F \oplus y_2F \oplus y_3F$ is a division algebra under certain conditions on a and b. Let $F = \mathbb{Q}$. Then, $a = b = -x$, $x > 0 \in \mathbb{Q}$ satisfy the condition that $f_0^2 = af_1^2 + bf_2^2 \Rightarrow f_0 = f_1 = f_2 = 0$. Thus, the crossed-product algebra $A(a,b)$ is a division algebra with $\mathbb{Q}$ as its center and $K = \mathbb{Q}(y_1)$, $(y_1^2 = -x)$, as a maximal subfield. The Galois group of $\mathbb{Q}(y_1)/\mathbb{Q}$ is $\{1, \sigma : y_1 \mapsto -y_1\}$. The set $\{1, y_2\}$, $(y_2^2 = -x)$, forms a Noether-Skolem basis of $A(a,b)$ seen as a $\mathbb{Q}(j)-$space. With this basis, we have $\phi(1,1) = \phi(1,\sigma) = \phi(\sigma,1) = 1$ and $\phi(\sigma,\sigma) = -x$. With this ϕ, the matrix representation of $k_0 + y_2k_1 \in A(a,b)$ over K is*

$$\begin{bmatrix} k_0 & -x\sigma(k_1) \\ k_1 & \sigma(k_0) \end{bmatrix}.$$

The field K can be seen as an n-dimensional F-vector space. Let $B = \{t_0, t_1, \ldots, t_{n-1}\}$ be a basis of K over F. Then, in (4.9), if we replace each of k_{σ_j}'s with the corresponding F-linear combination of t_i's, say $k_{\sigma j} = \sum_{i=0}^{n-1} f_{\sigma_j,i}t_i$, we get a rate-$n$ STBC for n transmit

antennas, over any finite subset of F. And since F is the fixed field of G, we have

$$\mathbf{M}_a = \frac{1}{\sqrt{P}} \begin{bmatrix} \sum_{i=0}^{n-1} f_{\sigma_0}^{(i)} t_i & \beta_0^{(1)} \sum_{i=0}^{n-1} f_{\mu_{0,1}}^{(i)} \sigma_1(t_i) & \cdots & \beta_0^{(n-1)} \sum_{i=0}^{n-1} f_{\mu_{0,n-1}}^{(i)} \sigma_{n-1}(t_i) \\ \sum_{i=0}^{n-1} f_{\sigma_1}^{(i)} t_i & \beta_1^{(1)} \sum_{i=0}^{n-1} f_{\mu_{1,1}}^{(i)} \sigma_1(t_i) & \cdots & \beta_1^{(n-1)} \sum_{i=0}^{n-1} f_{\mu_{1,n-1}}^{(i)} \sigma_{n-1}(t_i) \\ \sum_{i=0}^{n-1} f_{\sigma_2}^{(i)} t_i & \beta_2^{(1)} \sum_{i=0}^{n-1} f_{\mu_{2,1}}^{(i)} \sigma_1(t_i) & \cdots & \beta_2^{(n-1)} \sum_{i=0}^{n-1} f_{\mu_{2,n-1}}^{(i)} \sigma_{n-1}(t_i) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} f_{\sigma_{n-1}}^{(i)} t_i & \beta_{n-1}^{(1)} \sum_{i=0}^{n-1} f_{\mu_{n-1,1}}^{(i)} \sigma_1(t_i) & \cdots & \beta_{n-1}^{(n-1)} \sum_{i=0}^{n-1} f_{\mu_{n-1,n-1}}^{(i)} \sigma_{n-1}(t_i) \end{bmatrix} \tag{4.10}$$

where $\mu_{i,j} = \sigma_i \sigma_j^{-1}$, $\beta_i^{(j)} = \phi(\sigma_i \sigma_j^{-1}, \sigma_i)$ and P is a scaling factor to normalize the average total power of a codeword to n^2. It is equal to $\left(\sum_{i=0}^{n-1} |t_i|^2\right) \left(n + \sum_{i=0}^{n-1} \sum_{j=1}^{n-1} |\delta_{i,j}|^2\right) / n^2$ under the assumption that σ_j preserves the modulus of t_i. Throughout the chapter, we assume that $|\phi(\sigma_i, \sigma_j)| = |t_i| = 1$ for all $0 \leq i, j \leq n-1$ unless specified explicitly. From now on we use this matrix for $\mathbf{M}_a$ instead of the one in (4.9). For instance, in Example 4.3.1, if we replace each of c_i with the corresponding linear combination over $\mathbb{R}$, i.e., $c_i = r_{i,0} + j r_{i,1}$, we have a rate-2, full-rank STBC over any finite subset of $\mathbb{R}$ whose codewords are of the form

$$\frac{1}{\sqrt{2}} \begin{bmatrix} f_{\sigma_0}^{(0)} + j f_{\sigma_0}^{(1)} & -(f_{\sigma_1}^{(0)} - j f_{\sigma_1}^{(1)}) \\ f_{\sigma_1}^{(0)} + j f_{\sigma_1}^{(1)} & f_{\sigma_0}^{(0)} - j f_{\sigma_0}^{(1)} \end{bmatrix}.$$

Now, since the crossed-product algebra (K, G, ϕ) is a central simple algebra for any K and ϕ, we get rate-n STBCs for arbitrary number of transmit antennas and over any a priori specified signal set as follows: If S is the signal set over which we want the STBC to be and n is the number of transmit antennas, then take $F = \mathbb{Q}(S)$ and let K be an n-th degree Galois extension of F, with Galois group G. Let ϕ be a map from $G \times G$ to K^* satisfying the cocycle condition, for example $\phi(\sigma, \tau) = 1$ for all $\sigma, \tau \in G$. Then, we have a crossed-product algebra using which we can construct rate-n STBCs. However, it is well known that not every crossed-product algebra is a division algebra. For instance, consider

a generalized Quaternion algebra given in Example 4.2.3. If the equation $d_0^2 = ad_1^2 + bd_2^2$ has non-zero solutions for $d_0, d_1, d_2 \in F$, we have seen that it is a not a division algebra. Thus, the rate-n STBC constructed using the crossed-product algebra A need not be of full-rank. However, by choosing the variables in the matrix given in (4.10) such that the element a comes from a subalgebra of A, which is a division algebra, we can make our STBC a full-rank STBC. But in this process, we might lose some of the rate. The following example illustrates one such method, from which we get rate-1, full-rank STBCs.

Example 4.3.3 *Let S be the signal set of interest and n be the number of transmit antennas. Then, taking $F = \mathbb{Q}(S)$ and $K = F(\alpha)$, such that K/F is an n-th degree Galois extension, we construct the crossed-product algebra (K, G, ϕ), where ϕ is a cocycle. Thus, we get an STBC with codewords as in (4.10). However, this need not be of full rank, in general. So, let $f_{\sigma_0}^{(j)}$ come from S and let $f_{\sigma_i}^{(j)} = 0$, for all $i \neq 0$, then we get a rate-1, full-rank STBC over S, with codewords of the form*

$$\begin{bmatrix} \sum_{i=0}^{n-1} f_{\sigma_0}^{(i)} t_i & 0 & 0 & \cdots & 0 \\ 0 & \sum_{i=0}^{n-1} f_{\mu_{1,1}}^{(i)} \sigma_1(t_i) & 0 & \cdots & 0 \\ 0 & 0 & \sum_{i=0}^{n-1} f_{\mu_{2,2}}^{(i)} \sigma_2(t_i) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sum_{i=0}^{n-1} f_{\mu_{n-1,n-1}}^{(i)} \sigma_{n-1}(t_i) \end{bmatrix}$$

The coding gain of this STBC is

$$C_g = \min_{\mathbf{c} \neq \mathbf{c}'} \left| N_{K/F}(k) \right|^{2/n}$$

where $N_{K/F}(k)$ denotes the algebraic norm of the element $k \in K$ from K to F and k is the first entry on the diagonal of the difference matrix $\mathbf{c} - \mathbf{c}'$. Thus, this STBC and the STBCs constructed in [39] using field extensions, have the same rank and coding gain. Indeed,

it can be checked that the above code is a unitary transformation of the code from field extensions. In particular if K/F is cyclic and a cyclotomic extension, then the unitary matrix $\mathbf{U}$, where the above code is $\mathbf{U}$ times the code from the field extension K/F, is

$$\mathbf{U} = \begin{bmatrix} 1 & \gamma_0 & \gamma_0^2 & \cdots & \gamma_0^{n-1} \\ 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{n-1} \\ 1 & \gamma_2 & \gamma_2^2 & \cdots & \gamma_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma_{n-1} & \gamma_{n-1}^2 & \cdots & \gamma_{n-1}^{n-1} \end{bmatrix}$$

where γ_i, $i, = 0, 1, \ldots, n-1$ are the n roots of $x^n - \gamma$.

In the above example, though the crossed-product algebra is not a division algebra, we obtained a full-rank STBC by appropriately assigning the values to the variables of the design such that the resultant algebra (which is a subalgebra of the crossed-product algebra A) of the matrices is a division algebra. Another way of obtaining full-rank STBCs from crossed-product algebras is by choosing the signal sets appropriately. The next example which gives us the well known quasi-orthogonal design [16], illustrates this method of obtaining full-rank STBCs. In Section 4.5, we construct crossed-product algebras which are division algebras and hence the resulting STBCs are full-rank STBCs.

Example 4.3.4 (Quasi-orthogonal designs) *Let $F = \mathbb{R}(x)$, where x is an indeterminate and $K = F(j, \sqrt{x})$, where $j = \sqrt{-1}$. Clearly, K/F is a Galois extension, with Galois group $G = \langle \sigma_1, \sigma_2 \rangle$, where $\sigma_1 : j \mapsto -j$, $\sigma_2 : \sqrt{x} \mapsto -\sqrt{x}$. The maps σ_1 and σ_2 act as identity on $\sqrt{x}$ and j respectively. Let y_1, y_2 be two commuting symbols. Then, consider the algebra*

$$A = (K, G, \phi) = K \oplus y_1 K \oplus y_2 K \oplus y_1 y_2 K$$

where $\phi(\sigma_1, \sigma_1) = \phi(\sigma_1\sigma_2, \sigma_1) = -1$ and $\phi(1, \tau) = \phi(\sigma_2, \sigma_2) = \phi(\sigma_1\sigma_2, \sigma 2) = 1$ for all $\tau \in G$. It is easy to check that this ϕ satisfies the cocycle condition. All other properties like y_i form a Noether-Skolem basis can be checked easily. Now, with this ϕ, the STBC

we obtain will have codewords of the form

$$\begin{bmatrix} k_0 & -\sigma_1(k_1) & \sigma_2(k_2) & -\sigma_1(\sigma_2(k_3)) \\ k_1 & \sigma_1(k_0) & \sigma_2(k_3) & \sigma_1(\sigma_2(k_2)) \\ k_2 & -\sigma_1(k_3) & \sigma_2(k_0) & -\sigma_1(\sigma_2(k_1)) \\ k_3 & \sigma_1(k_2) & \sigma_2(k_1) & \sigma_1(\sigma_2(k_0)) \end{bmatrix}$$

where $k_i = f_i^{(0)} + f_i^{(1)} j + f_i^{(2)} \sqrt{x} + f_i^{(3)} j\sqrt{x}$. *This STBC is not a full-rank STBC. Now, suppose* $f_i^{(2)} = f_i^{(3)} = 0$ *for* $i = 0, 1, 2, 3$. *Then,* $\sigma_1(k_i) = k_i^*$ *(complex conjugate of* k_i*) and* $\sigma_2(k_i) = k_i$. *Thus, we have a STBC with codewords of the form*

$$\begin{bmatrix} k_0 & -k_1^* & k_2 & -k_3^* \\ k_1 & k_0^* & k_3 & k_2^* \\ k_2 & -k_3^* & k_0 & -k_1^* \\ k_3 & k_2^* & k_1 & k_0^* \end{bmatrix}$$

where k_i *now come from arbitrary finite subset of the complex field. This is none other than the quasi-orthogonal design of the form* $\begin{bmatrix} X & Y \\ Y & X \end{bmatrix}$ *given in [16], where* X *and* Y *are Alamouti codes. By changing the cocycle map* ϕ *accordingly, we can get the other quasi-orthogonal designs too. A simple computation tells that the rank of this STBC is* 2. *However, if we restrict* k_0, k_1 *and* k_2, k_3 *to come from two algebraically independent signal sets, then the resulting STBC will be a full-rank STBC (in [15], the two signal sets are such that one is rotated version of the other, which is a special case of selecting two algebraically independent signal sets).*

From the preceding example, it is clear that by sacrificing the division property of a division algebra, we can obtain quasi-orthogonal designs. In the rest of this section, we describe what a cyclic algebra is and construct STBCs from cyclic algebras. The cyclic algebras are important as they constitute building blocks for other crossed-product algebras constructed in this chapter.

An F-central simple algebra is called a cyclic algebra, if A has a strictly maximal

subfield K which is a cyclic extension of the center F. Clearly, a cyclic algebra is a crossed-product algebra. Let σ be a generator of the Galois group G. If u_{σ^i}, $i = 0, 1, \ldots, n-1$ is a Noether-Skolem basis for the algebra A over the field K, then we have

$$\sigma^i(k) = u_{\sigma^i}^{-1} k u_{\sigma^i} = u_\sigma^{-1} \left(u_{\sigma^{i-1}} k u_{\sigma^{i-1}}\right) u_\sigma = \left(u_\sigma^i\right)^{-1} k \left(u_\sigma^i\right)$$

which implies $u_{\sigma^i} = u_\sigma^i$. Also,

$$\phi(u_{\sigma^i}, u_{\sigma^j}) = u_{\sigma^{i+j}}^{-1} u_{\sigma^i} u_{\sigma^j} = \left(u_\sigma^{i+j \ modulo \ n}\right)^{-1} \left(u_\sigma^{i+j}\right) = \begin{cases} 1 & \text{if } i+j < n \\ \delta & \text{if } i+j \geq n \end{cases}$$

where $u_\sigma^n = \delta$. Since, the cocycle now can be described by just one element δ and similarly G can be described by σ, we denoted the crossed-product algebra (K, G, ϕ) with (K, σ, δ). Thus, with $z = u_\sigma$, we have

$$A = (K, \sigma, \delta) = \bigoplus_{i=0}^{n-1} z^i K$$

where $z^n = \delta$ and $kz = z\sigma(k)$. It is easy to see that the algebras in Example 4.2.2 and 4.2.3 are cyclic algebras. Since the group multiplication is same as addition of the exponents of σ, we can replace σ^i with i, and use σ^i only if necessary. Using the above expressions, (4.10) reduces to (we use the notation $f_{i,j}$ for $f_i^{(j)}$ to make the notation simple)

$$\frac{1}{\sqrt{n}} \begin{bmatrix} \sum_{i=0}^{n-1} f_{0,i} t^i & \delta\sigma\left(\sum_{i=0}^{n-1} f_{n-1,i} t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-2,i} t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{1,i} t^i\right) \\ \sum_{i=0}^{n-1} f_{1,i} t^i & \sigma\left(\sum_{i=0}^{n-1} f_{0,i} t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-1,i} t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{2,i} t^i\right) \\ \sum_{i=0}^{n-1} f_{2,i} t^i & \sigma\left(\sum_{i=0}^{n-1} f_{1,i} t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{0,i} t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{3,i} t^i\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} f_{n-1,i} t^i & \sigma\left(\sum_{i=0}^{n-1} f_{n-2,i} t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{n-3,i} t^i\right) & \cdots & \sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{0,i} t^i\right) \end{bmatrix}. \tag{4.11}$$

The scaling factor before the matrix is to normalize the power transmitted by each transmit antenna per channel use to unity, under the assumptions that $|\delta| = |\sigma^j(t^i)| = |t^i| = 1$ for all $0 \leq i, j \leq n-1$.

Example 4.3.5 *Let $n = 2$ and let S be a QAM signal set. Then $F = \mathbb{Q}(j)$.*
(a) Clearly, the polynomial $x^2 - j$ is irreducible in $F[x]$. Thus, $K = F(\sqrt{j})$ is a cyclic extension of F. The generator of the Galois group is given by $\sigma : \sqrt{j} \mapsto -\sqrt{j}$. Now, let $\delta(|\delta| = 1)$ be any element in F. Then, we have the STBC $\mathcal{C}$ given by

$$\mathcal{C} = \left\{ \begin{bmatrix} k_0 & \delta\sigma(k_1) \\ k_1 & \sigma(k_0) \end{bmatrix} | k_0, k_1 \in K \right\}. \tag{4.12}$$

However, viewing K as a vector space over F, with the basis $\{1, \sqrt{j}\}$, we have a STBC over any finite subset of F with codewords given by

$$\frac{1}{\sqrt{2}} \begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{j} & \delta\sigma(f_{1,0} + f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & \sigma(f_{0,0} + f_{0,1}\sqrt{j}) \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{j} & \delta(f_{1,0} - f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & (f_{0,0} - f_{0,1}\sqrt{j}) \end{bmatrix}$$

where $f_{i,j} \in S \subset F$ for $i, j = 0, 1$ and the scaling factor $1/\sqrt{2}$ is to ensure that the average power transmitted by each antenna per channel use is one.
(b) In the above example, since $\{1, \sqrt{j}\}$ is a basis of K over F, every element $k \in K$ can be written as $a + b\sqrt{j}$. It is easy to see that the set $\{1 + \sqrt{j}, 1 - \sqrt{j}\}$ forms a basis of K over F, since $a + b\sqrt{j}$ can be written uniquely as $\frac{a+b}{2}(1 + \sqrt{j}) + \frac{a-b}{2}(1 - \sqrt{j})$. Thus, expanding each k_i in (4.12), with respect to this newly formed basis, we have a STBC with codewords given by

$$\frac{1}{2} \begin{bmatrix} f_{0,0}(1 + \sqrt{j} + f_{0,1}(1 - \sqrt{j}) & \delta(f_{1,0}(1 - \sqrt{j}) - f_{1,1}(1 + \sqrt{j})) \\ f_{1,0}(1 + \sqrt{j}) + f_{1,1}(1 - \sqrt{j}) & (f_{0,0}(1 - \sqrt{j}) - f_{0,1}(1 + sqrtj)) \end{bmatrix}.$$

(c) It is easy to check that the polynomial $x^2 - 2$ is irreducible in $F[x]$ and hence, $K = F(\sqrt{2})$ is a cyclic extension of F, of degree 2. Proceeding as above, we have a STBC with

codewords of the form

$$\frac{1}{\sqrt{3}}\begin{bmatrix} f_{0,0}+f_{0,1}\sqrt{2} & \delta(f_{1,0}-f_{1,1}\sqrt{2}) \\ f_{1,0}+f_{1,1}\sqrt{2} & (f_{0,0}-f_{0,1}\sqrt{2}) \end{bmatrix}.$$

4.4 Mutual Information

In this section, we give a condition under which our designs from crossed-product algebras achieve capacity, i.e., the STBCs from the crossed-product algebras are information-lossless. We will first obtain the equivalent channel matrix $\widehat{\mathbf{H}}$ for our STBCs ($l = n$ and $R = n$). Let $\mathbf{X}$ be a codeword matrix of the form given in (4.10). First by serializing the columns of $\mathbf{F}$, we have

$$vec(\mathbf{HX}) = \underbrace{\begin{bmatrix} \mathbf{H} & \mathbf{0}_{r\times n} & \cdots & \mathbf{0}_{r\times n} \\ \mathbf{0}_{r\times n} & \mathbf{H} & \cdots & \mathbf{0}_{r\times n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}_{r\times n} & \mathbf{0}_{r\times n} & \cdots & \mathbf{H} \end{bmatrix}}_{\mathcal{H}} \begin{bmatrix} \mathbf{X}_0 \\ \mathbf{X}_1 \\ \vdots \\ \mathbf{X}_{n-1} \end{bmatrix}$$

where $vec(\mathbf{HX})$ denotes the vector obtained by serializing the columns of $\mathbf{HX}$. And $\mathbf{X}_j$ denotes the j^{th} column of the matrix $\mathbf{X}$. The vector $\mathbf{X}_0$ can be written as

$$\mathbf{X}_0 = \frac{1}{\sqrt{P}}\Phi_0\mathbf{f} \tag{4.13}$$

where Φ_0 is an $n \times n^2$ block diagonal matrix, each of the diagonal entries is a $1 \times n$ vector $\frac{1}{\sqrt{P}}\mathbf{t} = \frac{1}{\sqrt{P}}[t_0\ t_1\ \cdots\ t_{n-1}]$ and $\mathbf{f} = [f_{\sigma_0,0}\ f_{\sigma_0,1}\ \cdots\ f_{\sigma_0,n-1}\ \cdots\ f_{\sigma_i,0}\ \cdots\ f_{\sigma_i,n-1}\ \cdots f_{\sigma_{n-1},0}\ \cdots f_{\sigma_{n-1},n-1}]^T$ is the information vector. Similarly, $\mathbf{X}_j$ can be written as

$$\mathbf{F}_j = \frac{1}{\sqrt{P}}\Phi_j\mathbf{f} \tag{4.14}$$

where Φ_j is a matrix with i^{th} row as

$$\left[\mathbf{0}_{1\times n}\ \mathbf{0}_{1\times n}\ \cdots\ \mathbf{0}_{1\times n}\ \phi(\sigma_i\sigma_j^{-1},\sigma_j)\sigma_j(\mathbf{t})\ \mathbf{0}_{1\times n}\cdots\mathbf{0}_{1\times n}\right]$$

where $\sigma_j(\mathbf{t})$ is the vector $[\sigma_j(t_0)\ \sigma_j(t_1)\ \cdots\ \sigma_j(t_{n-1})]$. The column at which the non-zero vector $\phi(\sigma_i\sigma_j^{-1},\sigma_j)\sigma_j(\mathbf{t})$ starts depends on the Galois group G of K/F. For instance, if $\sigma_i\sigma_j^{-1}=\sigma_l$, then the column at which this non-zero vector starts is after $l-1$ blocks of the vector $\mathbf{0}_{1\times n}$, i.e., at nl^{th} column. Note that any two rows of $\mathbf{X}_j$ have the non-zero vectors in completely disjoint set of columns. Moreover, they are always separated by an integral multiple of n columns. For instance, if G is a cyclic group, then Φ_i will be

$$\Phi_i = \begin{array}{c} \begin{matrix} \text{starts at} & & & \text{starts at} & \text{starts at} & \text{starts at} & & \\ \text{0-th} & & & \text{n(n-i-1)-th} & \text{n(n-i)-th} & \text{n(n-i+1)-th} & & \\ \text{col} & & & \text{col} & \text{col} & \text{col} & & \\ \downarrow & & & \downarrow & \downarrow & \downarrow & & \end{matrix} \\ \begin{bmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \delta\sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \delta\sigma^i(\mathbf{t}_n) \\ \sigma^i(\mathbf{t}_n) & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \sigma^i(\mathbf{t}_n) & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \sigma^i(\mathbf{t}_n) & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix} \end{array} \begin{array}{l} \\ \\ \\ \leftarrow (i-1)^{th}\text{ row} \\ \leftarrow i^{th}\text{ row} \\ \\ \\ \\ \end{array} \quad (4.15)$$

So, with $\Phi=[\Phi_0^T\ \Phi_1^T\ \cdots\Phi_{n-1}^T]^T$, we have

$$\begin{bmatrix} \mathbf{X}_0 \\ \mathbf{X}_1 \\ \vdots \\ \mathbf{X}_{n-1} \end{bmatrix} = \frac{1}{\sqrt{P}}\Phi\mathbf{f}.$$

Then, (4.5) becomes

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n}} \underbrace{\frac{1}{\sqrt{P}}\mathcal{H}\Phi}_{\widehat{\mathbf{H}}} \mathbf{f} + \widehat{\mathbf{w}}. \tag{4.16}$$

Thus, the equivalent channel for our STBCs is $\frac{1}{\sqrt{P}}\mathcal{H}\Phi$. Note that from the structure of each of Φ_j's, the k^{th} row of Φ contains the vector $\phi(\sigma_i\sigma_j^{-1}, \sigma_j)\sigma_j(\mathbf{t})$ as its non-zero vector, where $k = nj + i$. And this non-zero vector starts at column nl, where $\sigma_l = \sigma_i\sigma_j^{-1}$. The following theorem characterizes the information-losslessness of the STBCs from crossed-product algebras with K as a strictly maximal subfield and a basis of K over the center given as $\{t_0, t_1, \ldots t_{n-1}\}$.

Theorem 4.4.1 *The design $\mathbf{M}_a$, as in (4.10) constructed using a crossed product algebra $A = (K, G, \phi)$ and the basis $\{t_0, t_1, \ldots, t_{n-1}\}$, with the assumptions that $|\sigma_j(t_i)| = |t_i|$, $|\phi(i, j)| = 1$ for all $0 \leq i, j \leq n-1$, achieves the channel capacity if*

$$\sum_{i=0}^{n-1} \sigma_j(t_i)\left(\sigma_{j'}(t_i)\right)^* = 0 \text{ if } j \neq j'. \tag{4.17}$$

Proof: We will first see what $\Phi\Phi^H$ is. Since the $(k, l)^{th}$ entry of this product is the inner product between k^{th} and l^{th} rows of Φ, we have

$$(\Phi\Phi^H)_{k,l} = \sum_{a=0}^{n^2-1} \Phi_{k,a}\Phi^*_{a,l}.$$

From the structure of Φ, if the rows k and $l \neq k$ come from the same Φ_j, then their non-zero columns are disjoint and hence this inner product is zero. If k and l come from different Φ_js then either the columns of non-zero entries are disjoint or completely same. So, we have

$$\begin{aligned}
(\Phi\Phi^H)_{k,l} &= \sum_{a=0}^{n-1} \phi(\sigma_i\sigma_j^{-1}, \sigma_j)\sigma_j(t_a)\left(\phi(\sigma_{i'}\sigma_{j'}^{-1}, \sigma_{j'})\sigma_{j'}(t_a)\right)^* \\
&= \phi(\sigma_i\sigma_j^{-1}, \sigma_j)\phi(\sigma_{i'}\sigma_{j'}^{-1}, \sigma_{j'})^* \sum_{a=0}^{n-1} \sigma_j(t_a)\left(\sigma_{j'}(t_a)\right)^* \\
&= 0 \text{ (from the statement of the theorem).}
\end{aligned} \tag{4.18}$$

If $k = l$, then we have

$$(\Phi\Phi^H)_{k,k} = \sum_{a=0}^{n-1} |\sigma_j(t_a)|^2 = P.$$

Thus, $\Phi\Phi^H = PI_{n^2}$. Now from (4.6), with the equivalent channel $\widehat{\mathbf{H}}$, we have the capacity of our design as

$$\begin{aligned} C_{DA}(\mathsf{SNR}, n_t = n, n_r) &= \frac{1}{n}\mathcal{E}_{\mathbf{H}}\left\{\log_2\left(\det\left(I_{n_r n} + \frac{\mathsf{SNR}}{n_t}\frac{1}{P}\mathcal{H}\Phi\Phi^H\mathcal{H}^H\right)\right)\right\} \\ &= \frac{1}{n}\mathcal{E}_{\mathbf{H}}\left\{\log_2\left(\det\left(I_{n_r n} + \frac{\mathsf{SNR}}{n}\mathcal{H}\mathcal{H}^H\right)\right)\right\} \\ &= \frac{1}{n}\mathcal{E}_{\mathbf{H}}\left\{\log_2\left(\det\left(I_{n_r} + \frac{\mathsf{SNR}}{n}\mathbf{H}\mathbf{H}^H\right)^n\right)\right\} \\ &= \mathcal{E}_{\mathbf{H}}\left\{\log_2\left(\det\left(I_r + \frac{\rho}{n}\mathbf{H}\mathbf{H}^H\right)\right)\right\} = C(n_t = n, n_r, \mathsf{SNR}). \end{aligned}$$

■

Corollary 4.4.1 *The design $\mathbf{M}_a$, as in (4.10) constructed using a division algebra $D = (K, G, \phi)$ and the basis $\{t_0, t_1, \ldots, t_{n-1}\}$, with the assumptions that $|\sigma_j(t_i)| = |t_i|$, $|\phi(i,j)| = 1$ for all $0 \le i, j \le n-1$, achieves the channel capacity if*

$$\sum_{i=0}^{n-1} \sigma_j(t_i)\left(\sigma_{j'}(t_i)\right)^* = 0 \text{ if } j \neq j'. \tag{4.19}$$

The above theorem gives a condition on the basis of a Galois extension for which the STBC arising from the crossed-product algebra is information-lossless. Also, it assumes that the basis elements have the property that $|\sigma_j(t_i)| = |t_i|$ for all $0 \le i, j \le n-1$. Let us now derive a sufficient condition on the basis when they don't satisfy $|\sigma_j(t_i)| = |t_i|$. Let $\{t'_0, t'_1, \ldots, t'_{n-1}\}$ be such a basis of K over F. Now, every entry, k_i, of (4.9) can be written as $\sum_{j=0}^{n-1} f'_{i,j}t'_i$. Equating these two expansions of k_i, we obtain a unique representation of every $f'_{i,j}$ in terms of linear combination of $f_{i,j}$ over F. Thus, if $\mathbf{R_f} = \mathbf{I}_{n^2}$ implies $\mathbf{R_{f'}} = \mathbf{I}_{n^2}$ under the assumption that power is normalized to the same value in both the cases, the mutual information with the new basis is the same as the mutual information with the previous basis. For instance, the STBC obtained in Example 4.3.5(a) uses a

basis which satisfies (4.17) and hence is information lossless. And the STBC obtained in Example 4.3.5(b) uses a basis which does not satisfy the property that $|\sigma(t_i)| = |t_i|$, but still the STBC obtained is information-lossless, since

$$\frac{1}{2}\begin{bmatrix} f_{0,0}(1+\sqrt{j}+f_{0,1}(1-\sqrt{j}) & \delta(f_{1,0}(1-\sqrt{j})-f_{1,1}(1+\sqrt{j})) \\ f_{1,0}(1+\sqrt{j})+f_{1,1}(1-\sqrt{j}) & (f_{0,0}(1-\sqrt{j})-f_{0,1}(1+sqrtj)) \end{bmatrix} = \frac{1}{2}\begin{bmatrix} f'_{0,0}+f'_{0,1}\sqrt{j} & \delta(f'_{1,0}-f'_{1,1}\sqrt{j}) \\ f'_{1,0}+f'_{1,1}\sqrt{j} & f'_{0,0}-f'_{0,1}\sqrt{j} \end{bmatrix}$$

where $f'_{i,0} = f_{i,0} + f_{i,1}$ and $f_{i,1} = f_{i,0} - f_{i,1}$, and $\mathbf{R_f} = \mathbf{R_{f'}}$. Note that $\{1+\sqrt{j}, 1-2\sqrt{j}\}$ also forms a basis for K/F, but with this basis, $\mathbf{R_f} \neq \mathbf{R_{f'}}$ and hence the STBC obtained using this basis is not information-lossless.

