uOttawa

L'Université canadienne
Canada's university

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Terasan Niyomsataya
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

Ph.D. (Electrical Engineering)
GRADE / DEGREE

School of Information Technology and Engineering
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

On Designs and Fast Decoding Algorithms of Space-Time Codes and Group Codes

TITRE DE LA THÈSE / TITLE OF THESIS

Ali Miri
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

Monica Nevins
CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

EXAMINATEURS (EXAMINATRICES) DE LA THÈSE / THESIS EXAMINERS

Thomas A. Gulliver

Halim Yanikoeroglu

Claude D'Amours

Abbas Yongacoglu

Gary W. Slater
Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

On Designs and Fast Decoding Algorithms of Space-Time Codes and Group Codes

Terasan Niyomsataya

Thesis Submitted to
The Faculty of Graduate and Postdoctoral Studies
In Partial Fulfillment of The Requirements
For The Ph.D. Degree in Electrical Engineering

Ottawa-Carleton Institute for Electrical and Computer Engineering
School of Information Technology and Engineering
University of Ottawa

Your file Votre référence
ISBN: 978-0-494-52336-0
Our file Notre référence
ISBN: 978-0-494-52336-0

Abstract

This thesis consists of two main areas: space-time coding for multiple-input multiple-output (MIMO) wireless systems and group coding generated from affine reflection groups.

MIMO systems, using multiple antennas at the transmitter and receiver, employ multiplexing to increase the rate and diversity to improve the performance and spectral efficiency of data transmission in wireless communications. Space-time coding has been developed to achieve high data rate and reliability in MIMO wireless systems. The research on space-time coding (in code designs, performance analysis, decoding algorithms and its applications) has been growing rapidly in past decade.

We present systematic designs of full diversity unitary space-time codes with high coding gain, using group codes (permutation codes variant II and finite reflection group codes), the Bruhat decomposition and character tables of groups. We also analyze the pairwise error probability of space-time codes in a keyhole channel, and develop a fast optimization to the decision metric of multiple-symbol detection for differential unitary space-time modulation using a stack algorithm.

Group codes generated from affine reflection group codes are related to high dimensional constellations, that is, lattice codes. High dimensional constellations have been studied widely for problems in communication systems, with priority on finding those with good minimum nearest-neighbour distance and simple decoding algorithm.

We derive formulas for the initial vector and best minimum distance of affine reflection group codes of any rank. We also propose efficient decoding algorithms (from the geometrical analysis of groups and from their trellis diagram representations). This includes an original method to decode the codewords which lie outside the bounded region. Finally, we investigate their applications to orthogonal frequency division multiplexing (OFDM) systems to reduce a peak-to-average power ratio.

Acknowledgements

I would like to express my most sincere gratitude and deepest appreciation to my supervisors, Dr.Ali Miri and Dr.Monica Nevins for all their guidance, patience and support throughout the thesis process. Without their valuable efforts, I would not be able to complete the thesis.

Dr.Ali Miri has been very supportive and friendly since the first day I met him. Thank you for your belief to accept and give me a precious opportunity to work as your graduate student. I am truly indebted to your support, suggestions and encouragement for past 6 years.

I still remember the first (meeting) day I met Dr.Monica Nevins. On that day, I gave the presentation on space-time group coding and she showed up with her little cute newborn baby. Her valuable comments and energetic efforts always inspire and help me through the difficult time to finish this thesis.

I have been very fortunate and privileged to learn and work closely with Dr.Ali Miri and Dr.Monica Nevins. They will always be my role models for good professor and researcher.

I would like to thank all examiners, Dr.Halim Yanikomeroglu, Dr.Claude D'Amours, Dr.Abbas Yongacoglu and Dr.Thomas A. Gulliver, for making and coming to my oral defence, and also for their helpful comments and suggestions.

I am also grateful to the government of Canada for support funding on Ontario Graduate Scholarships (OGS) and also Faculty of Graduate and Postdoctoral Studies (FGPS) at University of Ottawa on Doctoral Research Scholarships for my Ph.D. program.

Finally, I dedicate this thesis to my parents for their love, support and inspiration to my life.

Contents

List of Symbols

$\boldsymbol{v}$	(Row or column) vector
$\boldsymbol{V}$	Matrix or vector space
$*$	Complex conjugate
$\dagger$	Complex conjugate transpose
t	Transpose
Tr	Trace of a matrix
det	Determinant
$\operatorname{diag}(a_1, \ldots, a_m)$	Diagonal matrix whose elements are $a_1, \ldots, a_m$
σ	Singular value of a matrix
$\|\boldsymbol{V}\|$	Norm of matrix $\boldsymbol{V}$
$\boldsymbol{I}_n$	$n \times n$ identity matrix
φ	Representation
j	$\sqrt{-1}$
$\cdot$	Dot product
$\oplus$	Direct sum
$\rtimes$	Semi direct product
$\star$	(Circular) convolution
$\langle \boldsymbol{v} \rangle$	span $\{\boldsymbol{v}\}$
$\mathbb{R}$	Real number
$\mathbb{C}$	Complex number
$\mathbb{Z}$	Integer number
n_T	Number of transmitter antennas
n_R	Number of receiver antennas
h	Channel fading coefficient

$\boldsymbol{H}$	Channel matrix
ρ	Signal-to-noise ratio
R	Data rate (bits/s)
L	Size (or order)
P_e	Probability of error
P_{PEP}	Probability of pairwise error
$\mathcal{V}$	Signal constellation (also refers to Bruhat constellation in Chapter 4)
$\mathcal{B}$	Hamiltonian Bruhat constellation (in Chapter 4)
$\zeta_{\mathcal{V}}$	Diversity product
$\xi_{\mathcal{V}}$	Diversity sum
N_d	Number of detected symbols
N_p	Number of distinct paths
N_{sp}	Number of survivor paths
B_c	Bandwidth of channel
B_n	Bandwidth of subchannel
B_s	Bandwidth of signal
T_n	Duration time of subchannel
L_c	Length of channel
G	Length of cyclic prefix
N_c	Number of subcarriers
Δf	Frequency spacing
W	Sampling factor
Φ	Root system
Φ^+	Positive root system
Δ	Simple system
Δ_p	Passive simple system
$\boldsymbol{r}$	Root
$\boldsymbol{\rho}$	Highest long root
$\boldsymbol{\lambda}$	Dual basis vector
$H_{\boldsymbol{r}}$	Hyperplane associated to root $\boldsymbol{r}$

$S_{\boldsymbol{r}}$	Reflection associated to root $\boldsymbol{r}$
D_Δ	Fundamental domain associated to simple system Δ
$\mathcal{G}$	Finite reflection group
$\mathcal{G}_a$	Affine reflection group (or affine Weyl group)
$\boldsymbol{x}_0$	Initial vector
$d_{\min}$	Nearest codeword distance (or minimum distance)
Λ	Lattice
$\Lambda^\vee$	Coroot lattice
Λ_L	Rectangular lattice
γ	Coding gain of lattice
$\boldsymbol{G}$	Generator matrix of lattice
$\mathcal{R}_M$	Bounded codeword region of radius M
N_{ct}	Number of subcarriers whose signals have more than one representation
J	Number of representations (in TI method, Chapter 9)
$(\ )^\pi$	Permutation (in Chapter 9)

List of Acronyms

ARG	Affine reflection group
ARGC	Affine reflection group code
BER	Bit error rate
BLER	Block error rate
CCDF	Complementary cumulative density function
CP	Cyclic prefix
DC	Design criterion
DFT	Discrete Fourier transform
DUSTM	Differential unitary space-time modulation
FRG	Finite reflection group
FRGC	Finite reflection group code
HEX	Hexagonal constellation
IDFT	Inverse Discrete Fourier transform
ISI	Intersymbol interference
MIMO	Multiple-input multiple-output
ML	Maximum likelihood
MSD	Multi-symbol detection
MGF	Moment Generating Function
OFDM	Orthogonal frequency division multiplexing
OSTBC	Orthogonal space-time block code
PAPR	Peak-to-average power ratio
PEP	Pairwise error proability
PSK	Phase shift keying
PTS	Partial transmit sequences

QAM	Quadrature amplitude modulation
SER	Symbol error rate
SNR	Signal-to-noise ratio
STBC	Space-time block code
STC	Space-time code
STTC	Space-time trellis code
TI	Tone injection
USTC	Unitary space-time code

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

In this thesis, we study problems in two main areas:: space-time coding and group coding. In the area of space-time coding, we construct new full diversity unitary space-time codes with high coding gain, propose decoding schemes with low complexity and investigate the code performance analysis. With regards to group coding, we present the construction and fast decoding algorithms of group codes generated from affine reflection groups. Furthermore we give an application of affine reflection group codes using the proposed decoding algorithms to orthogonal frequency division multiplexing systems.

1.1.1 Space-Time Coding

The challenges faced in the development of future fixed and mobile broadband wireless communications lie in high rate, reliable data transmission, bandwidth efficiency, and a good quality of service. *Multiple-input multiple-output (MIMO)* wireless systems, using multiple antennas at the transmitter and receiver, can achieve these goals. MIMO systems enhance the capacity and promise greater reliability of data transmission in a wireless channel [18, 19, 94]. *Space-time coding* which employs space diversity (from the correlation of signals across the different transmitter and receiver antennas) and time diversity (from the retransmission of messages) has been developed for use in MIMO systems to achieve high data rate and reliability.

We want to improve the performance of space-time coding for MIMO wireless systems in three aspects: code designs, decoding schemes and the performance analysis.

Code Designs

The main *rank and determinant criteria* for the design of *space-time codes (STC)* was first proposed in [93]. The paper also presented *space-time trellis codes (STTC)*. The disadvantage of STTC is its complexity which grows exponentially with the code rate and the number of memory states. Then *orthogonal space-time block codes (OSTBC)* were presented in [2, 91, 92]. The significant improvement of OSTBC is its simple decoding, using a technique of signal combining and maximum-likelihood (ML) detection.

In practical situations and without imposing any training schemes, the fading coefficient of the channel is generally not known to the receiver. *Differential unitary space-time modulation (DUSTM)* was presented for use in unknown fading channels where neither the transmitter nor the receiver antennas know the fading coefficient of the channel [35, 36, 41, 90]. The technique of DUSTM can be considered as an extension of differential detection of phase shift keying (PSK) modulation for single antenna systems. The signal constellation used in DUSTM is called a *unitary space-time code (USTC)*. The measurement of full diversity and high coding gain of USTC is defined from the *diversity product* and the *diversity sum* at high and low signal-to-noise ratio (SNR) respectively [49, 80].

The problem of constructing USTC with high diversity product or diversity sum has been studied in many prior works. For example, some of the group structures proposed to represent USTC are cyclic and dicyclic groups [35, 36, 37], fixed-point free groups [80], the compact symplectic group $Sp(2)$ for four transmitter antennas [44] and the special unitary group $SU(3)$ for three transmitter antennas [45]. Some examples of nongroup constellations include orthogonal designs [91, 97], parametric codes [49] and APSK Alamouti's codes [86] for only 2 transmitter antennas, numerical methods [28], the generalization and the product of fixed-point free groups [80] as well as Hamiltonian and Product constellations [57, 65]. Furthermore, there are works of several authors using ideas in number theory (particularly, division algebras and field extensions of the rationals), to produce effective linear STC [21, 70, 71, 75], some of which may be adapted to produce USTC using the Cayley transform [33] and threaded algebraic space time (TAST) codes [21].

With respect to the problem of designing of STC, we focus on developing new solutions for the systematic construction of full diversity USTC with high coding gain. The goal is to construct full diversity USTC to achieve a full rank criterion and maximize a determinant criterion as proposed in [93]. To this end, we present two group codes (permutation codes variant II and finite reflection group codes) to construct full diversity USTC with high diversity product for two transmitter antennas.

We also apply two mathematical methods (the Bruhat decomposition and character tables from group theory) as new systematic approaches to constructing unitary group STBCs for any number of transmitter antennas. The advantage of using the Bruhat decomposition to construct a unitary group constellation is that it allows us to choose disjoint non-overlapping cosets of a unitary diagonal subgroup in such a way that the full diversity is preserved. The application of the Bruhat decomposition to the design of full diversity USTC was first introduced in [47] for only 2 and 4 transmitter antennas.

The characteristic polynomial, which is derived from the character table of a group, has been first proposed as a method to compute the diversity product of a unitary group STBC in [79]. We also use a character table of a group to compute the diversity sum of a unitary group STBC. Having chosen a high diversity sum unitary group constellation from a character table, the superior performance in low SNR of the corresponding group constellation may be predicted in advance.

Low Complexity Decoding Algorithm

Multiple-symbol detection (MSD) was first introduced for DUSTM with two transmitter antennas in [17] to overcome the 3 dB loss in performance compared to coherent detection. The decision metric of MSD was proposed in [22], for any number of transmitter antennas. The complexity of the searching problem of the MSD decision metric is $O(L^{N_d})$ where L is the size of unitary signal constellation and N_d is the number of detected symbols. This exponential growth implies high complexity for large L and N_d.

Many prior works have presented methods to reduce the complexity. For example, the feedback and reduced search detections for two transmitter antennas [88], the (sub-optimal) approximation of the MSD decision metric with the Per-Survivor Processing (PSP) method [10], the bound-intersection detector (BID) method [15] which works only for diagonal USTC and the sphere and Fano detections in [72].

We present an optimal stack algorithm approach as a fast optimization of the MSD decision metric for DUSTM. The proposed stack algorithm allows us to consider a greater number of detected symbols which consequently increases the decoding performance with low additional complexity.

Performance Analysis

Recently, the papers [11, 25, 52] have shown that zero or low correlation of fading channel coefficients of a MIMO channel does not guarantee high channel capacity. *Keyholes*, whose fading coefficients are uncorrelated, cause a rank deficiency of the channel matrix. This degrades the channel capacity and the performance of STC over the channel [11, 52, 77, 78]. One example of keyholes, in practical situations, is the roof edge diffraction phenomenon, as explained in [11].

The symbol error rate (SER) performance of STBC in a keyhole channel was studied in [78]. The proposed SERs in [78] which are derived from a Moment Generating Function (MGF)-based approach to the conditional SER for a given instantaneous SNR are exact, but apply only to STBC. More generally, the calculation of average pairwise error proability (PEP) and a design criterion of STC in a keyhole channel have been presented in [87] (it was also investigated in [56] for STTC but only for two transmitter antennas and one receiver antenna). However when the eigenvalues of a codeword pair difference are not distinct (for example, in the 2×2 OSTBC), the PEPs proposed in [56, 87] do not apply.

We give an improvement of the tight upper bound on the average PEP of STC for a keyhole channel. The proposed PEP is given in closed form using hypergeometric functions. Furthermore it applies to all full rank STC (STBC and STTC) for any number of antennas.

1.1.2 Group Coding

In addition to using the group codes (such as finite reflection groups and permutation code variant II) to design full diversity USTC with high coding gain as we have mentioned above, we have also studied the problem of code construction and decoding methods of group codes themselves. In particular, we consider group codes generated from *affine reflection groups (ARG)* which has not been solved in the literature.

Code Construction and Decoding Algorithms

Slepian [84] introduced *group codes* for the Gaussian channel whose codewords represent a finite set of signals combining coding and modulation. The codewords lie on a sphere in $n-$dimensional Euclidean space $\mathbb{R}^n$ with equal nearest-neighbour distances. This gives congruent ML decoding regions, and hence equal error probability, for all codewords. The set of codewords of group codes are generated by operating with each element of the group on an optimal vector, called an *initial vector*. The initial vector problem is to choose a vector which maximizes the Euclidean distance between a codeword and its nearest neighbour, over all codewords. The problem has not been solved for general groups, but rather is known only for special cases such as for permutation codes [83], for cyclic groups [6], for the full homogeneous representation and the $(n-1)$-dimensional representation of the symmetric groups of rank n [8] and for finite reflection groups (FRG) [53, 54].

We consider a group code generated from ARGs [39]. More generally, a group may act on $\mathbb{R}^n$ via affine transformations (which include linear transformations as well as translations). In this case, the codewords are not constrained to lie on a sphere. We call a group code generated from ARG, an *affine reflection group code (ARGC)*.

We present the construction of ARGCs. This includes the solution of the initial vector problem and the nearest neighbour distance. We also propose an explicit method to draw a trellis diagram representation of the codes and develop efficient decoding methods for ARGCs of any rank.

Applications of Affine Reflection Group Codes To OFDM

We investigate the structure of ARGCs and conclude that they are cosets of the *coroot lattice* [4, 13]. Thus one could use ARGC as a high spectral efficiency multi-dimensional signal constellation in communication systems.

A multi-carrier spread spectrum transmission method based on orthogonal frequency division multiplexing (OFDM) enhances the capacity and performance of wireless communications on frequency-selective and time-variant channels [7, 32]. It combats multipath delay spreads (which severely limit the transmission rate) without decreasing the bandwidth efficiency. The signal is divided into subcarriers (with orthogonal frequencies) and transmitted on frequency-flat subchannels where each subcarrier signal is more immune against multipath fading. Inserting a guard interval (or a cyclic prefix) between subcarriers can completely eliminate the intersymbol and intersubchannel interference (ISI and ICI). This gives OFDM a simple implementation of equalizer at the receiver.

OFDM has been chosen for several wireless standards [26, 32, 98], for example, for digital audio/video broadcasting (DAB, DVB-T) in Europe, for wireless local area network (WLAN) *e.g.* IEEE 802.11a, g and n or HIPERLAN/2, and also for high speed digital subscriber line (DSL) modems.

One disadvantage of OFDM is high *peak-to-average power ratio (PAPR).* In practical situations, the operation of the power amplifier is nonlinear at high voltage (that is, has distortion). Hence we would like to reduce PAPR in order for the power amplifier to operate in its linear range which has its maximum efficiency. Many prior works have addressed the reduction of the PAPR of an OFDM transmitted signal. An overview of PAPR reduction methods and their comparisons can be found in [31, 50]. These methods include amplitude clipping, partial transmit sequences (PTS), selected mapping (SLM), constellation-trellis shaping and tone injection (TI).

We are interested in the TI method which was first presented in [95]. The TI method is done by substituting a point from the original constellation into a new (larger) constellation where one point could have more than one representation. This substitution is equivalent to injecting a tone of appropriate frequency and phase of the OFDM signal for the PAPR reduction. The advantages of TI method compared to other PAPR reduction methods are: it has medium complexity, is distortionless, has no loss in data rate and does not require the channel side information (CSI) between the transmitter and receiver. The larger size of constellation (which increases the average power transmission) is an disadvantage of TI method.

In particular interest, we consider the TI method from a hexagonal constellation presented in [29]. We give an application of an ARGC $\mathcal{A}_2$, using the proposed decoding methods, as a TI constellation to reduce PAPR of an OFDM system.

1.2 Contributions

The summary of our original contributions (as well as the connections between problems) in this thesis is shown in Figure 1.1.

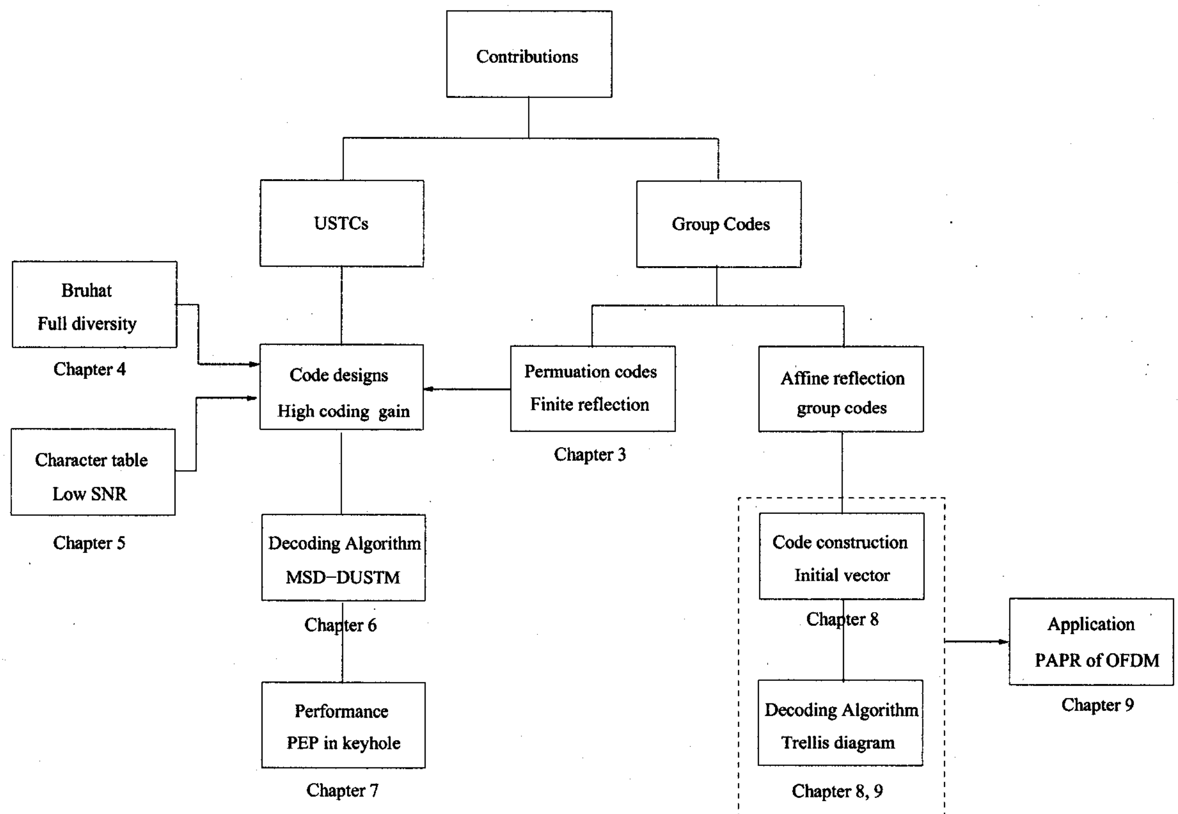

Figure 1.1: A summary of our original contributions

The details on a summary of our contributions as shown in Figure 1.1 are given as the following:

- We present new full diversity USTCs based on group codes (permutation codes variant II and FRGs) for two transmitter antennas. The proposed construction is algorithmic and requires no optimization (searching) steps. The new USTCs have excellent diversity products and also outperform other USTC designs in the literature.

This work is described in Chapter 3. It was presented at the IEEE Canadian Conference in Electrical and Computer Engineering, CCECE 2004 [61] (for permutation codes variant II) and at the Canadian Workshop in Information Theory, CWIT 2005 [62] (for finite reflection group codes (FRGC)). The full paper was published in the *Journal on Designs, Codes and Cryptography* in 2006 [63].

- We propose a new systematic design for constructing full diversity USTCs for any number of transmitter antennas, using the Bruhat decomposition. We also propose new full diversity Hamiltonian Bruhat USTCs (combining Hamiltonian and Bruhat unitary constellation) for even numbers of transmitter antennas. Our proposed Bruhat and Hamiltonian Bruhat USTCs perform well in unknown channel environment and outperform other full diversity USTC designs.

  The full diversity USTC constructed from Bruhat decomposition is presented in Chapter 4. It was presented at the 22nd Biennial Symposium on Communications 2004 [60] (for prime numbers of transmitter antennas) and in IEEE Information Theory Workshop, ITW 2004 [59] (for any number of transmitter antennas). The full paper (along with Hamiltonian Bruhat USTC) was submitted to *IEEE Transactions on Information Theory* in 2004 [58] (and remains in active submission).

- We propose a new method to compute the diversity sum of a unitary group STBC using a character table. We provide closed form formula to compute the diversity sum of unitary group STBCs from cyclic groups, dicyclic groups and finite special linear groups. We introduce the notion of a faithful unitary group STBC and also show how to obtain one from any nontrivial character of a group.

  The computation of the diversity sum from a group character table is presented in Chapter 5 and was submitted as a correspondence to *IEEE Transactions on Information Theory* in 2004 [69] (and remains in active submission).

  Note: All of our proposed USTC presented in this thesis (from permutation codes variant II, FRGCs, Bruhat decomposition as well as a character table method) can be used for both known and unknown fading channels.

- We give a simple closed form solution for the average PEP of STC in a keyhole channel. The proposed PEP is expressed as a hypergeometric function which works for any full rank STC and for any number of transmitter antennas. We also correspondingly develop the design criterion for STC in a keyhole channel from a computation of max-min eigenvalues.

The average PEP of STC in a keyhole channel is presented in Chapter 7 and was published in *IEE Proceedings on Communications* in 2007 [64].

- We present a fast MSD for DUSTM for any number of transmitter antennas, using a stack algorithm. The significant improvement from previous works in the literature is our proposed stack algorithm can be used for any (diagonalizable and nondiagonalizable) USTC and also without requiring any knowledge of their code's algebraic structure. Unlike most applications of using a stack algorithm, which are suboptimal, Theorem 6.2.1 shows that the proposed stack algorithm is equivalent to ML detection. The complexity required to maximize the decision metric using the proposed stack algorithm is reduced from $O(L^{N_d}N_d^2)$ to $O(LN_d^2)$ at high SNR.

  The proposed stack algorithm for optimizing the MSD decision metric is presented in Chapter 6, and it was accepted for presentation in the 24th Biennial Symposium on Communications 2008 [68].

- We present a construction of ARGCs. The closed-form solution of an initial vector as well as the formula for the nearest-neighbour distance of the corresponding ARGCs is given for all irreducible ARGs of any rank (and also for varying stabilizer subgroups).

  The summary of the solutions to the initial vector problem, together with the corresponding nearest distance are given in Chapter 8.

- We also propose the fast and low complexity decoding algorithms of ARGCs. The proposed decoding algorithm has 3 steps as shown in Figure 8.3. The step 1 and 2 are pioneering methods in the literature to decode the codewords which lie outside the bounded region. The step 3 which works well for ARGs of rank 2 and 3 has less complexity compared to lattice decoding.

  The construction and decoding algorithm of ARGCs are presented in Chapter 8. It was published in *IEEE Transactions on Information Theory* in 2008 [66] and also was accepted for presentation in the 24nd Biennial Symposium on Communications 2008 [67] (for the implementation of rank 2).

- We present a new method to construct the trellis diagram representation of ARGCs of any rank and also develop two efficient decoding (hybrid and lattice cosets) methods.
- We give the application of an ARGC of $\mathcal{A}_2$ using the proposed decoding methods to improve the PAPR reduction of OFDM systems. The two decoding methods and the application of ARGC $\mathcal{A}_2$ for OFDM systems are presented in Chapter 9.

1.3 The Outline of the Thesis

The content of this thesis is organized as follows. Chapter 2 contains the preliminaries of this thesis. We briefly give an overview of DUSTM, the design criteria of STC for a MIMO system, the diversity product and diversity sum, keyhole channel, MSD decision metric for DUSTM, group codes (including permutation code variant II, FRGCs), ARGs, lattices and their trellis diagram representation, OFDM system and PAPR.

Chapter 3 and 4 present the design of full diversity USTC with high diversity product constructed from group codes (permutation codes variant II and FRGCs) and from Bruhat decomposition respectively. The condition of full diversity for an arbitrary number of transmitter antennas and rate as well as the properties of diversity product of proposed Bruhat USTC are also discussed in this chapter. The new approach to the construction of unitary group STCs, with high diversity sum for low SNR using its character table is presented in Chapter 5. In this chapter, we also introduce the notion of faithful unitary group STC and give the example of PSL_2. The low complexity ML optimization of MSD decision metric for DUSTM using a stack algorithm is presented in Chapter 6. The proposed closed form of average PEP and design criterion for STC in keyhole channel are given in Chapter 7.

Chapter 8 presents the construction of ARGCs. We give the solution of optimal initial vector and nearest neighbour distance problems and also present low complexity decoding algorithms for ARG of low rank. The trellis diagram and two efficient decoding methods for any rank of ARGs are given in Chapter 9. The application to PAPR reduction of OFDM systems is also given in this chapter.

The summary and possible extensions of the work of this thesis are discussed in Chapter 10. Some mathematical background (on the Bruhat decomposition, representation theory, character tables of groups, MGF-based approach and hypergeometric functions) is summarized in Appendix A. The computing of optimal initial vectors for all irreducible ARGs listed in Table 8.1 is given in Appendix B. Appendix C lists our publications related to this thesis.

Chapter 2

Preliminaries

Remark on notations: We use a bold uppercase $\boldsymbol{V}$ to denote a matrix (in most chapters of this thesis) or as a vector space (in Section 2.2 and in Chapter 9, or as we mention in detail). A bold lowercase $\boldsymbol{v}$ denotes a vector.

2.1 MIMO Wireless System

Consider a *multiple-input multiple-output (MIMO)* wireless system, with n_T transmitter antennas and n_R receiver antennas in a Rayleigh flat fading channel. Denote by s_{ti} the transmitted signal at time t on transmitter antenna i, $i = 1, 2, \ldots, n_T$. The received signal x_{tj} at time t on a receiver antenna j is

$$x_{tj} = \sqrt{\rho} \sum_{i=1}^{n_T} h_{tij} s_{ti} + \omega_{tj}, \tag{2.1}$$

where ρ is the signal-to-noise ratio (SNR) at each receiver antenna, h_{tij} is the fading coefficient at time t from transmitter antenna i to receiver antenna j and ω_{tj} is the additive noise on receiver antenna j at time t. We assume h_{tij} and ω_{tj} are independent complex Gaussian variables with mean zero and variance one, that is, elements of $\mathcal{CN}(0, 1)$. At each time t, we normalize the expected value of the sum of all transmitted signal powers is equal to one, that is $E\left(\sum_{i=1}^{n_T} |s_{tm}|^2\right) = 1$.

Generally the transmitted signals can be transmitted in a block length of T, and we assume that the fading coefficients are constant within the block T but vary from block to block. Therefore from (2.1), a received signal $\boldsymbol{Y}_\tau$ can be written in a matrix form by

$$\boldsymbol{Y}_\tau = \sqrt{\rho}\boldsymbol{S}_\tau \boldsymbol{H}_\tau + \boldsymbol{W}_\tau \tag{2.2}$$

where $\tau = 0, 1, \ldots$ is the index of the block. The sizes of the received signal matrix $\boldsymbol{Y}_\tau$ and the transmitted signal matrix $\boldsymbol{S}_\tau$ are $T \times n_R$ and $T \times n_T$ respectively. $\boldsymbol{W}_\tau$ is the $T \times n_R$ additive noise matrix and we call $\boldsymbol{H}_\tau$ the $n_T \times n_R$ *channel matrix.*

Let a message sent to the *space-time encoder* be a sequence $z_0, z_1, z_2 \ldots$ with $z_\tau \in \{0, 1, \ldots L-1\}$. Then the transmitted signal matrix $\boldsymbol{S}_\tau$ is chosen from a *signal constellation* $\mathcal{V} = \{\boldsymbol{V}_l\}_{l=0}^{L-1}$ by index z_τ. Equivalently $\boldsymbol{S}_\tau = \boldsymbol{V}_{z_\tau}$ where $\boldsymbol{V}_l$ is a $T \times n_T$ matrix. We call a signal constellation $\mathcal{V}$ transmitted in a block length T, a *space-time block code (STBC).* The data rate (of space-time encoder) is

$$R = \frac{\log_2 L}{T} \text{ bits/s.} \tag{2.3}$$

The received signal matrix is defined by (2.2). Using the maximum-likelihood (ML) criterion, the receiver antenna will decode to a message $\hat{z}_\tau$ by

$$\hat{z}_\tau = \arg \min_{l=0,\ldots,L-1} \|\boldsymbol{Y}_\tau - \boldsymbol{V}_l \boldsymbol{H}_\tau\|^2 \tag{2.4}$$

where $\|\boldsymbol{A}\|^2 = \mathrm{Tr}(\boldsymbol{A}\boldsymbol{A}^\dagger) = \mathrm{Tr}(\boldsymbol{A}^\dagger \boldsymbol{A}) = \sum_{i,j} |a_{ij}|^2$; Tr denotes as the trace of a matrix and $\dagger$ denotes as the conjugate transpose.

2.1.1 Differential Unitary Space-Time Modulation (DUSTM)

In practical applications and without imposing any training schemes, the fading coefficients of the channel are generally not known to the receiver antenna. Hughes [36] and Hochwald *et.al.* [35] proposed *differential unitary space-time modulation (DUSTM)* for multiple antennas with no knowledge of the channel information.

In DUSTM, the signal constellation $\mathcal{V} = \{\boldsymbol{V}_l\}_{l=0}^{L-1}$ is $n_T \times n_T$ unitary (we choose $T = n_T$). The current transmitted signal $\boldsymbol{S}_\tau$ is obtained by multiplication of the previous signal $\boldsymbol{S}_{\tau-1}$ with the element $\boldsymbol{V}_l$ with index z_τ, that is,

$$\boldsymbol{S}_\tau = \boldsymbol{V}_{z_\tau} \boldsymbol{S}_{\tau-1} \tag{2.5}$$

with $\boldsymbol{S}_0 = \boldsymbol{I}_{n_T}$, the $n_T \times n_T$ identity matrix.

Since the channel matrix $\boldsymbol{H}_\tau$ is unknown, we have to modify the received signal $\boldsymbol{Y}_\tau$ of (2.2). We assume that the channel matrix $\boldsymbol{H}_\tau$ is constant over two consecutive time periods, $\boldsymbol{H}_\tau \approx \boldsymbol{H}_{\tau-1} = \boldsymbol{H}$. From (2.2), we will have

$$\begin{aligned} \boldsymbol{Y}_{\tau-1} &= \sqrt{\rho}\boldsymbol{S}_{\tau-1}\boldsymbol{H} + \boldsymbol{W}_{\tau-1}, &(2.6)\\ \boldsymbol{Y}_{\tau} &= \sqrt{\rho}\boldsymbol{S}_{\tau}\boldsymbol{H} + \boldsymbol{W}_{\tau}. &(2.7) \end{aligned}$$

Substiting $\boldsymbol{S}_\tau = \boldsymbol{V}\boldsymbol{S}_{\tau-1}$ in (2.6), and then subtracting the resulting equation to (2.7) gives

$$\boldsymbol{Y}_\tau = \boldsymbol{V}_{z_\tau}\boldsymbol{Y}_{\tau-1} + \boldsymbol{W}_\tau - \boldsymbol{V}_{z_\tau}\boldsymbol{W}_{\tau-1}. \tag{2.8}$$

Since additive noise is independent and invariant under multiplication with a unitary matrix, then the received signal matrix of DUSTM is

$$\boldsymbol{Y}_\tau = \boldsymbol{V}_{z_\tau}\boldsymbol{Y}_{\tau-1} + \sqrt{2}\boldsymbol{W}'_\tau \tag{2.9}$$

where $\boldsymbol{W}'_\tau$ is also an independent $\mathcal{CN}(0,1)$. Using the ML criterion, the receiver antenna decodes the message as $\hat{z}_\tau$ to be

$$\hat{z}_\tau = \arg \min_{l=0,\dots,L-1} \|\boldsymbol{Y}_\tau - \boldsymbol{V}_l\boldsymbol{Y}_{\tau-1}\|^2. \tag{2.10}$$

2.1.2 Multiple Symbol Detection (MSD) For DUSTM

DUSTM in Section 2.1.1 assumes the channel matrix is constant over two consecutive blocks, which allows the detection of one symbol for decoding. The performance of DUSTM loses approximately 3 dB compared to coherent detection [36, 35, 80]. *Multiple-symbol detection (MSD)* was introduced for DUSTM to overcome this loss in performance.

Consider DUSTM as explained in Section 2.1.1. Given N_d detected symbols for decoding, MSD assumes the channel matrix $\boldsymbol{H}$ is constant for N_d+1 blocks at the receiver. The general ML decision metric of MSD for DUSTM given in [22, 15] is

$$\hat{\boldsymbol{z}}_{\tau N_d} = \arg \min_{\substack{\tau \le k \le \tau+N_d-1 \\ 0 \le l_k \le L-1}} \sum_{i=1}^{N_d} \sum_{j=i+1}^{N_d+1} \|\boldsymbol{Y}_{\tau+j-1} - (\prod_{k=\tau+j-2}^{\tau+i-1} \boldsymbol{V}_{l_k})\boldsymbol{Y}_{\tau+i-1}\|^2 \tag{2.11}$$

where $\hat{\boldsymbol{z}}_{\tau N_d} = (\hat{z}_\tau, \hat{z}_{\tau+1} \ldots, \hat{z}_{\tau+N_d-1})$ is a decoded message of length N_d.

The decision metric shown in (2.11) is the sum of $(N_d + 1)N_d/2$ positive terms. For a given signal constellation $\mathcal{V}$ of size L and N_d detected symbols, we can see that the brute-force of the decision metric in (2.11) requires a minimization over all L^{N_d} possible candidates $\{\boldsymbol{V}_{\tau+1}, \boldsymbol{V}_{\tau+2}, \ldots, \boldsymbol{V}_{\tau+N_d}\}$. Hence the complexity is $O(L^{N_d})$ which is high for large L and N_d.

2.1.3 Design Criteria of USTC

The *pairwise error probability (PEP)* that the receiver antenna decodes an error from $\boldsymbol{V}$ to $\boldsymbol{V}'$ is approximated by [36, 35, 80]

$$P_e \leq \frac{1}{2} \prod_{i=1}^{n_T} \left[1 + \frac{\rho^2}{4(1+2\rho)} \sigma_i^2 (\boldsymbol{V} - \boldsymbol{V}') \right]^{-n_R} \tag{2.12}$$

where σ_i denotes the i^{th} singular value of $(\boldsymbol{V} - \boldsymbol{V}')$.

At High SNR

At a high SNR, the upper bound of PEP in (2.12) can be estimated by

$$P_e \leq \frac{1}{2} \left(\frac{8}{\rho} \right)^{n_T n_R} |\det(\boldsymbol{V} - \boldsymbol{V}')|^{-2n_R}. \tag{2.13}$$

It is well known that to minimize the PEP in (2.13) at a high SNR, we need to maximize the *diversity product* defined as [80]

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{\boldsymbol{V}, \boldsymbol{V}' \in \mathcal{V}} |\det(\boldsymbol{V} - \boldsymbol{V}')|^{\frac{1}{n_T}}. \tag{2.14}$$

We say a constellation has *full diversity* if it has $|\det(\boldsymbol{V} - \boldsymbol{V}')| > 0$ for all distinct $\boldsymbol{V}, \boldsymbol{V}' \in \mathcal{V}$. This requirement is called the (full) *rank criterion* in [93]. The design criteria for a full diversity signal constellation $\mathcal{V}$ is to find a set $\mathcal{V}$ of $n_T \times n_T$ unitary matrices which has $\zeta_{\mathcal{V}} \neq 0$ defined in (2.14) as large as possible. This is called the *determinant criterion* in [93].