Consider the STBC constructed in Example 4.3.5(c). Suppose, the extension K/F has a basis $\{a_1, a_2\}$. Since a_1, a_2 are in K, let $a_1 = p_1 + q_1\sqrt{2}$ and $a_2 = p_2 + \sqrt{2}q_2$, with $p_i, q_i \in F$. Then, it is easy to check that the equation

$$a_1\sigma(a_1)^* + a_2\sigma(a_2)^* = (p_1+q_1\sqrt{2})(p_1^* - q_1^*\sqrt{2}) + (p_2+q_2\sqrt{2})(p_2^* - q_2^*\sqrt{2}) = 0$$

does not have any solutions for p_1, q_1, p_2, q_2 in F. Thus, the extension K/F of Example 4.3.5(c) does not have any basis satisfying (4.17) and hence the STBC is not information-lossless.

Thus, if a basis does not satisfy the property that $|\sigma_j(t_i)| = |t_i|$, for all i and j, then the STBC obtained using such a basis will be information-lossless if there exists a basis satisfying all the assumptions and conditions given in Theorem 4.4.1 and such that covariance matrix is mapped to itself under the new basis. The following lemma is towards proving that the STBCs obtained in this chapter are information-lossless.

Lemma 4.4.1 *Let F be a field containing a primitive n^{th} root of unity. Let K/F be a cyclic extension of degree n, where $K = F(t_n = t^{1/n})$, $t \in F, |t| = 1$ and σ a generator of*

the Galois group. Then,

$$\sum_{i=0}^{n-1} t_n^i \left(\sigma^k(t_n^i)\right)^* = \begin{cases} n & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases}.$$

Proof: If $k = 0$, it is trivial. So, let $k \neq 0$. Then, proving that $\sum_{i=0}^{n-1} t_n^i \left(\sigma^k(t_n^i)\right)^* = 0$ is same as proving $\sum_{i=0}^{n-1} (t_n^*)^i \left(\sigma^k(t_n^i)\right) = 0$. So, we have

$$\begin{aligned} \sum_{i=0}^{n-1} (t_n^*)^i \left(\sigma^k(t_n^i)\right) &= \sum_{i=0}^{n-1} \left[(t_n^*)\left(\sigma^k(t_n)\right)\right]^i \\ &= \sum_{i=0}^{n-1} \left[(t_n^*)\left(\omega_n^k t_n\right)\right]^i \\ &= \sum_{i=0}^{n-1} \left(\omega_n^k\right)^i = 0. \end{aligned}$$

■

Then, we have the following theorem

Theorem 4.4.2 *Let $F = \mathbb{Q}(S, \omega_n, t)$, $|t| = 1$ and $K = F(t_n = t^{1/n})$ be a cyclic extension of F with $G = \langle\sigma\rangle$ as the Galois group. Let A be the crossed-product algebra (K, σ, δ) with $|\delta| = 1$. Then, the STBCs constructed using the cyclic algebra A as in Section 4.3 are information-lossless.*

The proof of Theorem 4.4.2 follows from Lemma 4.4.1 and Theorem 4.4.1. From the above theorem, STBCs in the examples of Section 4.3, namely Examples 4.3.5(a),(b) 4.5.3, 4.5.2 and 4.5.4, are information-lossless with the assumption that $|t| = 1, |\delta| = 1$. However, if $|t| \neq 1$ and $|\delta| \neq 1$, the information loss increases as $||t| - 1|$ and $||\delta| - 1|$ increase. Figure 4.2 gives the capacity of the designs from cyclic algebras for various values of $|t|$ and $|\delta|$. It can be seen that the loss in the mutual information is very less compared to the information loss of 2×2 COD, namely Alamouti code. Figure 4.3 gives the capacity of the designs from cyclic algebras for various values of $|t|$.

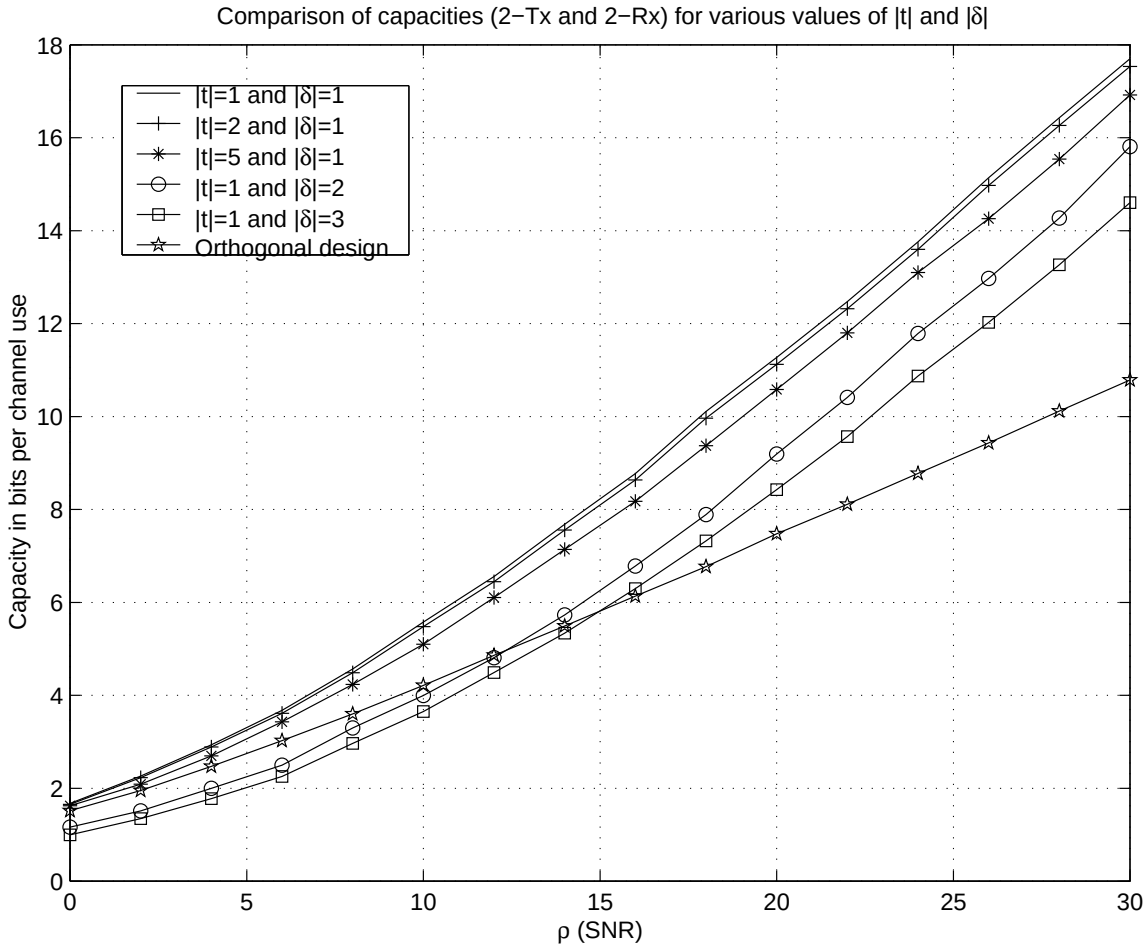


Figure 4.2: Comparison of capacities for various values of $|t|$ and $|\delta|$. The plain solid curve is the capacity of the channel too. Also, $\mathbf{R_f} \neq \mathbf{R_{f'}}$ in the cases where $|t| \neq 1$ or $|\delta| \neq 1$

4.5 Full-rank STBCs from Crossed-Product Division Algebras

We have seen in Section 4.2 that not all crossed-product algebras are division algebras. In this section, we identify some classes of crossed-product algebras which are division algebras and hence the STBCs from these algebras are of full-rank. We will first see when a cyclic algebra is a cyclic division algebra as cyclic division algebras constitute building blocks of other division algebras constructed in this chapter. We will only give a brief introduction and for more details on them the reader can refer to [39, 40].

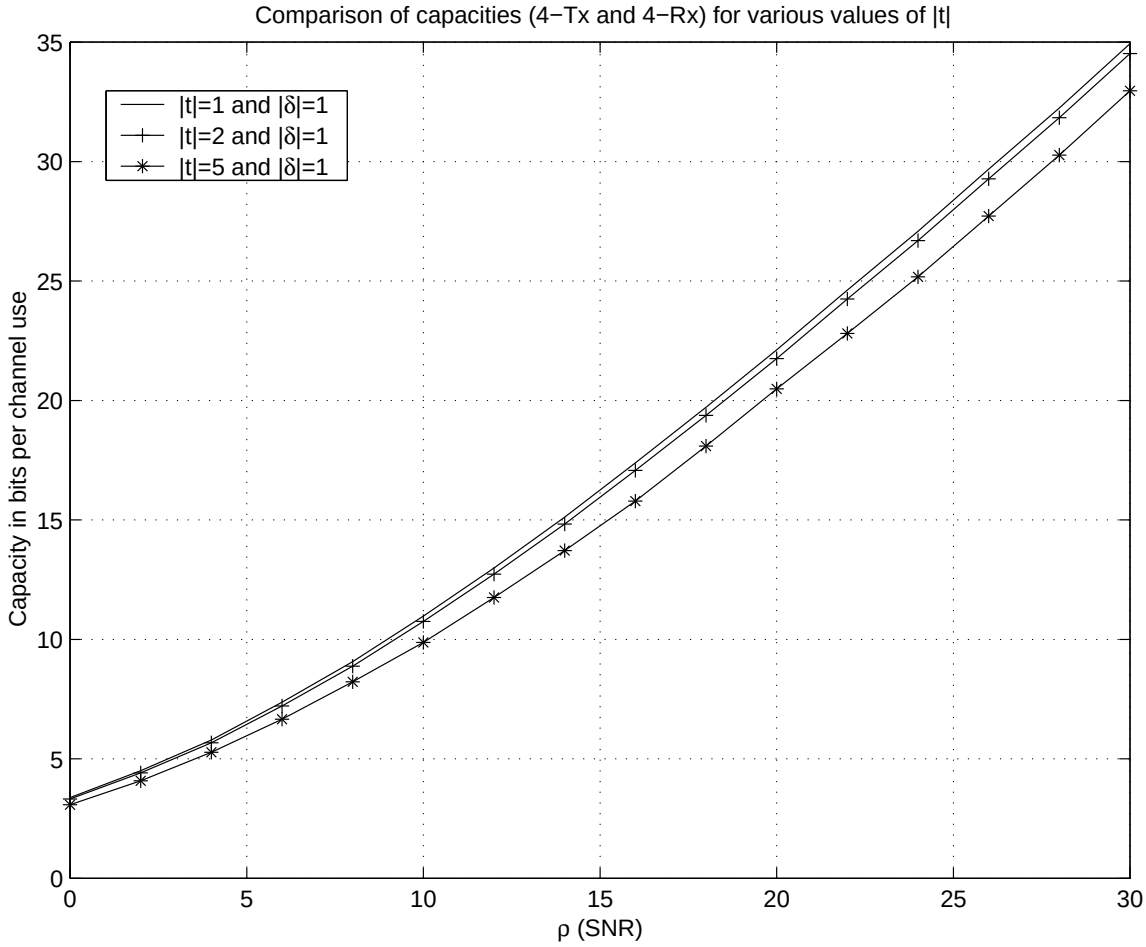


Figure 4.3: Comparison of capacities for various values of $|t|$. The plain solid curve is the capacity of the channel too.

4.5.1 Cyclic division algebras

In Chapter 2, we have given a brief introduction to cyclic division algebras. In this subsection, we will discuss in more detail about cyclic division algebras and the STBCs from them.

Let F be a field and K an extension of F, such that $[K : F] = n$. Also, let the extension K/F be a cyclic extension, i.e., the Galois group of the extension be a cyclic group generated by a single element, say σ. Let δ be a transcendental element over K. Then, we have the following algebra:

$$(K(\delta), \sigma, \delta) = K(\delta) \oplus zK(\delta) \oplus z^2K(\delta) \oplus \cdots \oplus z^{n-1}K(\delta)$$

where z is some symbol which satisfies the relations

$$kz = z\sigma(k) \text{ for all } k \in K \text{ and } z^n = \delta.$$

The above algebra has $F(\delta)$ as its center and has no nontrivial two sided ideals. Then, we recall the following theorem Chapter 2.

Theorem 4.5.1 ([39, 40, 55]) *With F, K, n, z and σ as above, the algebra $D = (K(\delta), \sigma, \delta)$ is a cyclic division algebra.*

From the above theorem, we have a cyclic division algebra, whenever we have a cyclic extension K/F and a transcendental element δ over F. We now give a general method of obtaining a cyclic extension. Towards finding such a method, we state the following lemma from [56].

Theorem 4.5.2 *Let F be a field containing a primitive n^{th} root of unity. Then, K/F is cyclic of degree n if and only if K is the splitting field over F of an irreducible polynomial $x^n - a \in F[x]$.*

Let S be the signal of interest and n be the number of transmit antennas. Then consider the field $F = \mathbb{Q}(S, \omega_n, \omega_m)$, where m is such that the polynomial $x^n - \omega_m$ is irreducible in $F[x]$. We can always find such m as S is a finite subset of $\mathbb{C}$. However, depending on the structure of S, the difficulty in finding such m varies. Let $K = F(\omega_{mn})$. To be able to use Theorem 4.5.2 it is sufficient to show that K is the splitting field of $x^n - \omega_m$. The roots of this polynomial are $\omega_{mn}\omega_n^i$ for $i = 0, 1, \ldots, n-1$. Since K contains ω_{mn}, all these roots also lie in K. Thus, K contains the splitting field of $x^n - \omega_m$. Since K is the smallest subfield containing F and ω_{mn}, K itself is the splitting field of $x^n - \omega_m$. Thus, by Theorem 4.5.2 K/F is a cyclic extension. We give some examples to illustrate the above construction.

Example 4.5.1 *Let $n = 2$ and $F = \mathbb{Q}(j)$, $K = F(\sqrt{j})$. Clearly, K is the splitting field of the polynomial $x^2 - j \in F[x]$ and hence K/F is cyclic of degree 2. Note that $x^2 - j$ is irreducible over F, since its only roots are $\pm\sqrt{j}$ and none of them is in F. The generator*

of the Galois group is given by $\sigma : \sqrt{j} \mapsto -\sqrt{j}$. *Now, let* δ *be any transcendental element over* K. *Then,* $(K(\delta)/F(\delta), \sigma, \delta)$ *is a cyclic division algebra. Thus, we have the STBC* $\mathcal{C}$ *given by*

$$\mathcal{C} = \left\{ \begin{bmatrix} k_0 & \delta\sigma(k_1) \\ k_1 & \sigma(k_0) \end{bmatrix} | k_0, k_1 \in K \right\}.$$

However, viewing K *as a vector space over* F, *with the basis* $\{1, \sqrt{j}\}$, *we have a STBC over any finite subset of* F *with codewords as follows*

$$\frac{1}{\sqrt{2}} \begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{j} & \delta\sigma(f_{1,0} + f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & \sigma(f_{0,0} + f_{0,1}\sqrt{j}) \end{bmatrix} =$$
$$\frac{1}{\sqrt{2}} \begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{j} & \delta(f_{1,0} - f_{1,1}\sqrt{j}) \\ f_{1,0} + f_{1,1}\sqrt{j} & (f_{0,0} - f_{0,1}\sqrt{j}) \end{bmatrix}$$

where $f_{ij} \in S \subset F$ *for* $i, j = 0, 1$ *and the scaling factor* $1/\sqrt{2}$ *is to ensure that the average power transmitted by each antenna per channel use is one.*

In the above example S can be any finite subset of F and hence, we have an STBC over any QAM constellation (since $F = \mathbb{Q}(j)$). From the structure of this STBC, we can see that it has a structure similar to the STBC proposed in [22]. Indeed, these two are similar in the sense of their capability of achieving the capacity, which will be shown in the next section. The code presented in [22] is of full rank for QAM constellations, as is the case with our code. However, we get STBC's for 2 antennas over any signal set, by choosing appropriate m. Say for instance, we want codes over 8PSK. In this case, we can take $m = 8$. However, the restriction on the choice of m affects the coding gain. This restriction on m is due to the signal set and n. And moreover, finding m such that the polynomial $x^n - \omega_m$ is irreducible over F depends on S, which might turn out to be involved sometimes. So, we next give constructions of cyclic extensions which do not depend on the signal set and n. But first we present an example for $n = 3$ transmit antennas.

Example 4.5.2 *Let* $n = 3$ *and suppose, we want* S *to be a QAM signal constellation.*

So, let $F = \mathbb{Q}(j, \omega_3)$. Then, the polynomial $x^3 - \omega_3$ is irreducible in $F[x]$. This is because, if it is reducible, then it should have a linear factor, which implies that this polynomial has a root in F, which is not true. Thus, $K = F(\omega_9)$ is a cyclic extension of F and $\sigma : \omega_9 \mapsto \omega_9\omega_3$ is a generator of the Galois group. Now, let δ ($|\delta| = 1$) be any transcendental element over K. Then, $(K(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have the STBC $\mathcal{C}$ with codewords of the form (obtained in a similar way as in the previous example)

$$\frac{1}{\sqrt{3}} \begin{bmatrix} f_{0,0} + f_{0,1}\omega_9 + f_{0,2}\omega_9^2 & \delta(f_{0,0} + f_{0,1}\omega_9\omega_3 + f_{0,2}\omega_9^2\omega_3^2) & \delta(f_{0,0} + f_{0,1}\omega_9\omega_3^2 + f_{0,2}\omega_9^2\omega_3) \\ f_{1,0} + f_{1,1}\omega_9 + f_{1,2}\omega_9^2 & f_{0,0} + f_{0,1}\omega_9\omega_3 + f_{0,2}\omega_9^2\omega_3^2 & \delta(f_{0,0} + f_{0,1}\omega_9\omega_3^2 + f_{0,2}\omega_9^2\omega_3) \\ f_{2,0} + f_{2,1}\omega_9 + f_{2,2}\omega_9^2 & f_{0,0} + f_{0,1}\omega_9\omega_3 + f_{0,2}\omega_9^2\omega_3^2 & f_{0,0} + f_{0,1}\omega_9\omega_3^2 + f_{0,2}\omega_9^2\omega_3 \end{bmatrix}$$

where $f_{i,j} \in S \subset F$ for $i, j = 0, 1, 2$.

We now give a construction of cyclic extensions which are independent of n and S to a large extent, in the following corollary.

Corollary 4.5.1 *Let $F = \mathbb{Q}(S, t, \omega_n)$, where t is a transcendental element over $\mathbb{Q}(S)$. Then, $K = F(t_n = t^{1/n})$ is a cyclic extension of F, and the degree of extension is n.*

The above corollary gives us a cyclic extension for any n and signal set S. The irreducible polynomial used to obtain the extension in the above corollary is $x^n - t$ and that this is a irreducible polynomial over F is proved in Chapter 2. So, the difficulty of finding an irreducible polynomial over F of degree n is overcome. Using the above corollary, we give some examples.

Example 4.5.3 *Let $n = 2$ and $F = \mathbb{Q}(S, t)$, where t ($|t| = 1$) is transcendental over $\mathbb{Q}(S)$. Then, $K = F(t_2 = \sqrt{t})$ is cyclic extension of F of degree 2. The generator of the Galois group is given by $\sigma : t_2 \mapsto -t_2$. Now, let $\delta(|\delta| = 1)$ be any transcendental element over K. Then, $(K(\delta)/F(\delta), \sigma, \delta)$ is a cyclic division algebra. Thus, we have the STBC $\mathcal{C}$*

with the codewords given by:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} f_{0,0}+f_{0,1}t_2 & \delta\sigma(f_{1,0}+f_{1,1}t_2) \\ f_{1,0}+f_{1,1}t_2 & \sigma(f_{0,0}+f_{0,1}t_2) \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} f_{0,0}+f_{0,1}t_2 & \delta(f_{1,0}-f_{1,1}t_2) \\ f_{1,0}+f_{1,1}t_2 & (f_{0,0}-f_{0,1}t_2) \end{bmatrix}$$

where $f_{0,0}, f_{0,1}, f_{1,0}, f_{1,1} \in S \subset F$. From the STBC construction in this example, it is clear that we have two degrees of freedom, i.e., both t_2 and δ can be chosen arbitrarily (almost), while the STBC in Example 4.5.1, we could choose only δ arbitrarily. This implies that the best coding gain possible for the STBC of Example 4.5.1, is less than the best possible with this example. Indeed, by computer search, we found that the best coding gain possible for the STBC in this example is at least 0.26 while the best coding gain possible for the STBC in Example 4.5.1 is only 0.22. Thus, this example shows that the dependence of the signal set and n have little effect on the constructions when $F/\mathbb{Q}$ is infinite, while the effect of the signal set and n is considerable when $F/\mathbb{Q}$ is finite.

Example 4.5.4 *Let $n = 4$ and S be the signal set. Then, with $F = \mathbb{Q}(\omega_4 = j, S, t)$ and $K = F(t_4 = t^{1/4})$, we have K/F cyclic and $\sigma : t_4 \mapsto jt_4$ is a generator of the Galois group. Thus, we have a full-rank STBC for 4 antennas as follows :*

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{4}}\begin{bmatrix} g_{0,0} & \delta g_{1,3} & \delta g_{2,2} & \delta g_{3,3} \\ g_{0,1} & g_{1,0} & \delta g_{2,3} & \delta g_{3,2} \\ g_{0,2} & g_{1,1} & g_{2,0} & \delta g_{3,3} \\ g_{0,3} & g_{1,2} & g_{2,1} & g_{3,0} \end{bmatrix} \right\}$$

where $g_{i,j} = \sum_{l=0}^{3} f_{j,l}(j^i t_4)^l$ and $f_{i,j} \in S \subset F$ for $i, j = 0, 1, 2, 3$.

STBCs from Brauer's division algebras

We give a construction of another class of cyclic division algebras due to Brauer [60, 69]. Let l and n be any two positive integers having same set of prime factors and such that l divides n. Let E be a field containing ω_l and such that $x^n - \omega_l$ is irreducible in $E[x]$. Let $K = E(x_0, x_1, \ldots, x_{n-1})$, where x_i are independent transcendental elements over E. Let

$\sigma : x_i \mapsto x_{i+1 \ mod \ n}$ be an automorphism of K, fixing every element of E and F be the fixed field of σ. Since, the order of σ is n, the extension K/F is cyclic with Galois group $\langle\sigma\rangle$. Consider the following algebra

$$B = (K, \sigma, \omega_l) = \bigoplus z^i K$$

where z is some symbol satisfying $kz = z\sigma(k)$ and $z^n = \omega_l$. Then, we have the following theorem due to Brauer.

Theorem 4.5.3 ([60, 69]) *With the notation as above, the algebra $B = (K, \sigma, \omega_l)$ is a cyclic division algebra of index n, with center F.*

Type-I STBCs from Brauer division algebras:

Let S be the signal set over which we want the STBC. Then, let $E = \mathbb{Q}(S, \omega_l)$. Assume, in addition, that $x^n - \omega_l$ is irreducible in $E[x]$. Then, F, the fixed field of σ will contain E. With $\delta = \omega_l$ and $\sigma : x_i \mapsto x_{i+1 \ mod \ n}$, we get a STBC with codewords as in (4.9), with $k_i \in F[x_0, x_1, \ldots, x_{n-1}]$. Since F contains E, we can restrict the coefficients of the polynomials k_i to come from E and in particular S only, to obtain a STBC over S. The STBC obtained this way is full-rank. And the symbol rate of this STBC depends on the degree of the polynomials k_i. If the degree is restricted to d, then the rate will be $\sum_{i=0}^{d} {}^{n+i-1}C_{n-1}$ symbols per channel use. We call the STBCs constructed this way type-I STBCs from Brauer division algebras. The following theorem, namely Lindemann-Weierstrass Theorem, suggests a method to find n algebraically independent transcendental numbers.

Theorem 4.5.4 ([69]) *If $u_1, u_2, \ldots, u_n$ are algebraic numbers that are linearly independent over $\mathbb{Q}$, then the exponentials $e^{u_1}, e^{u_2}, \ldots, e^{u_n}$ are algebraically independent over the field of algebraic numbers.*

We illustrate this construction with an example.

Example 4.5.5 *Let $n = 3$ and S be a QAM signal set. Then, let $E = \mathbb{Q}(j, \omega_3)$. It is easy to see that $x^3 - \omega_3$ is irreducible in $E[x]$. Let x_0, x_1, x_2, (say $e^j, e^{j\sqrt{2}}, e^{j\sqrt{3}}$), be*

three independent transcendental elements over E and $K = E(x_0, x_1, x_2)$. Then, $B = (K, \sigma, \omega_3) = K + zK + z^2K$ is a cyclic division algebra of index 3. Thus, we have a STBC with codewords as follows :

$$\begin{bmatrix} k_0(x_0,x_1,x_2) & \omega_l k_2(x_2,x_0,x_1) & \omega_l k_1(x_1,x_2,x_0) \\ k_1(x_0,x_1,x_2) & \omega_l k_0(x_2,x_0,x_1) & \omega_l k_2(x_1,x_2,x_0) \\ k_2(x_0,x_1,x_2) & k_1(x_2,x_0,x_1) & k_0(x_1,x_2,x_0) \end{bmatrix}$$

where $k_i(x_0, x_1, x_2)$ is a polynomial in x_0, x_1, x_2 with coefficients from S. If we allow the degree of these polynomials to be 1, then we have a symbol rate of 4. However, if we allow the degree of the polynomials to be any positive integer d, then the symbol rate will be $\sum_{i=0}^{d} {}^{2+i}C_2$.

If $n = 2$ in the above example, it is not possible to obtain a STBC over a QAM signal set, from Brauer division algebras. This is because, our E will be $\mathbb{Q}(j)$ and the polynomial $x^2 + 1$ is not irreducible in $E[x]$, which is a necessary condition for constructing a Brauer division algebra. However, if the signal set is a 5-PSK signal set, we can obtain a STBC for 2 transmit antennas.

Type-II STBCs from Brauer division algebras:

Till now, we have constructed STBCs using Brauer division algebra viewing the field K as an extension of E. However, if we view K as an extension of F (which we have been doing till the last subsection), we get a different STBC. Let $\omega_n \in E$. Since, K/F is cyclic, there exists an element $t \in K$, such that $K = F(t)$. Let us define $t = x_0 + x_1\omega_n + \ldots + x_{n-1}\omega_n^{n-1}$. Clearly, σ maps t to $t\omega_n^{-1}$ and hence $t^n \in F$. Thus, $K = F(t)$. Now, expanding each entry k_i in (4.9) as $\sum_{j=0}^{n-1} f_{i,j}t^j$, we get a STBC with codewords of the form as in (4.11). STBCs obtained this way will be called type-II STBCs from Brauer division algebras.

Example 4.5.6 (Example 4.5.5 contd.) *Expanding each k_i as $\sum_{j=0}^{2} f_{i,j}t^j$, and considering only degree zero polynomials in F, we get a STBC with codewords as follows.*

$$\begin{bmatrix} \sum_{j=0}^{2} f_{0,j}t^j & \omega_3\sum_{j=0}^{2} f_{2,j}t^j\omega_3^{2j} & \omega_3\sum_{j=0}^{2} f_{1,j}t^j\omega_3^{j} \\ \sum_{j=0}^{2} f_{1,j}t^j & \sum_{j=0}^{2} f_{0,j}t^j\omega_3^{2j} & \omega_3\sum_{j=0}^{2} f_{2,j}t^j\omega_3^{j} \\ \sum_{j=0}^{2} f_{2,j}t^j & \sum_{j=0}^{2} f_{1,j}t^j\omega_3^{2j} & \sum_{j=0}^{2} f_{0,j}t^j\omega_3^{j} \end{bmatrix}$$

where $f_{i,j} \in S \subset E \subset F$.

It is shown at the end of this section that the type-I STBCs from Brauer division algebras are not information-lossless if $|x_i| = 1$ and might be information-lossless if $|x_i| \neq 1$, while the type-II STBCs are information-lossless under certain conditions.

Coding gain of STBCs from cyclic division algebras

We conclude this subsection, giving a closed form expression for coding gains of STBCs constructed in this subsection. Let K/F be a cyclic extension and let $\mathcal{N}_{K/F}(k)$ denote the algebraic norm from K to F, of an element in $k \in K$.

Proposition 4.5.1 *Let $\mathcal{C}$ be the rate-n STBC constructed from the cyclic division algebra $(K(\delta), \sigma, \delta)$. Let the codewords of $\mathcal{C}$ be as in (4.11). Then, the coding gain of the code $\mathcal{C}$ is*

$$C_g = \min_{\mathbf{f}\neq\mathbf{f}'} \left|(-1)^{n-1}\mathcal{N}_{K/F}(\Delta k_{n-1}) + \ldots + \mathcal{N}_{K/F}(\Delta k_0)\right|^{2/n}$$

where $\mathbf{f} = [f_{0,0}, \ldots, f_{0,n-1}, \ldots, f_{n-1,0}, \ldots, f_{n-1,n-1}]$ and $\mathbf{f}' = [f'_{0,0}, \ldots, f'_{0,n-1}, \ldots, f'_{n-1,0}, \ldots, f'_{n-1,n-1}]$ are two distinct information vectors. And $\Delta k_i = \sum_{j=0}^{n-1} \left(f_{i,j} - f'_{i,j}\right) t^i$.

Proof: Follows from Proposition 16.2b of [55] (page 298) and the definition of coding gain. ■

4.5.2 STBCs from tensor-product division algebras

In the last few subsections, we have seen how to construct cyclic division algebras and STBCs from them. In this section, we construct division algebras from some known division algebras and hence construct STBCs from them. One of such constructions is given by tensor product (see appendix for definitions and properties of tensor products) of two division algebras as in the following theorem:

Theorem 4.5.5 ([54]) *Let D_1 and D_2 be two division algebras with the same center F. If $[D_1 : F]$ is relatively prime to $[D_2 : F]$ then $D_1 \otimes_F D_2$ is a division algebra with F as the center.*

So, given any two division algebras, D_1 and D_2 with the same center and relatively prime indices, the tensor product $D_1 \otimes_F D_2$ of them is also a division algebra with the same center. So, the index of $D_1 \otimes_F D_2$ is $\sqrt{[D_1 : F][D_2 : F]}$. If both D_1 and D_2 are cyclic division algebras, then the resulting tensor product division algebra is also a cyclic division algebra. The following example illustrates the construction of STBCs from such a tensor product division algebra obtained from two cyclic division algebras.

Example 4.5.7 *Suppose, we want an STBC over a QAM signal set for 6 transmit antennas. Then, let $F = \mathbb{Q}(j, \omega_3)$. Let $K_1 = F(\sqrt{j})$ and $K_2 = F(\sqrt[3]{j})$. Let δ be a transcendental element over F. Obviously, δ is a transcendental element over K_1 and K_2 also. Then, from Theorem 4.5.1, the crossed-products algebras $D_1 = (K_1(\delta), G_1, \delta) = K_1(\delta) \oplus z_1 K_1(\delta)$ and $D_2 = (K_2(\delta), G_2, \delta) = K_2(\delta) \oplus z_2 K_2(\delta) \oplus z_2^2 K_2(\delta)$ are division algebras where G_1 and G_2, the Galois groups of $K_1(\delta)/F(\delta)$ and $K_2(\delta)/F(\delta)$, are given by $G_1 = \{\sigma_{1,0} = 1, \sigma_{1,1} : \sqrt{j} \mapsto -\sqrt{j}\}$ and $G_2 = \{\sigma_{2,0} = 1, \sigma_{2,1} : \sqrt[3]{j} \mapsto \sqrt[3]{j}\omega_3, \sigma_{2,2} : \sqrt[3]{j} \mapsto \sqrt[3]{j}\omega_3^2\}$. And z_1 and z_2 are elements of D_1 and D_2 respectively such that*

$$z_1^2 = \delta \text{ and } k_1 z_1 = z_1 \sigma_{1,1}(k_1) \quad \forall\ k_1 \in K_1(\delta)$$

and

$$z_2^3 = \delta \text{ and } k_2 z_2 = z_2 \sigma_{2,1}(k_2) \quad \forall\ k_2 \in K_2(\delta).$$

It is easy to see that $K(\delta) = K_1(\delta) \otimes_F K_2(\delta)$ *is a maximal subfield of* $D = D_1 \otimes_F D_2$ *and that the Galois group of* $K(\delta)/F(\delta)$ *is* $G = \{\sigma_0 = 1, \sigma_1 = \sigma_{1,1}, \sigma_2 = \sigma_{2,1}, \sigma_3 = \sigma_{2,2} = \sigma_{2,1}^2, \sigma_4 = \sigma_{1,1}\sigma_{2,1}, \sigma_5 = \sigma_{1,1}\sigma_{2,2}\}$. *Note that* G *is a cyclic group with* σ_4 *as a generator. Also, the set* $\{u_{\sigma_0} = 1, u_{\sigma_1} = z_1 \otimes 1, u_{\sigma_2} = 1 \otimes z_2, u_{\sigma_3} = 1 \otimes z_2^2, u_{\sigma_4} = z_1 \otimes z_2, u_{\sigma_5} = z_1 \otimes z_2^2\}$ *forms a Noether-Skolem basis of* D *over* $K(\delta)$. *Thus,*

$$D = K(\delta) + u_{\sigma_1}K(\delta) + u_{\sigma_2}K(\delta) + u_{\sigma_3}K(\delta) + u_{\sigma_4}K(\delta) + u_{\sigma_5}K(\delta)$$

And the cocycle ϕ *is given in the following table:*

$\phi(\sigma_i, \sigma_j)$	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_0	1	1	1	1	1	1
σ_1	1	δ	1	1	δ	δ
σ_2	1	1	1	δ	1	δ
σ_3	1	1	δ	δ	δ	δ
σ_4	1	δ	1	δ	δ	δ^2
σ_5	1	δ	δ	δ	δ^2	δ^2

Substituting the above ϕ *in (4.9), we get an STBC with codewords of the form as follows:*

$$\frac{1}{\sqrt{6}}\begin{bmatrix} k_0 & \delta\sigma_1(k_1) & \delta\sigma_2(k_3) & \delta\sigma_3(k_2) & \delta^2\sigma_4(k_5) & \delta^2\sigma_5(k_4) \\ k_1 & \sigma_1(k_0) & \delta\sigma_2(k_5) & \delta\sigma_3(k_4) & \delta\sigma_4(k_3) & \delta\sigma_5(k_2) \\ k_2 & \delta\sigma_1(k_4) & \sigma_2(k_0) & \delta\sigma_3(k_3) & \delta\sigma_4(k_1) & \delta^2\sigma_5(k_5) \\ k_3 & \delta\sigma_1(k_5) & \sigma_2(k_2) & \sigma_3(k_0) & \delta^2\sigma_4(k_4) & \delta\sigma_5(k_1) \\ k_4 & \sigma_1(k_2) & \sigma_2(k_1) & \delta\sigma_3(k_5) & \sigma_4(k_0) & \delta\sigma_5(k_3) \\ k_5 & \sigma_1(k_3) & \sigma_2(k_4) & \sigma_3(k_1) & \sigma_4(k_2) & \sigma_5(k_0) \end{bmatrix}$$

where $k_i = f_{i,0} + f_{i,1}\sqrt{j} + f_{i,2}\sqrt[3]{j} + f_{i,3}\sqrt[3]{j}^2 + f_{i,4}\sqrt{j}\sqrt[3]{j} + f_{i,5}\sqrt{j}\sqrt[3]{j}^2$ *and* $f_{i,j} \in S(QAM) \in F$.

The above example shows how to construct STBCs from the tensor product division algebra of two cyclic division algebras (note that it is not necessary that we use cyclic

division algebras only) with relatively prime indices. This can be extended to tensor product of any number of division algebras with relatively prime indices using the following corollary.

Corollary 4.5.2 *Let D_i, $i = 0, 1, 2, \ldots, s-1$ be s F-division algebras with the index of D_i as $p_i^{\alpha_i}$, where p_i, $i = 0, 1, 2, \ldots, s-1$, are distinct primes and α_i are positive integers. Then, the algebra $D = \bigotimes_F D_i$ is an F-division algebra.*

Using the above method of constructing division algebras, we cannot construct division algebras from known division algebras of not relatively prime degrees. For instance, we cannot construct division algebras of degree 4 from two division algebras of degree 2. The following theorem helps us in such cases, where we construct a division algebra which is isomorphic to the tensor product of two cyclic division algebras with some constraints. However, we do not use the language of tensor product in constructing the division algebra.

Theorem 4.5.6 *Let δ_1, δ_2, x, and y be algebraically independent elements over a field L containing n_1-th and n_2-th primitive roots of unity, where n_1 and n_2 are positive integers. Let $F = L(x, y)$ and $K = F(x_1 = x^{1/n_1}, y_1 = y^{1/n_2}, \delta_1, \delta_2)$. Clearly, $K(\delta_1, \delta_2)$ is a Galois extension of $F(\delta_1, \delta_2)$, with the Galois group as $G = \langle \sigma_x, \sigma_y \rangle$, where $\sigma_x : x_1 \mapsto x_1 \omega_{n_1} x_1$ and acts as identity on the other three variables, and where similarly, $\sigma_y : y_1 \mapsto \omega_{n_2} y_1$ and acts as identity on the other three variables. Consider the associative algebra*

$$D = (K(\delta_1, \delta_2), G, \phi) = \bigoplus_{\substack{0 \le i < n_1 \\ 0 \le j < n_2}} u_{\sigma_x}^i u_{\sigma_y}^j K(\delta_1, \delta_2)$$

where u_{σ_x} and u_{σ_y} are two symbols commuting with each other and satisfying

$$u_{\sigma_x}^{n_1} = \delta_1; \quad u_{\sigma_y}^{n_2} = \delta_2$$

$$k u_{\sigma_x} = u_{\sigma_x} \sigma_x(k) \quad \textit{and} \quad k u_{\sigma_y} = u_{\sigma_y} \sigma_y(k).$$

for all $k \in K(\delta_1, \delta_2)$. Then, D is a division algebra.

Proof: To prove that D is a division algebra, it is sufficient to show that every non-zero element in D is invertible. Let $d = \sum_{i=0}^{n_1-1} u_{\sigma_x}^i \left(\sum_{j=0}^{n_2-1} u_{\sigma_y}^j k_{i,j} \right) \in D$ (we use i, j as the subscript of k instead of $u_{\sigma_x^i} u_{\sigma_y^j}$ to make the notations simpler). And let λ_d be the left regular representation of d over $K(\delta_1, \delta_2)$, i.e., $\lambda_d : a \mapsto da$ for all $a \in D$. Then, we have

$$\lambda_d = \begin{bmatrix} \eta_0 & \delta_1\sigma_x(\eta_{n_1-1}) & \delta_1\sigma_x^2(\eta_{n_1-2}) & \cdots & \delta_1\sigma_x^{n_1-1}(\eta_1) \\ \eta_1 & \sigma_x(\eta_0) & \delta_1\sigma_x^2(\eta_{n-1}) & \cdots & \delta_1\sigma_x^{n_1-1}(\eta_2) \\ \eta_2 & \sigma_x(\eta_1) & \sigma_x^2(\eta_0) & \cdots & \delta_1\sigma_x^{n_1-1}(\eta_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \eta_{n_1-1} & \sigma_x(\eta_{n_1-2}) & \sigma_x^2(\eta_{n_1-3}) & \cdots & \sigma_x^{n_1-1}(\eta_0) \end{bmatrix}$$

where η_i is

$$\eta_i = \begin{bmatrix} k_{i,0} & \delta_2\sigma_y(k_{i,n_2-1}) & \delta_2\sigma_y^2(k_{i,n_2-2}) & \cdots & \delta_2\sigma_y^{n_2-1}(k_{i,1}) \\ k_{i,1} & \sigma_y(k_{i,0}) & \delta_2\sigma_y^2(k_{i,n_2-1}) & \cdots & \delta_2\sigma_y^{n_2-1}(k_{i,2}) \\ k_{i,2} & \sigma_y(k_{i,1}) & \sigma_y^2(k_{i,0}) & \cdots & \delta_2\sigma_y^{n_2-1}(k_{i,3}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{i,n_2-1} & \sigma_y(k_{i,n_2-2}) & \sigma_y^2(k_{i,n_2-3}) & \cdots & \sigma_y^{n_2-1}(k_{i,0}) \end{bmatrix}.$$

Notice that $k_{i,j}$ are rational functions of polynomials of the two variables δ_1 and δ_2. However, we can assume $k_{i,j}$ are polynomials in δ_1 and δ_2 instead of rational functions in them, as we can take the LCM of all $k_{i,j}$ and factor it out. Let $\rho_d(\delta_1, \delta_2)$ denote the determinant of λ_d. Since δ_1 and δ_2 are algebraically independent of each other, it is sufficient to show that $\rho_d(\delta_1, \delta_2)$ is not a zero polynomial to show that d is invertible, For this let us assume that there exists some j for which $k_{0,j} \neq 0$. If there doesn't exist any j for which $k_{0,j} \neq 0$, then we can factor out u_{σ_x} from d and since u_{σ_x} is invertible, it is

sufficient to prove that d/u_{σ_x} is invertible. Thus, we have

$$\rho_d(0,\delta_2) = \det(\lambda_d)|_{\delta_1=0} = \det \begin{bmatrix} \eta_0 & 0 & 0 & \cdots & 0 \\ \eta_1 & \sigma_x(\eta_0) & 0 & \cdots & 0 \\ \eta_2 & \sigma_x(\eta_1) & \sigma_x^2(\eta_0) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \eta_{n_1-1} & \sigma_x(\eta_{n_1-2}) & \sigma_x^2(\eta_{n_1-3}) & \cdots & \sigma_x^{n_1-1}(\eta_0) \end{bmatrix}.$$

In the above expression, η_0 can become zero matrix when δ_1 is set to zero. This can happen only if δ_1 divides $k_{0,j}$ for all j. If $k_{i,j}$ has δ_1 as a factor for all i and j, then it is sufficient to prove that $d' = d/\delta_1$ is invertible. So, without loss of generality, we can assume that there exists a $k_{i,j}$ which does not have δ_1 as a factor. Let m be the smallest integer such that δ_1 does not divide $k_{m,j}$ for some j. Then

$$d' = u_{\sigma_x}^{n_1-m} d \delta_1^{-1} = \sum_{i=0}^{n_1-1} u_{\sigma_x}^i \left(\sum_{j=0}^{n_2-1} u_{\sigma_y}^j k'_{i,j} \right)$$

has the property that there exists some j such that δ_1 does not divide $k'_{0,j}$. Also notice that all $k'_{i,j}$ are again polynomials only and not rational functions. And to prove d is invertible it is enough to prove that d' is invertible. So we can assume that there exists a j such that δ_1 does not divide $k_{0,j}$. Now, since $(K(\delta_1,\delta_2),\sigma_2,\delta_2)$ is a cyclic division algebra with center $F(\delta_1,\delta_2,x_1)$, we have $\det(\eta_0) \neq 0$. Thus, we have

$$\rho_d(0,\delta_2) = \prod_{i=0}^{n_1-1} \det(\sigma_x^i(\eta_0)) = \prod_{i=0}^{n_1-1} \sigma_x^i(\det(\eta_0)) \neq 0.$$

This implies $\rho_d(\delta_1,\delta_2)$ is not a zero polynomial because δ_1 and δ_2 are independent transcendental elements over K. ■

If S is the signal set of interest, then we take $L = \mathbb{Q}(S)$. Obtaining 4 algebraically independent transcendental elements over L is not a difficult task as according to Lindemann-Weierstrass Theorem [69], we have that for any two algebraic numbers a_1 and a_2 linearly independent of each other over $\mathbb{Q}$, the numbers e^{a_1} and e^{a_2} are algebraically independent

transcendental numbers. Thus, we can take e^{ja_1}, e^{ja_2}, e^{ja_3} and e^{ja_4} for x, y, δ_1 and δ_2 respectively. We could use e^{a_i} instead but we will see that having all of them on the unit circle will give us information-lossless STBCs.

In Theorem 4.5.6, $K(\delta_1, \delta_2)$ is a cyclic Galois extension of $F(\delta_1, \delta_2)$, if n_1 and n_2 are relatively prime to each other. We give an example to show how to obtain STBC from the division algebra of Theorem 4.5.6.

Example 4.5.8 *Let S be the signal set of interest, say a QAM signal set. Let $n = 4$, i.e, we want STBC for four transmit antennas. Then, we take $F = \mathbb{Q}(j, x, y)$, where x and y are two transcendentals independent over $\mathbb{Q}(j)$. Then $K = F(\sqrt{x}, \sqrt{y})$ is a Galois extension of F with the Galois group $G = \langle \sigma_x, \sigma_y \rangle$, where $\sigma_x : \sqrt{x} \mapsto -\sqrt{x}$ and $\sigma_y : \sqrt{y} \mapsto -\sqrt{y}$. Then, from Theorem 4.5.6, the algebra*

$$(K(\delta_1, \delta_2), G, \phi) = K(\delta_1, \delta_2) \oplus u_{\sigma_x} K(\delta_1, \delta_2) \oplus u_{\sigma_y} K(\delta_1, \delta_2) \oplus u_{\sigma_x} u_{\sigma_y} K(\delta_1, \delta_2)$$

is a division algebra, where δ_1, δ_2 are independent transcendentals elements over K. And

$$\phi(\sigma_x, \sigma_x) = \phi(\sigma_x\sigma_y, \sigma_x) = \delta_1; \qquad \phi(\sigma_y, \sigma_y) = \phi(\sigma_x\sigma_y, \sigma_y) = \delta_2;$$

$$\phi(\sigma_x, \sigma_y) = 1; \quad \textit{and} \quad \phi(\sigma_x\sigma_y, \sigma_x\sigma_y) = \delta_1\delta_2.$$

Substituting for ϕ in (4.10), we have an STBC with codewords of the form

$$\frac{1}{\sqrt{P}} \begin{bmatrix} k_{0,0} & \delta_2\sigma_y(k_{0,1}) & \delta_1\sigma_x(k_{1,0}) & \delta_1\delta_2\sigma_x\sigma_y(k_{1,1}) \\ k_{0,1} & \sigma_y(k_{0,0}) & \delta_1\sigma_x(k_{1,1}) & \delta_1\sigma_x\sigma_y(k_{1,0}) \\ k_{1,0} & \delta_2\sigma_y(k_{1,1}) & \sigma_x(k_{0,0}) & \delta_2\sigma_x\sigma_y(k_{0,1}) \\ k_{1,1} & \sigma_y(k_{1,0}) & \sigma_x(k_{0,1}) & \sigma_x\sigma_y(k_{0,0}) \end{bmatrix} \tag{4.20}$$

where $k_{i,j} = f_{i,j}^{(0)} + f_{i,j}^{(1)}\sqrt{x} + f_{i,j}^{(2)}\sqrt{y} + f_{i,j}^{(3)}\sqrt{xy}$ and $f_{i,j}^{(l)} \in S \subset \mathbb{Q}(j) \subset F$. Thus, we have an STBC over a QAM signal set for 4 transmit antennas.

Corollary 4.5.3 *Let x_i, $i = 0, 1, \ldots, s-1$, be s transcendental elements over a field L containing n_i-th primitive roots of unity, where $n_i, i = 0, 1, 2, \ldots, s-1$ are positive integers.*

Assume in addition that $x_i, i = 0, 1, 2, \ldots, s-1$ *are independent of each other. Let* $F = L(x_0, x_1, \ldots, x_{s-1})$ *and* $K = F(t_0 = x_0^{1/n_0}, t_1 = x_1^{1/n_1}, \ldots, t_{s-1} = x_{s-1}^{1/n_{s-1}})$. *Clearly,* K *is a Galois extension of* F, *with the Galois group as* $G = \left\langle \sigma_{x_0}, \sigma_{x_1}, \cdots, \sigma_{x_{s-1}} \right\rangle$. *Let* $\delta_i, i = 0, 1, 2, \ldots, s-1$ *be* s *commuting indeterminates (one can assume them to be transcendental elements over* F, *independent of each other). Also, let* $u_{\sigma_{x_i}}, i = 0, 1, 2, \ldots, s-1$ *be* s *symbols commuting with each other and satisfying*

$$u_{\sigma_{x_i}}^{n_i} = \delta_i \quad \textit{and} \quad k u_{\sigma_{x_i}} = u_{\sigma_{x_i}} \sigma_{x_i}(k) \ \ \forall\ k \in K(\delta_0, \delta_1, \ldots, \delta_{s-1}).$$

Then, the algebra

$$D = (K(\delta_1, \delta_2, \ldots, \delta_{s-1}), G, \phi)$$

is a division algebra.

Thus, given an abelian group G, we have constructed a division algebra which is a crossed product of a field K and the group G with respect to some cocycle ϕ. Such constructions are called generic constructions of abelian crossed-product algebras.

Example 4.5.9 *Let* S *be the 8-PSK signal set, and* $n = 6$, *i.e., we want STBC for 6 transmit antennas. Then, let* $F = \mathbb{Q}(\omega_8, \omega_3, x_1, x_2)$ *($|x_i| = 1$), where* x_1 *and* x_2 *are two transcendental elements independent over* F. *Then* $K = F(\sqrt{x_1}, \sqrt[3]{x_2})$ *($n_1 = 2, n_2 = 3$) is a Galois extension of* $F(x_1, x_2)$ *with Galois group* $G = \langle \sigma_{x_1}, \sigma_{x_2} \rangle$ *where* $\sigma_{x_1} : \sqrt{x_1} \mapsto -\sqrt{x_1}$ *and* $\sigma_{x_2} : \sqrt[3]{x_2} \mapsto \omega_3 \sqrt[3]{x_2}$. *Let* δ_1, δ_2 *($|\delta_i| = 1$) be two independent transcendental elements over* K. *Then, from Theorem 4.5.6,*

$$D = (K(\delta_1, \delta_2), G, \phi) = \bigoplus_{0 \le i \le 1} \bigoplus_{0 \le j \le 2} u_{\sigma_{x_1}}^i u_{\sigma_{x_2}}^j K(\delta_1, \delta_2)$$

is a division algebra, where $u_{\sigma_{x_1}}$ *and* $u_{\sigma_{x_2}}$ *are symbols satisfying*

$$u_{\sigma_{x_1}}^2 = \delta_1; \quad k u_{\sigma_{x_1}} = u_{\sigma_{x_1}} \sigma_{x_1}(k); \quad u_{\sigma_{x_2}}^3 = \delta_2 \quad \textit{and} \quad k u_{\sigma_{x_2}} = u_{\sigma_{x_2}} \sigma_{x_2}(k).$$

Proceeding in a similar manner as in Example 4.5.8, we get a STBC with codewords as

follows:

$$\frac{1}{\sqrt{6}}\begin{bmatrix} k_{0,0} & \delta_2\sigma_{x_2}(k_{0,2}) & \delta_2\sigma_{x_2}^2(k_{0,1}) & \delta_1\sigma_{x_1}(k_{1,0}) & \delta_1\delta_2\sigma_{x_1}\sigma_{x_2}(k_{1,2}) & \delta_1\delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{1,1}) \\ k_{0,1} & \sigma_{x_2}(k_{0,0}) & \delta_2\sigma_{x_2}^2(k_{0,2}) & \delta_1\sigma_{x_1}(k_{1,1}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{1,0}) & \delta_1\delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{1,2}) \\ k_{0,2} & \sigma_{x_2}(k_{0,1}) & \sigma_{x_2}^2(k_{0,0}) & \delta_1\sigma_{x_1}(k_{1,2}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{1,1}) & \delta_1\sigma_{x_2}^2\sigma_{x_1}(k_{1,0}) \\ k_{1,0} & \delta_2\sigma_{x_2}(k_{1,2}) & \delta_2\sigma_{x_2}^2(k_{1,1}) & \sigma_{x_1}(k_{0,0}) & \delta_2\sigma_{x_1}\sigma_{x_2}(k_{0,2}) & \delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{0,1}) \\ k_{1,1} & \sigma_{x_2}(k_{1,0}) & \delta_2\sigma_{x_2}^2(k_{1,2}) & \sigma_{x_1}(k_{0,1}) & \sigma_{x_1}\sigma_{x_2}(k_{0,0}) & \delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{0,2}) \\ k_{1,2} & \sigma_{x_2}(k_{1,1}) & \sigma_{x_2}^2(k_{1,0}) & \sigma_{x_1}(k_{0,2}) & \sigma_{x_1}\sigma_{x_2}(k_{0,1}) & \sigma_{x_2}^2\sigma_{x_1}(k_{0,0}) \end{bmatrix} \tag{4.21}$$

where $k_{i,j} = f_{i,j}^{(0)} + f_{i,j}^{(1)}\sqrt[3]{x_2} + f_{i,j}^{(2)}\sqrt[3]{x_2^2} + f_{i,j}^{(3)}\sqrt{x_1} + f_{i,j}^{(4)}\sqrt[3]{x_2}\sqrt{x_1} + f_{i,j}^{(5)}\sqrt[3]{x_2^2}\sqrt{x_1}$, *with* $f_{i,j}^{(l)} \in 8-PSK \subset F$. *Thus, we have an STBC over the 8-PSK signal set for 6 transmit antennas.*

Example 4.5.10 *Let S be the 8-PSK signal set, and $n = 12$, i.e., we want STBC for 12 transmit antennas. Then, let $F = \mathbb{Q}(\omega_8, \omega_3, x_0, x_1, x_2)$ ($|x_i| = 1$), where x_0, x_1 and x_2 are transcendental elements independent over F. Then $K = F(\sqrt{x_0}, \sqrt{x_1}, \sqrt[3]{x_2})$ ($n_0 = 2, n_1 = 2, n_2 = 3$) is a Galois extension of $F(x_0, x_1, x_2)$ with Galois group $G = \langle\sigma_{x_0}, \sigma_{x_1}, \sigma_{x_2}\rangle$ where $\sigma_{x_0} : \sqrt{x_0} \mapsto -\sqrt{x_0}$, $\sigma_{x_1} : \sqrt{x_1} \mapsto -\sqrt{x_1}$ and $\sigma_{x_2} : \sqrt[3]{x_2} \mapsto \omega_3\sqrt[3]{x_2}$. Let δ_0, δ_1 and δ_2 ($|\delta_i| = 1$) be independent transcendental elements over K. Then, from Theorem 4.5.6,*

$$D = (K(\delta_1, \delta_2), G, \phi) = \bigoplus_{\substack{0\le h\le 1\\ 0\le i\le 1\\ 0\le j\le 2}} u_{\sigma_{x_0}}^h u_{\sigma_{x_1}}^i u_{\sigma_{x_2}}^j K(\delta_1, \delta_2)$$

is a division algebra, where $u_{\sigma_{x_0}}$, $u_{\sigma_{x_1}}$ and $u_{\sigma_{x_2}}$ are symbols satisfying

$$u_{\sigma_{x_0}}^2 = \delta_0; \quad u_{\sigma_{x_1}}^2 = \delta_1; \quad u_{\sigma_{x_2}}^3 = \delta_2 \quad \text{and} \quad ku_{\sigma_{x_i}} = u_{\sigma_{x_i}}\sigma_{x_i}(k).$$