Upper bounds of the possible values of diversity products for $n_T \geq 2$ as given in [49] are

$$\zeta_{\mathcal{V}\text{ upper}} \leq \sqrt{\frac{L}{2(L-1)}} \quad \text{for } 2 \leq L \leq 2n_T^2 + 1 \tag{2.15}$$
$$\leq \frac{1}{\sqrt{2}} \quad \text{for } 2n_T^2 + 1 < L \leq 4n_T^2 \tag{2.16}$$
$$< \frac{1}{\sqrt{2}} \quad \text{for } L > 4n_T^2. \tag{2.17}$$

We call a signal constellation whose diversity product achieves the upper bound as above, an optimal diversity product constellation. Furthermore, (2.15) is also the exact value of optimal diversity product for $L = 2$ to 5 of any $n_T \geq 2$ transmitter antennas. Table 2.1 shows the largest possible values of diversity product for $L = 2$ to 5.

L	2	3	4	5
$\zeta_{\mathcal{V}} = \sqrt{\frac{L}{2(L-1)}}$	1.0000	0.8660	0.8165	0.7906

Table 2.1: Optimal diversity product for $L = 2$ to 5

At Low SNR

At a low SNR, using a first order approximation, the PEP in (2.12) can be approximated by [49]

$$P_e \leq \frac{1}{2}\left[1 + \frac{\rho^2}{4(1+2\rho)}\sum_{i=1}^{n_T}\sigma_i^2(\boldsymbol{V} - \boldsymbol{V}')\right]^{-n_R}. \tag{2.18}$$

Thus in this case we want to minimize the PEP by maximizing the *diversity sum* which is defined as [49]

$$\xi_{\mathcal{V}} = \frac{1}{2\sqrt{n_T}} \min_{\boldsymbol{V},\boldsymbol{V}' \in \mathcal{V}} \|\boldsymbol{V} - \boldsymbol{V}'\|. \tag{2.19}$$

Properties

When a unitary constellation $\mathcal{V}$ has zero diversity product, that is, when there exists $\boldsymbol{V} \neq \boldsymbol{V}' \in \mathcal{V}$ such that $|\det(\boldsymbol{V} - \boldsymbol{V}')| = 0$, then the upper bound on P_e at high SNR as estimated by the equation (2.13) tends to infinity which is meaningless. For the case of low SNR, the upper bound on P_e given by the equation (2.18) is always finite, because $\sum_{i=1}^{n_T} \sigma_i^2(\boldsymbol{V} - \boldsymbol{V}')$ is always greater than or equal to zero.

2.1.4 Keyhole Channel

The model of a keyhole is shown in Figure 2.1. It is a screen with a small hole (called a *keyhole*) between n_T transmitter and n_R receiver antennas in a Rayleigh-flat fading channel.

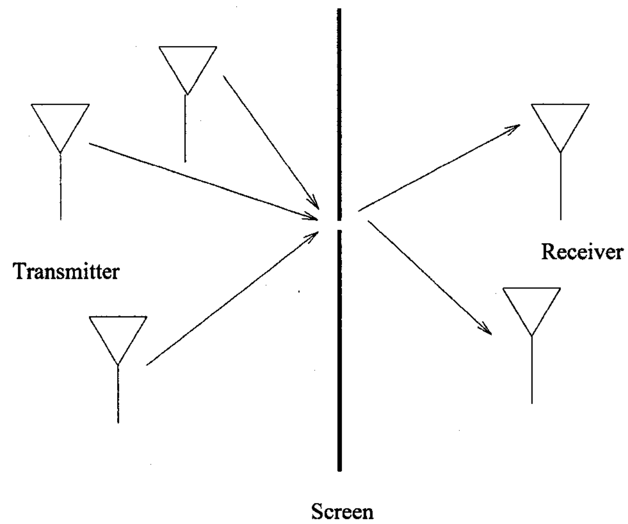

Figure 2.1: Keyhole channel

The transmitted signals can propagate to the receiver antennas only by passing through the keyhole. This situation is modelled by assuming that the fading coefficients of the $n_R \times n_T$ channel matrix $\boldsymbol{H}$ are a product of two uncorrelated Gaussian random variables. Specifically, set $\boldsymbol{\beta} \in \mathbb{C}^{n_R \times 1} = [\beta_1, \beta_2, \ldots, \beta_{n_R}]^t$ and $\boldsymbol{\alpha} \in \mathbb{C}^{n_T \times 1} = [\alpha_1, \alpha_2, \ldots, \alpha_{n_T}]^t$, where β_i and α_j are assumed to be independent $\mathcal{CN}(0,1)$ random variables, representing scattering at the transmitter and receiver antennas respectively. Then, by [11], the channel matrix is defined as

$$\boldsymbol{H} = \boldsymbol{\beta}\boldsymbol{\alpha}^t. \tag{2.20}$$

The rank of $\boldsymbol{H}$ is 1. In other words, a keyhole causes a rank deficiency of the channel matrix $\boldsymbol{H}$ which degrades the channel capacity and the performance of STC over the channel [11, 52, 77, 78].

2.2 Groups

A summary of finite and affine reflection groups (and also related crystallographic finite reflection groups, coroots and lattices) is given in this section. The finite and affine reflection groups are used to generated group codes, called finite reflection and affine reflection group codes respectively.

2.2.1 Finite Reflection Groups

Let $\mathcal{G}$ be a *finite reflection group (FRG)* which is generated by linear reflections. We define a *root system* Φ of a FRG $\mathcal{G}$ from a set of vectors in the vector space $\boldsymbol{V}$ such that (R1) for all *roots* $\boldsymbol{r} \in \Phi$, $t\boldsymbol{r} \in \Phi$ if and only if $t = \pm 1$ and (R2) for all $g \in \mathcal{G}$, $g\Phi \subset \Phi$, that is, the group preserves the set of roots. Then $\mathcal{G}$ is in fact generated from the *reflections* $S_{\boldsymbol{r}}$ in the *hyperplanes* $H_{\boldsymbol{r}}$, for $\boldsymbol{r} \in \Phi$. The reflection $S_{\boldsymbol{r}} \in \mathcal{G}$ of a vector $\boldsymbol{x} \in \mathbb{R}^n$ is explicitly defined via [54]

$$S_{\boldsymbol{r}}\boldsymbol{x} = \boldsymbol{x} - 2\frac{\boldsymbol{x} \cdot \boldsymbol{r}}{\boldsymbol{r} \cdot \boldsymbol{r}}\boldsymbol{r}. \tag{2.21}$$

Let $H = \{H_{\boldsymbol{r}}, \boldsymbol{r} \in \Phi\}$ be the set of all hyperplanes. The FRG $\mathcal{G}$ is *irreducible* if there does not exist a partition of H into mutually orthogonal sets; equivalently, if there does not exist a proper nonzero subspace of span Φ which is preserved by all reflections in $\mathcal{G}$. The root systems of all irreducible FRGs are given in [54, Table II]. Figure 2.2 shows all roots (the solid lines) and hyperplanes (the dashed lines) of the irreducible FRG $\mathcal{A}_2$.

A *simple system* Δ which is a subset of a root system Φ satisfies (S1) span(Δ) = span(Φ), (S2) Δ is linearly independent and (S3) every $\boldsymbol{r}' \in \Phi$ is a linear combination $\sum_{\boldsymbol{r}_i \in \Delta} c_i \boldsymbol{r}_i$ such that either all c_i are ≥ 0 or all c_i are ≤ 0. That is to say, all roots lie in the cone determined by the simple roots. The *rank* of FRG is n, the number of simple roots, and we write $\Delta = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_n\}$. A root system has the property that $\Phi = \Phi^+ \cup -(\Phi^+)$ where the positive root system Φ^+ is the set of roots which are nonnegative linear combinations of elements of the simple system Δ. Tables of simple system, of all roots, and of the cardinalities of the corresponding irreducible FRGs can also be found in [5, Table 5.1 and 5.2] or in [54, Table I and II].

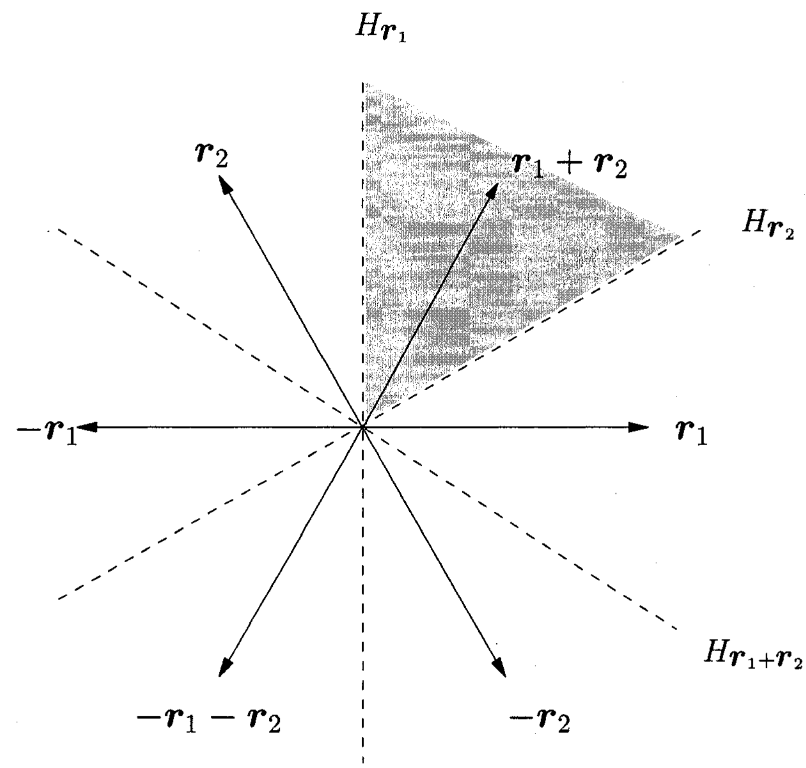

Figure 2.2: All roots and hyperplanes of the irreducible finite reflection group $\mathcal{A}_2$

We define a *fundamental domain* D_Δ of $\mathcal{G}$ associated with a simple system Δ by [54]

$$D_\Delta = \{\boldsymbol{x} \in \mathbb{R}^n : \ (\boldsymbol{x}, \boldsymbol{r}) \geq 0, \ \forall \boldsymbol{r} \in \Delta\} \tag{2.22}$$

The fundamental domain of FRG $\mathcal{A}_2$ is shown in the shaded region in Figure 2.2.

Every element of a FRG can be written as a product of reflections corresponding to simple roots; so instead of using all of a root system Φ to generate $\mathcal{G}$, it suffices to take $\{S_{\boldsymbol{r}} : \boldsymbol{r} \in \Delta\}$ [39]. One way to represent a FRG is its *Coxeter graph* Γ, using its simple system as shown in [54, Figure 2] for all irreducible FRGs. The Coxeter graph is obtained by making one vertex for each simple root and drawing an edge from i to j if $\boldsymbol{r}_i$ and $\boldsymbol{r}_j$ are not orthogonal with the relation $(S_{\boldsymbol{r}_i} S_{\boldsymbol{r}_j})^{m_{ij}} = 1$ where m_{ij} is the label on the edge from i to j. We label the edge with the number $m_{ij} \geq 3$, and π/m_{ij} is also the angle between $H_{\boldsymbol{r}}$ and $H_{\boldsymbol{r}'}$. The Coxeter graph, in turn, uniquely identifies the group.

2.2.2 Crystallographic Finite Reflection Groups

The root system Φ of a *crystallographic finite reflection group* (or a *finite Weyl group*) satisfies (R1),(R2) and also (R3) [39]

$$2\frac{\boldsymbol{r}\cdot\boldsymbol{r}'}{\boldsymbol{r}\cdot\boldsymbol{r}} \in \mathbb{Z} \tag{2.23}$$

for all $\boldsymbol{r}, \boldsymbol{r}' \in \Phi$. The condition (R3) is particularly relevant for us to study affine reflection groups.

The *highest long root* $\boldsymbol{\rho}$ of $\mathcal{G}$ is a positive root $\boldsymbol{\rho} = \sum_{i=1}^{n} a_i \boldsymbol{r}_i$ which is defined by the property that the sum of its coordinates $\sum_{i=1}^{n} a_i$ with respect to the simple system Δ is maximal among all roots. Furthermore, these coefficients a_i are all strictly positive integers. The simple systems and highest long roots of all irreducible finite Weyl groups are also given in Table 2.2. We use $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_k\}$ to denote the standard basis of $\boldsymbol{V} = \mathbb{R}^k$. Note that the roots Φ of $\mathcal{A}_n$, $\mathcal{E}_6$ and $\mathcal{E}_7$ are given so that span(Φ) is a proper subspace of $\boldsymbol{V}$; this is convention, see Section 8.1 for further discussion.

2.2.3 Coroots

For each root $\boldsymbol{r}$, we define its coroot as

$$\boldsymbol{r}^\vee = \frac{2\boldsymbol{r}}{\boldsymbol{r}\cdot\boldsymbol{r}}. \tag{2.24}$$

Given a crystallographic root system Φ (that is, all $\boldsymbol{r} \in \Phi$ satisfy (R1), (R2) and (R3)), the coroot system $\Phi^\vee = \{\boldsymbol{r}^\vee : \boldsymbol{r} \in \Phi\}$ is also crystallographic. Furthermore if Δ is a simple system for Φ then $\Delta^\vee$ is a simple system for $\Phi^\vee$ [39].

Example 2.2.1. *From Table 2.2, the simple roots of $\mathcal{A}_n$ are*

$$(1, -1, 0, \cdots, 0), \cdots, (0, 0, \cdots, 0, 1, -1)$$

(embedded in $\mathbb{R}^{n+1}$) then these all have length $\sqrt{2}$ so the coroots coincide exactly with the roots.

Example 2.2.2. *The simple roots of $\mathcal{A}_2$ given in Table 2.2 are* $(1, -1, 0)$ *and* $(0, 1, -1)$. *To embed them in $\mathbb{R}^2$, we use the Gram-Schmidt method to give* $(1, 0)$ *and* $(-1/2, \sqrt{3}/2)$.

Group	Simple system Δ	Highest long root $\boldsymbol{\rho}$
$\mathcal{A}_n$	$\boldsymbol{r}_i = (\boldsymbol{e}_{i+1} - \boldsymbol{e}_i)\,,\ 1 \le i \le n$	$\boldsymbol{r}_1 + \boldsymbol{r}_2 + \cdots + \boldsymbol{r}_n$
$\mathcal{B}_n$ $(n\geq 2)$	$\boldsymbol{r}_1 = \boldsymbol{e}_1,$ $\boldsymbol{r}_i = \boldsymbol{e}_i - \boldsymbol{e}_{i-1},\ 2 \le i \le n$	$2\boldsymbol{r}_1 + 2\boldsymbol{r}_2 + \cdots + 2\boldsymbol{r}_{n-1} + \boldsymbol{r}_n$
$\mathcal{C}_n$ $(n\geq 3)$	$\boldsymbol{r}_1 = 2\boldsymbol{e}_1,$ $\boldsymbol{r}_i = \boldsymbol{e}_i - \boldsymbol{e}_{i-1},\ 2 \le i \le n$	$\boldsymbol{r}_1 + 2\boldsymbol{r}_2 + \cdots + 2\boldsymbol{r}_{n-1} + 2\boldsymbol{r}_n$
$\mathcal{D}_n$ $(n\geq 4)$	$\boldsymbol{r}_1 = \boldsymbol{e}_1 + \boldsymbol{e}_2,$ $\boldsymbol{r}_i = \boldsymbol{e}_i - \boldsymbol{e}_{i-1},\ 2 \le i \le n,\ n \ge 4$	$\boldsymbol{r}_1 + \boldsymbol{r}_2 + \cdots + 2\boldsymbol{r}_{n-2} + 2\boldsymbol{r}_{n-1} + \boldsymbol{r}_n$
$\mathcal{E}_6$	$\boldsymbol{r}_1 = \frac{1}{2}\left(\boldsymbol{e}_1 + \boldsymbol{e}_8 - \sum_{i=2}^{7} \boldsymbol{e}_i\right),$ $\boldsymbol{r}_2 = \boldsymbol{e}_1 + \boldsymbol{e}_2$ $\boldsymbol{r}_i = \boldsymbol{e}_{i-1} - \boldsymbol{e}_{i-2},\ 3 \le i \le 6$	$\boldsymbol{r}_1 + 2\boldsymbol{r}_2 + 2\boldsymbol{r}_3 + 3\boldsymbol{r}_4 + 2\boldsymbol{r}_5 + \boldsymbol{r}_6$
$\mathcal{E}_7$	$\boldsymbol{r}_1, \ldots, \boldsymbol{r}_6,\ \boldsymbol{r}_7 = \boldsymbol{e}_6 - \boldsymbol{e}_5$	$2\boldsymbol{r}_1 + 2\boldsymbol{r}_2 + 3\boldsymbol{r}_3 + 4\boldsymbol{r}_4 + 3\boldsymbol{r}_5 + 2\boldsymbol{r}_6$ $+\boldsymbol{r}_7$
$\mathcal{E}_8$	$\boldsymbol{r}_1, \ldots, \boldsymbol{r}_7,\ \boldsymbol{r}_8 = \boldsymbol{e}_7 - \boldsymbol{e}_6$	$2\boldsymbol{r}_1 + 3\boldsymbol{r}_2 + 4\boldsymbol{r}_3 + 6\boldsymbol{r}_4 + 5\boldsymbol{r}_5 + 4\boldsymbol{r}_6$ $+3\boldsymbol{r}_7 + 2\boldsymbol{r}_8$
$\mathcal{F}_4$	$\boldsymbol{r}_1 = \boldsymbol{e}_2 - \boldsymbol{e}_3,\ \boldsymbol{r}_2 = \boldsymbol{e}_3 - \boldsymbol{e}_4,$ $\boldsymbol{r}_3 = \boldsymbol{e}_4$ $\boldsymbol{r}_4 = \frac{1}{2}\boldsymbol{e}_1 - \frac{1}{2}\sum_{i=2}^{4} \boldsymbol{e}_i$	$2\boldsymbol{r}_1 + 3\boldsymbol{r}_2 + 4\boldsymbol{r}_3 + 2\boldsymbol{r}_4$
$\mathcal{G}_2$	$\boldsymbol{r}_1 = (1,0), \boldsymbol{r}_2 = \left(-\frac{3}{2}, \frac{\sqrt{3}}{2}\right)$	$3\boldsymbol{r}_1 + 2\boldsymbol{r}_2$

Table 2.2: The simple systems and the highest long roots of the irreducible finite Weyl groups [54, 39, 5]

Then since $(\boldsymbol{r}, \boldsymbol{r}) = 1$ *for each simple root, we have that the scaling of going to* $\Phi^\vee$ *is to double the lengths of all the roots. Thus the corresponding simple coroots are* $(2,0)$ *and* $(-1, \sqrt{3})$.