Proceeding in a similar manner as in Example 4.5.8, we get a STBC with codewords as follows:

$$\frac{1}{\sqrt{12}}\begin{bmatrix} \eta_0 & \delta_0\sigma_{x_0}(\eta_1) \\ \eta_1 & \sigma_{x_0}(\eta_0) \end{bmatrix} \tag{4.22}$$

where

$$\eta_h = \begin{bmatrix} k_{h,0,0} & \delta_2\sigma_{x_2}(k_{h,0,2}) & \delta_2\sigma_{x_2}^2(k_{h,0,1}) & \delta_1\sigma_{x_1}(k_{h,1,0}) & \delta_1\delta_2\sigma_{x_1}\sigma_{x_2}(k_{h,1,2}) & \delta_1\delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{h,1,1}) \\ k_{h,0,1} & \sigma_{x_2}(k_{h,0,0}) & \delta_2\sigma_{x_2}^2(k_{h,0,2}) & \delta_1\sigma_{x_1}(k_{h,1,1}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{h,1,0}) & \delta_1\delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{h,1,2}) \\ k_{h,0,2} & \sigma_{x_2}(k_{h,0,1}) & \sigma_{x_2}^2(k_{h,0,0}) & \delta_1\sigma_{x_1}(k_{h,1,2}) & \delta_1\sigma_{x_1}\sigma_{x_2}(k_{h,1,1}) & \delta_1\sigma_{x_2}^2\sigma_{x_1}(k_{h,1,0}) \\ k_{h,1,0} & \delta_2\sigma_{x_2}(k_{h,1,2}) & \delta_2\sigma_{x_2}^2(k_{h,1,1}) & \sigma_{x_1}(k_{h,0,0}) & \delta_2\sigma_{x_1}\sigma_{x_2}(k_{h,0,2}) & \delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{h,0,1}) \\ k_{h,1,1} & \sigma_{x_2}(k_{h,1,0}) & \delta_2\sigma_{x_2}^2(k_{h,1,2}) & \sigma_{x_1}(k_{h,0,1}) & \sigma_{x_1}\sigma_{x_2}(k_{h,0,0}) & \delta_2\sigma_{x_2}^2\sigma_{x_1}(k_{h,0,2}) \\ k_{h,1,2} & \sigma_{x_2}(k_{h,1,1}) & \sigma_{x_2}^2(k_{h,1,0}) & \sigma_{x_1}(k_{h,0,2}) & \sigma_{x_1}\sigma_{x_2}(k_{h,0,1}) & \sigma_{x_2}^2\sigma_{x_1}(k_{h,0,0}) \end{bmatrix}$$

where $k_{h,i,j} = \sum_{a=0}^{1}\sum_{b=0}^{1}\sum_{c=0}^{2} f_{h,i,j}^{(a,b,c)}\sqrt{x_0}^a\sqrt{x_1}^b\sqrt[3]{x_2}^c$, *with* $f_{h,i,j}^{(a,b,c)} \in 8-PSK \subset F$. *Thus, we have an STBC over the 8-PSK signal set for 12 transmit antennas.*

4.5.3 Rates beyond n symbols per channel use

Till now, we have constructed rate-n, full-rank STBCs using division algebras. Recall that the division algebras we used are the ones with center a transcendental field over $\mathbb{Q}$. Consider the case of the STBCs from cyclic division algebras. The division algebras we considered are of the form $(K(\delta), \sigma, \delta)$ where $K(\delta)$ is a cyclic extension of $F(\delta)$, with δ a transcendental element over F. Recall that F is a field extension of $\mathbb{Q}$ such that it contains the signal set S. Now the codeword matrices with this division algebra will be of the form (4.11) with $f_{\sigma_i,j}$ coming from $F(\delta)$, since the center is $F(\delta)$. And an element of $F(\delta)$ will be of the form $a(\delta)/b(\delta)$, where $a(\delta)$ and $b(\delta)$ are polynomials in δ. So, each entry in (4.11) is of the form $a(\delta)/b(\delta)$. But since, two different pairs of $(a(\delta), b(\delta))$ can give rise to the same $a(\delta)/b(\delta)$, we assume that the entries of (4.11) are of the form $a(\delta)$ only. Thus, if $f_{\sigma_i,j,l}$ come from the signal set S, then our codeword matrices are of the form (4.11), with $f_{\sigma_i,j} = \sum_l f_{\sigma_i,j,l}\delta^l$, where the subscript l can range from 0 to any positive integer. With this, our STBC constructed from the division algebra $(K(\delta), \sigma, \delta)$ can have arbitrary rate. For instance, the STBC constructed in Example 4.5.1, will have

the codewords of the form as below:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} \sum_l f_{0,0,l}\delta^l + \sum_l f_{0,1,l}\delta^l\sqrt{j} & \delta\left(\sum_l f_{1,0,l}\delta^l - \sum_l f_{1,1,l}\delta^l\sqrt{j}\right) \\ \sum_l f_{1,0,l}\delta^l + \sum_l f_{1,1,l}\delta^l\sqrt{j} & \sum_l f_{0,0,l}\delta^l - \sum_l f_{0,1,l}\delta^l\sqrt{j} \end{bmatrix}.$$

In a similar way, STBCs constructed from other division algebras, as in Section 4.5.2, can have arbitrary rate. But note that in the case of non-cyclic division algebras, each entry of the codeword matrix is a polynomial in more than one transcendental element. Though, we have arbitrary-rate STBCs, for the purpose of clarity, we concentrate only on the rate-n STBCs constructed till the previous subsection.

4.5.4 Mutual Information

In this section, we show that, under certain conditions, our designs arising from the division algebras we have discussed so far achieve capacity, i.e., the STBCs from these division algebras are information-lossless.

Mutual information of STBCs from Brauer division algebras

We show that the type-I STBCs from Brauer division algebras are not information-lossless. Recall from Subsection 4.5.1, that in Brauer division algebras, i.e., (K, σ, ω_l), σ takes x_i to $x_{i+1 \ mod \ n}$. Thus, the LHS of (4.17) is

$$\sum_{i=0}^{n-1} x_{i+j \ mod \ n}\left(x_{i+j' \ mod \ n}\right)^* = \sum_{i=0}^{n-1} \frac{x_{i+j \ mod \ n}}{x_{i+j' \ mod \ n}} \quad (\text{if } |x_i| = 1\ ).$$

Since the x_i's are independent transcendental elements over E, the above expression will not be equal to zero and hence the type-I STBCs from Brauer division algebras are not information-lossless.

The type-II STBCs from Brauer division algebras are information-lossless if $|t| = 1$. This condition that $|t| = 1$ can be met, by choosing $x_1, x_2, \ldots, x_{n-1}$ arbitrarily and then choosing x_0 such that $t = x_0 + \omega_n x_1 + \cdots + \omega_n^{n-1} x_{n-1}$ lies on unit circle. Figure 4.4 shows the capacities of both the type-II and type-II STBCs constructed from Brauer division

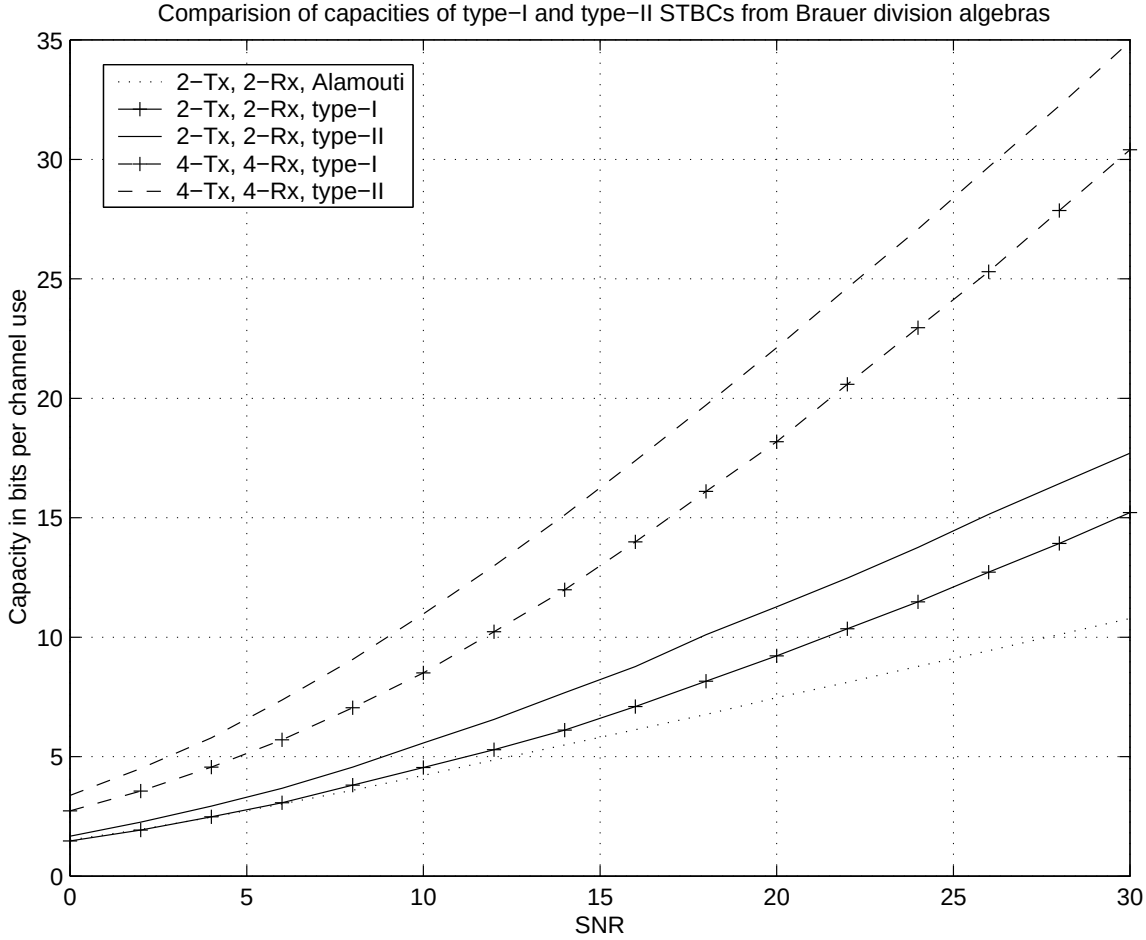


Figure 4.4: Comparison of capacities of type-I and type-II STBCs from Brauer division algebras. The plain solid curve is the capacity of the channel for 2-transmit and 2-receive antennas. And the plain dashed curve is the capacity of the channel for 4-transmit and 4-receive antennas.

algebras. It can be seen from the figure that the information loss in type-I STBCs is less than the loss due to the Alamouti code.

Mutual information of STBCs from tensor-product division algebras

In the following theorem, we show that the STBCs constructed in Subsection 4.5.2 are information-lossless.

Theorem 4.5.7 *Let K, F, x_i, δ_i be as in Theorem 4.5.6 with $|x_i| = |\delta_i| = 1$ for all $0 \leq i \leq s-1$. Then, the STBC arising from the division algebra $D = (K(\delta_0, \delta_1, \ldots, \delta_{s-1}), G, \phi)$ is information-lossless.*

Proof: It is sufficient to prove that

$$\sum_{i_0,\ldots,i_{s-1}} \left[\sigma_0^{j_0}\ldots\sigma_{s-1}^{j_{s-1}}\left((x_0')^{i_0}\ldots(x_{s-1}')^{i_{s-1}}\right)\right]^* \left[\sigma_0^{j_0'}\ldots\sigma_{s-1}^{j_{s-1}'}\left((x_0')^{i_0}\ldots(x_{s-1}')^{i_{s-1}}\right)\right] = 0 \tag{4.23}$$

if $(j_0, j_1, \ldots, j_{s-1}) \neq (j_0', j_1', \ldots, j_{s-1}')$. Since, each of σ_i's act as identity on x_j' if $i \neq j$, and $\sigma_i(x_i') = x_i'\omega_{n_i}$, LHS of (4.23) can be written as

$$\sum_{i_0,\ldots,i_{s-1}} \left\{\left[(x_0')^{i_0}\omega_{n_0}^{i_0 j_0}\right]\cdots\left[(x_{s-1}')^{i_{s-1}}\omega_{n_{s-1}}^{i_{s-1}j_{s-1}}\right]\right\}^* \left\{\left[(x_0')^{i_0}\omega_{n_0}^{i_0 j_0'}\right]\cdots\left[(x_{s-1}')^{i_{s-1}}\omega_{n_{s-1}}^{i_{s-1}j_{s-1}'}\right]\right\}.$$

Since $|x_i| = 1$ for all i, the above expression can be written as

$$\sum_{i_0,\ldots,i_{s-1}} \left[\omega_{n_0}^{i_0(j_0'-j_0)}\right]\cdots\left[\omega_{n_{s-1}}^{i_{s-1}(j_{s-1}'-j_{s-1})}\right].$$

Expanding the above sum with respect to each variable, we have

$$\sum_{i_0}\left\{\omega_{n_0}^{i_0(j_0'-j_0)}\sum_{i_1}\left[\omega_{n_1}^{i_1(j_1'-j_1)}\cdots\left(\omega_{n_{s-2}}^{i_{s-2}(j_{s-2}'-j_{s-2})}\sum_{i_{s-1}}\omega_{n_{s-1}}^{i_{s-1}(j_{s-1}'-j_{s-1})}\right)\right]\right\} = 0.$$

The rest follows from Theorem 4.4.1. ∎

From the above theorem, it follows that the designs of Examples 4.5.8, 4.5.9 and 4.5.10 achieve capacity.

Theorem 4.5.8 *Let D_i, $i = 0, 1, 2, \ldots, s-1$ be s number of crossed-product division algebras.Let each of the STBCs arising from these division algebras be information-lossless. Then the STBC arising from the division algebra $D = D_0 \otimes_F D_1 \otimes_F \cdots \otimes_F D_{s-1}$ is also information-lossless if $|\phi_i(.,.)| = 1$ for all $i = 0, 1, 2, \ldots, s-1$, where ϕ_i is a cocycle for the division algebra D_i.*

The above theorem can be proved in a similar manner as in Theorem 4.5.7.

4.6 Decoding and Simulation Results

Maximum Likelihood (ML) decoding of our STBCs in general involves exhaustive search which increases exponentially with the number of transmit antennas. In [63], sphere decoder was proposed, which uses the algorithm to find the closest lattice point to a given point [62]. This algorithm uses the fact that the column rank of the generator matrix of the lattice, is at least the number of dimensions in the lattice. Damen *et al.* in [64], have shown that sphere decoder can be applied for multiple antenna systems if perfect CSI is known at the receiver. If $\mathbf{f}$ is the transmitted vector from n antennas, we have

$$\mathbf{x} = \sqrt{\frac{\rho}{n}} H\mathbf{f} + \mathbf{w} \tag{4.24}$$

where $\mathbf{x}$ is the received $r \times 1$ vector (r receive antennas), H is the $n \times r$ channel matrix and $\mathbf{w}$ is the AWGN. Then, the lattice representation of the system model is given by

$$\mathbf{x}' = \sqrt{\frac{\rho}{n}} H'\mathbf{f}' + \mathbf{w}' \tag{4.25}$$

where

$$\begin{aligned}
\mathbf{x}' &= [\mathcal{R}e(\mathbf{x}^T)\mathcal{I}m(\mathbf{x}^T)]^T, \\
\mathbf{f}' &= [\mathcal{R}e(\tilde{\mathbf{f}}^T)\ \mathcal{I}m(\tilde{\mathbf{f}}^T)]^T, \\
H' &= \begin{bmatrix} \mathcal{R}e(H) & -\mathcal{I}m(H) \\ \mathcal{I}m(H) & \mathcal{R}e(H) \end{bmatrix}, \\
\mathbf{w}' &= [\mathcal{R}e(\mathbf{w})^T\ \mathcal{I}m(\mathbf{w})^T]^T.
\end{aligned}$$

Since, the channel matrix H is of full rank almost surely, the equivalent channel matrix, H', is also of full rank. Hence, the sphere decoder can be applied whenever f is from a constellation which is a subset of a lattice. Hence, SD achieves ML performance with a significantly reduced complexity which is roughly cubic in n at high SNRs [65]. Though PSK constellations are not a subset of any lattice, we can still use the sphere decoder, known as complex sphere decoder, as shown by Hochwald and Brink in [61]. The

algorithm for the case of a PSK constellation searches through the phase angles of the constellation points instead of the lattice point coordinates and since the phase angles of the constellation points are integer multiples of $2\pi/M$ (for M-PSK), the search is over a finite set. The complexity of complex sphere decoder is less than the complexity of the sphere decoder for lattice constellations. This is because we search for n points in the case of complex sphere decoder, while we search for $2n$ points in the case of lattice sphere decoder.

In our case, the equivalent channel model is

$$\widehat{\mathbf{x}} = \sqrt{\frac{\rho}{n}} \underbrace{\frac{1}{\sqrt{P}} \mathcal{H} \Phi}_{\widehat{\mathbf{H}}} \mathbf{f} + \widehat{\mathbf{w}}.$$

Since, the rank of the matrix $\mathcal{H}$ is $\min(nr, n^2)$ and the matrix Φ is invertible, the rank of the matrix $\widehat{\mathbf{H}}$ is also the $\min(nr, n^2)$. Now, since the rate of our STBCs is n, we can use the sphere decoder efficiently if $\min(nr, n^2) \geq n^2$, which implies that the number of receive antennas is at least the number of transmit antennas. However, if the number of receive antennas is less than the number of transmit antennas, we can use the generalized sphere decoder proposed in [66], which involves more computational complexity. However, we can still use the sphere decoder if we decrease the rate of our STBC. If the number of receive antennas is r, then the rate of our STBC has to be r for efficient use of sphere decoder.

4.6.1 Capacity approaching codes

In this section, we present simulation results for 2,3 and 4 transmit antennas with 2, 3 and 4 receive antennas respectively, over 4-QAM and 16-QAM signal sets. Figure 4.5 shows the plots for 2 transmit and 2 receive antennas. We used the STBC of Example 4.3.5, with $\delta = e^{0.5j}$. This value of δ is chosen arbitrarily. It can be seen from the figure that with our code, we gain by about 3 dB over the uncoded case at 10^{-4} BER and by about 0.75 dB, at 10^{-6} BER, over the STBC of [22](named as $B_{2,\phi}$), which is known to be one

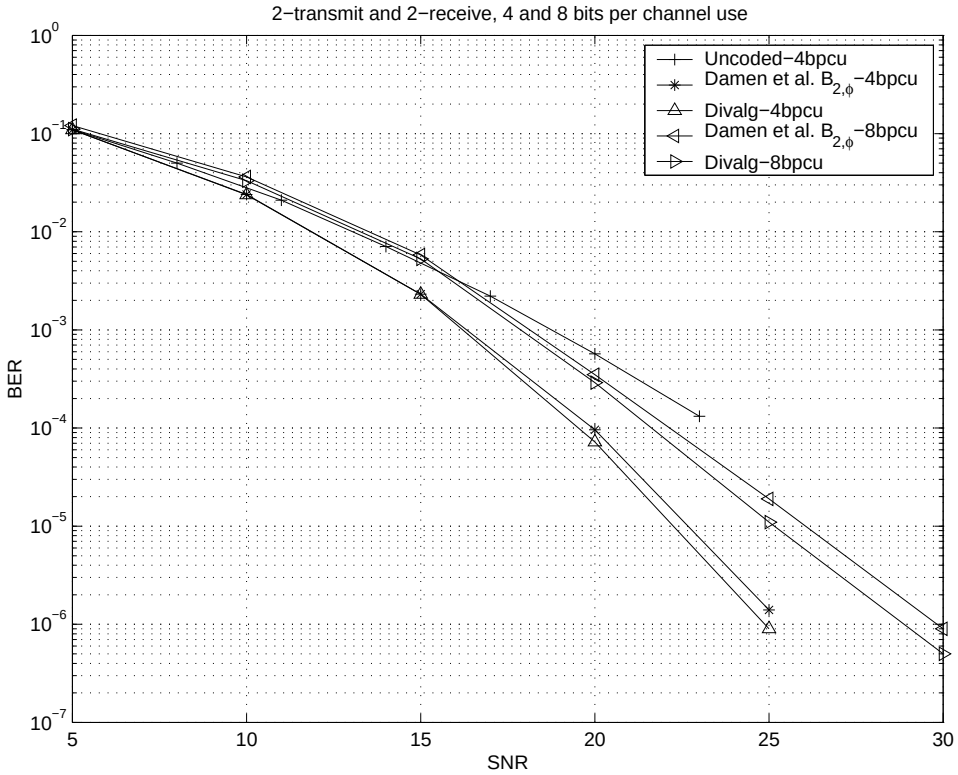


Figure 4.5: Comparison of STBCs with 2 transmit and 2 receive antennas

of the best codes. By choosing δ to maximize the coding gain, we can further improve the performance of our STBC.

Figure 4.6 shows the plots for 3 transmit and 3 receive antennas. The STBC we used is from Example 4.5.2. We gain by about 4 dB over the uncoded case at 10^{-4} BER.

Figure 4.7 shows the plots for 4 transmit and 4 receive antennas. We used the following STBC (obtained with $F = \mathbb{Q}(j)$ and $K = F(\omega_{16})$):

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{4}} \begin{bmatrix} g_{0,0} & \delta g_{1,3} & \delta g_{2,2} & \delta g_{3,3} \\ g_{0,1} & g_{1,0} & \delta g_{2,3} & \delta g_{3,2} \\ g_{0,2} & g_{1,1} & g_{2,0} & \delta g_{3,3} \\ g_{0,3} & g_{1,2} & g_{2,1} & g_{3,0} \end{bmatrix} \right\}$$

where $g_{i,j} = \sum_{l=0}^{3} f_{j,l}(j^i \omega_{16})^l$ and $f_{i,j} \in S \subset F$ for $i, j = 0, 1, 2, 3$ and $\delta = e^{0.5j}$ (chosen arbitrarily). We gain by about 5 dB, at 10^{-5} BER, over the uncoded and by about

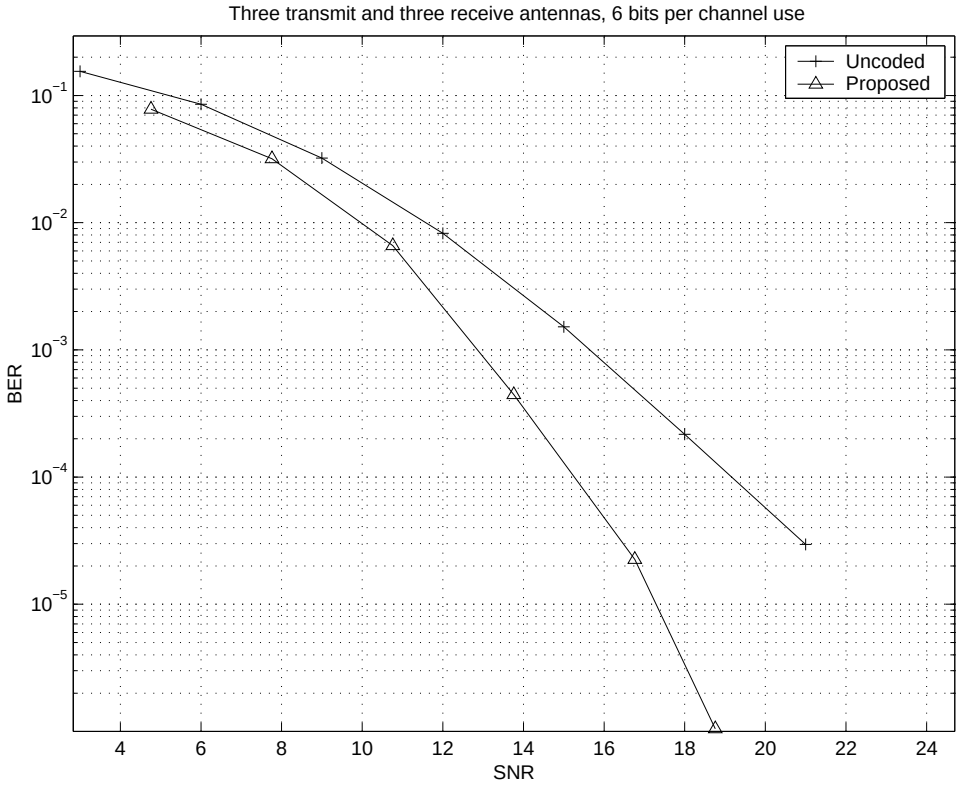


Figure 4.6: Comparison of STBCs with 3 transmit and 3 receive antennas

0.8 dB, at 10^{-6} BER, over the STBC of [43], which is claimed to maximize the mutual information.

Figure 4.8 shows the performance of the STBCs obtained using the division algebras of Section 4.5.2. The division algebra construction-1 curve is for the STBC of Example 4.5.8, with $x_1 = e^{j\sqrt{2}}, x_2 = e^{j\sqrt{3}}$ and $\delta_1 = e^{j\sqrt{5}}, \delta_2 = e^{j\sqrt{7}}$. These values are chosen arbitrarily. The division algebra construction-2 curve is for the same STBC with $x_1 = e^{j\sqrt{2}}, x_2 = e^{j\sqrt{3}}$ and $\delta_1 = e^{j\sqrt{0.23}}, \delta_2 = e^{j\sqrt{0.26}}$. The values of x_1 and x_2 are chosen arbitrarily, while the values of δ_1 and δ_2 are chosen to be close to the value of δ in STBC used in Figure 4.7. We can see that the STBC, where the parameters x_1, x_2, δ_1 and δ_2 are chosen arbitrarily, performs better than the STBC of [43] by about 0.25 dB, but is poorer than the STBC constructed from cyclic division algebra by about 0.5dB. However, the STBC, for which the x_1, x_2 are chosen arbitrarily and δ_1, δ_2 are chosen close to δ, performs better than the STBC of [43] by about 0.9 dB, and better than the STBC from cyclic division algebra by

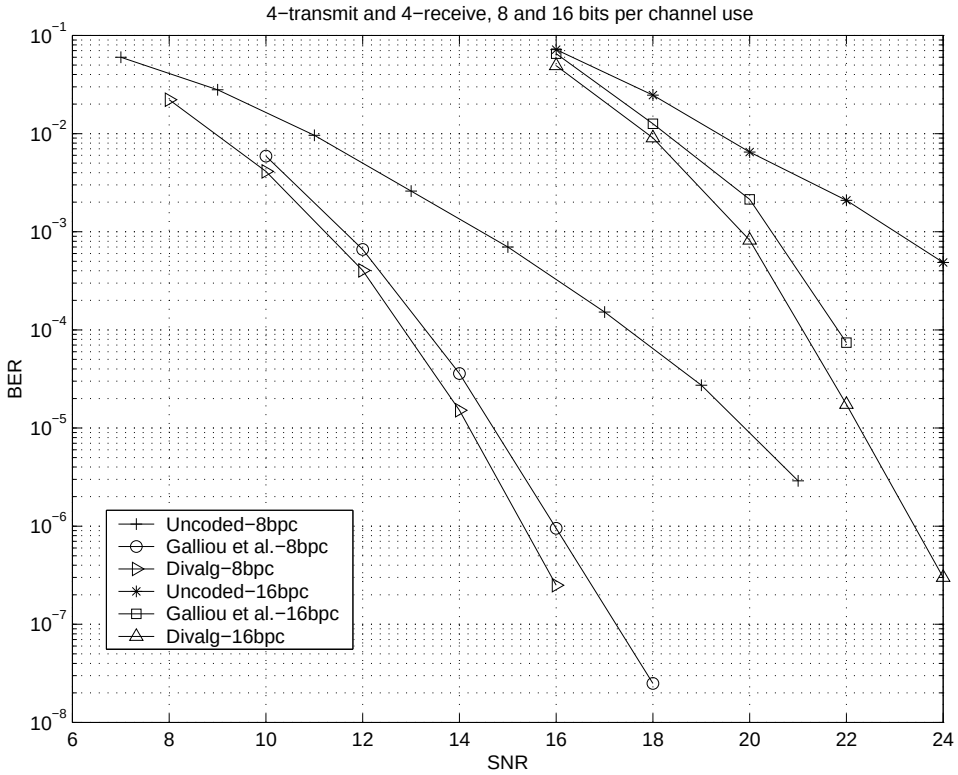


Figure 4.7: Comparison of STBCs with 4 transmit and 4 receive antennas

about 0.1dB. We could perform even better by choosing a better x_1, x_2, δ_1 and δ_2.

From these simulation results and [61], it can be seen that our codes are approximately 1 dB away from the capacity of the channel with QAM symbols as input.

4.7 Summary

In this chapter,

- Using crossed-product algebras, we have constructed arbitrary rate STBCs over apriori specified arbitrary finite subsets of the complex field $\mathbb{C}$. In particular, when the crossed-product algebras are division algebras, we get full-rank STBCs.
- We have shown that Alamouti code and the quasi-orthogonal design of [16] are special cases of our constructions.
- We have also shown that our constructions give STBCs with rank and coding gain

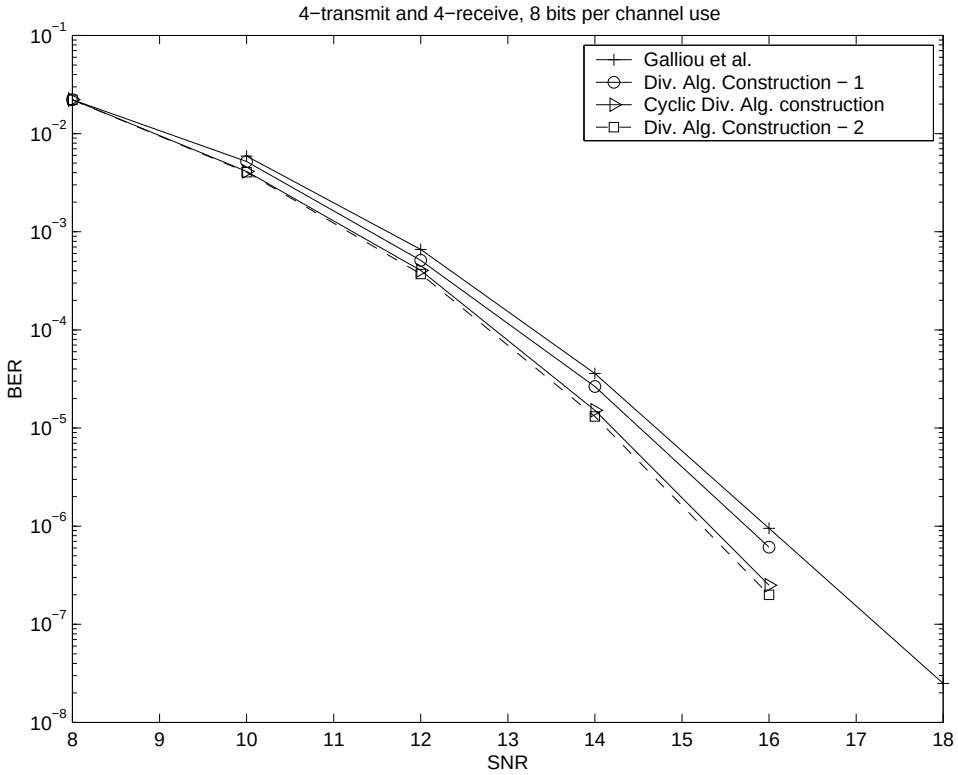


Figure 4.8: Comparison of STBCs with 4 transmit and 4 receive antennas

same as that of the STBCs obtained using field extensions [39].

- We have given a sufficient condition for our STBCs under which they are information-lossless.

- We have identified two classes of division algebras that are crossed-product algebras and constructed rate-n, full-rank STBCs from these crossed-product division algebras. These STBCs include the STBCs of [39, 40] as special cases.

- We have proved that the STBCs obtained from the crossed-product division algebras in this chapter, are information-lossless.

- We have presented simulation results to show that we perform better than the best known codes and can do even better if the best codes from division algebras are used. Also, the simulation results show that we are about 1 dB away from the capacity of the channel with QAM as the input [61].

Chapter 5

Asymptotic-Information-Lossless Designs and Diversity-Multiplexing Tradeoff

In this chapter, we introduce the notion of Asymptotic-Information-Losslessness and then discuss its significance in the context of diversity-multiplexing tradeoff of a given scheme.

The content of this chapter is organized as follows: In the next section, we present in brief, an introduction to the diversity-multiplexing tradeoff of any given scheme and discuss the tradeoff achieved by some well known schemes. In Section 5.2, we define asymptotic-information-lossless STBCs and show that asymptotic-information-losslessness is a necessary condition for achieving the optimal diversity-multiplexing tradeoff. In the same section, we discuss the tradeoff achievability of some well known codes like STBCs from OD and QOD. We obtain lower bound on the diversity-multiplexing tradeoff for the STBCs obtained from field extensions [39] and non-commutative division algebras [39, 40] in Section 5.3 and 5.4 respectively. In Section 5.5, we present simulation results for 2, 3, and 4 transmit antennas and show that the DA codes achieve the optimal diversity-multiplexing tradeoff.

[1]Part of the results presented in this chapter are available in publications [57–59].

5.1 Introduction and Preliminaries

In this section, for the sake of completeness, we shall recall some basics of MIMO systems.

Let $\mathcal{C}$ be an $n_t \times l$ STBC for n_t transmit antennas. Then, if $\mathbf{X} \in \mathcal{C}$ is the codeword transmitted, we have

$$\mathbf{Y} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\mathbf{H}\mathbf{X} + \mathbf{W} \tag{5.1}$$

where $\mathbf{Y} \in \mathbb{C}^{n_r \times l}$ is the received matrix, $\mathbf{H} \in \mathbb{C}^{n_r \times n_t}$ is the channel matrix with entries independent complex Gaussian with zero mean and unit variance and $\mathbf{W} \in \mathbb{C}^{n_r \times l}$ is the additive noise with entries independent complex Gaussian with zero mean and unit variance. Under the assumption that $\mathcal{E}[tr(\mathbf{X}\mathbf{X}^*)] = n_t l$, the average signal-to-noise (SNR) at each receive antenna is SNR. We have seen in Chapter 2, that at high SNRs, the pair-wise error probability that the received matrix $\mathbf{Y}$ is decoded to a codeword matrix $\mathbf{X}' \neq \mathbf{X}$ is

$$P(\mathbf{X} \to \mathbf{X}') = \left(\prod_{i=1}^{\Lambda} \lambda_i^2\right)^{-n_r} \mathsf{SNR}^{-n_r\Lambda}$$

where $\lambda_1, \lambda_2, , \ldots, \lambda_\Lambda$ are the Λ non-zero singular values of $\Delta = \mathbf{X} - \mathbf{X}'$. The gain due to the spatial diversity provided by n_t transmit and n_r receive antennas is, quantitatively, termed as *diversity gain of the code* $\mathcal{C}$, d, and is equal to the negative of the exponent of SNR in the above expression. The value of d, intuitively, corresponds to the number of paths with independent fades that a symbol passes through. Note that, here the diversity gain is defined under the assumption that the data rate is fixed for all SNRs. Full-rank STBCs have been constructed by several authors and some of the important and well known constructions are Orthogonal Designs (OD) [5,6,8,10], Coordinate Interleaved Orthogonal designs (CIODs) [7, 12] Quasi-orthogonal designs (QODs) [14–17], STBCs from division algebras [34–37, 39–41] and quaternionic lattices [43, 44], Diagonal Algebraic STBCs [18], Space-Time constellation rotation STBCs [19], Threaded Algebraic STBCs [21, 22] and STBCs from maximal rank distance codes [47].

Another advantage due to the multiple transmit and receive antennas is based on capacity analysis of the channel. At high SNRs, the capacity of a Rayleigh fading channel

with n_t transmit and n_r receive antennas is

$$C(n_t, n_r, \mathsf{SNR}) = \min\{n_t, n_r\} \log \mathsf{SNR} + O(1).$$

From the above expression it is clear that the achievable data rate increases with SNR as $\min\{n_t, n_r\} \log \mathsf{SNR}$. Since, this value is $\min\{n_t, n_r\}$ times the capacity of a single-antenna channel, a multiple-antenna channel can be viewed as $\min\{n_t, n_r\}$ parallel channels and hence $\min\{n_t, n_r\}$ is the total number of degrees of freedom (independent information symbols that can be communicated). Since the capacity increases linearly with $\log \mathsf{SNR}$, it is expected that the rate of data transmission also increase linear with $\log \mathsf{SNR}$. This advantage due to the multiple antennas is called *spatial multiplexing* [48]. If the data rate increases with SNR as $r \log \mathsf{SNR}$, we say that a multiplexing gain of r is achieved. Some of the schemes that exploit spatial multiplexing are Bell LAbs Space-Time (BLAST) architectures [49] like Diagonal BLAST (D-BLAST) and Vertical BLAST (V-BLAST).

Though most of the research in designing good STBCs has been either in obtaining the full-diversity codes or codes with maximum spatial multiplexing, it has been shown recently in [50], that both diversity and spatial multiplexing can be obtained simultaneously but with a fundamental tradeoff between them. We will first give some necessary definitions and then briefly discuss the optimal tradeoff curve obtained by Zheng and Tse in [50].

Let $\mathcal{C}(\mathsf{SNR})$ be the code corresponding to the SNR level SNR and the data rate in bits per channel use achieved by $\mathcal{C}(\mathsf{SNR})$ be $R(\mathsf{SNR})$. Then, the set of all codes $\{\mathcal{C}(\mathsf{SNR})\}$ is called a scheme.

Definition 5.1.1 ([50]) *A scheme $\{\mathcal{C}(\mathsf{SNR})\}$ is said to achieve a spatial multiplexing gain r and diversity gain d if*

$$\lim_{\mathsf{SNR}\to\infty} \frac{R(\mathsf{SNR})}{\log \mathsf{SNR}} = r \quad \textit{and} \quad \lim_{\mathsf{SNR}\to\infty} \frac{\log P_e}{\log \mathsf{SNR}} = -d$$

where P_e is the error probability.

Following the notation of [50], we use $\doteq$ for exponential equality. Thus, $2^R(\mathsf{SNR}) \doteq \mathsf{SNR}^r$ and $P_e \doteq \mathsf{SNR}^{-d}$. Similarly, we use $\dot{\geq}$ and $\dot{\leq}$ for exponential inequalities.

Though a scheme means a family of codes, one for each SNR level, a simple way of describing a scheme is to give a design. We recall the definition of a design from Chapter 2.

Definition 5.1.2 *A rate-k/l, $n \times l$* **design** *over a subfield K of the complex field $\mathbb{C}$, is an $n \times l$ matrix $\mathbf{M}(x_1, x_2, \ldots, x_k)$ with entries K-linear combinations of k variables and their conjugates. We call $\mathbf{M}$ a full-rank design over a field F if every finite subset of the set $E = \{\mathbf{M}(x_1, x_2, \ldots, x_k) | x_i \in F, i = 1, 2, \ldots, k\}$, is a full-rank STBC.*

Restricting the variables x_i to come from a finite subset, called the signal set or constellation, of the field F, we get a full-rank STBC. Notice that though x_i come from a signal set, the complex symbols that are transmitted can be from a different set.

By changing the signal sets such that their size increases with SNR we get a scheme. Thus, a scheme can be described by a design and a class of signal sets. For example, the Alamouti code is a rate-1, 2×2 design over the field of complex numbers, $\mathbb{C}$. Similarly, the 4×4 real orthogonal design is a rate-1, 4×4 design over the real field $\mathbb{R}$ [6]. Designs over other subfields of $\mathbb{C}$ have been studied in [37, 39, 40]. Thus, a design and a signal set jointly constitute an STBC. By changing the signal sets such that their size increases with SNR we get a scheme. Thus, a scheme can be described by a design and a class of signal sets.

Zheng and Tse in [50] have obtained lower and upper bound on the optimal diversity-multiplexing tradeoff curve. The upper bound is given by the exponent d_{out} of the outage probability. The lower bound for the case $l \geq n_t + n_r - 1$ is again given by d_{out}. Hence, for the case $l \geq n_t + n_r - 1$, the optimal diversity-multiplexing tradeoff is $d(r) = d_{out}(r) = (n_t - r)(n_r - r)$. For the case $l < n_t + n_r - 1$, the lower bound does not match with the upper bound and hence there is no exact expression for the optimal tradeoff. When $n_t = n_r = 2$ and $l \geq 2$, however, it has been proved that the lower bound and the upper bound coincide. Figure 5.1 shows these bounds for some cases.

We say a **design achieves the optimal tradeoff** if there exists a class of signal sets, one for each SNR level, such that the scheme described by the design and the class of

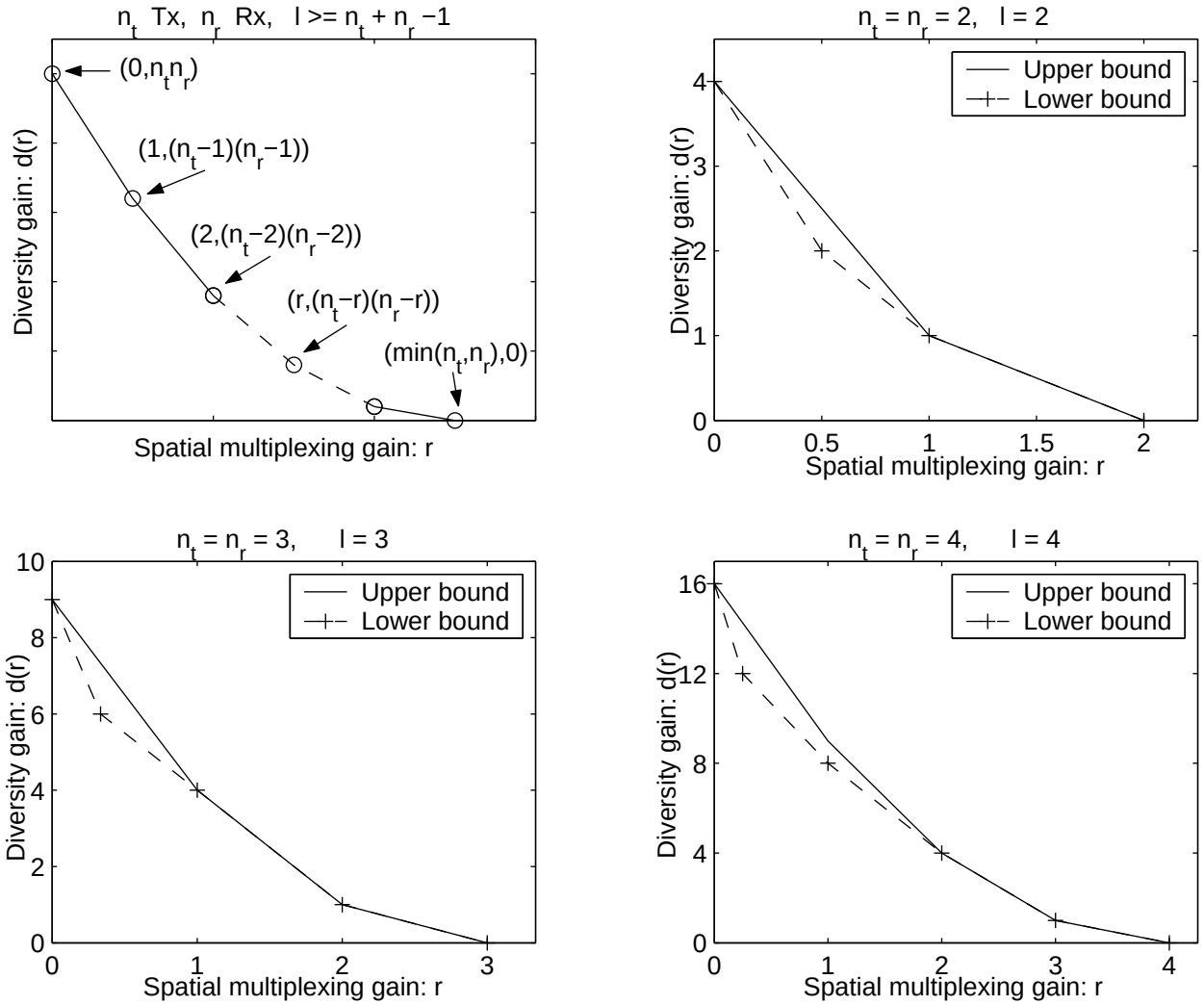


Figure 5.1: Optimal diversity-multiplexing tradeoff for some specific cases

signal sets achieves the optimal tradeoff. If a scheme is described by a full-rank design over a field F and a class of signal sets which are subsets of F, then the maximum diversity gain achieved by such a scheme is the diversity gain of any code in the scheme. This can be seen as follows:

$$P_e(\mathbf{X}) \dot{\geq} \sum_{\mathbf{X}' \neq \mathbf{X}} P(\mathbf{X} \to \mathbf{X}').$$

Since $R \doteq r \log \mathsf{SNR}$, where $r = 0$, the data rate is fixed and the number of codewords

and the coding gain are independent of SNR and hence we have

$$P_e \doteq \mathsf{SNR}^{-n_t n_r}.$$

Thus, a scheme which is a family of full-rank codes achieves the point $(0, n_t n_r)$ of the optimal diversity-multiplexing tradeoff. Schemes like V-BLAST achieve the point $(\min\{n_t, n_r\}, 0)$ of the optimal tradeoff curve. It is also known that D-BLAST scheme achieves the optimal diversity-multiplexing tradeoff for n number of transmit and n number of receive antennas, under the assumption that the leading and trailing zeros are ignored. However, without any such assumptions, the D-BLAST achieves the point corresponding to zero multiplexing gain, but not the point corresponding to the zero diversity gain. Figure 5.2 and Figure 5.3 show the tradeoff achieved by Alamouti and BLAST schemes respectively. The tradeoff shown for the BLAST schemes is with successive nulling and canceling detection. It is known that D-BLAST achieves the optimal tradeoff with minimum mean square error detection, ignoring the initial and trailing zeros.

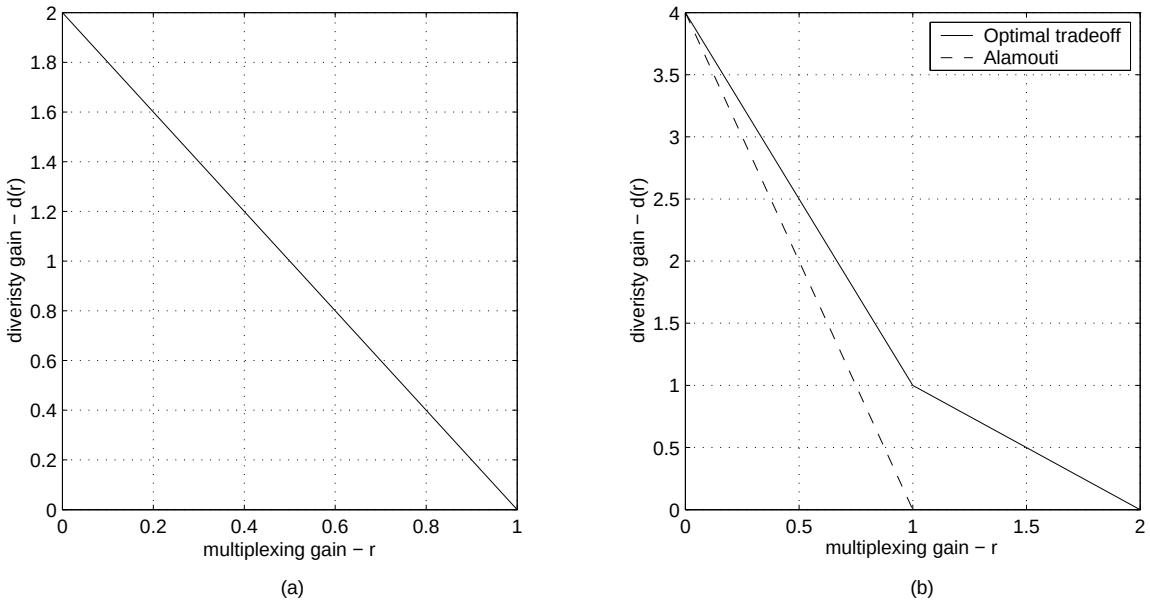


Figure 5.2: The diversity-multiplexing tradeoff achieved by Alamouti scheme (a) 1 receive antenna, (b) 2 receive antennas.

In [51], a scheme for 2 transmit and 2 receive antennas was constructed which achieves

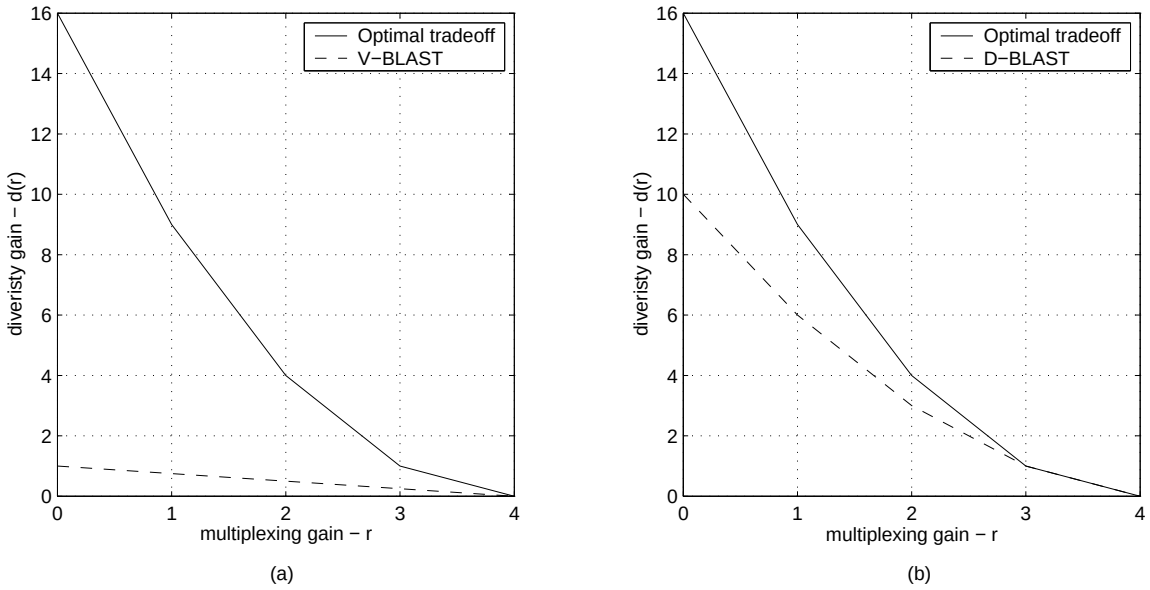


Figure 5.3: The diversity-multiplexing tradeoff achieved by BLAST schemes for 4 transmit and 4 receive antennas (a) V-BLAST, (b) D-BLAST.

the optimal tradeoff for all $0 \leq r \leq 2$. In [52], it has been shown that the lattice coding and decoding achieve the optimal tradeoff.

5.2 Asymptotic-Information-Lossless Designs

In this section, we define Asymptotic-Information-Lossless (AILL) Designs and show that it is a necessary condition for achieving the optimal diversity-multiplexing tradeoff. We also give a sufficient condition under which a design is AILL.

If $\mathbf{A}$ is a $n \times m$ complex matrix, then let $\widehat{\mathbf{A}}$ denote the $2n \times 2m$ real matrix

$$\begin{bmatrix} \mathbf{A}_I & -\mathbf{A}_Q \\ \mathbf{A}_Q & \mathbf{A}_I \end{bmatrix}$$

where $\mathbf{A} = \mathbf{A}_I + j\mathbf{A}_Q$. Similarly, if $\mathbf{b}$ is a $n \times 1$ complex vector, then $\widehat{\mathbf{b}}$ denotes the $2n \times 1$ real vector $[\mathbf{b}_I^T \ \mathbf{b}_Q^T]^T$, where $\mathbf{b} = \mathbf{b}_I + j\mathbf{b}_Q$.

Let $\mathbf{X}$ be a rate-k/l, $n_t \times l$ design with $a_1, a_2, \ldots, a_k$ as the variables. Let $\mathbf{a} =$

$[a_1\ a_2\ \cdots\ a_k]^T$. If $\mathbf{X}$ is the design used to describe an STBC, then the received matrix is $\mathbf{Y}$ as in (5.1). We can rewrite (5.1) as

$$\mathbf{y} = \sqrt{\frac{\mathsf{SNR}}{n_t}} \underbrace{\begin{bmatrix} \mathbf{H} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{H} & \cdots & \mathbf{0} \\ \vdots & \vdots & \cdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{H} \end{bmatrix}}_{\mathcal{H}} \underbrace{\begin{bmatrix} \mathbf{X}_1 \\ \mathbf{X}_2 \\ \vdots \\ \mathbf{X}_l \end{bmatrix}}_{\mathbf{x}} + \mathbf{w}.$$

where $\mathbf{y}$ and $\mathbf{w}$ are the column vectors obtained by serializing the columns of $\mathbf{Y}$ and $\mathbf{W}$ respectively and $\mathbf{X}_i$ denotes the i-th column of $\mathbf{X}$. Since the design $\mathbf{X}$ has the entries that are complex linear combinations of the k variables and their complex conjugates, we can rewrite the above equation as

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n_t}} \widehat{\mathcal{H}} \Phi \widehat{\mathbf{a}}$$

where Φ is a $2nl \times 2k$ matrix such that $\Phi\widehat{\mathbf{a}} = \widehat{\mathbf{x}}$. We call the matrix Φ as generator of $\mathbf{X}$. Then, we define the capacity of the design $\mathbf{X}$ as the capacity of the equivalent channel $\tilde{\mathbf{H}} = \widehat{\mathcal{H}}\Phi$ given by

$$C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}, \mathbf{H}) = \frac{1}{2l} \log_2 \left(\det \left(\mathbf{I}_{2n_r l} + \frac{\mathsf{SNR}}{n_t} \tilde{\mathbf{H}} \tilde{\mathbf{H}}^\dagger \right) \right).$$

Clearly, $\mathcal{E}_{\mathbf{H}} \left[C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}, \mathbf{H}) \right] = C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}) \leq C(n_t, n_r, \mathsf{SNR})$.

Definition 5.2.1 *We call* $\mathbf{X}$ *an asymptotic-information-lossless (AILL) design for* n_r *receive antennas if*

$$\lim_{\mathsf{SNR} \to \infty} \frac{C(n_t, n_r, \mathsf{SNR})}{C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR})} = 1.$$

Theorem 5.2.1 *The design* $\mathbf{X}$ *is AILL design for* n_r *receive antennas if and only if the matrix* $\tilde{\mathbf{H}}$ *has rank at least* $\min\{n_t, n_r\} \times 2l$.

Proof: Let the rank of the matrix $\tilde{\mathbf{H}}$ be τ and the singular value decomposition of $\tilde{\mathbf{H}}\tilde{\mathbf{H}}^T$

be $\mathbf{UDV}^T$. Then, we have

$$\begin{aligned} C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}, \mathbf{H}) &= \frac{1}{2l}\log_2\left(\det\left(\mathbf{I}_{2n_rl} + \frac{\mathsf{SNR}}{n_t}\mathbf{UDV}\right)\right) \\ &= \frac{1}{2l}\log_2\left(g(\mathsf{SNR})\right), \end{aligned}$$

where g is a τ-th degree polynomial. Clearly, at high SNRs,

$$C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}) = \frac{\tau}{2l}\log_2 \mathsf{SNR} + O(1).$$

Thus, if $\tau = \min\{n_t, n_r\} \times 2l$, $\mathbf{X}$ is an AILL design and vice versa. ■

Since, the rank of the matrix Φ is bounded above by $2k$, twice the number of variables in the design, and if the design is AILL, then it is necessary but not sufficient that $k \geq l \times \min\{n_t, n_r\}$. The following example gives a design which satisfies the necessary condition but still fails to be an AILL design.