Example 2.2.3. *From Table 2.2, the finite Weyl group* $\mathcal{B}_n$ *has the simple roots*

$$(1,0,0,\cdots,0), (-1,1,0,\cdots,0), \cdots, (0,0,\cdots,0,-1,1)$$

whose corresponding coroots are

$$(2,0,0,\cdots,0), (-1,1,0,\cdots,0), \cdots, (0,0,\cdots,0,-1,1)$$

which are exactly the simple roots of the root system for type $\mathcal{C}_n$. *(Similarly the coroot system of* $\mathcal{C}_n$ *is of type* $\mathcal{B}_n$.*)*

Example 2.2.4. *From Table 2.2 , the simple roots of $\mathcal{D}_n$ are*

$$(1,1,0,\cdots,0),(-1,1,0,\cdots,0),\cdots,(0,0,\cdots,0,-1,1)$$

whose corresponding coroots are

$$(1,1,0,\cdots,0),(-1,1,0,\cdots,0),\cdots,(0,0,\cdots,0,-1,1)$$

that is, $\Phi = \Phi^\vee$.

2.2.4 Lattices

A *lattice* is a group under addition (an additive group). A lattice Λ in $\mathbb{R}^n$ is defined as the set of all the possible integer combination of all basis vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_n$, that is,

$$\Lambda = \left\{ \sum_{i=1}^{n} a_i \boldsymbol{v}_i, \ a_i \in \mathbb{Z} \right\}. \tag{2.25}$$

The choice of basis vectors is not unique. The lattice vector $\boldsymbol{x} \in \Lambda$ can be expressed in matrix-form as [13]

$$\boldsymbol{x} = \boldsymbol{G}\boldsymbol{a} \tag{2.26}$$

where we call $\boldsymbol{G} = [\boldsymbol{v}_1 \ \boldsymbol{v}_2 \ \cdots \ \boldsymbol{v}_n]$ a *generator matrix* of the lattice. A simple example of a lattice is the integer lattice $\Lambda = \mathbb{Z}^2$ whose basis vectors are $(1,0)$ and $(0,1)$.

We define a *root lattice* spanned by a simple system $\Delta \subset \Phi$ as

$$\Lambda(\Phi) = \left\{ \sum_{i} a_i \boldsymbol{r}_i, \ a_i \in \mathbb{Z}, \ \boldsymbol{r}_i \in \Delta \right\}. \tag{2.27}$$

Moreover, given a coroot system $\Phi^\vee$, the *coroot lattice* $\Lambda(\Phi^\vee)$ is defined as the lattice spanned by $\Delta^\vee \subset \Phi^\vee$. If Φ is crystallographic then $\Phi \subseteq \Lambda(\Phi)$ and $\Phi^\vee \subseteq \Lambda(\Phi^\vee)$. The root lattice $\mathcal{A}_2$ is shown in Figure 2.3, where the lattice vectors are the intersections of the hyperplanes.

2.2.5 Affine Reflection Groups

An *affine reflection group (ARG)* $\mathcal{G}_a$ (also known as an *affine Weyl group*) is a group generated by reflections in certain affine hyperplanes of $\mathbb{R}^n$. More precisely, given a crystallographic finite reflection group with a root system Φ, we define the associated ARG to the be the group generated by the reflections in all the affine hyperplanes

$$H_{\boldsymbol{r},k} = \{\boldsymbol{x} \in \boldsymbol{V} : \boldsymbol{r} \cdot \boldsymbol{x} = k\} \tag{2.28}$$

for all $\boldsymbol{r} \in \Phi$ and $k \in \mathbb{Z}$.

The affine reflection in the hyperplane of (2.28) is denoted $S_{\boldsymbol{r},k} \in \mathcal{G}$ which is calculated via [39]

$$\begin{aligned} S_{\boldsymbol{r},k}\boldsymbol{x} &= \boldsymbol{x} - (\boldsymbol{x} \cdot \boldsymbol{r} - k) \cdot \frac{2\boldsymbol{r}}{\boldsymbol{r} \cdot \boldsymbol{r}} && (2.29) \\ &= S_{\boldsymbol{r}}\boldsymbol{x} + 2k\boldsymbol{r}^{\vee} && (2.30) \end{aligned}$$

where $S_{\boldsymbol{r}}\boldsymbol{x}$ and $\boldsymbol{r}^{\vee}$ are defined in (2.21) and (2.24) respectively. The group $\mathcal{G}_a$ is generated by the set of all affine reflections $S_{\boldsymbol{r},k}$, and it is infinite. The simple roots $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ and hyperplanes of the affine Weyl group $\mathcal{A}_2$ are shown in Figure 2.3.

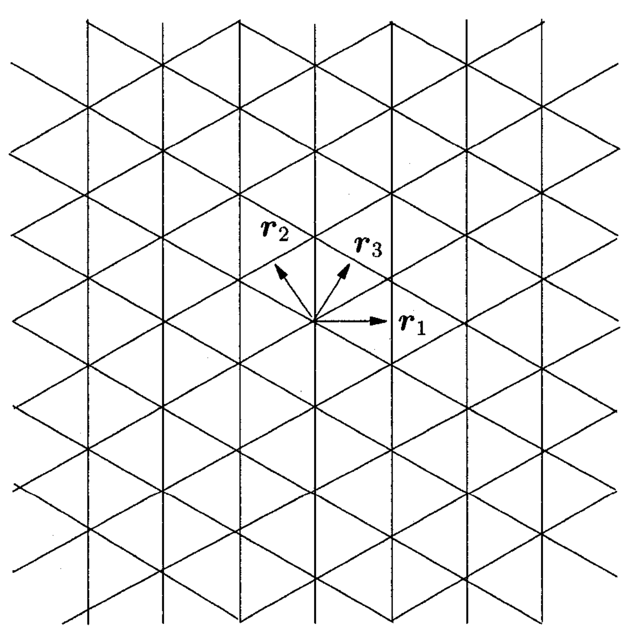

Figure 2.3: Hyperplanes of the affine reflection group $\mathcal{A}_2$

It is proven in [39, Section 4.10] that all irreducible ARGs are generated by an irreducible finite Weyl group, together with a single affine reflection. From (2.29) and (2.30), we can see that $S_{\boldsymbol{r},0} = S_{\boldsymbol{r}}$ is a linear reflection for each $\boldsymbol{r}$. The subgroup of $\mathcal{G}_a$ generated by these linear reflections is the corresponding finite Weyl group $\mathcal{G}$. A key fact is that a minimal generating set for $\mathcal{G}_a$ is [39, Prop. 4.3]

$$\{S_{\boldsymbol{r},0} \colon \boldsymbol{r} \in \Delta\} \cup \{S_{\boldsymbol{\rho},1}\} \tag{2.31}$$

where $\boldsymbol{\rho}$ is a highest long root.

On other hand, from (2.29), we can say that every element $S_{\boldsymbol{r},k} \in \mathcal{G}_a$ can be expressed as a linear reflection $S_{\boldsymbol{r}}$ (from the corresponding finite Weyl group $\mathcal{G}$) followed by a translation by an element $k\boldsymbol{r}^\vee$, which is a vector in the coroot lattice, that is, $k\boldsymbol{r}^\vee \in \Lambda(\Phi^\vee)$. This claim leads us to Theorem 2.2.1.

Theorem 2.2.1. *From [39, Prop 4.2], let $\mathcal{G}_a$ be an ARG, $\mathcal{G}$ be the corresponding finite reflection group and $\Lambda(\Phi^\vee)$ be the coroot lattice. Then $\mathcal{G}_a$ can be expressed by*

$$\mathcal{G}_a = \Lambda(\Phi^\vee) \rtimes \mathcal{G} \tag{2.32}$$

where $\rtimes$ denotes a semi-direct product.

Theorem 2.2.1 means every element (not just the affine reflections) of the affine Weyl group $\mathcal{G}_a$ can be expressed as the composition of an element of the finite Weyl group $\mathcal{G}$ with the translation by a vector in the coroot lattice $\Lambda(\Phi^\vee)$.

2.3 Group Codes

A thorough survey of group codes can be found in [40]. In this section, we first introduce a basic group code, permutation code variant II, which can be obtained by simple structures. Then the group codes generated from finite reflection and its decoding method (the length reduction) are described.

2.3.1 Definition of Group Codes

An (L, n) *group code* is a set of L vectors (codewords) in the Euclidean space of dimension n, $\mathbb{R}^n$. Basically we can think that all L codewords are on the surface of unit sphere in n dimensional space, see Figure 2.4. Let $\{\boldsymbol{x}_l\}_{l=0}^{L-1}$ be codewords and assume that all $\boldsymbol{x}_l$ are equiprobable. This means that the distance from any codeword $\boldsymbol{x}_l$ to all nearest neighbours is the same as from codeword $\boldsymbol{x}_k$ to all nearest neighbours for all $l, k = 0, 1, \ldots, L-1$, or equivalently, all codewords have the same error probability.

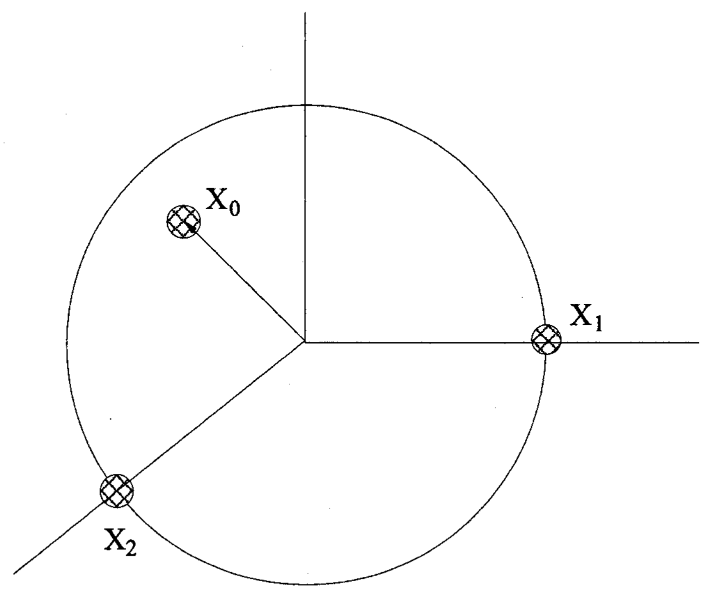

Figure 2.4: Group code

Let $\mathcal{G}$ be a group such that $|\mathcal{G}| = L$ with a representation (action) on $\mathbb{R}^n$, that is, an orthogonal $n \times n$ matrix $\boldsymbol{O}_g$ for each $g \in \mathcal{G}$, such that $\boldsymbol{O}_g \boldsymbol{O}_n = \boldsymbol{O}_{gn}$ and $\boldsymbol{O}_g^{-1} = \boldsymbol{O}_{g^{-1}}$. A group code generated from $\mathcal{G}$ is the set of all

$$\boldsymbol{x}_g = \boldsymbol{O}_g \boldsymbol{x}_0 \tag{2.33}$$

for all $g \in \mathcal{G}$ where $\boldsymbol{x}_0 = (x_1, \ldots, x_n)^t \in \mathbb{R}^n$ is called an *initial vector.* To be able to generate L codewords, the initial vector $\boldsymbol{x}_0$ cannot be an eigenvector of unit eigenvalue of any $\boldsymbol{O}_g$. Otherwise, there will be L' codewords and L' divides L. More precisely, let $\mathcal{H} = \{g \in \mathcal{G} | \boldsymbol{O}_g \boldsymbol{x}_0 = \boldsymbol{x}_0\}$. Then $\mathcal{H}$ is a subgroup of $\mathcal{G}$ and the size of the group code generated by $\boldsymbol{x}_0$ is $L' = |\mathcal{G}|/|\mathcal{H}|$.

The initial vector problem is to choose a vector $\boldsymbol{x}_0$ which maximizes the Euclidean distance between a codeword and its nearest neighbour, over all codewords. The problem has not been solved for general groups, but rather is known only for special cases such as for permutation codes [83], for cyclic groups [6], for the full homogeneous representation and the $(n-1)$-dimensional representation of the symmetric groups of rank n [8] and for FRGs [53, 54].

Furthermore, relaxing the requirement that the action of $\mathcal{G}$ on $\mathbb{R}^n$ be linear gives a large class of group codes, which include lattices (the translation of $\boldsymbol{x}_0$ by $\mathcal{G} \in \mathbb{Z}^n$ acting from the translation by the basis vectors of lattice) and ARGCs.

2.3.2 Permutation Codes Variant II

Let μ_i appear m_i times in a vector $\boldsymbol{x} \in \mathbb{R}^n$ and $n = m_1 + m_2 + \ldots + m_k$. We call $\boldsymbol{m} = (m_1, m_2, \ldots, m_k)$ the *distribution* of a vector $\boldsymbol{x}$. The codewords of a *permutation code variant II* of order L are all of the form [83]

$$\{\boldsymbol{x}_i\}_{i=0}^{L-1} = (\pm\mu_1, \pm\mu_1, \ldots, \pm\mu_1, \pm\mu_2, \ldots, \pm\mu_2, \ldots, \pm\mu_k, \ldots, \pm\mu_k)^P \tag{2.34}$$

where $\{\mu_i\}_{i=1}^{k} \in \mathbb{R}$ and $0 < \mu_1 < \mu_2 < \ldots < \mu_k$. Here $(\ )^P$ and $\pm$ denote all possible permutations and combinations of sign changes of the components in $\boldsymbol{x}_i$ respectively. (So here $\mathcal{G}$ is the group of all permutation and sign changes.) Thus the order of a permutation code variant II is

$$\begin{aligned} L &= \frac{(m_1 + m_2 + \cdots + m_k)!}{m_1!\ m_2!\ \cdots m_k!} \times 2^{m_1+m_2+\cdots+m_k} &(2.35)\\ &= \frac{n!}{m_1!\ m_2!\ \cdots m_k!} \times 2^n. &(2.36)\end{aligned}$$

The first and the second terms in (2.35) and (2.36) are from possible permutations and combinations of sign changes in $\boldsymbol{x}_i$ respectively. The minimum square distance between codewords can be computed from

$$d_{\min}^2 = \min\{\min_{i \neq j} 2(\mu_i - \mu_j)^2, 4\mu_1^2\} \tag{2.37}$$

where $i, j = 1, 2, \ldots, k$. The term $\min_{i\neq j} 2(\mu_i - \mu_j)^2$ is from the nearest distance of two different codewords, and the term $4\mu_1^2$ is from the same component codeword with one different sign at μ_1. The energy of each codeword is computed by

$$E = \sum_{i=1}^{k} m_i \mu_i^2. \tag{2.38}$$

2.3.3 Finite Reflection Group Codes (FRGC)

Given $\mathcal{G}$, Φ, Δ, $\boldsymbol{V}$ =span(Δ) and dim $\boldsymbol{V} = n$ as in Section 2.2.1, we can define a reflection group code. The n-dimensional FRG codewords are generated from $\mathcal{G}$ by setting $\boldsymbol{O}_g = g$, that is, for any $\boldsymbol{x} \in \mathbb{R}^n$, we define

$$g : \boldsymbol{x} \longmapsto g \cdot \boldsymbol{x} \tag{2.39}$$

Given an initial vector $\boldsymbol{x_0}$ in the fundamental domain D_Δ, we define the corresponding *passive simple system* as [54]

$$\Delta_p = \{\boldsymbol{r}_i \in \Delta \ : \ S_{\boldsymbol{r}_i}\boldsymbol{x_0} = \boldsymbol{x_0}\}. \tag{2.40}$$

Let $\mathcal{H}$ be the subgroup of $\mathcal{G}$ generated by the reflections in the simple roots of Δ_p; then the size of the group code derived from $\mathcal{G}$ and $\boldsymbol{x_0}$ is $L = |\mathcal{G}|/|\mathcal{H}|$. This relationship of passive simple roots to the simple system can be described most succinctly in terms of a Coxeter graph Γ of $\mathcal{G}$. Each subgraph $\{\Gamma_i\}_{i=1}^{l}$ (denoting a subgraph with l connected components) corresponds to a choice of passive simple system $\Delta_p = \bigcup_{i=1}^{l} \Delta_{p_i}$. In this case

$$\mathcal{H} = \mathcal{G}_{\Gamma_1} \times \mathcal{G}_{\Gamma_2} \times \cdots \times \mathcal{G}_{\Gamma_l}, \tag{2.41}$$

where $\mathcal{G}_{\Gamma_i}$ is an irreducible FRG corresponding to the subgraph Γ_i.

Given a passive simple system Δ_p, an optimal initial vector $\boldsymbol{x_0}$ is given by [54]

$$\boldsymbol{x_0} = \frac{\sum_{\boldsymbol{r}_i \in \Delta\setminus\Delta_p} \frac{\|\boldsymbol{r}_i\|}{2} \boldsymbol{\lambda}_i}{\left\| \sum_{\boldsymbol{r}_i \in \Delta\setminus\Delta_p} \frac{\|\boldsymbol{r}_i\|}{2} \boldsymbol{\lambda}_i \right\|} \tag{2.42}$$

where $\boldsymbol{\lambda_i}$ is a dual basis vector of $\boldsymbol{r}_i$, that is, $\boldsymbol{\lambda_i} \cdot \boldsymbol{r}_j = \delta_{ij}$ for all $i, j \in \{1, 2, \ldots, n\}$.

The minimum distance between two codewords is given by [54]

$$d_{\min}^2 = \frac{4}{\sum_{\boldsymbol{r}_i \in \Delta\backslash\Delta_p} \sum_{\boldsymbol{r}_j \in \Delta\backslash\Delta_p} (\|\boldsymbol{r}_i\| \cdot \|\boldsymbol{r}_j\|) \boldsymbol{\lambda}_i \cdot \boldsymbol{\lambda}_j}. \tag{2.43}$$

A FRG can be decoded using the length-reduction algorithm [53] or the permutation-decoding algorithm [54]. The permutation-decoding algorithm has less complexity however it requires more knowledge of group structure. For example, the permutation-decoding algorithm was proposed for $\mathcal{E}_7$ in [54], which used the existence of a permutation subgroup and knowledge of its index. On other hand, the length-reduction algorithm is more general which works well for any FRGs without the knowledge of group structure. In this thesis, we use the length-reduction algorithm [53] to decode a FRGC in Chapter 8 and use it in our complexity comparison in Chapter 9.

Length-Reduction Algorithm

For a given received vector $\boldsymbol{y} \in \mathbb{R}^n$, we summarize the *length-reduction algorithm* as follows:

1. Set $P = \emptyset$, an empty array.
2. Compute $Q = \{\boldsymbol{r}_i \in \Delta : \ \boldsymbol{r}_i \cdot \boldsymbol{y} < 0\}$.
3. If $Q = \emptyset$ go to (4), else choose any $\boldsymbol{r}_i \in Q$ and store the index i in P. Then set

$$\boldsymbol{y} = S_{\boldsymbol{r}_i}\boldsymbol{y} = \boldsymbol{y} - 2\frac{\boldsymbol{y} \cdot \boldsymbol{r}_i}{\|\boldsymbol{r}_i\|^2}\boldsymbol{r}_i$$

and go to (2).