Example 5.2.1 *Let* $\mathbf{X}$ *be the* 2×2 *COD (the Alamouti code) given by* $\begin{bmatrix} x_0 & -x_1^* \\ x_1 & x_0^* \end{bmatrix}$. *Then, the generator matrix of the design* $\mathbf{X}$ *is*

$$\Phi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}.$$

Clearly, the rank of the matrix Φ *is equal to* 2. *Thus, the* 2×2 *COD is AILL for* 1 *receive antenna and Asymptotic-Information-Lossy (AIL) for more than* 1 *receive antennas. For*

1 *receive antenna, let* $\mathbf{H} = [h_1 h_2]$. *Then,* $\widehat{\mathcal{H}}$ *is*

$$\widehat{\mathcal{H}} = \begin{bmatrix} h_{1I} & h_{2I} & 0 & 0 & -h_{1Q} & -h_{2Q} & 0 & 0 \\ 0 & 0 & h_{1I} & h_{2I} & 0 & 0 & -h_{1Q} & -h_{2Q} \\ h_{1Q} & h_{2Q} & 0 & 0 & h_{1I} & h_{2I} & 0 & 0 \\ 0 & 0 & h_{1Q} & h_{2Q} & 0 & 0 & h_{1I} & h_{2I} \end{bmatrix}$$

It can be checked that $\widehat{\mathcal{H}}\Phi\Phi^T\widehat{\mathcal{H}}^T$ *is equal to* $(|h_1|^2 + |h_2|^2)\, I_4$. *Thus, the capacity of the* 2×2 *COD for* 1 *receive antenna is*

$$C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}, H) = \frac{1}{4}\log_2\left(1 + |h_1|^2 + |h_2|^2\right)^4$$

which is same the capacity of the channel. Thus, the 2×2 *COD is also ILL for* 1 *receive antenna.*

Example 5.2.2 *Let* $n_t = 2$. *Let* $\mathbf{X}$ *be the design [39]*

$$\begin{bmatrix} a_0 + za_1 & \delta(a_2 + za_3) \\ a_2 + za_3 & a_0 + za_1 \end{bmatrix}$$

where z *and* δ *are two independent transcendental elements over the rational number field* $\mathbb{Q}$. *This design is obtained using field extensions of* $\mathbb{Q}(j)$ *and is a full-rank design over the field* $\mathbb{Q}(j)$. *Clearly, the number of variables in the design* $\mathbf{X}$ *is* $k = 4$ *and hence the design satisfies the necessary condition* $k \geq l \times \min\{n_t, n_r\}$. *The generator matrix* Φ *of*

this design is

$$\Phi = \begin{bmatrix} 1 & z_I & 0 & 0 & 0 & -z_Q & 0 & 0 \\ 0 & 0 & 1 & z_I & 0 & 0 & 0 & -z_Q \\ 0 & 0 & \delta_I & \delta_I z_I - \delta_Q z_Q & 0 & 0 & -\delta_I z_Q - \delta_Q z_I & \\ 1 & z_I & 0 & 0 & 0 & -z_Q & 0 & 0 \\ 0 & z_Q & 0 & 0 & 1 & z_I & 0 & 0 \\ 0 & 0 & 0 & z_Q & 0 & 0 & 1 & z_I \\ 0 & 0 & \delta_Q & \delta_I z_Q + \delta_Q z_I & 0 & 0 & \delta_I z_I - \delta_Q z_Q & \\ 0 & z_Q & 0 & 0 & 1 & z_I & 0 & 0 \end{bmatrix}.$$

Clearly, the rank of Φ *is* 4 *and hence from Theorem 5.2.1, this design is AIL for* 2 *transmit antennas. However, it is AILL for* 1 *receive antenna. Figure 5.4 shows the capacities of the channel and the above design. Also, shown is the capacity of the Alamouti scheme for 2 receive antennas. It can be seen that while for 1 receive antenna, the loss in the capacity of the above design is a constant independent of* SNR *at high SNRs, the loss in the capacity for 2 receive antennas is increasing with* SNR*. The same is true with Alamouti, except that for one receive antenna, the loss is zero.*

It can be checked that except the Alamouti code, all other complex ODs (CODs) are AIL for any number of receive antennas. The 2×2 COD is AILL for 1 receive antenna and AIL for $n_r \geq 2$ receive antennas. Similarly, the QODs for $n_t = 2, 3, 4$ are AILL for 1 receive antenna and AIL for $n_r \geq 2$ receive antennas. All other QODs and CIODs are AIL for any number of receive antennas.

In [23], codes called Linear Dispersion (LD) codes were constructed to obtain maximum mutual information. The number of variables were chosen to be $\min\{n_t, n_r\} \times l$. It can be checked easily that for all the LD codes presented in [23], the rank of the matrix $\widehat{\mathbf{H}}$ is equal to $\min\{n_t, n_t\} \times l$ and hence all the LD codes of [23] are AILL designs.

Example 5.2.3 (Coordinate Interleaved Orthogonal Desings) *An rate-*k/p*,* $n \times p$ *Coordinate Interleaved Orthogonal Design (CIOD) in the* k*-variables* x_i*,* $i = 0, 1, 2 \ldots, k-$

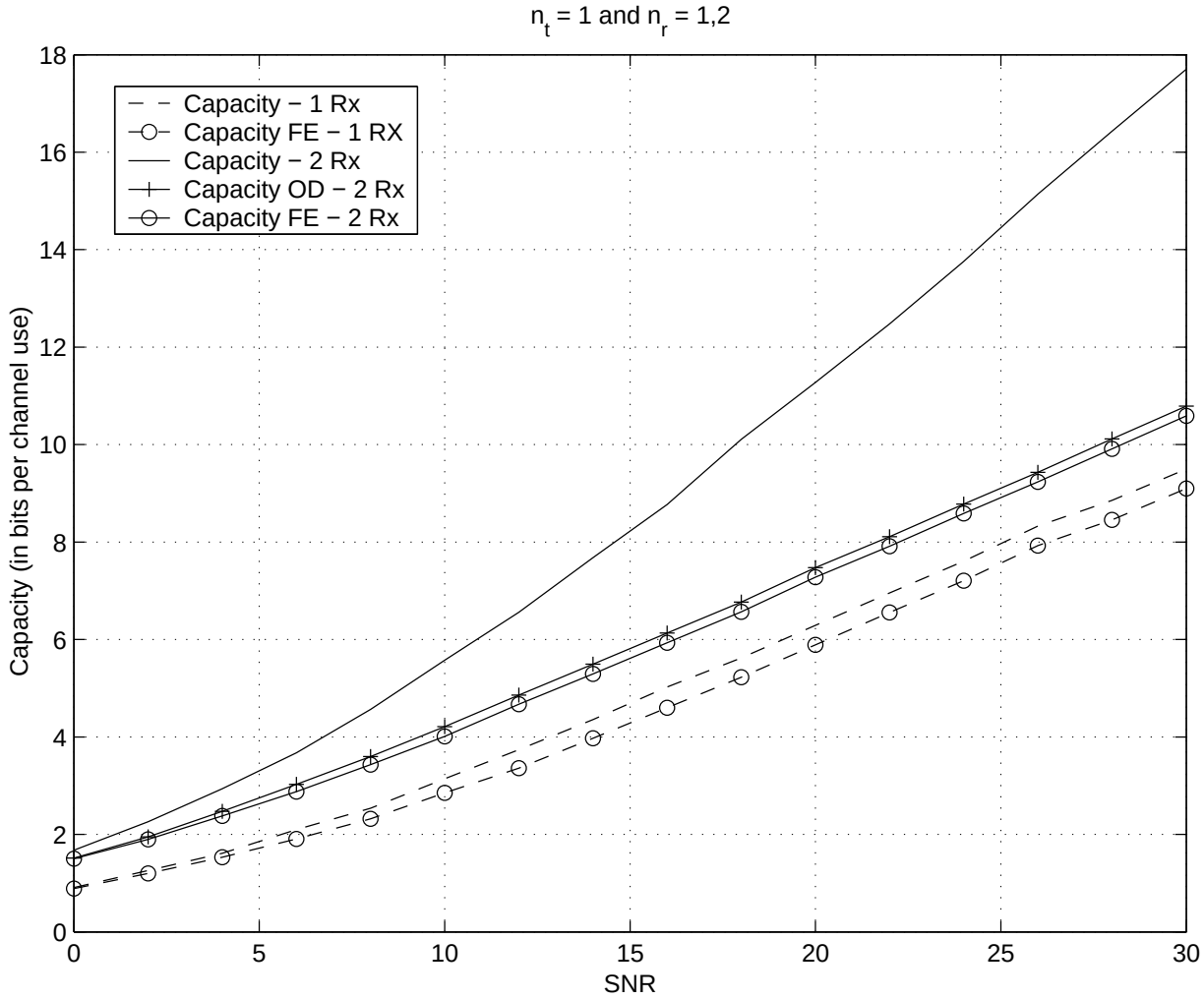


Figure 5.4: Capacities of the actual channel and the design in Example 5.2.2 for 1 and 2 receive antennas.

1 *is an* $n \times p$ *matrix given by*

$$\begin{bmatrix} \Theta_{n/2,n/2}(\tilde{x}_0, \ldots, \tilde{x}_{k/2-1}) & \mathbf{0} \\ \mathbf{0} & \Theta_{n/2,n/2}(\tilde{x}_{k/2}, \ldots, \tilde{x}_{k-1}) \end{bmatrix}$$

where $\Theta_{n/2,n/2}(x_0, x_1, \ldots, x_{n/2-1})$ *is a rate-*k/p *generalized complex linear processing orthogonal design of size* $n/2$ *[6]. It has been shown that rate-*1*,* $n \times p$ *CIOD exists only for*

$n = 2, 3, 4$. *They are*

$$\begin{bmatrix} \tilde{x}_0 & 0 \\ 0 & \tilde{x}_1 \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} \tilde{x}_0 & \tilde{x}_1 & 0 & 0 \\ -\tilde{x}_1^* & \tilde{x}_0^* & 0 & 0 \\ 0 & 0 & \tilde{x}_2 & \tilde{x}_3 \\ 0 & 0 & -\tilde{x}_3^* & \tilde{x}_2^* \end{bmatrix}.$$

The CIOD for 3 *transmit antennas can be obtained by removing a row from the CIOD for* 4 *transmit antennas. It can be seen easily that CIODs are AILL designs for* 2, 3 *and* 4 *transmit antennas and* 1 *receive antennas. Thus, a CIOD for* n_t *transmit antennas is AILL if the QOD for* n_t *transmit antennas is AILL.*

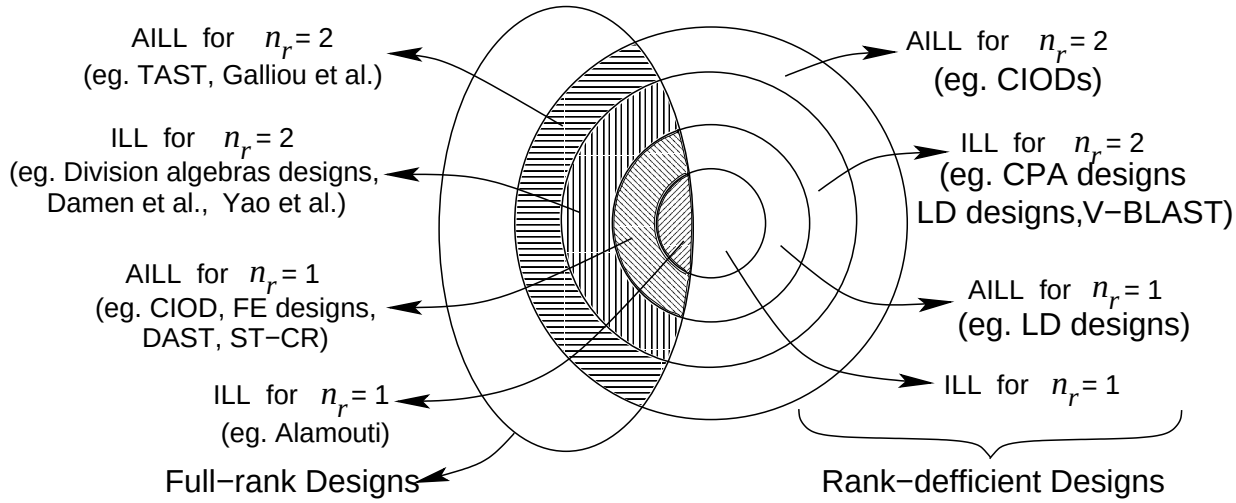


Figure 5.5: Various ILL and AILL designs for $n_t = 2$ transmit antennas. CPA designs means the designs from crossed-product algebras [41]

Most of the well known designs like DAST [18], designs from field extensions [39] are AILL for 1 receive antenna. Figure 5.5 and Figure 5.6 show various ILL designs and AILL designs for $n_t = 2$ and $n_t \geq 3$ transmit antennas. We have identified QODs and CIODs as rank-deficient designs as they are designs over the complex field and are not full-rank in general. However, the STBCs obtained from these designs are full-rank STBCs under certain restrictions on the symbol constellations used.

Corollary 5.2.1 *Let* $\mathbf{X}$ *be a rate-*k/l*,* $n_t \times l$ *AILL design for any number of receive*

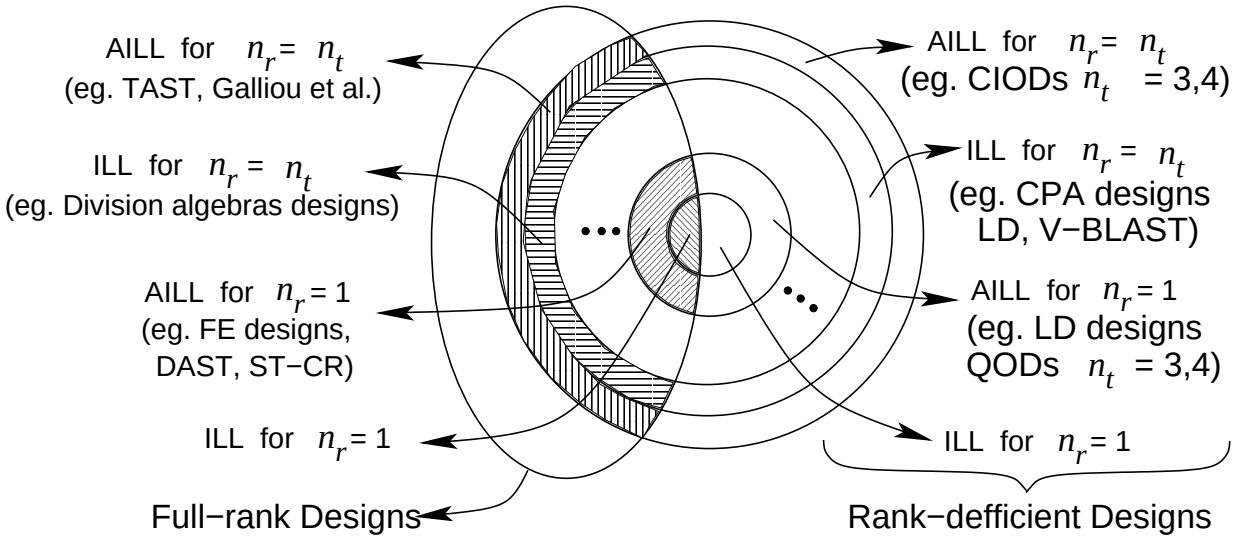


Figure 5.6: Various ILL and AILL designs for $n_t \geq 3$ transmit antennas. CPA designs means the designs from crossed-product algebras [41]

antennas. Then, $k \geq n_t l$.

Example 5.2.4 *Let* $n_t = 2$. *Let* $\mathbf{X}$ *be the design [39, 40]*

$$\begin{bmatrix} a_0 + a_1\sqrt{j} & \delta(a_2 - a_3\sqrt{j}) \\ a_2 + a_3\sqrt{j} & a_0 - a_1\sqrt{j} \end{bmatrix}$$

where δ *(*$|\delta| = 1$*) is a transcendental element over* $\mathbb{Q}$. *This design is a full-rank design over* $\mathbb{Q}(j)$. *The generator matrix* Φ *is*

$$\Phi = \begin{bmatrix} 1 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 1 & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \delta_I & \frac{\delta_I}{\sqrt{2}} - \frac{\delta_Q}{\sqrt{2}} & 0 & 0 & -\delta_Q & -\frac{\delta_I}{\sqrt{2}} - \frac{\delta_Q}{\sqrt{2}} \\ 1 & -\frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 1 & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 & 0 & 1 & \frac{1}{\sqrt{2}} \\ 0 & 0 & \delta_Q & \frac{\delta_I}{\sqrt{2}} + \frac{\delta_Q}{\sqrt{2}} & 0 & 0 & \delta_I & \frac{\delta_I}{\sqrt{2}} - \frac{\delta_Q}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{2}} & 0 & 0 & 1 & -\frac{1}{\sqrt{2}} & 0 & 0 \end{bmatrix}.$$

It is easy to check that the rank of the matrix Φ is 4 and hence is AILL for any number of receive antennas. Also, it is clear that $\Phi\Phi^T = I_{2n_t^2}$ and can be checked that this design is, in fact, an ILL design. This design is same as the design obtained in [44] with $\delta = 1+2j$, in which case the design is not ILL but continues to be AILL.

Analogous to the sufficient condition that full-rank designs achieve the point corresponding to the zero multiplexing gain of the optimal diversity-multiplexing tradeoff, we now give a necessary and sufficient condition for any design to achieve the point corresponding to the zero diversity gain of the optimal diversity-multiplexing tradeoff. With $R = r \log \mathsf{SNR}$ as the data rate we have the codeword error probability given by

$$P_e(\mathsf{SNR}) \doteq P_{out,\mathbf{X}}(r) + P(\text{error} \mid \text{no outage}) \geq P_{out}(r) \tag{5.2}$$

where $P_{out,\mathbf{X}}(r) = P(C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}) \leq r \log \mathsf{SNR})$. Clearly, $P_{out,\mathbf{X}}(r)$ is greater than or equal to the channel outage probability $P_{out}(r)$ given by $P(C(n_t, n_r, \mathsf{SNR}) \leq R)$. From (5.2) note that

$$d_{\mathbf{X}}(r) \leq d_{out,\mathbf{X}}(r) \leq d_{out}(r)$$

where $P_{out,\mathbf{X}}(r) \doteq \mathsf{SNR}^{-d_{out,\mathbf{X}}(r)}$ and $P_{out}(r) \doteq \mathsf{SNR}^{-d_{out}(r)}$. This tells us that the optimal diversity-multiplexing tradeoff curve is upper bounded by $d_{out}(r)$ [50]. Since, the number of variables in the design $\mathbf{X}$ is k, the capacity of the design at high SNRs is equal to $\frac{s}{l}\log_2 \mathsf{SNR} + O(1)$, where s is the rank of the matrix Φ. Thus, as long as the data rate is less than or equal to $\frac{s}{l}\log_2 \mathsf{SNR}$, it is possible to have a reliable communication using the design $\mathbf{X}$. But, if the data rate is greater than $\frac{s}{l}\log_2 \mathsf{SNR}$, no matter what the value of SNR is, the error probability is bounded away from zero. Thus, intuitively the limiting value of the multiplexing gain r, for which the diversity gain $d(r)$ is zero, is less than or equal to $\frac{s}{l}$. We prove this formally in the following theorem.

Theorem 5.2.2 *Let $\mathbf{X}$ be a rate-k/l, $n_t \times l$ design which achieves optimal diversity-multiplexing tradeoff for n_r receive antennas. Then, $\mathbf{X}$ is an AILL design for n_r receive antennas. In other words asymptotic-information-losslessness is a necessary condition for a design to achieve the optimal diversity-multiplexing tradeoff.*

Proof: We have

$$\begin{aligned} P_{out,\mathbf{X}}(r) &= P(C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}, \mathbf{H}) < r \log \mathsf{SNR}) \\ &= 1 - P(\mathbf{c} \geq r \log \mathsf{SNR}). \end{aligned}$$

Let the ergodic capacity of the design $\mathbf{X}$ be $\tau \log \mathsf{SNR}$ and $p(c)$ denote the probability density function of $\mathbf{c} = C_{\mathbf{X}}(n_t, n_r, \mathsf{SNR}, \mathbf{H})$. Then, we have

$$\begin{aligned} P(c \geq r \log \mathsf{SNR}) &= \int_{c \geq r \log \mathsf{SNR}} p(c)\, dc \\ &\leq \frac{1}{r \log \mathsf{SNR}} \int_{c \geq r \log \mathsf{SNR}} cp(c)\, dc \\ &\leq \frac{\tau}{r}. \end{aligned}$$

Thus,

$$P_{out,\mathbf{X}}(r) \geq 1 - \frac{\tau}{r}.$$

Since $\mathbf{X}$ achieves the optimal diversity-multiplexing tradeoff, $P_{out,\mathbf{X}}(r) \doteq \mathsf{SNR}^{-(n_t-r)(n_r-r)}$. This indicates that for every value of $r \in [0, \min\{n_t, n_r\}]$, the value of $\frac{\tau}{r} \geq 1$. Thus, $\tau = \min\{n_t, n_r\}$. ■

We now show that AILL is also a sufficient condition for a design to achieve the point $(0, \min\{n_t, n_r\})$ of the tradeoff curve.

Theorem 5.2.3 *The design* $\mathbf{X}$ *achieves the point* $(\min\{n_t, n_r\}, 0)$ *of the diversity-multiplexing tradeoff curve if and only if* $\mathbf{X}$ *is an AILL design for* n_r *receive antennas.*

Proof: Let $\mathbf{X}$ be an AILL design for n_r receive antennas. Then, we have two cases:
Case 1. $n_r \geq n_t$. Then, the generator matrix Φ of $\mathbf{X}$ has rank at least $2n_t l$. Let the singular value decomposition Φ be $\Phi = \mathbf{UDV}^T$. Then, the equivalent system model for the design $\mathbf{X}$ is

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n_t}} \widehat{\mathcal{H}} \mathbf{UDV}^T \widehat{\mathbf{a}} + \widehat{\mathbf{w}}$$

If the number of variables $k > n_t l$, we allow only $n_t l$ of the k variables to take values from some constellation, while restrict the remaining to zero. Thus, without loss of generality let $k = n_t l$. To obtain the error probability, let us restrict ourselves to QAM signal constellations. If the data rate $R = r \log \mathsf{SNR}$, then a_i should take values from $\mathsf{SNR}^{lr/k}$-QAM. If $d_{\min}$ is minimum Euclidean distance of the $\mathsf{SNR}^{lr/k}$-QAM constellation, then the minimum Euclidean distance of the constellation of the vectors $\mathbf{UDV}^T\widehat{\mathbf{x}}$ is at least $\lambda_{\min} d_{\min}$, where $\lambda_{\min}$ is the minimum among all the non-zero diagonal elements of the diagonal matrix $\mathbf{D}$. Also, it is easy to see that the number of nearest neighbors in the constellation $\mathbf{UDV}^T\widehat{\mathbf{x}}$ is a constant. Thus, we can view the system now as

$$\widehat{\mathbf{y}} = \sqrt{\frac{\mathsf{SNR}}{n_t}}\widehat{\mathcal{H}}\widehat{\widehat{\mathbf{x}}} + \widehat{\mathbf{w}}$$

where $\widehat{\widehat{\mathbf{x}}} = \mathbf{UDV}^T\widehat{\mathbf{x}}$. Now, entries of $\widehat{\widehat{\mathbf{x}}}$ come from a constellation whose minimum distance is greater than or equal to $\lambda_{\min} d_{\min}$ and the number of nearest neighbors is a constant independent of SNR. Using the technique of successive nulling and canceling of V-BLAST, we have the equivalent system of the channel as

$$\widehat{\mathbf{y}}_i = \sqrt{\frac{\mathsf{SNR}}{n_t}} g_i \widehat{\widehat{\mathbf{x}}}_i + \widehat{\mathbf{w_i}} \quad i = 0, 1, 2, \ldots, 2n_t l - 1$$

where g_i^2 is the i-th decorrelator SNR gain and is a chi-squared distributed random variable with $2j$ degrees of freedom where $j = i \bmod n_r$. From [50], the pairwise error probability for i-th decorrelator is

$$\begin{aligned} P_e(x_i \to x_i') &\doteq P\left(\frac{\mathsf{SNR}}{n_t} g_i^2 ||x_i - x_i'||^2 < 1\right) \\ &\doteq P\left(g_i^2 < \frac{n_t}{\mathsf{SNR}||x_i - x_i'||^2}\right). \end{aligned}$$

Since the minimum squared Euclidean distance of the $\mathsf{SNR}^{lr/k}$-QAM is equal to $\mathsf{SNR}^{-lr/k}$, we have

$$P_e(x_i \to x_i') \doteq P\left(g_i^2 < \frac{n_t}{\mathsf{SNR}^{1-lr/k}}\right) \doteq \mathsf{SNR}^{-(1-lr/k)}.$$

Since, the number of nearest numbers is a constant independent of SNR, the actual error probability for i-th decorrelator is

$$P_e^{(i)}(\mathsf{SNR}) \doteq \mathsf{SNR}^{-(1-lr/k)}.$$

Since $P_e^{(1)}(\mathsf{SNR}) \leq P'_e(\mathsf{SNR}) \leq \sum_i P_e^{(i)}(\mathsf{SNR})$, where $P'_e(\mathsf{SNR})$ is the error probability with successive nulling and canceling detection, we have the actual error probability with ML detection given by

$$P_e(\mathsf{SNR}) \leq P'_e(\mathsf{SNR}) \doteq \mathsf{SNR}^{-(1-lr/k)}.$$

Since, $\mathbf{X}$ is an AILL design, we have $l/k = 1/n_t$. Hence, $d_{\mathbf{X}}(r)$ is equal to zero when $r = n_t$, i.e., the point corresponding to zero diversity is $(n_t, 0)$.

Case 2. $n_t \geq n_r$. In this case, we can assume that the design has $n_r l$ variables. Now, the matrix $\widehat{\mathcal{H}}\Phi$ is a $2n_r l \times 2n_r l$ matrix with entries as linear combinations of the entries of $\widehat{\mathbf{H}}$. Hence, the entries of the matrix $\widehat{\mathcal{H}}\Phi$ are Gaussian distributed and the rank of $\widehat{\mathcal{H}}\Phi$ is $2n_r l$. Following the method given in Case 1., we have the probability of error upper bounded by

$$P_e(\mathsf{SNR}) \dot{\leq} \mathsf{SNR}^{-(1-r/n_r)}$$

and hence the point $(n_r, 0)$ of the optimal tradeoff curve is achieved. ■

Since in any $n_t \times l$ orthogonal design ($n_t \neq 2$) $\mathbf{X}$, the number of the variables is strictly less than l, $\mathbf{X}$ is AIL and hence from the above theorem, all the orthogonal designs except Alamouti scheme do not achieve the optimal tradeoff for any number of receive antennas. Alamouti scheme has been shown to achieve the optimal tradeoff for 1 receive antenna. Similarly, QODs for $n_t \geq 5$ do not achieve the optimal tradeoff for any number of receive antennas. For $n_t = 2, 3, 4$, the QODs achieve the point $(0, 1)$ of the tradeoff curve for 1 receive antenna.

Corollary 5.2.2 *If $\mathbf{X}$ is a full-rank design for n_t transmit antennas, such that the STBCs constructed using the design $\mathbf{X}$ are completely over a signal set S, i.e., entries of the codeword matrices in the STBC are from the signal set S over which the STBC is constructed,*

then the design $\mathbf{X}$ *does not achieve the point corresponding to the zero diversity gain of the tradeoff curve for more than one receive antenna.*

Remark 5.2.1 *Let* $\mathbf{X}$ *be an ILL design and* $\mathbf{X}'$ *be an AILL design but not ILL. Suppose, both* $\mathbf{X}$ *and* $\mathbf{X}'$ *achieve the optimal diversity-multiplexing tradeoff. Then, clearly, it is preferable to use the design* $\mathbf{X}$ *to the design* $\mathbf{X}'$ *because the former is ILL while the later is not ILL. So, it is important to construct designs which not only achieve optimal diversity-multiplexing tradeoff, but also are ILL.*

5.3 Diversity-Multiplexing Tradeoff of Designs from Field Extensions

Let $\mathbf{X}$ be a rate-k/n_t $n_t \times n_t$ design obtained from the field extension of $\mathbb{Q}(S, z)$ using a minimal polynomial of the form $x_t^n - \gamma$, where $\gamma \in \mathbb{Q}(S, z)$ and S is the signal set of interest. Then, the design $\mathbf{X}$ is of the form

$$\begin{bmatrix} f_0(z) & \gamma f_{n_t-1}(z) & \cdots & \gamma f_1(z) \\ f_1(z) & f_0(z) & \cdots & \gamma f_2(z) \\ \vdots & \vdots & \ddots & \vdots \\ f_{n_t-1}(z) & f_{n_t-2}(z) & \cdots & f_0(z) \end{bmatrix} \tag{5.3}$$

where $f_i(z)$ are polynomials of arbitrary degree. If every polynomial f_i is of degree $R-1$, then the rate of this design is R. It can be checked that the generator matrix of this design has rank n_t. Thus, $\mathbf{X}$ is an AILL design only for 1 receive antenna. From Theorem 5.2.3, the diversity-multiplexing tradeoff of this design for 1 receive antenna is lower bounded by $d(r) = 1 - r$ for $0 < r \leq 1$ and since the design is a full-rank design, we also have $d(0) = n_t$. Also note that the tradeoff achieved by this design is independent of the degree of the polynomials f_i. So, we can assume that all f_i are degree zero polynomials over S.

Example 5.3.1 *Let* S *be a QAM signal set and* $n_t = 3$*. Then, the polynomial* $x^3 - \omega_6$ *is*

irreducible in $\mathbb{Q}(S, \omega_3)[x]$ *[39]. The design constructed using this irreducible polynomial is*

$$\begin{bmatrix} f_0 & \omega_6 f_2 & \omega_6 f_1 \\ f_1 & f_0 & \omega_6 f_2 \\ f_2 & f_2 & f_0 \end{bmatrix}.$$

The lower bound on the tradeoff achieved by this design is $d(r) = 1 - r$.