4. From $P = \{i_1, i_2, \ldots, i_l\}$, we decode

$$\boldsymbol{x} = S_{\boldsymbol{r}_{i_1}} S_{\boldsymbol{r}_{i_2}} \cdots S_{\boldsymbol{r}_{i_l}} \boldsymbol{x}_0. \tag{2.44}$$

To analyze the complexity of this algorithm, note that, the maximum size of the array P is called the *length* of the FRG $\mathcal{G}$ which is $|\Phi^+| = \frac{|\Phi|}{2}$ where Φ and Φ^+ are the root and the positive root system of $\mathcal{G}$ respectively [39].

The step (2) of the length-reduction method needs n comparisons, n^2 multiplications and $n(n-1)$ additions[1]. Assume $\|\boldsymbol{r}_i\|^2 = 1$ for all i, then the step (3) has n

[1]The number of additions given in [53] is n^2 which is the upper bound.

multiplications and n additions (the value of $\boldsymbol{y} \cdot \boldsymbol{r}_i$ was stored from the step (2)). As we have mentioned, the step (2) and (3) will repeat no more than the length of $\mathcal{G}$ times, that is, $\frac{|\Phi|}{2}$. Consequently we need no more than $\frac{|\Phi|}{2}n$ comparisons, $\frac{|\Phi|}{2}(n^2+n)$ multiplications and $\frac{|\Phi|}{2}(n(n-1)+n)$ additions to obtain the set P with l indices. The step (4) needs no more than $\frac{|\Phi|}{2}2n$ multiplications and $\frac{|\Phi|}{2}(2n-1)$ additions.

The summary of the decoding complexity of the length-reduction method is given in Table 2.3.

Comparisons	Multiplications	Additions
$\leq \frac{\lvert\Phi\rvert}{2}n$	$\leq \frac{\lvert\Phi\rvert}{2}(n^2+3n)$	$\leq \frac{\lvert\Phi\rvert}{2}(n^2+2n-1)$

Table 2.3: Decoding complexity of the length-reduction method

2.4 Trellis Diagram of a Lattice

A lattice (and also an ARGC) can be represented by a trellis diagram and decoded using the Viterbi algorithm. In this section, we summarize the method to construct a trellis diagram of lattice proposed in [24, 4]. We also illustrate the construction of the trellis diagram with the root lattices $\mathcal{A}_2$, $\mathcal{A}_3$ and $\mathcal{B}_2$.

2.4.1 Construction of a Trellis Diagram

A *trellis diagram* of a lattice $\Lambda \subseteq \mathbb{R}^n$ is described as a nested sequence of vector spaces,

$$\{\mathbf{0}\} = \boldsymbol{V}_0 \subset \boldsymbol{V}_1 \subset \cdots \subset \boldsymbol{V}_n = \mathbb{R}^n \tag{2.45}$$

where the dimension of $\boldsymbol{V}_i$ is i. Let $\boldsymbol{W}_i$ be the orthogonal complement of $\boldsymbol{V}_{i-1}$ in $\boldsymbol{V}_i$ for $1 \leq i \leq n$ and the dimension of $\boldsymbol{W}_i$ is 1. Let $\boldsymbol{W}_i$ =span $(\boldsymbol{w}_i)$. We call the vectors $\boldsymbol{w}_i$ the *trellis coordinate system* of the lattice Λ for its corresponding trellis diagram. The two components of a trellis diagram are nodes (or state space) and branches (connected from node to node). Note that the structure (the number of nodes and branches) of a trellis diagram depends on the choice of $\boldsymbol{V}_i$ and $\boldsymbol{W}_i$.

We denote the projection and the intersection of a lattice Λ on the vector space $\boldsymbol{V}_i$ as $P_{\boldsymbol{V}_i} \triangleq \mathrm{Proj}_{\boldsymbol{V}_i}(\Lambda)$ and $\Lambda_{\boldsymbol{V}_i} \triangleq \Lambda \cap \boldsymbol{V}_i$ respectively; $\Lambda_{\boldsymbol{V}_i}$ is a subgroup of $P_{\boldsymbol{V}_i}$. A node or state space at level i, $\Sigma_i(\Lambda)$, $i = 0, 1, \ldots, n$ is an element of the quotient

$$\Sigma_i(\Lambda) = P_{\boldsymbol{V}_i}/\Lambda_{\boldsymbol{V}_i}. \tag{2.46}$$

The number of nodes at each level i is $|\Sigma_i(\Lambda)|$.

We also write $P_{\boldsymbol{W}_i} \triangleq \mathrm{Proj}_{\boldsymbol{W}_i}(\Lambda)$ and $\Lambda_{\boldsymbol{W}_i} \triangleq \Lambda \cap \boldsymbol{W}_i$. The label of a branch at level i, $i = 1, 2, \ldots, n$, is computed from the the quotient

$$G_i(\Lambda) = P_{\boldsymbol{W}_i}/\Lambda_{\boldsymbol{W}_i}. \tag{2.47}$$

Similarly, $\Lambda_{\boldsymbol{W}_i}$ is a subgroup of $P_{\boldsymbol{W}_i}$, and the number of branches at level i is $|G_i(\Lambda)|$. The label appearing in a trellis diagram is with respect to the trellis coordinate vector $\boldsymbol{w}_i$. This means that the label of a lattice vector $\boldsymbol{y} \in \Lambda$ at level i is the equivalence class modulo $\Lambda_{\boldsymbol{W}_i}$ of

$$\frac{(\boldsymbol{y}, \boldsymbol{w}_i)}{||\boldsymbol{w}_i||^2} \tag{2.48}$$

for all $i = 1, 2, \ldots, n$. That is, if $\Lambda_{\boldsymbol{W}_i} = \mathbb{Z} \cdot r\boldsymbol{w}_i$ then the modulus (or *repeat*) is $r\mathbb{Z}$.

The path corresponding to all zero labels gives elements of the rectangular sublattice

$$\Lambda_L = \Lambda_{\boldsymbol{w}_1} \times \cdots \times \Lambda_{\boldsymbol{w}_n} \tag{2.49}$$

of Λ. Thus each path corresponds to a coset $\boldsymbol{x} + \Lambda_L$ of this rectangular sublattice.

We illustrate with the examples of constructing the trellis diagram from the root lattices $\mathcal{A}_2$, $\mathcal{A}_3$ and $\mathcal{B}_2$.

Example 2.4.1. *From Example 2.2.2, the simple system (in 2 dimensions) of the crystallographic FRG $\mathcal{A}_2$ is $\boldsymbol{r}_1 = (1, 0)$ and $\boldsymbol{r}_2 = (-1/2, \sqrt{3}/2)$. Thus the generator matrix of the root lattice $\mathcal{A}_2$ is*

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}. \tag{2.50}$$

This is a 2-D hexagonal lattice whose lattice codewords are the vectors

$$a_1(1, 0) + a_2\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = \left(a_1 - \frac{a_2}{2}, \frac{a_2\sqrt{3}}{2}\right) \tag{2.51}$$

where $a_1, a_2 \in \mathbb{Z}$.

From the generator matrix $\boldsymbol{G}$ *in (2.50), we can set* $\boldsymbol{V}_0 = \boldsymbol{0}$, $\boldsymbol{V}_1 = \langle(1,0)\rangle$ *and* $\boldsymbol{V}_2 = \langle(1,0), (-1/2, \sqrt{3}/2)\rangle = \mathbb{R}^2$. *The orthogonal complement of these vector spaces are* $\boldsymbol{W}_1 = \langle \boldsymbol{w}_1 = (1,0)\rangle$ *and* $\boldsymbol{W}_2 = \langle \boldsymbol{w}_2 = (0,1)\rangle$ *respectively. We now begin to compute the nodes and the labels of the branches at each level:*

<u>At level 0</u>: *It is straightforward to see that* $\Sigma_0(\Lambda) = 1$ *from* $\boldsymbol{V}_0 = \boldsymbol{0}$. *It has one (starting) node.*

<u>At level 1</u>:

Node 1: *To compute* $P_{\boldsymbol{V}_1}$, *the projection of lattice to* $\boldsymbol{V}_1 = \langle(1,0)\rangle$, *from (2.51), we are interested in only the first coordinate so* $P_{\boldsymbol{V}_1} = \{a_1 - a_2/2, 0 | a_1, a_2 \in \mathbb{Z}\} = (\mathbb{Z}/2, 0)$. *For the intersection of lattice to* $\boldsymbol{V}_1$, *from (2.51), we need the second coordinate to be 0, that is,* $a_2\sqrt{3}/2 = 0 \Rightarrow a_2 = 0$. *Hence* $\Lambda_{\boldsymbol{V}_1} = \{a_1 + 0/2, 0) = (a_1, 0) | a_1 \in \mathbb{Z}\} = (\mathbb{Z}, 0)$. *Consequently the quotient* $\Sigma_1(\Lambda) = P_{\boldsymbol{V}_i}/\Lambda_{\boldsymbol{V}_i} = \{0, 1/2\}$ *which gives 2 nodes.*

Branch 1: *Same as Node 1 since* $\boldsymbol{W}_1 = \boldsymbol{V}_1 = \langle(1,0)\rangle$. *Therefore* $G_1(\Lambda)$ *has 2 branches with the label* $\{\mathbb{Z}, \mathbb{Z} + 1/2\}$.

<u>At level 2</u>:

Node 2: $P_{\boldsymbol{V}_2}$ *and* $\Lambda_{\boldsymbol{V}_2}$ *are L itself, that is,* $P_{\boldsymbol{V}_2} = P_{\mathbb{R}^2} = \Lambda$ *and* $\Lambda_{\boldsymbol{V}_2} = \Lambda \cap \mathbb{R}^2 = \Lambda$. *Thus* $\Sigma_2(\Lambda) = \Lambda/\Lambda = 1$ *which has 1 (ending) node.*

Branch 2: *For the projection of lattice to* $\boldsymbol{W}_2 = \langle(0,1)\rangle$, *we are interested in only for the second coordinate of (2.51). Therefore* $P_{\boldsymbol{W}_2} = \{0, a_2\sqrt{3}/2) | a_2 \in \mathbb{Z}\} = (0, \mathbb{Z}\sqrt{3}/2)$. *To compute* $\Lambda \cap \boldsymbol{W}_2$, *we want the first coordinate of (2.51) to be 0, that is,* $a_1 - a_2/2 = 0 \Rightarrow a_2 = 2a_1$ *or* $a_2 \in 2\mathbb{Z}$ *since* $a_1 \in \mathbb{Z}$. *This gives* $\Lambda_{\boldsymbol{W}_2} = (0, 2\mathbb{Z}\sqrt{3}/2) = (0, \sqrt{3}\mathbb{Z})$. *The quotient* $G_2(\Lambda) = P_{\boldsymbol{W}_2}/\Lambda_{\boldsymbol{W}_2}$ *has 2 branches with the label* $\{\sqrt{3}\mathbb{Z}, \sqrt{3}\mathbb{Z} + \sqrt{3}/2\}$.

The trellis diagram of the root lattice $\mathcal{A}_2$ *is drawn in Figure 2.5.*

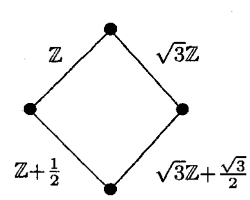

Figure 2.5: The trellis diagram of the root lattice $\mathcal{A}_2$

Example 2.4.2. *Consider the coroot lattice of* $\mathcal{A}_2$ *in Example 2.4.1. The coroot lattice has the same shape as the root lattice* $\mathcal{A}_2$ *with all roots doubled, see Figure 2.6. The* *solid circles represent the codewords of the coroot lattice. Now the simple roots are* $\boldsymbol{r}_1 = (2,0)$ *and* $\boldsymbol{r}_2 = (-1,\sqrt{3})$*. The generator of the new coroot lattice* $\Lambda(\Phi^\vee)$ *is*

$$\boldsymbol{G} = \begin{bmatrix} 2 & 0 \\ -1 & \sqrt{3} \end{bmatrix}. \tag{2.52}$$

We set $\boldsymbol{V}_0 = \boldsymbol{0}$, $\boldsymbol{V}_1 = \langle(2,0)\rangle$ *and* $\boldsymbol{V}_2 = \langle(2,0),(-1,\sqrt{3})\rangle$*. The orthogonal complement of these vectors are* $\boldsymbol{W}_1 = \langle \boldsymbol{w}_1 = (2,0)\rangle$ *and* $\boldsymbol{W}_2 = \langle \boldsymbol{w}_2 = (0,2)\rangle$*. Using the similar calculation explained in Example 2.4.1, we find that the trellis diagram of the coroot lattice of* $\mathcal{A}_2$ *is same as that of the root lattice* $\mathcal{A}_2$ *(Figure 2.5). This happens because we doubled the length of the trellis coordinate system as well as the roots, so the quotient (2.48) is the same.*

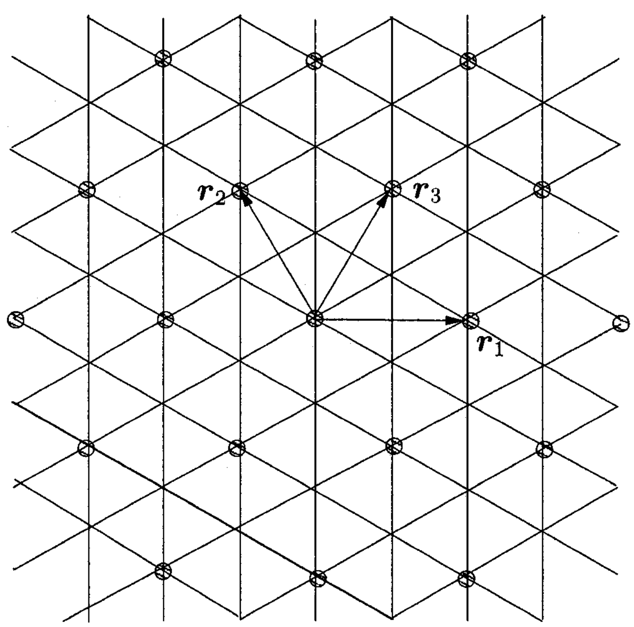

Figure 2.6: The coroot lattice $\mathcal{A}_2$

Example 2.4.3. *From the simple system listed in Table 2.2, a generator matrix of the root lattice* $\mathcal{A}_3$ *is*

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \\ 0 & -\frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \end{bmatrix}. \tag{2.53}$$

To get the minimum number of paths of trellis diagram, we use the permutation

$(1, 3, 2)$ *of the rows of* $\boldsymbol{G}$ *as suggested in Table 5.2 in [4]. Thus the new generator matrix is*

$$\boldsymbol{G}' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} & 0 \end{bmatrix}. \tag{2.54}$$

The lattice codewords are the vectors

$$\left(a_1 - \frac{a_3}{2}, -\frac{a_2}{\sqrt{3}} + a_3\frac{\sqrt{3}}{2}, a_2\sqrt{\frac{2}{3}}\right) \tag{2.55}$$

where $a_1, a_2, a_3 \in \mathbb{Z}$. *From (2.54), we set*

$$\begin{aligned}
&\boldsymbol{V}_0 = \boldsymbol{0}, && \boldsymbol{W}_1 = \langle \boldsymbol{w}_1 = (1,0,0)\rangle, \\
&\boldsymbol{V}_1 = \langle \boldsymbol{v}_1 = (1,0,0)\rangle, && \boldsymbol{W}_2 = \langle \boldsymbol{w}_2 = \left(0, -\tfrac{1}{\sqrt{3}}, \sqrt{\tfrac{2}{3}}\right)\rangle, \\
&\boldsymbol{V}_2 = \langle \boldsymbol{v}_1, \boldsymbol{v}_2 = \left(0, -\tfrac{1}{\sqrt{3}}, \sqrt{\tfrac{2}{3}}\right)\rangle, && \boldsymbol{W}_3 = \langle \boldsymbol{w}_3 = \left(0, \sqrt{\tfrac{2}{3}}, \tfrac{1}{\sqrt{3}}\right)\rangle, \\
&\boldsymbol{V}_3 = \langle \boldsymbol{v}_1, \boldsymbol{v}_2, \left(-\tfrac{1}{2}, \tfrac{\sqrt{3}}{2}, 0\right)\rangle.
\end{aligned}$$

Then a similar calculation as that described in Example 2.4.1 gives the trellis diagram of the root lattice $\mathcal{A}_3$ *shown in Figure 2.7.*

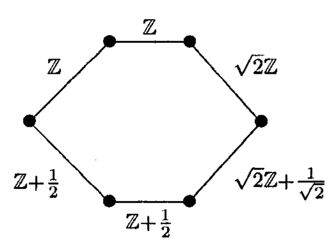

Figure 2.7: The trellis diagram of the root lattice $\mathcal{A}_3$

Example 2.4.4. *Consider the root lattice* $\mathcal{B}_2$ *whose generator matrix is (from Table 2.2)*

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}. \tag{2.56}$$

The lattice codewords are the vectors

$$a_1(1,0) + a_2(-1,1) = (a_1 - a_2, a_2) \tag{2.57}$$

where $a_1, a_2 \in \mathbb{Z}$. *We set* $\boldsymbol{V}_0 = \mathbf{0}$, $\boldsymbol{V}_1 = \langle(1,0)\rangle$, $\boldsymbol{V}_2 = \langle(1,0),(-1,1)\rangle$, *and* $\boldsymbol{W}_1 = \langle \boldsymbol{w}_1 = (1,0)\rangle$ $\boldsymbol{W}_2 = \langle \boldsymbol{w}_2 = (0,1)\rangle$. *Following a similar calculation, we get the trellis diagram of the root lattice* $\mathcal{B}_2$ *as shown in Figure 2.8 which is just the integer lattice* $\mathbb{Z}^2$.

Figure 2.8: The trellis diagram of the root lattice $\mathcal{B}_2$

Example 2.4.5. *Now consider the coroot lattice of* $\mathcal{B}_2$. *Use the formula of coroot in (2.24) on (2.56), the generator matrix of the coroot lattice of* $\mathcal{B}_2$ *is*

$$\boldsymbol{G} = \begin{bmatrix} 2 & 0 \\ -1 & 1 \end{bmatrix} \tag{2.58}$$

whose lattice codewords are the vectors

$$a_1(2,0) + a_2(-1,1) = (2a_1 - a_2, a_2). \tag{2.59}$$

Setting $\boldsymbol{V}_0 = \mathbf{0}$, $\boldsymbol{V}_1 = \langle(2,0)\rangle$, $\boldsymbol{V}_2 = \langle(2,0),(-1,1)$ *and* $\boldsymbol{W}_1 = \langle \boldsymbol{w}_1 = (1,0)\rangle$ $\boldsymbol{W}_2 = \langle \boldsymbol{w}_2 = (0,1)\rangle$ *gives the trellis diagram of the coroot lattice* $\mathcal{B}_2$ *in Figure 2.9.*

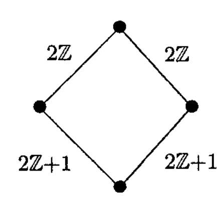

Figure 2.9: The trellis diagram of the coroot lattice of $\mathcal{B}_2$, with respect to $\boldsymbol{w}_1 = (1,0)$ and $\boldsymbol{w}_2 = (0,1)$

Example 2.4.6. *Same as Example 2.4.5, but now we use the permutation* $(2,1)$ *on the rows of* $\boldsymbol{G}$. *So we set* $\boldsymbol{V}_0 = \mathbf{0}$, $\boldsymbol{V}_1 = \langle(-1,1)\rangle$, $\boldsymbol{V}_2 = \langle(-1,1),(2,0)\rangle$ *and* $\boldsymbol{W}_1 = \langle \boldsymbol{w}_1 = (-1,1)\rangle$ $\boldsymbol{W}_2 = \langle \boldsymbol{w}_2 = (1,1)\rangle$. *The trellis diagram of the coroot lattice of* $\mathcal{B}_2$ *with respect to* $\boldsymbol{w}_1 = (-1,1)$ *and* $\boldsymbol{w}_2 = (1,1)$ *is shown in Figure 2.10. It has only one path, and so this choice of trellis coordinate system gives a minimal trellis diagram (as opposed in Example 2.4.5).*

$$\bullet \xrightarrow[\mathbb{Z}]{} \bullet \xrightarrow[\mathbb{Z}]{} \bullet$$

Figure 2.10: The trellis diagram of the coroot lattice of $\mathcal{B}_2$ with respect to $\boldsymbol{w}_1 = (-1, 1)$ and $\boldsymbol{w}_2 = (1, 1)$

2.4.2 Decoding Complexity of a Trellis Diagram

The *coding gain* γ of a lattice $\Lambda \in \mathbb{R}^n$ is defined from [4, 3] as

$$\gamma = \lambda^2 \det(\Lambda)^{-\frac{2}{n}} \tag{2.60}$$

where λ is the length of the *shortest nonzero vector* in Λ and

$$\det(\Lambda) = \det(\boldsymbol{G}\boldsymbol{G}^t)^{\frac{1}{2}} \tag{2.61}$$

where $\boldsymbol{G}$ is a generator matrix of Λ.

The complexity of decoding from a trellis diagram is determined from the number of *distinct paths* (N_p) appearing in the diagram [4, 3]. In general, a lower bound of N_p for the trellis diagram representing a lattice $\Lambda \in \mathbb{R}^n$ is [3]

$$N_p \geq \lceil \gamma^{\frac{n}{2}} \rceil \tag{2.62}$$

where $\lceil t \rceil$ denotes a higher integer closest to t.

We can also compute the number of distinct paths N_p by considering the rectangular sublattice Λ_L (see (2.49)), via [3]

$$N_p = \frac{\det(\Lambda_L)}{\det(\Lambda)}. \tag{2.63}$$

The calculation of N_p from (2.63) is exact since N_p is the number of distinct cosets of Λ_L in Λ. However the computation of (2.63) is not easy in practise. One can only use (2.63) if one has chosen Λ_L and identified a generator matrix, which is almost equivalent to construct the trellis diagram. On other hand, the approximation of N_p from (2.62) is simpler and requires little knowledge of the lattice structure. The minimal trellis diagram as well as the value of distinct paths N_p and $\lceil \gamma^{\frac{n}{2}} \rceil$ of many root lattice $\Lambda(\Phi)$ are given in [4, 3].

Decoding

As mentioned previously, the trellis diagram decomposes a lattice into a union of cosets of a rectangular sublattice Λ_L (corresponding to the path with all zero labels). The number of cosets is N_p. For example, from Figure 2.5, the root lattice $\mathcal{A}_2$ is the union of 2 cosets (has $N_p = 2$) of the rectangular sublattices, $\Lambda_{\boldsymbol{w}_1} \times \Lambda_{\boldsymbol{w}_2}$ which is spanned by $(1,0)$ and $(0,\sqrt{3})$. We use the *Viterbi algorithm* to decode a trellis diagram where the decoding for each rectangular coset can be done easily by rounding off at each label.

Let $a_i^{(j)}\mathbb{Z} + b_i^{(j)}$, $a_i^{(j)} > 0$ be the label of a trellis diagram of path j at level i, $j = 1,\ldots,N_p$ and $i = 1,\ldots,n$. For a given received vector $\boldsymbol{y}$ (which is given in coordinates with respect to a trellis coordinate system $\boldsymbol{w}_i$), we compute the decision metric of path j at level i via

$$D_{y_i}^{(j)} = \left| y_i - \left(\left\lceil \frac{y_i - b_i^{(j)}}{a_i^{(j)}} \right\rfloor a_i^{(j)} + b_i^{(j)} \right) \right|^2 = a_i^{(j)2} \left| \frac{y_i - b_i^{(j)}}{a_i^{(j)}} - \left\lceil \frac{y_i - b_i^{(j)}}{a_i^{(j)}} \right\rfloor \right|^2 \tag{2.64}$$

where we denote $\lceil t \rfloor$ as the closest integer to t. The decision metric of path j is $\sum_{i=1}^{n} D_{y_i}^{(j)}$. Then the decoded message is chosen from

$$\min_j \sum_{i=1}^{n} D_{y_i}^{(j)}. \tag{2.65}$$

The decision metric in (2.64) has 3 multiplications and 2 additions (if $a_i^{(j)} = 1$, the complexity of the decision metric (2.64) is reduced to 1 multiplication and 2 additions). Thus the decoding complexity of a trellis diagram with N_p distinct paths and n levels, using a Brute-force minimization (search all paths) on (2.65), has $N_p - 1$ comparisons, $3nN_p$ multiplications and $(2n + (n-1))N_p = (3n-1)N_p$ additions.

2.5 OFDM

An excellent summary of *orthogonal frequency division multiplexing (OFDM)* can be found in [32, 7, 26]. OFDM is a technique of multicarrier transmission for a high data rate wireless communication to mitigate the effect of delay spread in a frequency-selective fading channel. The delay spread causes intersymbol-interference (ISI) at the receiver resulting in an irreducible error rate (or error floor) in performance. Let B_c

be the bandwidth of a channel and B_s be the bandwidth of a signal. Then $B_s \gg B_c$ in a frequency-selective fading channel.

The idea of OFDM transmission is to divide the main (signal) stream into N_c substreams, as in Figure 2.11. Each substream uses a frequency which is orthogonal to those of the other subcarriers², that is, $f_n = n\Delta f$ where $n = 0, 1, \ldots, N_c - 1$. Here Δf is a *frequency spacing* where $\Delta f = \frac{1}{N_c T_n}$ and T_n is the duration time of each subchannel. Then the bandwidth of each subchannel is $B_n = \frac{B_s}{N_c} < B_c$ so that now the bandwidth of each subchannel is less than the bandwidth of a channel. This makes the channel become less flat to the subchannel. When we choose sufficient large N_c such that $B_n \ll B_c$ so $T_n \approx \frac{1}{B_n} \gg \frac{1}{B_c} \approx T_l$ where T_l is the time delay of a channel; $T_n \gg T_l$ means a subchannel has small ISI degradation.

The parallel OFDM modulations are implemented from *inverse discrete Fourier transform (IDFT)* and *discrete discrete Fourier transmform (DFT)* at the transmitter and receiver respectively. Furthermore, by inserting a guard interval (or a *cyclic prefix (CP)*), it completely eliminates ISI without the requirement of an equalizer at the receiver.

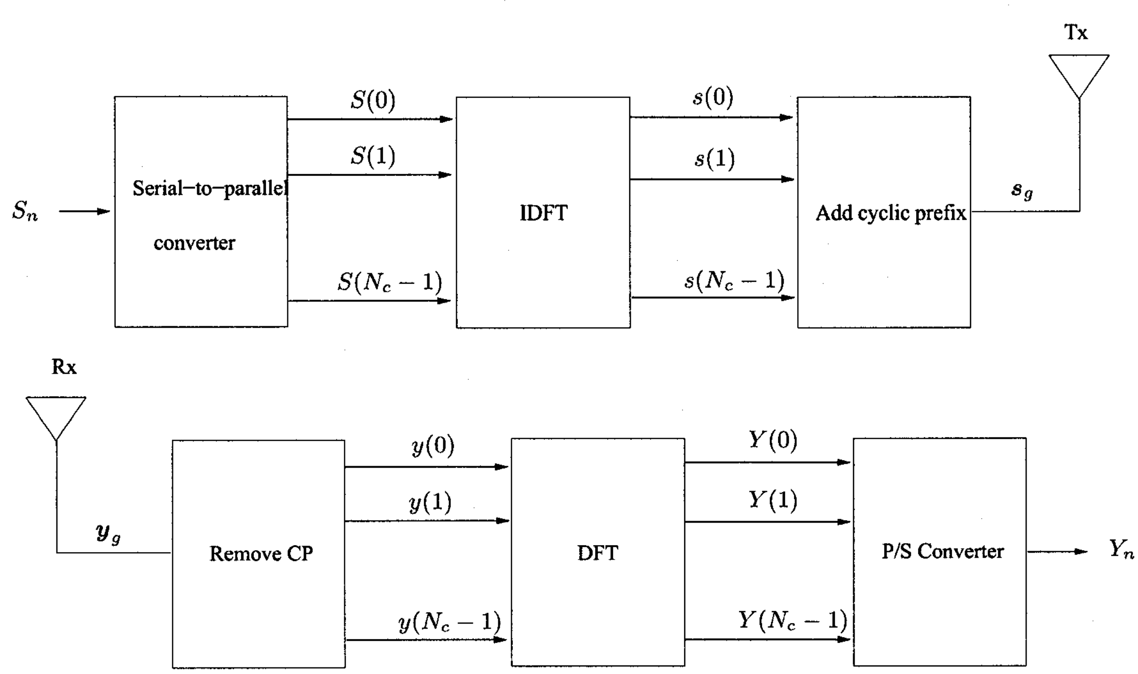

Figure 2.11: OFDM system

[2]Some papers call these tones or frequency bins.

2.5.1 OFDM Transmission

Let S_n be an input sequence, $\{S(0), S(1), \ldots, S(N_c - 1)\}$, chosen from QAM signal constellation. The transmitted OFDM signal is the IDFT of the input sequence, given by

$$s(t) = \text{IDFT}\{S_n\} = \frac{1}{\sqrt{N_c}} \sum_{k=0}^{N_c-1} S(k) e^{j\frac{2\pi kt}{N_c T_n}}, \; 0 \le t < N_c T_n. \tag{2.66}$$

Here $N_c T_n$ is the duration time of an OFDM data block. Let $\boldsymbol{h}_\tau$ be the channel response at time τ, defined by

$$h_\tau = \sum_{l=0}^{L_c-1} h(l)\delta(\tau - \tau_l) \tag{2.67}$$

where $h(l)$ is the channel coefficient at the path l and we assume the $h(l)$'s are complex Gaussian random variables with zero mean and normalized so that $\sum_{l=0}^{L_c-1} |h(l)|^2 = 1$. We call L_c the length of a channel where $h(l) = 0$ when $l > L_c$. Recall τ_l is the time delay at the path l so τ_{L_c-1} is the time delay of the channel.

From Figure 2.11, the output sequence from the IDFT is considered from (2.66) at time $t = nT_n$, that is,

$$s(n) = \frac{1}{\sqrt{N_c}} \sum_{k=0}^{N_c-1} S(k) e^{j\frac{2\pi nk}{N_c}} \tag{2.68}$$

where $n = 0, 1, \ldots, N_c - 1$. (Note: we can consider $S(n)$ and $s(n)$ in frequency and time domains respectively where $s(n) = \text{IDFT}\{S(n)\}$.)

After IDFT, we add a CP of length G (generally $G \ge L_c$ and less than 10% of N_c [32]), using the last G bits of $\boldsymbol{s}_n = (s(0), s(1), \ldots, s(N_c - 1))$ so we have an OFDM sequence with the CP as

$$\boldsymbol{s}_g = (s(N_c - G), \ldots, s(N_c - 1), s(0), s(1), \ldots, s(N_c - 1)). \tag{2.69}$$

We can see that $\boldsymbol{s}_g$ has a circular convolution, that is,

$$s_g(n) = s_g(n - N_c) \tag{2.70}$$

where $n = N_c \ldots, N_c + G + 1$. The property of this circular convolution will give a simple equation of the OFDM channel model as we will express later in (2.74).

At the receiver, the received sequence is

$$y_g(n) = s_g(n) \star h_\tau + w(n) \tag{2.71}$$

where $n = 0, 1, \ldots, N_c+G+1$, $\star$ denotes the convolution operation and $w(n)$ represents complex Gaussian noise at the receiver. We remove the first G bits of the sequence $\boldsymbol{y}_g$, that is, the output is

$$y(n) = y_g(n+G), \tag{2.72}$$

$n = 0, 1, \ldots, N_c - 1$. Then the received sequence is

$$Y(n) = \mathrm{DFT}\{y(n)\} = \frac{1}{\sqrt{N_c}} \sum_{k=0}^{N_c-1} y(k) e^{-j\frac{2\pi nk}{N_c}}. \tag{2.73}$$

The Fourier transform of a convolution in the time domain is a multiplication in the frequency domain. Hence, applying this property to the circular convolution in (2.71), we can simply write the received sequence after removing the CP as [51]

$$Y(n) = H(n)S(n) + W(n) \tag{2.74}$$

where $n = 0, 1, \ldots, N_c - 1$ and $H(n)$ is the DFT of the channel impulse response at the n-th subcarrier, that is,

$$H(n) = \sum_{l=0}^{L_c-1} h(l) e^{-j\frac{2\pi nl}{N_c}}. \tag{2.75}$$

We can see that now the received sequence in an OFDM system as expressed in (2.74) has the same format as a typical received signal in a Rayleigh fading channel where $H(n)$ is a complex fading coefficient of the subcarrier n. The equivalent OFDM channel model in (2.74) is useful for simulation (and for quick analysis) since we can avoid the steps which require the IDFT and DFT.

Using the ML criterion, we decode a message of the n-th subcarrier by $\min \|Y(n) - H(n)\hat{S}\|^2$ for all $\hat{S} \in$ QAM. We use the OFDM representation given in (2.74) for the simulation of symbol error rate (SER) performance of our proposed OFDM in Section 9.4.

2.5.2 Peak-to-Average Power Ratio (PAPR)

The *peak-to-average power ratio (PAPR)* of an OFDM transmitted signal is computed via

$$\mathrm{PAPR} = \frac{\max\limits_{0\leq t\leq N_c T_n} |s(t)|^2}{1/N_c T_n \int_0^{N_c T_n} |s(t)|^2 dt} \tag{2.76}$$

where $s(t)$ is the transmitted OFDM signal defined in (2.66). A large value of PAPR indicates that the average and peak values are far apart.

The PAPR in (2.76) is calculated from a continuous-time signal $s(t)$. However, in practical situations, we measure and compute the PAPR from the discrete time signals of $s(t)$, by a sampling method. We sample the transmitted OFDM signal $s(t)$ by a sampling factor W. The discrete time signal at the sampling time $t = n'\frac{T_n}{W}$ is

$$s(n') = \frac{1}{\sqrt{N_c}} \sum_{k=0}^{N_c-1} S(k) e^{j\frac{2\pi k n'}{N_c W}} \tag{2.77}$$

where $n' = 0, 1, \ldots, N_c W - 1$. It is clear that if we choose a sampling factor $W = 1$, (2.77) is the same as (2.68). It has been shown in [96] that $W = 4$ is sufficient to capture the peaks of the signal and gives an accurate PAPR. Hence, the PAPR from the sampling signals of factor W is

$$\mathrm{PAPR} = \frac{\max\limits_{0\leq n'\leq N_c W-1} |s(n')|^2}{E|s(n')|^2} \tag{2.78}$$

where $s(n')$ is defined in (2.77) and $E|s(n')|^2$ denotes the expectation of $|s(n')|^2$. We use the formula (2.78) and the sampling factor $W = 4$ to compute the PAPR of our proposed OFDM system in Chapter 9.

In particular interest, we consider a PAPR reduction method using the *tone injection (TI)* on a hexagonal constellation introduced in [29]. The improvement of PAPR reduction comes from the large degree of freedom of a hexagonal constellation (which is more dense compared to QAM for given the same minimum distance). In [29], the authors use the (suboptimal) technique of partial transmit sequence (PTS) introduced in [46] to map from the input sequence S_n chosen from QAM to the hexagonal constellation. They show that this does not increase signal power nor increase data rate loss. Moreover, the subcarrier frequency from a hexagonal constellation is shown to be detected and synchronized easily at the receiver [99].

The ARGC $\mathcal{A}_2$ is related to hexagonal constellations, as we will show in Chapter 8, and we will use it to further reduce the PAPR of an OFDM system in Section 9.4.

Chapter 3

USTC From Group Codes

In this chapter, we present new full diversity space-time constellations for DUSTM with two transmitter antennas. The proposed constellations are based on permutation codes variant II and finite reflection group codes (FRGCs) as explained in Section 2.3.2 and 2.3.3 respectively. The constellations themselves are not groups, but belong to the larger class of nongroup constellations. An advantage of using group codes to construct USTC in this way is that the problem of finding the best initial vector, and the value of the nearest distance, has been solved for permutation code variant II and for all irreducible FRGs in [83] and [54] respectively. Consequently, the performance of the USTC constructed from these group codes may be predicted in advance. Having chosen a high-performance group code, the construction of the corresponding USTC is algorithmic and requires no optimization steps. The proposed constellations have excellent diversity products. Simulations show that they outperform other USTC designs in the literature.

3.1 USTC From Permutation Codes Variant II

Define a 2×2 full diversity unitary space-time constellation for two transmitter antennas via

$$\boldsymbol{V}(x_1, x_2, x_3, x_4) = \begin{bmatrix} x_1 + jx_2 & -(x_3 - jx_4) \\ x_3 + jx_4 & x_1 - jx_2 \end{bmatrix}. \tag{3.1}$$

Here $\boldsymbol{x} = (x_1, x_2, x_3, x_4) \in \mathcal{X}$, where $\mathcal{X}$ is a four-dimensional permutation code variant II of order L normalized by its codeword's energy $\sqrt{E}$, that is

$$\mathcal{X} = \frac{1}{\sqrt{E}}\{\boldsymbol{x}_i\}_{i=0}^{L-1}. \tag{3.2}$$

The codeword's energy E is computed by (2.38). The order of the unitary constellation in (3.1) is equal to L defined in (2.36).

For the given dimension $n = \sum_{i=1}^{k} m_i = 4$, we maximize the diversity product of this constellation by choosing the distributions m as

$$m_1 \geq m_2 \geq \ldots \geq m_k \tag{3.3}$$

and also setting

$$\mu_i = \frac{1}{\sqrt{2}} + i - 1. \tag{3.4}$$

This condition on μ_i makes the minimum square distance of codewords $d^2_{\min}$ in (2.37) equal to 2.