Notice that the lower bound we have from Theorem 5.2.3 when used for the designs from field extensions is independent of the number of transmit and receive antennas.

We now obtain a tighter bound for the tradeoff achieved by $\mathbf{X}$. Let $\mathcal{C}(\mathsf{SNR})$ be the code obtained by restricting the variables f_i to a finite subset S of the 2-dimensional lattice $\mathbb{Z}[\omega_m]$ generated by 1 and ω_m. The size of the signal set S is chosen to be SNR^r such that the data rate of the code $\mathcal{C}(\mathsf{SNR})$ is $r \log \mathsf{SNR}$ bits per channel use. If $\mathbf{C}, \mathbf{C}' \in \mathcal{C}(\mathsf{SNR})$ and $\mathbf{C} \neq \mathbf{C}'$, then the determinant of $\mathbf{C} - \mathbf{C}'$ is given by the norm of the element $\sum_{i=0}^{n_t-1}(s_i - s_i')\omega_{mn_t}$, where s_i and s_i' are the values taken by the variables f_i in the codewords $\mathbf{C}$ and $\mathbf{C}'$ respectively [37, 39]. Since, the norm of any element in $\mathbb{Z}[\omega_{mn_t}]$ belongs to the lattice $\mathbb{Z}[\omega_m]$, the minimum value of the determinants is lower bounded by the minimum distance of the lattice $\mathbb{Z}[\omega_m]$ [37, 39]. Thus, the coding gain of the resulting STBC, with the assumption that the signal set is scaled to have unit average energy, is SNR^{-r}. Then, the pairwise error probability is given by

$$P_e(\mathbf{X} \to \mathbf{X}') \doteq \mathsf{SNR}^{rn_tn_r}\mathsf{SNR}^{-n_rn_t} = \mathsf{SNR}^{-n_rn_t(1-r)}.$$

Then, using the union bound, we have an upper bound on the probability of error given by

$$P_e(\mathsf{SNR}) \dot{\leq} \mathsf{SNR}^{n_tr}\mathsf{SNR}^{-n_rn_t(1-r)}.$$

Thus, for the case $r \leq 1$, we have a lower bound on $d_{\mathbf{X}}(r)$ given by $d_{\mathbf{X}}(r) \geq n_tn_r - rn_t(n_r + 1)$. Since there are SNR^{n_tr} codewords and since the range of the determinant $\det \mathbf{C} - \mathbf{C}'$ is SNR^r, we assume that there are $\mathsf{SNR}^{r(n_t-1)}$ codewords such that the $\det \mathbf{C} - \mathbf{C}'$ is the minimum. Though, this need not be true in general, we have observed through numerical

simulations that this is true for $2, 3$ and 4 transmit antennas. Thus, the union bound can be tightened as

$$P_e(\mathsf{SNR}) \dot{\leq} \mathsf{SNR}^{r(n_t-1)}\mathsf{SNR}^{-n_t n_r(1-r)}.$$

Thus, we have a lower bound on the tradeoff achieved by the design $\mathbf{X}$ given by

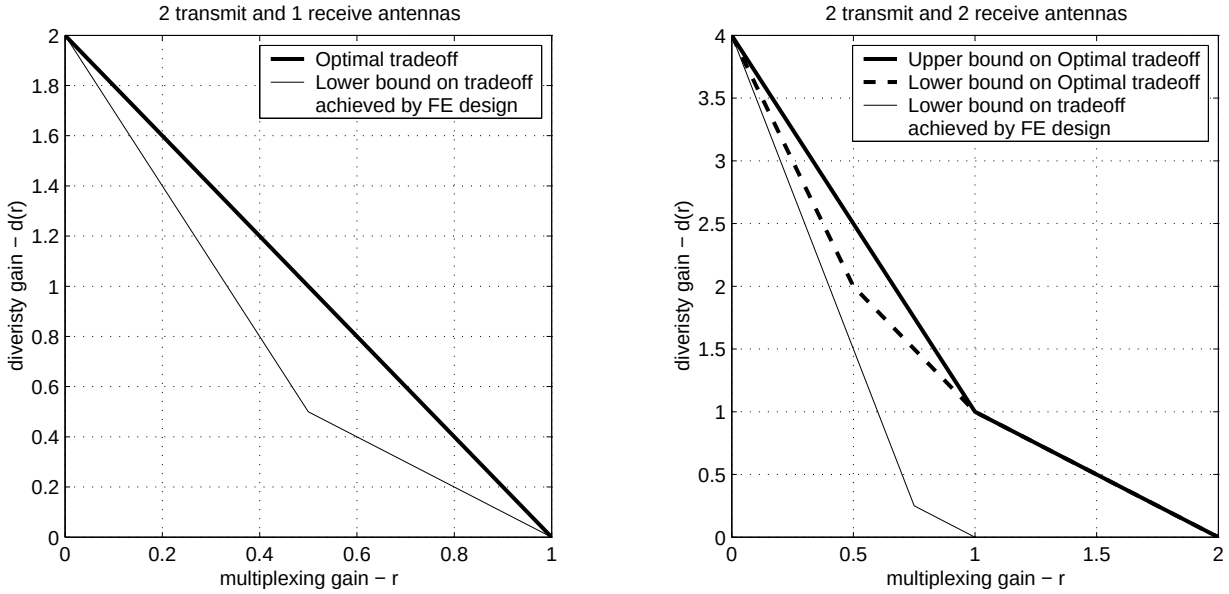


Figure 5.7: Diversity-multiplexing tradeoff achieved by design from field extensions for 2 transmit and 1,2 receive antennas

$$d_{\mathbf{X}}(r) \geq n_t n_r(1-r) - r(n_t - 1).$$

Figure 5.7 and 5.8 show the tradeoff curve for $n_t = 2$, $n_r = 1, 2$ and $n_t = 3$, $n_r = 1, 3$ respectively.

5.4 Diversity-Multiplexing Tradeoff of Designs from Division Algebras

In this section we consider cyclic division algebras only. The results of this section are also valid for other division algebras also.

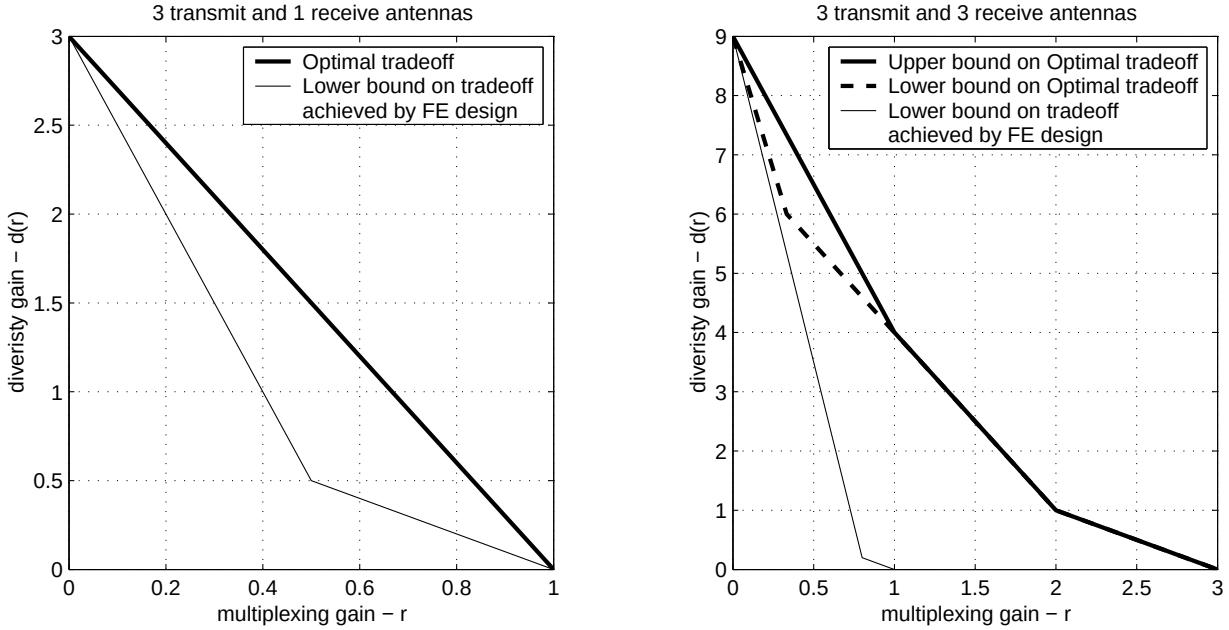


Figure 5.8: Diversity-multiplexing tradeoff achieved by design from field extensions for 3 transmit and 1,3 receive antennas

Let $\mathbf{X}$ be the design obtained from a cyclic division algebra $(K(\delta), \sigma, \delta)$, where K is a cyclic extension of the field $F = \mathbb{Q}(S, \omega_n, t)$ and σ is a generator of the Galois group. Then, the design $\mathbf{X}$ is of the form

$$\frac{1}{\sqrt{n}} \begin{bmatrix} \sum_{i=0}^{n-1} f_{0,i}t^i & \delta\sigma\left(\sum_{i=0}^{n-1} f_{n-1,i}t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-2,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{1,i}t^i\right) \\ \sum_{i=0}^{n-1} f_{1,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) & \delta\sigma^2\left(\sum_{i=0}^{n-1} f_{n-1,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{2,i}t^i\right) \\ \sum_{i=0}^{n-1} f_{2,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{1,i}t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) & \cdots & \delta\sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{3,i}t^i\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{i=0}^{n-1} f_{n-1,i}t^i & \sigma\left(\sum_{i=0}^{n-1} f_{n-2,i}t^i\right) & \sigma^2\left(\sum_{i=0}^{n-1} f_{n-3,i}t^i\right) & \cdots & \sigma^{n-1}\left(\sum_{i=0}^{n-1} f_{0,i}t^i\right) \end{bmatrix} \tag{5.4}$$

where $f_{i,j} \in F$. Since the number of variables in the above matrix is n^2, if the size of the signal set S as a function of SNR is equal to $\mathsf{SNR}^{r/n}$, the bit rate of the code in bits per channel use will be $\frac{1}{n}\log_2\left(\mathsf{SNR}^{r/n}\right)^{n^2} = r\log\mathsf{SNR}$.

Theorem 5.4.1 *The diversity-multiplexing tradeoff $d_{DA}(r)$ of the design from division algebras satisfies*

$$d_{DA}(r) \geq 1 - r/\min\{n_t, n_r\} \quad \textit{and} \quad d_{DA}(0) = n^2.$$

If the number of receive antennas is 1, then the tradeoff achieved by the designs from division algebras is same as that of achieved by the designs from field extensions.

Example 5.4.1 (Example 4.3.5 continued) *The determinant of the design obtained in Example 4.3.5 is*

$$\det \mathbf{X} = N_{K/F}\left(f_{0,0} + \sqrt{j} f_{0,1}\right) - \delta N_{K/F}\left(f_{1,0} + \sqrt{j} f_{1,1}\right)$$

where $N_{K/F}(x)$ is the algebraic norm of the element $x \in K$ from K to F. If $f_{k,l} \in \mathbb{Z}[j]$ for all k and l, then the determinant belongs to the set $\mathbb{Z}[j]$. Thus, the coding gain of the STBC obtained from the design $\mathbf{X}$ is lower bounded by the minimum distance of the set $\mathbb{Z}_\delta = \mathbb{Z}[j] + \delta\mathbb{Z}[j]$. Since, δ is a transcendental element, it is very difficult to obtain the minimum distance of the set $\mathbb{Z}_\delta$. To avoid this difficulty, with $\delta \approx e^j$, we let the entries $f_{1,0}$ and $f_{1,1}$ come from a signal set whose minimum distance is at least 4 times greater than the maximum distance of the signal set from which the entries $f_{0,0}$ and $f_{0,1}$ take values. To obtain a data rate of $r \log \mathsf{SNR}$, we use a constellation of size $\mathsf{SNR}^{r/2}$ carved from $\mathbb{Z}[j]$ for the entries $f_{0,0}$ and $f_{0,1}$, and for the entries $f_{1,0}$ and $f_{1,1}$ we use a constellation of size $\mathsf{SNR}^{r/2}$ carved from $\mathsf{SNR}^{r/4}\mathbb{Z}[j]$. With this selection of constellations, the minimum value of the determinant is lower bounded by 1. Scaling the constellations such that the variance of each entry in the design is 1, we have the coding gain of the design $\mathbf{X}$ lower bounded by $\frac{1}{\mathsf{SNR}^{r/2}+\mathsf{SNR}^r} \geq \frac{1}{2\mathsf{SNR}^r}$. Thus, the pairwise error probability is given by

$$P_e(\mathbf{C} \to \mathbf{C}') \dot{\leq} \left(\frac{1}{\mathsf{SNR}^{r/2} + \mathsf{SNR}^r}\mathsf{SNR}\right)^{-4} \dot{\leq} \mathsf{SNR}^{-4(1-r)}.$$

Since, the range of the determinant $\det \mathbf{C} - \mathbf{C}'$ is SNR^r while the total number of possible determinants is SNR^{2r}, we assume that each determinant occurs SNR^r times. Thus, using

the union bound, we have the exact probability of error upper bounded as

$$P_e \dot{\leq} \mathsf{SNR}^{-4+5r}$$

and thus, the tradeoff achieved by $\mathbf{X}$ *is lower bounded by* $d_{\mathbf{X}}(r) \geq 4 - 5r$.

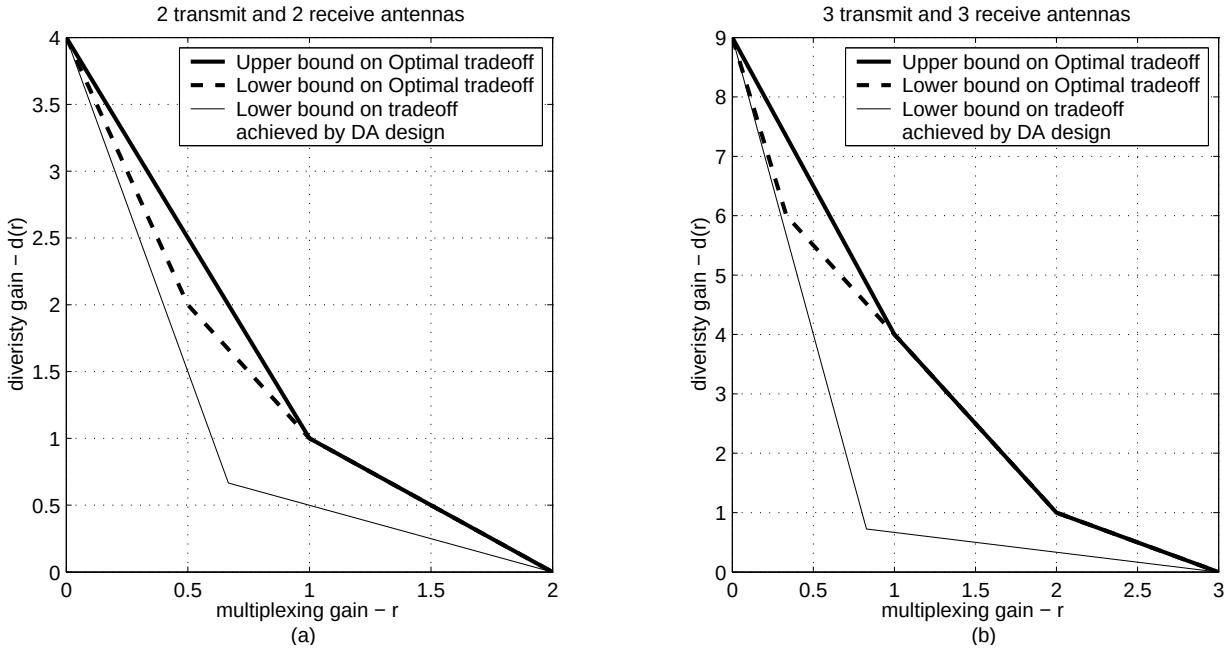


Figure 5.9: Diversity-multiplexing tradeoff achieved by design from division algebras for (a) 2 transmit and 2 receive antennas, (b) 3 transmit and 3 receive antennas.

Figure 5.9 shows the lower bound on the tradeoff achieved by the designs from division algebras for 2 and 3 transmit antennas. In the next section, we show by simulations that the designs from division algebras achieve the optimal diversity-multiplexing tradeoff for $n_t = 2, 3, 4$ and $n_r = n_t$.

Example 5.4.2 *In [44], cyclic division algebras from number fields were used to construct STBCs for* $2, 3$ *and* 4 *transmit antennas. The cyclic division algebras used in [44] for* 2 *transmit antennas is* $\left(\mathbb{Q}(\sqrt{j}), \sigma, 1 + 2j\right)$*, where* $\sigma : \sqrt{j} \mapsto -\sqrt{j}$*. The design obtained*

using this cyclic division algebra is

$$\frac{1}{\sqrt{2}}\begin{bmatrix} f_{0,0}+f_{0,1}\sqrt{j} & (1+2j)(f_{1,0}-f_{1,1}\sqrt{j}) \\ f_{1,0}+f_{1,1}\sqrt{j} & (f_{0,0}-f_{0,1}\sqrt{j}) \end{bmatrix}. \tag{5.5}$$

The determinant of the above matrix with $f_{i,j} \in \mathbb{Z}[j]$ *is lower bounded by* $\frac{1}{2}$. *Thus, following the method used in Section 5.3, we obtain a lower bound on the tradeoff achieved by the above design, given by*

$$d(r) = 4 - 3r.$$

In a similar manner, we can prove that the tradeoff achieved by the designs obtained using cyclic division algebras from number fields for $n_t = 3$ *and* $n_t = 4$ *satisfy*

$$d(r) = n_t n_r - r n_r - r n_t + r.$$

The lower bound indicates that the tradeoff achieved is optimal for $0 \leq r \leq 1$. *In particular using the procedure of [51] for* $n_t = 2$, *we can show that the design in (5.5) achieves the optimal diversity-multiplexing tradeoff.*

5.5 Simulations

In this section, we present simulation results for 2, 3 and 4 transmit antennas to show that DA codes achieve the optimal diversity-multiplexing tradeoff.

We have used the design obtained in Example 4.3.5 for 2 transmit and 2 receive antennas.

Figure 5.10 shows the error probability curves for various data rates. It can be seen that at high SNRs, the gap between two adjacent curves, with data rates differing by 4 bits per channel use, is 6 dB. This indicates that at $d = 0$, the data rate grows with SNR as $R = 2\log \mathsf{SNR}$. Thus, the point $(2, 0)$ of the tradeoff curve is achieved. We have also plotted the outage probabilities (dashed curves). It can be seen that curves for P_e match with outage probability at high SNRs and hence the DA code for 2 transmit and 2 receive

antennas achieves the optimal tradeoff.

For 3 transmit antennas, we have used the design of Example 4.5.2. Figure 5.11 shows the error probability curves for various data rates. At high SNRs, the gap between two adjacent curves with data rates differing by 6 bits per channel use, is 6 dB. Thus, at $d = 0$, the data rate grows with SNR as $R = 3\log \mathsf{SNR}$. Also, outage probabilities we have plotted coincide with error probability curves at high SNRs indicating that our code achieves optimal diversity-multiplexing tradeoff. The design we have used for 4 transmit

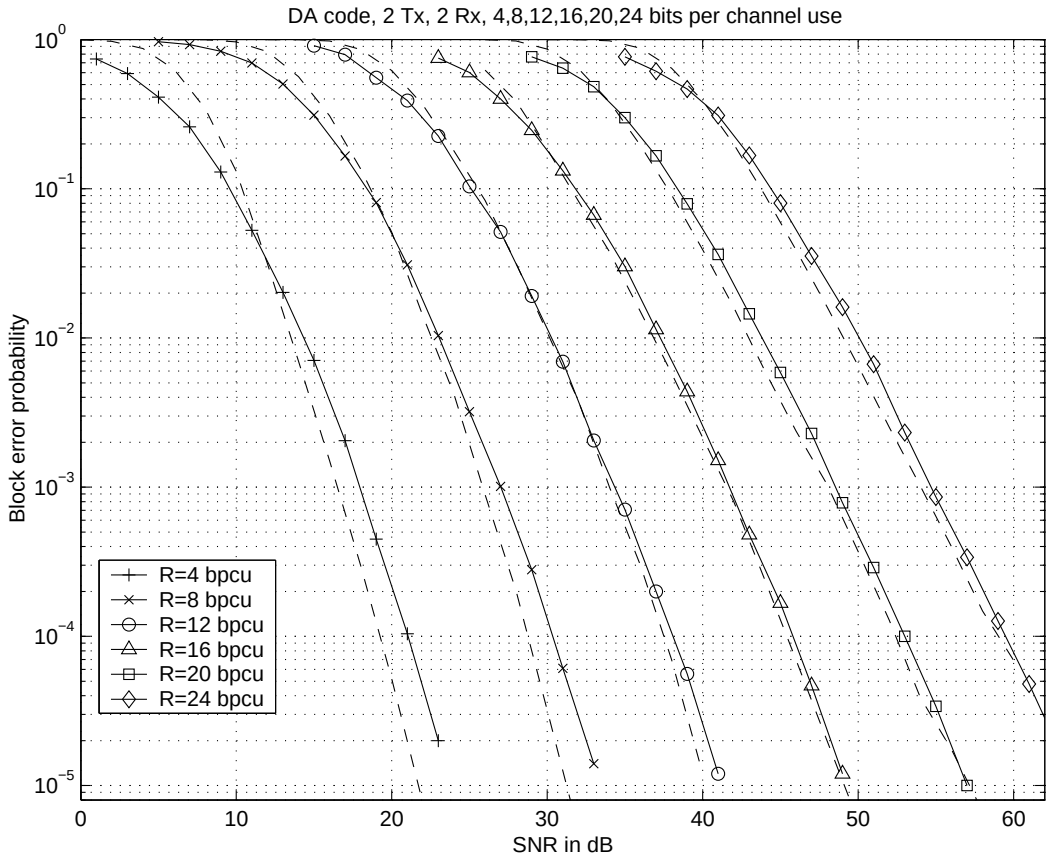


Figure 5.10: Error probability curves (solid) and outage probability curves (dashed)for 2 transmit and 2 receive antennas.

antennas is

$$\mathcal{C} = \left\{ \frac{1}{\sqrt{4}} \begin{bmatrix} g_{0,0} & \delta g_{1,3} & \delta g_{2,2} & \delta g_{3,3} \\ g_{0,1} & g_{1,0} & \delta g_{2,3} & \delta g_{3,2} \\ g_{0,2} & g_{1,1} & g_{2,0} & \delta g_{3,3} \\ g_{0,3} & g_{1,2} & g_{2,1} & g_{3,0} \end{bmatrix} \right\}$$

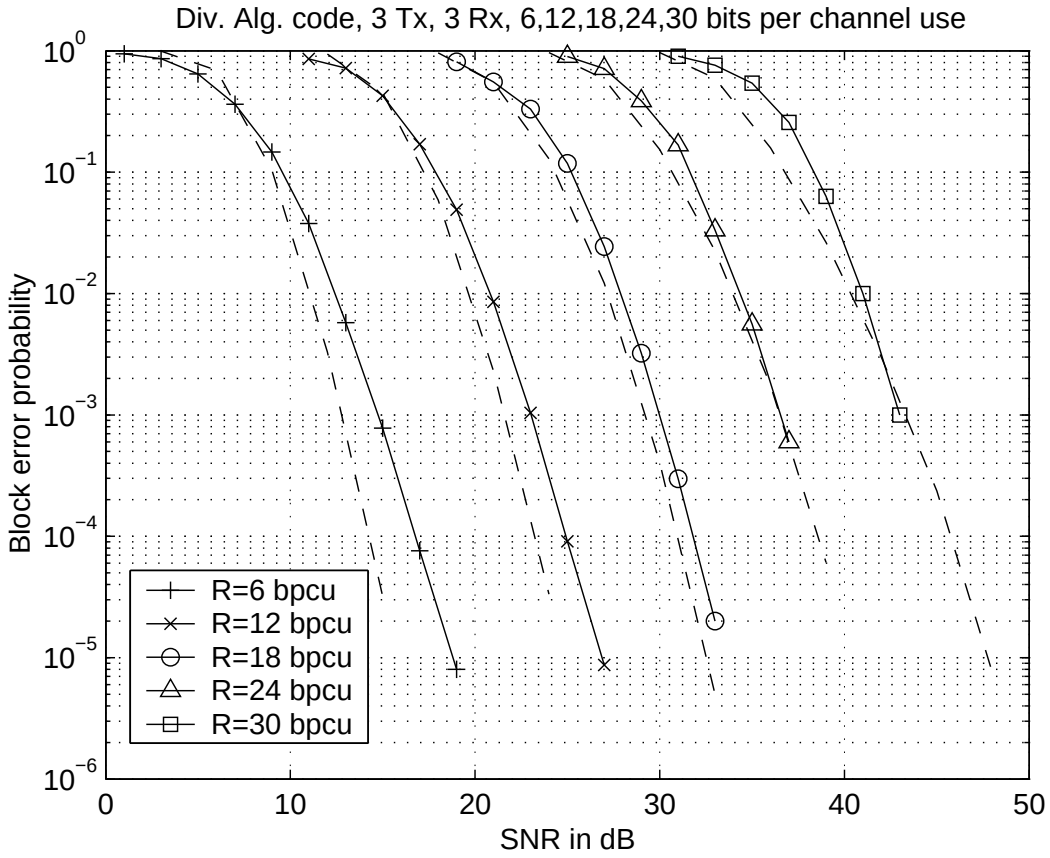


Figure 5.11: Error probability curves (solid) and outage probability curves (dashed)for 3 transmit and 3 receive antennas.

where $g_{i,j} = \sum_{l=0}^{3} f_{j,l}(j^i\omega_{16})^l$ and $f_{i,j} \in \mathsf{SNR}^{r/4} - QAM$ for $i,j = 0,1,2,3$. Figure 5.12 shows the error probability curves and outage probability curves. It can be seen that at high SNRs both the set of curves match which indicates that our scheme achieves optimal tradeoff.

5.6 Summary

In this chapter we have defined Asymptotic-Information-Lossless designs for n_r receive antennas. We also obtained a necessary and sufficient condition under which a design is AILL. We have shown that it is necessary for a design to be AILL to achieve the optimal diversity-multiplexing tradeoff and have shown that "AILL" is also a sufficient condition for which a design achieves the point $(\min\{n_t, n_r\}, 0)$ of the optimal tradeoff curve. It is

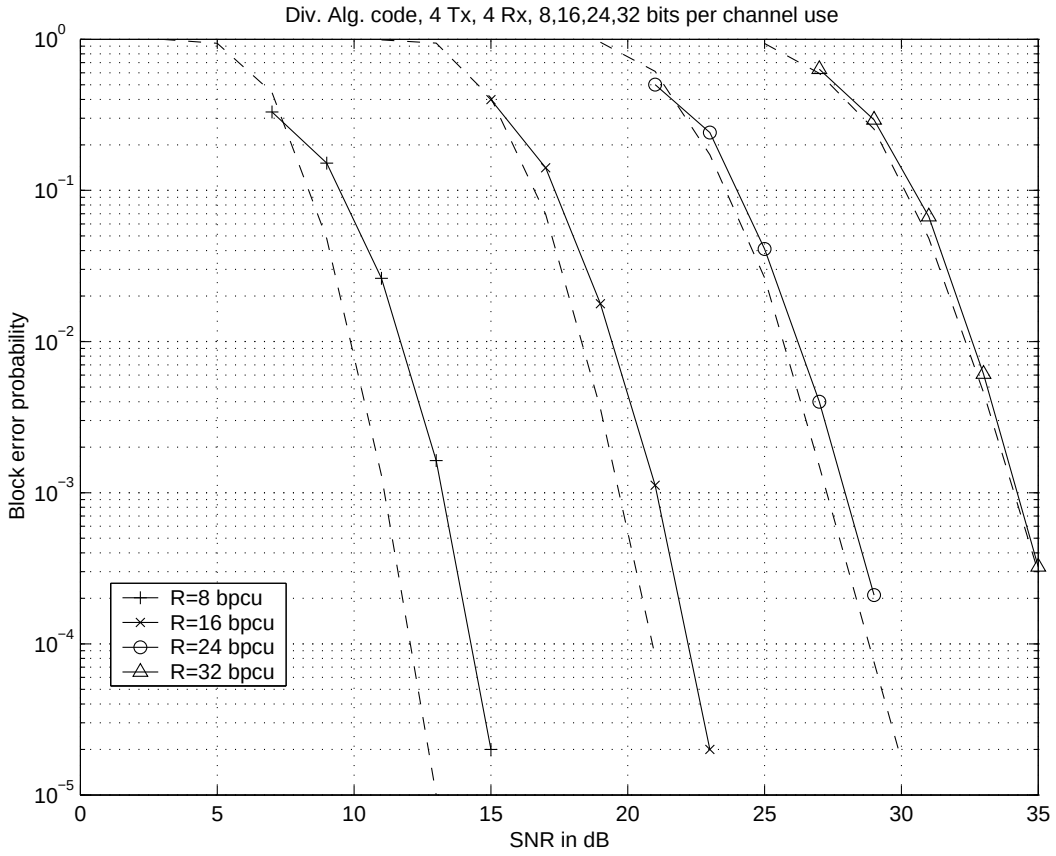


Figure 5.12: Error probability curves (solid) and outage probability curves (dashed)for 4 transmit and 4 receive antennas.

shown that the well known codes like DAST, designs from field extensions and ST-CR are AILL for 1 receive antennas. We have obtained a lower bound on the tradeoff achieved by the designs from field extensions and have shown that the lower bound is close to the optimal tradeoff for the case of 1 receive antenna. We have also obtained a lower bound on the tradeoff achieved by the designs from division algebras. The lower bound indicates that we achieve both the extreme points corresponding to zero diversity and zero multiplexing gain of the optimal tradeoff curve. We have given simulations for 2, 3 and 4 transmit antennas and show that the designs from division algebras meet all the points of the optimal tradeoff curve.