Theorem 3.1.1. *The diversity product of the proposed USTC in (3.1) is*

$$\zeta_{\mathcal{V}} = \frac{1}{\sqrt{2E}}. \tag{3.5}$$

Proof. From the definition of diversity product given in (2.14), we have

$$\begin{aligned}
\zeta_{\mathcal{V}} &= \min_{\boldsymbol{V},\boldsymbol{V}'\in\mathcal{V}} \frac{1}{2}|\det(\boldsymbol{V}-\boldsymbol{V}')|^{\frac{1}{2}} \\
&= \min_{\boldsymbol{x},\boldsymbol{x}'\in\mathcal{X}} \frac{1}{2}\left|\det\left[\begin{array}{cc} (x_1-x_1')+j(x_2-x_2') & -((x_3-x_3')-j(x_4-x_4')) \\ (x_3-x_3')+j(x_4-x_4') & (x_1-x_1')-j(x_2-x_2') \end{array}\right]\right|^{\frac{1}{2}} \\
&= \min_{\boldsymbol{x},\boldsymbol{x}'\in\mathcal{X}} \frac{1}{2}[(x_1-x_1')^2+(x_2-x_2')^2+(x_3-x_3')^2+(x_4-x_4')^2]^{\frac{1}{2}} \\
&= \frac{1}{2}\sqrt{\frac{d^2_{\min}}{E}}, \text{ from (3.2)} \\
&= \frac{1}{2}\sqrt{\frac{2}{E}}, \text{ from the condition of } \mu_i \text{ in (3.4)} \\
&= \frac{1}{\sqrt{2E}}.
\end{aligned} \tag{3.6}$$

$\square$

Our proposed unitary constellations with their distributions, orders and diversity products are listed in Table 3.1. They are found by all combinations of the condition $n = m_1 + m_2 + \ldots + m_k = 4$ in (3.3).

m	L	$\zeta_\mathcal{V}$	
4	16	0.5000	
(3,1)	64	0.3367	Figure 3.1
(2,2)	96	0.2706	
(2,1,1)	192	0.2109	Figure 3.2
(1,1,1,1)	384	0.1429	

Table 3.1: Our proposed USTC from permutation codes variant II and their diversity products

We illustrate two examples of constructing proposed USTCs from permutation codes variant II as listed in Table 3.1 at the date rate $R = 3.00$ and 4.00 bits/s.

R = 3.00 bits/s

From Table 3.1, our proposed USTC at $L = 64$ and $R = 3.00$ bits/s has the distribution $m = (3, 1)$. Hence the energy is

$$E = 3 \times (\frac{1}{\sqrt{2}})^2 + 1 \times (\frac{1}{\sqrt{2}} + 1)^2 = 4.4142. \tag{3.7}$$

This implies the alphabet of this unitary constellation is

$$\mathcal{X} = \left\{ \frac{1}{\sqrt{4.4142}} \left(\pm\frac{1}{\sqrt{2}}, \pm\frac{1}{\sqrt{2}}, \pm\frac{1}{\sqrt{2}}, \pm(\frac{1}{\sqrt{2}} + 1) \right)^P \right\}. \tag{3.8}$$

From 3.5, the diversity product is

$$\zeta_\mathcal{V} = \frac{1}{\sqrt{2 \times 4.4142}} = 0.3366 \tag{3.9}$$

which is the largest diversity product among different 2×2 USTC at the same rate $R = 3.00$ bit/s as shown in Table 3.2.

The performance of our proposed USTCs is done from Monte-Carlo simulation in MATLAB. The code performance is considered by plotting the *block error rate (BLER)* against SNR in dB. All plots are considered in an unknown Rayleigh flat fading channel using DUSTM and the ML criterion in (2.10) for decoding as explained in Section 2.1.1. The fading coefficients and additive noise are independent complex Gaussian variables with mean zero and variance one $\mathcal{CN}(0,1)$ and the channel matrix is assumed to be constant within two consecutive time periods.

Figure 3.1 shows the BLER performance of our proposed USTC with $m = (3,1)$ and $R = 3.00$ bits/s for two receiver antennas $n_R = 2$. We can see that our proposed USTC performs very well for high SNR, and outperforms the other four designs.

USTC designs	$\zeta_{\mathcal{V}}$
Dicyclic group Q_5 [36]	0.0980
Cyclic group $u = (1, 19)$ [35]	0.1985
Orthogonal with 8^{th}-roots of unity [90]	0.2706
Parametric code, $k = (7, 10, 0)$ [49]	0.3070
Numerical method $A^k B^k$ [28]	0.3090
Proposed constellation	0.3366

Table 3.2: Comparison of different 2×2 USTC designs for $R = 3.00$ bits/s. Our proposed constellation is highlighted in grey.

$\mathbf{R \approx 4.00}$ bits/s

From Table 3.1, the distribution of proposed USTC at $L = 192$, $R = 3.79$ bit/s/Hz is $m = (2,1,1)$. Hence the energy is

$$E = 2 \times (\frac{1}{\sqrt{2}})^2 + 1 \times (\frac{1}{\sqrt{2}} + 1)^2 + 1 \times (\frac{1}{\sqrt{2}} + 2)^2 = 11.2426. \tag{3.10}$$

This constellation has the alphabet

$$\mathcal{X} = \left\{ \frac{1}{\sqrt{11.2426}} \left(\pm\frac{1}{\sqrt{2}}, \pm\frac{1}{\sqrt{2}}, \pm(\frac{1}{\sqrt{2}} + 1), \pm(\frac{1}{\sqrt{2}} + 2) \right)^P \right\} \tag{3.11}$$

with the diversity product

$$\zeta_{\mathcal{V}} = \frac{1}{\sqrt{2 \times 11.2426}} = 0.2109. \tag{3.12}$$

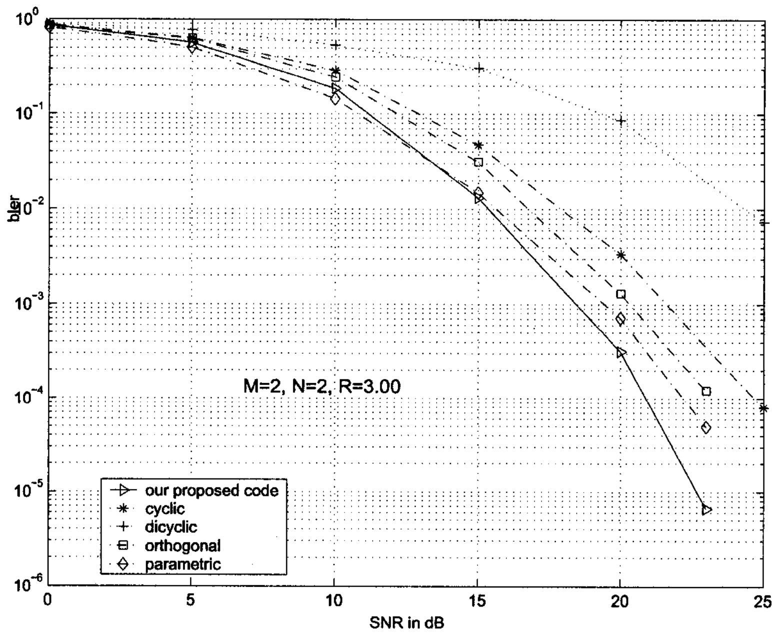

Figure 3.1: BLER performance of different USTCs for $n_T = 2$, $n_R = 2$ at $R = 3.00$ bits/s. Our proposed constellation is permutation code variant II with $m = (3, 1)$.

We give a comparison of the diversity products of this proposed unitary constellation with different 2×2 unitary designs at the same data rate $R \approx 4.00$ bits/s in Table 3.3. We can see that the proposed USTC from permutation code variant II has the largest diversity product, and also outperforms the other three designs as displayed in Figure 3.2, with one receiver antenna, $n_R = 1$.

USTC designs	R	$\zeta_{\mathcal{V}}$
Dicyclic group Q_7 [36]	4.00	0.0245
Cyclic group $u = (1, 151)$ [35]	3.95	0.1045
Orthogonal 16^{th}-roots of unity [90]	4.00	0.1379
Proposed constellation	3.79	0.2109

Table 3.3: Comparison of different 2×2 USTC designs for $R \approx 4.00$ bits/s. Our proposed constellation is highlighted in grey.

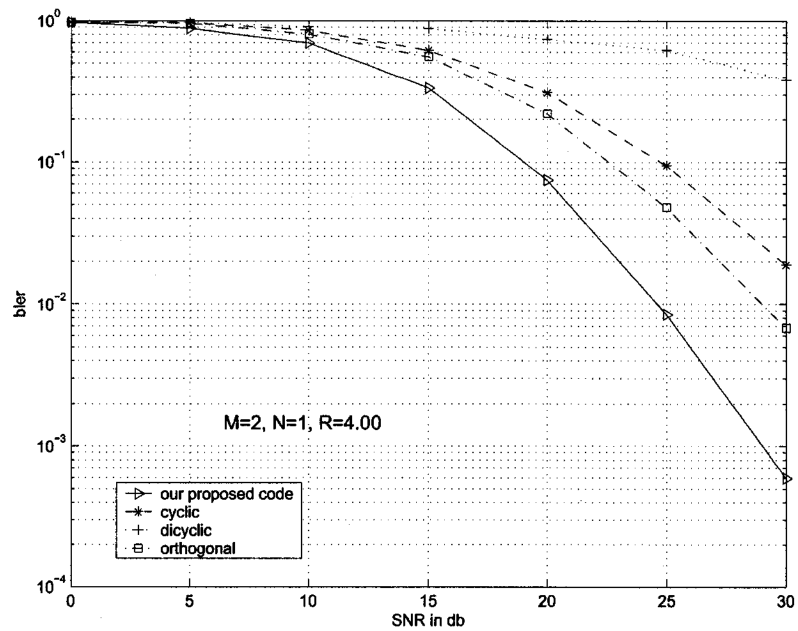

Figure 3.2: BLER performance of different USTCs for $n_T = 2$, $n_R = 1$ at $R \approx 4.00$ bits/s. Our proposed constellation is permutation code variant II with $m = (2, 1, 1)$.

3.2 USTC From Finite Reflection Group Codes

Consider an irreducible FRG $\mathcal{G}$ of rank $n = 4$, such as $\mathcal{B}_4$, $\mathcal{I}_4$ and $\mathcal{F}_4$ in Section 2.3.3. Choose a normalized initial vector $\|\boldsymbol{x}_0\| = 1$, $\boldsymbol{x}_0 \in \mathbb{R}^4$ from (2.42). The proposed 2×2 full diversity USTC obtained from these FRGCs $\mathcal{X}$ consist of $\boldsymbol{V}(x_1, x_2, x_3, x_4)$ defined in (3.1) where $\boldsymbol{x} = (x_1, x_2, x_3, x_4) \in \mathcal{X}$.

Let an initial vector be $\boldsymbol{x_0} = (x_{01}, x_{02}, x_{03}, x_{04})$ and $\boldsymbol{r} = (r_1, r_2, r_3, r_4)$ be a simple root of an irreducible FRG $\mathcal{G}$. We compute the 4-dimensional orthogonal reflection matrix $S_{\boldsymbol{r}}$ of $\mathcal{G}$ of rank 4, as follows. From (2.21), the FRG codeword generated from the reflection $S_{\boldsymbol{r}} \in \mathcal{G}$ to $\boldsymbol{x_0}$ is computed via

$$
\begin{aligned}
S_{\boldsymbol{r}}\boldsymbol{x_0} &= \boldsymbol{x_0} - 2\frac{\boldsymbol{x_0}\cdot\boldsymbol{r}}{\boldsymbol{r}\cdot\boldsymbol{r}}\boldsymbol{r} \qquad (3.13)\\
&= \begin{bmatrix} x_{01} \\ x_{02} \\ x_{03} \\ x_{04} \end{bmatrix} - 2\frac{\boldsymbol{x_0}\cdot\boldsymbol{r}}{\boldsymbol{r}\cdot\boldsymbol{r}} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{bmatrix} = \begin{bmatrix} x_{01}\left(1-\frac{2r_1}{\boldsymbol{r}\cdot\boldsymbol{r}}\right) - \frac{2x_{02}r_1}{\boldsymbol{r}\cdot\boldsymbol{r}} - \frac{2x_{03}r_1}{\boldsymbol{r}\cdot\boldsymbol{r}} - \frac{2x_{04}r_1}{\boldsymbol{r}\cdot\boldsymbol{r}} \\ \frac{2x_{01}r_2}{\boldsymbol{r}\cdot\boldsymbol{r}} + x_{02}\left(1-\frac{2r_2}{\boldsymbol{r}\cdot\boldsymbol{r}}\right) - \frac{2x_{03}r_2}{\boldsymbol{r}\cdot\boldsymbol{r}} - \frac{2x_{04}r_2}{\boldsymbol{r}\cdot\boldsymbol{r}} \\ -\frac{2x_{01}r_3}{\boldsymbol{r}\cdot\boldsymbol{r}} - \frac{2x_{02}r_3}{\boldsymbol{r}\cdot\boldsymbol{r}} + x_{03}\left(1-\frac{2r_3}{\boldsymbol{r}\cdot\boldsymbol{r}}\right) - \frac{2x_{04}r_3}{\boldsymbol{r}\cdot\boldsymbol{r}} \\ -\frac{2x_{01}r_4}{\boldsymbol{r}\cdot\boldsymbol{r}} - \frac{2x_{02}r_4}{\boldsymbol{r}\cdot\boldsymbol{r}} - \frac{2x_{03}r_4}{\boldsymbol{r}\cdot\boldsymbol{r}} + x_{04}\left(1-\frac{2r_4}{\boldsymbol{r}\cdot\boldsymbol{r}}\right) \end{bmatrix}. \qquad (3.14)
\end{aligned}
$$

Hence, for a given simple root $\boldsymbol{r} = (r_1, r_2, r_3, r_4)$, the 4-dimensional orthogonal reflection matrix is

$$S_{\boldsymbol{r}} = \begin{bmatrix} 1 - p_1 r_1 & -p_1 r_2 & -p_1 r_3 & -p_1 r_4 \\ -p_2 r_1 & 1 - p_2 r_2 & -p_2 r_3 & -p_2 r_4 \\ -p_3 r_1 & -p_3 r_2 & 1 - p_3 r_3 & -p_3 r_4 \\ -p_4 r_1 & -p_4 r_2 & -p_4 r_3 & 1 - p_4 r_4 \end{bmatrix} \tag{3.15}$$

where

$$p_i = \frac{2r_i}{\boldsymbol{r} \cdot \boldsymbol{r}}, \quad i = 1, 2, 3, 4. \tag{3.16}$$

The codewords $\mathcal{X}$ obtained from the FRGC (and hence, via the formula (3.1), the elements of the proposed unitary constellation $\mathcal{V}$) are thus obtained from $\boldsymbol{x_0}$ by

$$\mathcal{X} = \left\{ \prod_{i_j} S_{\boldsymbol{r}_{i_j}} \boldsymbol{x_0} \right\} \tag{3.17}$$

where the indices $i_j \in \{1, 2, 3, 4\}$ are determined by the presentation of the FRG (using, for example, [1]), and $S_{\boldsymbol{r}_i}$ is defined in (3.15).

The data rate of the proposed USTC from FRG is $R = \log_2 L/2$ bits/s where $L = |\mathcal{G}|/|\mathcal{H}|$ and $\mathcal{H}$ is the subgroup of $\mathcal{G}$ generated from the reflections of the passive simple system Δ_p.

Since we set an initial vector $\|\boldsymbol{x}_0\| = 1$, the energy $E = 1$ for all FRG codewords (all codewords lie on a unit sphere). Thus, from (3.6), the diversity product is $d_{\min}/2$. Finally, from (2.43), the diversity product of the proposed USTC obtained from irreducible FRGCs as defined in (3.1) is

$$\zeta_{\mathcal{V}} = \left[\sum_{\boldsymbol{r_i} \in \Delta \backslash \Delta_p} \sum_{\boldsymbol{r_j} \in \Delta \backslash \Delta_p} (\|\boldsymbol{r_i}\| \cdot \|\boldsymbol{r_j}\|) \boldsymbol{\lambda_i} \cdot \boldsymbol{\lambda_j} \right]^{-\frac{1}{2}} \tag{3.18}$$

where Δ and Δ_p are the simple and passive simple systems of FRG $\mathcal{G}$ respectively, and $\boldsymbol{\lambda}_i$ is the dual vector to the simple root $\boldsymbol{r}_i$.

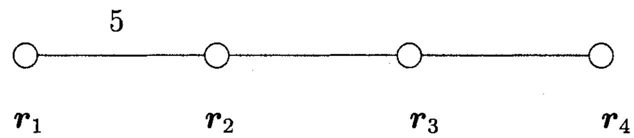

Figure 3.3: The Coxeter graph of the irreducible FRG $\mathcal{I}_4$

Proposed USTC From $\mathcal{I}_4$

We give an example of constructing a full diversity USTC based on the irreducible FRG $\mathcal{I}_4$. The Coxeter graph of $\mathcal{I}_4$ is shown in Figure 3.3. From [54, Table I], the simple system $\Delta = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_3}, \boldsymbol{r_4}\}$ of $\mathcal{I}_4$ consists of the 4 simple roots:

$$\begin{aligned}
\boldsymbol{r_1} &= \cos\frac{2\pi}{5}(2\cos\frac{\pi}{5}+1, 1, -2\cos\frac{\pi}{5}, 0), \\
\boldsymbol{r_2} &= \cos\frac{2\pi}{5}(-2\cos\frac{\pi}{5}-1, 1, 2\cos\frac{\pi}{5}, 0), \\
\boldsymbol{r_3} &= \cos\frac{2\pi}{5}(2\cos\frac{\pi}{5}, -2\cos\frac{\pi}{5}-1, 1, 0), \\
\boldsymbol{r_4} &= \cos\frac{2\pi}{5}(-2\cos\frac{\pi}{5}, 0, -2\cos\frac{\pi}{5}-1, 1).
\end{aligned}$$

From Section 2.2.1, we can express the presentation of $\mathcal{I}_4$ from its Coxeter graph in Figure 3.3 as

$$\begin{aligned}
\mathcal{I}_4 \;=\; & \langle S_{\boldsymbol{r_1}}, S_{\boldsymbol{r_2}}, S_{\boldsymbol{r_3}}, S_{\boldsymbol{r_4}} | S^2_{\boldsymbol{r_1}} = S^2_{\boldsymbol{r_2}} = S^2_{\boldsymbol{r_3}} = S^2_{\boldsymbol{r_4}} = (S_{\boldsymbol{r_1}}S_{\boldsymbol{r_2}})^5 = (S_{\boldsymbol{r_1}}S_{\boldsymbol{r_3}})^2 = \\
& (S_{\boldsymbol{r_1}}S_{\boldsymbol{r_4}})^2 = (S_{\boldsymbol{r_2}}S_{\boldsymbol{r_3}})^3 = (S_{\boldsymbol{r_2}}S_{\boldsymbol{r_4}})^2 = (S_{\boldsymbol{r_3}}S_{\boldsymbol{r_4}})^3 = \boldsymbol{I}\rangle \qquad (3.19)
\end{aligned}$$

where $\boldsymbol{I}$ denotes the identity matrix. The order is $|\mathcal{I}_4| = 14400$. Using the formula given in (3.15), the 4-dimensional orthogonal reflection matrices of these simple roots $\boldsymbol{r_1}$, $\boldsymbol{r_2}$, $\boldsymbol{r_3}$ and $\boldsymbol{r_4}$ are

$$S_{\boldsymbol{r_1}} = \begin{bmatrix} -\cos\frac{2\pi}{5} & -\frac{1}{2} & \cos\frac{\pi}{5} & 0 \\ -\frac{1}{2} & \cos\frac{\pi}{5} & \cos\frac{2\pi}{5} & 0 \\ \cos\frac{\pi}{5} & \cos\frac{2\pi}{5} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, S_{\boldsymbol{r_2}} = \begin{bmatrix} -\cos\frac{2\pi}{5} & \frac{1}{2} & \cos\frac{\pi}{5} & 0 \\ \frac{1}{2} & \cos\frac{\pi}{5} & -\cos\frac{2\pi}{5} & 0 \\ \cos\frac{\pi}{5} & -\cos\frac{2\pi}{5} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$S_{\boldsymbol{r_3}} = \begin{bmatrix} \frac{1}{2} & \cos\frac{\pi}{5} & -\cos\frac{2\pi}{5} & 0 \\ \cos\frac{\pi}{5} & -\cos\frac{2\pi}{5} & \frac{1}{2} & 0 \\ -\cos\frac{2\pi}{5} & \frac{1}{2} & \cos\frac{\pi}{5} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad S_{\boldsymbol{r_4}} = \begin{bmatrix} \frac{1}{2} & 0 & -\cos\frac{\pi}{5} & \cos\frac{2\pi}{5} \\ 0 & 1 & 0 & 0 \\ -\cos\frac{\pi}{5} & 0 & -\cos\frac{2\pi}{5} & \frac{1}{2} \\ \cos\frac{2\pi}{5} & 0 & \frac{1}{2} & \cos\frac{\pi}{5} \end{bmatrix}$$

respectively.