Chapter 6

Conclusions

6.1 Summary of the results

In this thesis we have constructed high-rate, full-diversity STBCs using both commutative (field extensions) and non-commutative algebras.

For the STBCs from field extensions, we gave exact expressions for the coding gain. We also obtained a lower bound on the coding gain of certain special cases. The lower bound indicates that some of our STBCs are optimal in terms of coding gain. We also gave capacity analysis and proved that the STBCs from field extensions are information-lossy. On the other hand, however, we have shown by simulations that the finite-signal-set capacity of our STBCs approaches that of the channel as the symbol rate is increased. Finally, we presented simulation results to show that our codes perform better than some of well known codes like ST-CR, in terms of bit error rate.

For the STBCs from non-commutative algebras, we restricted ourselves to those algebras which were crossed-product algebras. We have given a general technique of constructing STBCs from crossed-product algebras, which include several well known codes like Damen *et al.* [22], Alamouti Code, Quasi-Orthogonal Designs etc. A sufficient condition on the CPAs, under which these STBCs arising from them are information-lossless, was obtained. We identified two classes of CPAs satisfying the sufficient condition. We identified two classes of CPAs which were division algebras and hence the STBCs arising

from them are full-diversity STBCs. We presented some simulation results to show that our codes perform better than well known codes in terms of bit error rate.

In Chapter 5, we introduced the notion of Asymptotic-Information-Losslessness. We derived a necessary and sufficient condition under which a design is AILL and showed that many well known codes like DAST, ST-CR are AILL for 1 receive antennas, while codes like TAST, Damen *et al.* [22], STBCs from quaternionic lattices [44] are AILL for any number of receive antennas. We then, showed that any AILL design achieves the point corresponding to the zero diversity gain of the optimal diversity-multiplexing tradeoff. A lower bound the diversity-multiplexing tradeoff achieved by the STBCs from field extensions was obtained, which indicates that the STBCs from field extensions achieve the maximum multiplexing gain for 1 receive antenna only. Similarly, we obtained a lower bound on the tradeoff achieved by the STBCs from division algebras. The lower bound indicates that they achieve both maximum diversity gain and maximum multiplexing for any number of transmit and receive antennas. We explicitly showed by simulations that STBCs from division algebras achieve the optimal diversity-multiplexing tradeoff for n transmit and n receive antennas, $n = 2, 3$ and 4.

6.2 Directions for further research

- In Chapter 3, we have shown that our high-rate codes do not admit sphere decoding but admit the generalized sphere decoding. It would be interesting to know if there are any good decoding algorithms which can be used for our high-rate codes.

- We have studied primarily cyclotomic field extensions in constructing STBCs using field extensions in Chapter 3. Code constructions using non-cyclotomic field extensions may yield some interesting codes.

- We have discussed capacity only for codes from cyclotomic field extensions in Chapter 3. It will be interesting to see the capacity of the codes obtained using non-cyclotomic field extensions also.

- We have seen in Chapter 4, that we can construct the Alamouti code and 4×4 quasi-orthogonal design of [16] using crossed-product algebras. It would be interesting to see if we can construct orthogonal designs other than Alamouti code and other quasi-orthogonal designs like $\begin{bmatrix} A & B \\ -B^* & A^* \end{bmatrix}$, using crossed-product algebras.

- It would be interesting to see if there exits a closed form expression for coding gain of the STBCs arising from non-cyclic division algebras.

- We have used only abelian CPAs in constructing information-lossless STBCs. It would be interesting to see if other crossed-product algebras give rise to better information-lossless STBCs in terms of bit error rate performance.

- In Chapter 4, we obtained a sufficient condition on the CPAs, under which the STBCs arising from them are ILL. It would be interesting to characterize all the CPAs which satisfy the sufficient condition.

- We have shown that we can use the sphere decoder to decode our codes obtained from crossed-product algebras when the number of receive antennas is greater than or equal to the number of transmit antennas. It would be interesting to see if there exist any simpler decoding algorithms when the number of receive antennas is less than the number of transmit antennas.

- We have shown that AILL designs achieve the extreme point corresponding to the zero diversity gain of the optimal tradeoff. It would be interesting to find necessary and sufficient conditions for achieving other points on the tradeoff curve.

- In obtaining a lower bound on the tradeoff curve achieved by the designs from field extensions and division algebras, we have found that STBCs having non-vanishing coding gain as SNR increases, are very important. Thus, it would be interesting to obtain designs with non-vanishing coding gain for arbitrary number of transmit antennas. At the same time, the design should also be an AILL design.

- All the designs corresponding to the well known STTCs are rate-1 designs. And from the results of this paper, clearly, these designs can achieve optimal tradeoff only for 1 receive antenna. Since, STTCs have the property that the coding is lower bounded by the minimum squared Euclidean distance of the signal set used, it would be interesting to find STTCs with higher symbol rates. For instance, if we can find an STTC with rate-2 symbols per channel use, then the STTC can achieve the optimal tradeoff for 2 receive antennas.

Appendix A

Preliminaries and Basics of Algebra

A.1 Ring homomorphisms

Definition A.1.1 *Let R and R' be two rings with identity. Then, a ring homomorphism ψ from R to R' is a map ψ satisfying the following properties:*

- $\psi(a+b) = \psi(a) + \psi(b),\ \psi(ab) = \psi(a)\psi(b)\ \forall a, b \in R$,
- $\psi(0) = 0$,

where the $a + b$ is addition in R and $\psi(a) + \psi(b)$ is the addition is R'. Similarly the multiplication. The set of elements that map to zero under ψ is called the kernel of ψ and is denoted $ker\psi$.

A simple example of ring homomorphism is the complex conjugation in the complex field $\mathbb{C}$, i.e., $\psi(c) = c^*$, for $c \in \mathbb{C}$.

A left ideal I of a ring R is an additive subgroup of R that satisfies the property that $ar \in I$ for all $r \in R$ and $a \in I$. Similarly a right ideal I of a Ring R is an additive subgroup of R that satisfies the property that $ra \in I$ for all $r \in R$ and $a \in I$. An ideal is called two-sided ideal if it both left and right ideal.

A ring is called simple if it has no non-trivial two-sided ideals, i.e., the only ideals are the sets $\{0\}$ and the ring itself. Fields and matrix algebras are simple examples of simple rings.

The kernel of any ring homomorphism from R to R' is a two-sided ideal of R. Thus, when R is in particular a field, the kernel is zero or the entire field R. Thus, any non-zero homomorphism of a field into any ring is an injective map. Any injective ring homomorphism of a ring R into a ring R' is called an **embedding** of R into the ring R'.

A.2 Algebraic and transcendental extensions of fields

Since in this thesis we consider only characteristic zero fields, we focus only on characteristic zero fields. Let F and K be two such fields. Then, we call K an field extension of F if F is a proper subfield of K and the extension is denoted as K/F.

Definition A.2.1 *Let K be field extension of F. Then, an element $\alpha \in K$ is said to be an* **algebraic element** *over F, if there exists a polynomial $f(x)$ in $F[x]$ satisfying k, i.e., $f(\alpha) = 0$. If there doesn't exist any such polynomial then α is said to be a* **transcendental element** *over F.*

For example, consider the real field $\mathbb{R}$ which is an extension of the rational number field $\mathbb{Q}$. Elements like $\sqrt{2}, \sqrt{5}$ are algebraic over $\mathbb{Q}$, but elements like e, π etc are transcendental elements over $\mathbb{Q}$.

We call a field extension K of F, an algebraic extension of F if every element in K is algebraic over F. Otherwise we call K as a transcendental extension. Thus $\mathbb{R}$ is a transcendental extension of $\mathbb{Q}$ and the complex field $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

Every field extension K of F can be seen as a F-space, i.e., a vector space over F. If the vector space dimension of K over F is finite, then K is called a finite extension of F and otherwise an infinite extension of F. The vector space dimension is called the **degree of extension** and is denoted $[K : F]$. Every extension K of F of the form $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a finite extension if each of the α_i is an algebraic element over F. The notation $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ means the smallest field containing both F and α_i, $i = 1, 2, \ldots, n$. For example $\mathbb{C}/\mathbb{R}$ is a degree 2 extension and $\mathbb{R}/\mathbb{Q}$ is an infinite extension.

If L is an extension of K of degree n and K/F is of degree m, then we have

$$[L : F] = [L : K][K : F].$$

Theorem A.2.1 (Primitive element theorem) *Let $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_i \in K$, $i = 1, 2, \ldots, n$. Then, if α_i, $i = 1, 2, \ldots, n$ are algebraic over F, there exists an element $\alpha \in K$ such that $K = F(\alpha)$, i.e., K is a simple extension of F.*

From the above theorem, it is clear that all finite extensions of F can be expressed as $F(\alpha)$ for some algebraic element α over F. An **automorphism** of a field K is a bijective ring homomorphism from K to K. Consider the set of all automorphisms of K. This set forms a group under composition and is denoted $Aut(K)$. If F is a subfield of K, then the set of all automorphisms of K that act as an identity map on F are called automorphisms of K fixing F. The set of all such automorphisms form a subgroup of $Aut(K)$ and is denoted $Aut_F(K)$. Similarly, consider a subgroup H of $Aut(K)$ and the set of all elements that are fixed by every element in H. This set forms a field and is called the fixed field of H. Then, we have the following theorem.

Theorem A.2.2 *Let K be a finite extension of F of degree n. Then, the cardinality of the group of automorphisms fixing F is less than or equal to n, i.e., $|Aut_F(K)| \leq n$.*

We say a polynomial $f(x)$ over F splits in K if $f(x)$ can be factored into linear factors over K. If K is the smallest field over which the $f(x)$ splits into linear factors, then K is called splitting field.

We call a field extension K/F a **normal extension** if every irreducible polynomial has either all its roots in K or is irreducible over K also. In other words, if K has a root of a polynomial $f(x) \in F[x]$, then, K splits the polynomial $f(x)$. It is known that if K/F is not a normal extension, then there exists a field L containing K, such that L/F is a normal extension.

Let K/F a finite extension of degree n and L be the normal extension of F, such that $F \subset K \subset L$. Then, it is known that there exist exactly n isomorphisms (injective homomorphisms) of K onto subfields of L.

Definition A.2.2 *Let σ_i, $i = 0, 1, 2 \ldots, n-1$ denote the n distinct isomorphisms of K into L. Then, the norm of an element $k \in K$ into F, denoted $N_{K/F}(k)$, is defined as*

$$N_{K/F}(k) = \prod_{i=0}^{n-1} \sigma_i(k).$$

It is known $N_{K/F}(k) \in F$ for all $k \in K$.

In Theorem A.2.2 if $|Aut_F(K)| = n$, then we call the field extension K/F as a **Galois extension**. The group of automorphisms $Aut_F(K)$ fixing F is called the **Galois group** of the extension K/F.

Theorem A.2.3 *A finite extension K/F is a Galois extension if and only K/F is a normal extension.*

A Galois extension is called cyclic or abelian or solvable if the corresponding Galois group is cyclic or abelian or solvable respectively.

A.3 Tensor products

To define tensor product of two algebras, we will first define tensor product of two vector spaces. Since any algebra is a vector space, we will extend the definition of tensor product of two spaces to tensor product of two algebras [55, Chap 9].

Definition A.3.1 *Let V and W be two F-vector spaces. A* **tensor product** *of V and W is an F-vector space $V \otimes_F W$, together with a bilinear mapping $V \times W \mapsto V \otimes_F W$ denoted by $(v, w) \mapsto v \otimes_F w$ such that*

1. *$V \otimes_F W$ is generated as an F-space by $\{v \otimes_F w | v \in V, w \in W\}$,*
2. *(Universality) if $\psi : V \times W \mapsto P$ is a bilinear map, where P is another F-space, then there is an F-linear map $\kappa : V \otimes_F W \mapsto P$ such that $\kappa(v \otimes_F w) = \psi(v, w)$.*

The following sequence of theorems lists some of the useful properties of tensor products.

Theorem A.3.1 *Let V and W be two F-vector spaces. Then,*

1. *The homomorphism κ in the definition of tensor product $V \otimes_F W$ is unique.*

2. *If $V \otimes_F W$ and $V \otimes'_F W$ are tensor products of V and W, then there is a unique isomorphism $\phi : V \otimes_F W \mapsto V \otimes'_F W$ such that $\phi(v \otimes_F w) = v \otimes'_F w$ for all $v \in V$ and $w \in W$.*

From the above theorem, since any two tensor products of two vector spaces are isomorphic to each other, we can write "a tensor product" of two vector spaces as "the tensor product" of two vector spaces. The following theorem guarantees us the existence of the tensor product of two vector spaces.

Theorem A.3.2 *The tensor product of two F-vector spaces V and W exists.*

Now, since F-algebras are F-vector spaces, we can define tensor product of two F-algebras as the the tensor product of the corresponding vector spaces with a suitably defined multiplication. The following theorem assures us of such a multiplication.

Theorem A.3.3 *If A and B are F-algebras, then there is a multiplication operation on $A \otimes_F B$ that satisfies*

$$(x_1 \otimes_F y_1)(x_2 \otimes_F y_2) = x_1x_2 \otimes_F y_1y_2.$$

This multiplication is associative and $1_A \otimes_F 1_B = 1_{A \otimes_F B}$.

Theorem A.3.4 *Let K be a field containing F and A be an F-algebra. Then, $A \otimes_F K$ is a K-algebra satisfying*

$$(x \otimes_F k)(y \otimes_F k') = xy \otimes_F kk'$$

for all $x, y \in A$ and $k, k' \in K$. The scalar operations by elements of K on $A \otimes_F K$ is defined by

$$xk = x(1 \otimes_F k)$$

for all $x \in A \otimes_F K$ and $k \in K$.

Bibliography

[1] E. Telatar, "Capacity of multi-antenna Gaussian channels," AT & T Bell Labs., Tech. Report, June 1995 and European Transactions on Telecommunications, vol.10, pp.585-595, Nov 1999.

[2] G. J. Foschini and M. Gans, "On the limits of wireless communication in a fading environment when using multiple antennas," Wireless Personal Communications, vol.6 pp.311-335, Mar 1998.

[3] Vahid Tarokh, Nambi Seshadri and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inform. Theory,* vol.44, no.2, pp.744-765, March 1998.

[4] J. -C. Guey, M. P. Fitz, M. R. Bell and W. Y. Kuo, "Signal design for transmitter diversity wireless communication systems over Rayleigh fading channels," *Proc. IEEE Vehicular Technology Conf.*, 1996, pp.136-140. Also in *IEEE Trans. Commun.*, vol.47, no.4, pp.527-537, April 1999.

[5] S. M. Alamouti, "A simple transmit diversity technique for wireless communication," *IEEE J. on Select. Areas in Commun.*, vol.16, no.8, pp.1451-1458, Oct. 1998.

[6] Vahid Tarokh, H. Jafarkhani and A. R. Calderbank, "Space-Time block codes from orthogonal designs," *IEEE Trans. Inform. Theory,* vol.45, pp.1456-1467, July 1999. Also "Correction to "Space-time block codes from orthogonal designs"," *IEEE Trans. Inform. Theory*, vol. 46, no.1, p.314, Jan. 2000.

[7] Zafar Ali Khan and B. Sundar Rajan, " Space-time block codes from co-ordinate interleaved orthogonal designs," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT 2002)*, Lausanne, Switzerland, June 2002, p.275.

[8] G. Ganesan and P. Stoica, "Space-time diversity using orthogonal and amicable orthogonal designs," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP 2000)*, Istanbul, Turkey, 2000, pp. 2561-2564.

[9] G. Ganesan and P. Stoica,"Space-time diversity,"*Signal Processing Advances in Wireless and Mobile Communications*, vol.1, ch.2, pp.59-87, Prentice Hall PTR, 2001.

[10] O. Tirkonen and A. Hottinen, "Square-matrix embeddable space-time block codes for complex signal constellations," *IEEE Trans. Inform. Theory*, vol.48, no.2, Feb. 2002.

[11] Weifung Su and Xiang-Gen Xia, "Two generalized complex orthogonal space-time block codes of rates 7/11 and 3/5 for 5 and 6 transmit antennas", *IEEE Trans. Inform. Theory*, vol.49, no.1, pp.313 -316, Jan. 2003.

[12] Zafar Ali Khan, B. Sundar Rajan and Moon Ho Lee, " On single-symbol and double-symbol decodable designs," in *Proc. IEEE Int. Symp. Information Theory (ISIT 2003)*, Yokohama, Japan, June 29-July 4, p.127.

[13] Haiquan Wang and Xiang-Gen Xia, "Upper bounds of rates of complex orthogonal space-time block codes", IEEE Trans. Inform. Theory, vol.49, no.10, pp.2788 - 2796, Oct. 2003

[14] H. Jafarkhani,"A quasi-orthogonal space-time block code," *ÌEEE Trans. Commun.*, vol.49, no.1, pp.1-4, Jan. 2001.

[15] Weifung-Su and Xiang-Gen Xia, "Quasi-orthogonal space-time block codes with full Diversity," in *Proc. IEEE GLOBECOM*, vol.2, 2002, pp.1098-1102.

[16] Olav Tirkkonen and Ari Hottinen, "Complex space-time block codes for four Tx antennas," in *Proc. IEEE GLOBECOM*, vol.2, 2000, pp.1005-1009.

[17] Naresh Sharma and C. B. Papadias, "Improved quasi-orthogonal Codes," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2002),* March 17-21, vol.1, pp.169-171.

[18] M. O. Damen, K. Abed-Meraim and J. -C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inform. Theory*, vol.48, no.3, pp.628-636, Mar. 2002.

[19] J.Boutrous and E.Viterbo, "Signal Space Diversity : A power and bandwidth efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol.44, pp.1453-1467, Jul 1998.

[20] Y. Xin, Z. Wang and G. B. Giannakis, "Space-time constellation-rotating codes maximizing diversity and coding gains," in *Proc. IEEE GLOBECOM*, vol.1, 2001, pp.455-459.

[21] Hesham El Gamal and M. O. Damen, "Universal space-time coding,", *IEEE Trans. Inform. Theory*, vol.49, no.5, pp.1097-1119, May 2003.

[22] M. O. Damen, Ahmed Tewfik and J. -C. Belfiore, "A construction of a space-time code based on number theory", *IEEE Trans. Inform. Theory*, vol.48, no.3, pp.753-760, Mar.2002.

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

[24] A. Roger Hammons and Hesham El Gamal, "On the theory of space-time codes for PSK modulation," *IEEE Trans. Inform. Theory,* vol.46, no.2, pp.524-542, March 2000.

[25] Y.Liu, M.P.Fitz and O.Y.Takeshita, "A rank criterion for QAM space-time codes,"*IEEE Trans. Inform. Theory*, vol.48 no.12, pp.3062-3079, Dec. 2002

[26] B.Hassibi, B.M.Hochwald, A.Shokrollahi and W.Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Trans. Inform. Theory,* vol.47, no.6, pp.2335-2367, Sept. 2001.

[27] B.Hasssibi and M.Khorrami, "Fully-diverse multiple-antenna signal constellations and fixed-point-free Lie groups," in *Proc. IEEE Int. Symp. Information Theory (ISIT 2001)*, Washington D.C., June 2001, p.199. Download available from *http://mars.bell-labs.com.*

[28] A. Shokrollahi, "Design of unitary space-time codes from representations of SU(2)," in *Proc. IEEE. Int. Symp. Information Theory (ISIT 2001)*, Washington D.C., June 2001, p.241. Download available from *http://mars.bell-labs.com.*

[29] B.Hughes, "Optimal space-time constellations from groups," *IEEE Trans. Inform. Theory,* vol.49, no.2, pp.401-410, Feb.2003.

[30] B.Hochwald, T.Marzetta, T.Richardson, W.Sweldens and R.Urbanke, "Systematic design of unitary space-time constellations," *IEEE Trans. Inform. Theory,* vol.46, no.6, pp.1692-1973, Sept. 2000.

[31] B.M.Hochwald and T.L.Marzetta, "Unitary space-time modulation for multiple antenna communication in Rayleigh flat-fading," *IEEE Trans. Inform. Theory,* vol.46, no.2, pp.543-564, March 2000.

[32] T.M.Marzetta, B.Hassibi and B.M.Hochwald, "Structured unitary space-time autocoding constellations," *IEEE Trans. Inform. Theory*, vol.48, no.4, pp.942-950, Apr. 2002.

[33] B.M.Hochwald and M.Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Commun.*, vol.48, no.12, pp.2041-2052 , Dec. 2000.

[34] B. A. Sethuraman and B. Sundar Rajan, "Optimal STBCs over PSK signal sets from cyclotomic field extensions," in *Proc. IEEE Int. Conf. Comm.(ICC 2002)*, April 28-May 2, New York City, U.S.A., vol.3, pp.1783-1787.

[35] B. A. Sethuraman and B. Sundar Rajan, "STBCs from field extensions of the rational field," in *Proc. IEEE Int. Symp. Inform. Theory,(ISIT 2002)*, Lausanne, Switzerland, June 30-July 5, 2002, p.274.

[36] B. A. Sethuraman and B. Sundar Rajan, "An algebraic description of orthogonal designs and the uniqueness of the Alamouti code," in *Proc. IEEE GLOBECOM 2002*, Taipai, Nov. 17-21, 2002, pp.1088-1092.

[37] V. Shashidhar, K. Subrahmanyam, R. Chandrasekharan, B. Sundar Rajan and B. A. Sethuraman, "High-rate, full-diversity STBCs from field extensions", in *Proc. IEEE Int. Symp. Inform. Theory (ISIT 2003)*, Yokohama, Japan, June 29-July 4, p.126.

[38] V. Shashidhar, B. Sundar Rajan and R. Chandrasekharan, "Finite-signal-set capacity of STBCs from field extensions", submitted to Globecom 2004, Dallas, Texas.

[39] B. Sethuraman, B. Sundar Rajan and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory: Special Issue on Space-Time Transmission, Reception, Coding and Signal Design,* vol. 49, no. 10, pp. 2596-2616, Oct. 2003.

[40] V. Shashidhar, B. Sundar Rajan and B. A. Sethuraman,"STBCs using capacity achieving designs from cyclic division algebras", *Proc. GLOBECOM 2003, Communication Theory Symposium*, pp. 1957-1962, San Francisco, Dec.1-4, 2003.

[41] V. Shashidhar, B. Sundar Rajan and B. A. Sethuraman, "STBCs using capacity achieving designs from crossed-product division algebras", accepted for presentation in ICC 2004, Paris, France, June 20-24, 2004.

[42] V. Shashidhar, B. Sundar Rajan and B. A. Sethuraman, "Information-lossless STBCs from crossed-product algebras", accepted for presentation at ISIT 2004, Chicago, June 27-July 2, 2004.

[43] S. Galliou and J. -C. Belfiore, "A new family of full rate fully diverse space-time codes based on Galois theory", in *Proc. IEEE Int. Symp. Inform. Theory (ISIT 2002)*, Lausanne, Switzerland, 2002, p.419.

[44] J-C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding", in *Proc. IEEE Int. Workshop on Inform. Theory (ITW 2003)*, Paris, France, Mar.31 - Apr.4, 2003, pp.267-270.

[45] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol.28, no.1, pp.55-67, Jan 1982.

[46] R.G.Gallager, *Information theory and reliable communication*, New York, Wiley, 1968.

[47] Hsiao-feng Lu and P. Vijay Kumar, "Rate-diversity tradeoff of space-time codes with fixed alphabet and optimal constructions," Proc. *IEEE Int. Symp. Inform. Theory*, Yokohoma, Japan, June 29 - July 4, 2003, p. 242.

[48] R. Heath Jr. and A. Paulraj, "Switching between multiplexing and diversity based on constellation distance," in *Proc. Allerton Conf. Communication, Control and Computing,* Sep 30-Oct 2, 2000.

[49] G. J. Foschini, "Layered space-time architecture for wireless communications in a fading environment when using multi-element antennas," Bell Labs, Tech. J., vol.1, no.2, pp.41-59, 1996.

[50] LiZhong Zheng, David N. C. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels", *IEEE Trans. Inform. Theory*, vol.49, no.5, pp.1073-1096, May 2003.

[51] Huan Yao and Gregory W. Wornell, "Structured space-time block codes with optimal diversity-multiplexing tradeoff and minimum delay", *Proc. GLOBECOM 2003, Communication Theory Symposium*, San Francisco, Dec.1-5, 2003, pp. 1941-1945.

[52] Hesham El Gamal, Giuseppe Caire, M. O. Damen, "Lattice coding and decoding achieve the optimal diversity-vs-multiplexing tradeoff of MIMO channels," submitted to *Trans. Inform. Theory.*

[53] P. K. Draxl, *Skew Fields*, Cambridge University Press, 1983.

[54] I. N. Herstein, *Non-commutative Rings*, Carus Mathematical Monographs, Math. Assocn. of America, 1968.

[55] Richard S. Pierce, *Associative Algebras*, Springer-Verlag, Grad Texts in Math number 88, 1982.

[56] Paul J. McCarthy, *Algebraic extensions of fields*, Dover Publications Inc., New York.

[57] V. Shashidhar, B. Sundar Rajan and P. Vijay Kumar, "STBCs with optimal diversity-multiplexing tradeoff for 2, 3 and 4 transmit antennas," accepted for presentation at ISIT 2004, Chicago, June 27-July 2, 2004.

[58] V. Shashidhar, B. Sundar Rajan and P. Vijay Kumar, "Asymptotic-information-lossless designs and diversity-multiplexing tradeoff", submitted to IEEE Trans. Information theory.

[59] V. Shashidhar, B. Sundar Rajan and P. Vijay Kumar, "Asymptotic-information-lossless designs and diversity-multiplexing tradeoff", submitted to Globecom 2004, Dallas, Texas.

[60] Richard Brauer, Über den index und den exponenten von divisionalgebren, Tohuku Math. J., **37** 1933, pp.77–87.

[61] Bertrand M. Hochwald and Stephan ten Brink , "Achieving near-capacity on a multiple-antenna channel," Mathematical Science Research Center, Bell labs, Lucent technologies, Download available from *http://mars.bell-labs.com.*

[62] U.Fincke and M.Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, "*Math. Comput.*, vol.44, p.463-471, Apr.1985.

[63] E.Viterbo and J.Boutros, "A universal lattice code decoder for fading channel,"*IEEE Trans. Inform. Theory*, vol.45, pp.1639-1642, July 1999.

[64] M.O.Damen, A.Chkeif and J.-C.Belfiore, "Lattice code decoder for space-time codes," *IEEE Commun. Lett.*, vol.4, pp.161-163, May 2000.

[65] B.Hassibi and H.Vikalo, "On the expected complexity of sphere decoding," in *35th Asilomar Conf. Signals, Syst., Comput.,* vol.2, Nov 2001, pp.1051-1055.

[66] M.O.Damen, K.Abed-Merriam and J.-C.Belfiore, "Generalized sphere decoder for asymmetrical space-time communication architecture," *IEE Electronics letters*, vol.36, no.2, 20 Jan 2000, pp.166-167.

[67] C.P.Schnorr and M.Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Programming*, vol.66, pp.181-191, 1994.

[68] Albert M.Chan and Inkyu Lee, "A new reduced-complexity sphere decoder for multiple antenna systems," *Proc. IEEE Int. Conf. Commun. (ICC 2002)*, vol.1, April28-May 2, 2002, pp.460-464.

[69] N. Jacobson, Basic Algebra I, Second Edition, W.H.Freeman and Company, New York, 1985.

[70] N. Jacobson, Finite-dimensional Division Algebras over Fields, Springer-Verlag, New York, 1996.