Choose the initial vector $\boldsymbol{x_0} = (0,0,0,1)$ which corresponds to the passive simple system $\Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_3}\}$ since $S_{\boldsymbol{r}_i}\boldsymbol{x_0} = \boldsymbol{x_0}$ for all $i = 1, 2$ and 3. This gives a unitary constellation[1] of order $L = 14400/120 = 120$ which has the data rate $R = \log_2 120/2 \approx 3.45$ bits/s. The comparison of this proposed USTC with different 2×2 USTC designs at the same data rate $R \approx 3.45$ bits/s is given in Table 3.4. We can see that our proposed USTC has the highest diversity product $\zeta_{\mathcal{V}} = 0.3090$ which equals that of the excellent USTC obtained from a fixed-point free group $SL_2(\mathbb{F}_5)$ presented in [80].

USTC designs	L	R	$\zeta_{\mathcal{V}}$
Dicyclic group Q_6 [36]	128	3.50	0.0491
Cyclic group $u = (1, 43)$ [35]	120	3.45	0.1353
Orthogonal 11^{th}-roots of unity [2, 91]	121	3.46	0.1992
$SL_2(\mathbb{F}_5)$ [80]	120	3.45	0.3090
Proposed USTC from $\mathcal{I}_4$, $\Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_3}\}$	120	3.45	0.3090

Table 3.4: Comparison of different 2×2 USTC designs for $R \approx 3.45$ bits/s. Our proposed constellation is highlighted in grey.

Figure 3.4 shows the BLER performance of this proposed USTC from $\mathcal{I}_4$ when $\Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_3}\}$ compared to different 2×2 USTC designs at the same data rate $R \approx 3.45$ with $n_R = 1$ receiver antenna. We can see that the proposed USTC outperforms the dicyclic, cyclic and orthogonal designs.

Proposed USTC From $\mathcal{B}_4$

From Table 2.2, the 4 simple roots of the irreducible FRG $\mathcal{B}_4$ are $\boldsymbol{r_1} = (1,0,0,0)$, $\boldsymbol{r_2} = (-1,1,0,0)$, $\boldsymbol{r_3} = (0,-1,1,0)$ and $\boldsymbol{r_4} = (0,0,-1,1)$. The Coxeter graph of $\mathcal{B}_4$ is given in Figure 3.5. The 4-dimensional orthogonal reflection matrices $S_{\boldsymbol{r}_i}$ of these

[1]We have used GAP [1] to determine the indices i_j in (3.17) to generate these codewords.

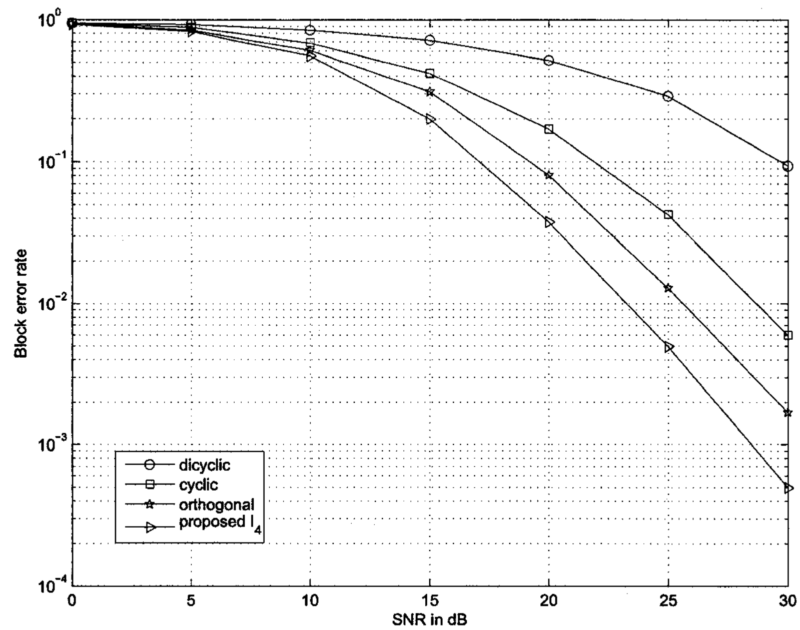

Figure 3.4: BLER performance of different USTCs for $n_R = 1$ at $R \approx 3.45$ bits/s. Our proposed constellation is $\mathcal{I}_4$ when $\Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_3}\}$.

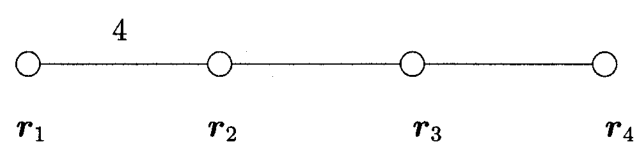

Figure 3.5: The Coxeter graph of the irreducible FRG $\mathcal{B}_4$

simple roots are also computed from (3.15) as

$$S_{\boldsymbol{r_1}} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; S_{\boldsymbol{r_2}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$S_{\boldsymbol{r_3}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; S_{\boldsymbol{r_4}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

From its Coxeter graph in Figure 3.5, we can write the presentation of $\mathcal{B}_4$ as

$$\begin{aligned}\mathcal{B}_4 &= \langle S\boldsymbol{r_1}, S\boldsymbol{r_2}, S\boldsymbol{r_3}, S\boldsymbol{r_4} | S^2_{\boldsymbol{r_1}} = S^2_{\boldsymbol{r_2}} = S^2_{\boldsymbol{r_3}} = S^2_{\boldsymbol{r_4}} = (S\boldsymbol{r_1} S\boldsymbol{r_2})^4 = (S\boldsymbol{r_1} S\boldsymbol{r_3})^2 = \\ &\quad (S\boldsymbol{r_1} S\boldsymbol{r_4})^2 = (S\boldsymbol{r_2} S\boldsymbol{r_3})^3 = (S\boldsymbol{r_2} S\boldsymbol{r_4})^2 = (S\boldsymbol{r_3} S\boldsymbol{r_4})^3 = \boldsymbol{I} \rangle \end{aligned} \tag{3.20}$$

with its order $|\mathcal{B}_4| = 384$.

Choose the initial vector

$$\boldsymbol{x_0} = \frac{1}{(3+\sqrt{2})^{\frac{1}{2}}} \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 1 + \frac{1}{\sqrt{2}} \right)$$

corresponding to the passive simple system $\Delta_p = \{\boldsymbol{r_2}, \boldsymbol{r_3}\}$. Hence the proposed constellation has $L = 384/6 = 64$ giving the data rate $R = \log_2 64/2 = 3.00$ bits/s. This proposed unitary constellation $\mathcal{B}_4$ has the highest diversity product compared to different 2×2 USTC designs at the same data rate $R = 3.00$ as listed in Table 3.5.

Unitary space-time constellation designs $L = 64, R = 3.00$	$\zeta_{\mathcal{V}}$
Dicyclic group Q_5 [36]	0.0980
Cyclic group $u = (1, 19)$ [35] and $G_{64,1}$ [80]	0.1985
Orthogonal 8^{th}-roots of unity [2, 91]	0.2706
Proposed code from $\mathcal{B}_4$, $\Delta_p = \{\boldsymbol{r_2}, \boldsymbol{r_3}\}$	0.3363

Table 3.5: Comparison of different 2×2 USTC designs for $R = 3.00$ bits/s. Our proposed constellation is highlighted in grey.

The BLER performance of the proposed USTC obtained from $\mathcal{B}_4$ when $\Delta_p = \{\boldsymbol{r_2}, \boldsymbol{r_3}\}$ compared to different 2×2 USTC designs at the same data rate $R = 3.00$ bits/s/Hz is shown in Figure 3.6, for $n_R = 2$ receiver antennas. We can see that the proposed USTC outperforms the dicyclic, cyclic and orthogonal constellation designs.

Other Examples

We also give several other examples of the proposed USTCs obtained from irreducible FRGs of rank 4 ($\mathcal{B}_4, \mathcal{F}_4$ and $\mathcal{I}_4$) with their best diversity products in Table 3.6.

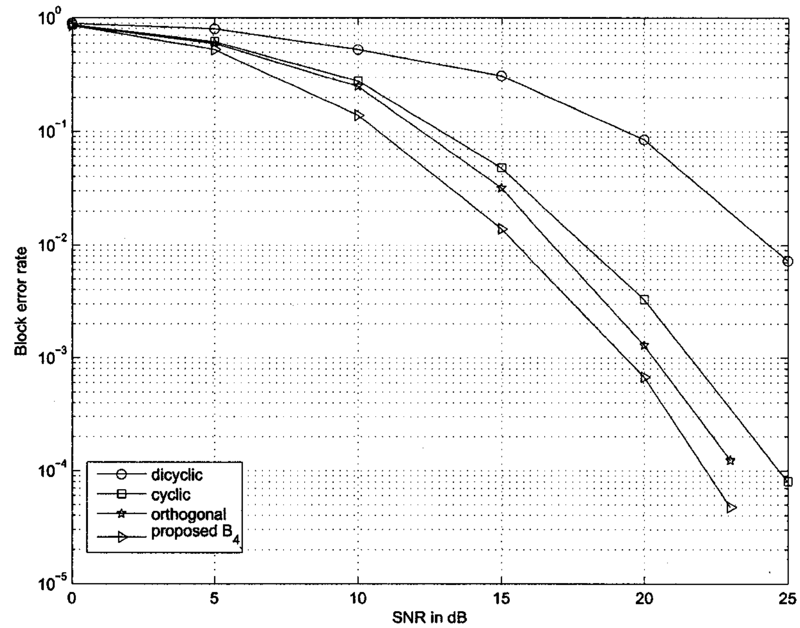

Figure 3.6: BLER performance of different USTCs for $n_R = 2$ at $R = 3.00$ bits/s. Our proposed constellation is $\mathcal{B}_4$ when $\Delta_p = \{\boldsymbol{r_2}, \boldsymbol{r_3}\}$.

Irreducible finite reflection groups of rank 4	L	R	$\zeta_{\mathcal{V}}$
$\mathcal{F}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_3}\}$	24	2.29	0.5000
$\mathcal{B}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_3}\}$	96	3.29	0.2861
$\mathcal{F}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_4}\}$	96	3.29	0.2887
$\mathcal{F}_4, \quad \Delta_p = \{\boldsymbol{r_2}, \boldsymbol{r_3}\}$	144	3.59	0.2706
$\mathcal{F}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}\}$	192	3.79	0.1890
$\mathcal{F}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_3}\}$	288	4.09	0.1913
$\mathcal{F}_4, \quad \Delta_p = \{\boldsymbol{r_2}\}$	576	4.59	0.1429
$\mathcal{I}_4, \quad \Delta_p = \{\boldsymbol{r_2}, \boldsymbol{r_3}, \boldsymbol{r_4}\}$	600	4.61	0.1350
$\mathcal{I}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_4}\}$	720	4.75	0.1625
$\mathcal{F}_4, \quad \Delta_p = \{\emptyset\}$	1152	5.09	0.0967
$\mathcal{I}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_3}, \boldsymbol{r_4}\}$	1200	5.11	0.1102
$\mathcal{I}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_2}\}$	1440	5.25	0.1077
$\mathcal{I}_4, \quad \Delta_p = \{\boldsymbol{r_2}, \boldsymbol{r_3}\}$	2400	5.61	0.0955
$\mathcal{I}_4, \quad \Delta_p = \{\boldsymbol{r_1}, \boldsymbol{r_3}\}$	3600	5.91	0.0823
$\mathcal{I}_4, \quad \Delta_p = \{\boldsymbol{r_2}\}$	7200	6.41	0.0604
$\mathcal{I}_4, \quad \Delta_p = \{\emptyset\}$	14400	6.91	0.0391

Table 3.6: Some examples of USTCs from irreducible finite reflection groups of rank 4

Chapter 4

Full Diversity USTC From Bruhat Decomposition

In this chapter, we present a new Bruhat decomposition design for constructing full diversity USTC for any number of transmitter antennas. The *Bruhat decomposition*[1] allows us to choose n_T disjoint non-overlapping cosets of a unitary diagonal subgroup $\mathcal{D}$ in such a way that *full diversity* is preserved.

Let $\mathcal{V} = \{\boldsymbol{V}_l\}_{l=0}^{L-1}$ be a set of $n_T \times n_T$ unitary matrices called a *signal constellation* where n_T is the number of transmitter antennas. The design problem of DUSTM is to maximize the minimum value of the distance

$$d(l, l') = |\det(\boldsymbol{V}_l - \boldsymbol{V}_{l'})| \geq 0, \tag{4.1}$$

for all distinct $\boldsymbol{V}_l, \boldsymbol{V}_{l'} \in \mathcal{V}$. A constellation $\mathcal{V}$ for which $d(l, l') > 0$ for all $l \neq l'$ is said to have *full diversity.* It has been shown that the finite simple unitary groups having full diversity are the *fixed-point free groups* [80]. It has also been proven that $U(1)$ and $SU(2)$ are the only two infinite full diversity unitary groups [34]. The application of the Bruhat decomposition to the design of full diversity unitary subgroup constellations of $U(2)$ and $U(4)$ was first introduced in [47] using a method which was developed for 2 and 4 transmitter antennas respectively, but which is not applicable to an odd number of transmitter antennas.

[1] Some background on the Bruhat decomposition is given in Appendix A.3

The diversity product defined in (2.14) can be written in the terms of $d(l,l')$ as

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{l,l'} d(l,l')^{\frac{1}{n_T}}. \tag{4.2}$$

We will construct a unitary (non-diagonal) constellation $\mathcal{V}$ as a union of cosets of diagonal unitary matrices $\mathcal{D}$ (see (4.3)). Then the diversity product of our proposed unitary constellation using Bruhat decomposition will be the lesser of the diversity product of $\mathcal{D}$ and a constant nonzero value coming from the calculation of $d(l,l')$ for $\boldsymbol{V}_l$ and $\boldsymbol{V}_{l'}$ in distinct cosets of $\mathcal{D}$. The proposed full diversity USTC using Bruhat decomposition, denoted as $\mathcal{V}$, is presented in Section 4.1. The properties on the condition of full diversity and some examples of $\mathcal{V}$ are discussed in Sections 4.1.1 and 4.1.2 respectively.

In Section 4.2, for the case where n_T is even, we consider an extension of these constellation designs using a Hamiltonian constellation [57] in place of $\mathcal{D}$. The resulting constellation is called Hamiltonian Bruhat USTC, and is denoted as $\mathcal{B}$. This approach gives a constellation with higher diversity product. Although our proposed constellations are not groups, we show that they are extremely symmetric in that the minimum value of $d(l,l')$ can be determined by checking only $L-1$ distinct elements in $\mathcal{V}$.

We consider the performance of both Bruhat designs in Section 4.3. Simulations show that our proposed constellations perform well in unknown Rayleigh flat fading channel, and also outperform other full diversity USTC designs.

4.1 Bruhat Constellation

We develop the design of a full diversity unitary Bruhat constellation $\mathcal{V}$ for any number of transmitter antennas using Bruhat decomposition as explained in Appendix A.3.

Let $\boldsymbol{\omega}$ be an $n_T \times n_T$ matrix representing the full permutation $(123\cdots n_T)$ in the natural representation. Following from (A.22), this cycle has the property that neither $\boldsymbol{\omega}$, nor any power of $\boldsymbol{\omega}$ (up to $\boldsymbol{\omega}^{n_T} = I$), has any fixed points. Consequently, the positions of the nonzero entries in $\boldsymbol{\omega}^i$, or equivalently, in $\boldsymbol{\omega}^i\mathcal{T}$, are entirely disjoint from those for $\boldsymbol{\omega}^j$ for any $i \neq j$ where $\mathcal{T}$ is a subgroup of all unitary matrices in the group of all invertible upper triangular matrices. (This property makes the computation of the distance between distinct cosets more accessible to theoretical analysis because the permutation $\boldsymbol{\omega}^i$ allows us to have a possible nonzero determinant of a difference of two distinct nonoverlapping cosets). From (A.24), this subgroup does not have full diversity since $\mathcal{T}$ itself does not. Thus to obtain a full diversity constellation, we restrict to a full diversity subgroup of $\mathcal{T}$ and then construct our (nongroup) constellation from its cosets.

Choose a finite full diversity subgroup $\mathcal{D}$ of diagonal unitary matrices having determinant equal to 1 (more precise conditions to be specified in (4.9)). Set $\lambda = e^{2\pi j/n_T^2}$. Our proposed unitary *Bruhat constellation* $\mathcal{V}$ is a subset of $S_n \ltimes \mathcal{T}$, given by the disjoint union of sets of unitary matrices defined by

$$\mathcal{V} = \bigcup_{i=0}^{n_T-1} \lambda^i \boldsymbol{\omega}^i \mathcal{D}. \tag{4.3}$$

Write $\boldsymbol{D} \in \mathcal{D}$ as $\boldsymbol{D} = \mathrm{diag}(d_1, d_2, \ldots, d_{n_T})$, then $|d_j| = 1\ \forall j$ and $d_1 d_2 \cdots d_{n_T} = 1$. Hence

$$\det(\lambda^i \boldsymbol{\omega}^i \boldsymbol{D}) = \pm e^{2\pi j i/n_T} \tag{4.4}$$

for all $i = 0, 1, \ldots, n_T - 1$. In order for $\mathcal{V}$ to be a *full diversity* constellation, we need to have $d(l, l') > 0$ (see the equation (4.1)). This problem can be broken into two cases:

i) Same Coset (sc) Case

Suppose $\boldsymbol{V}_l, \boldsymbol{V}_{l'} \in \mathcal{V}$ lie in the same coset $\lambda^i \boldsymbol{\omega}^i \mathcal{D}$. Then we can write $\boldsymbol{V}_l = \lambda^i \boldsymbol{\omega}^i \boldsymbol{D}$ and $\boldsymbol{V}_{l'} = \lambda^i \boldsymbol{\omega}^i \boldsymbol{D}'$ for some $\boldsymbol{D}, \boldsymbol{D}' \in \mathcal{D}$. We compute the distance between these codewords as

$$\begin{aligned} d_{sc}(l, l') &= |\det(\boldsymbol{V}_l - \boldsymbol{V}_{l'})| \\ &= |\det(\lambda^i \boldsymbol{\omega}^i \boldsymbol{D} - \lambda^i \boldsymbol{\omega}^i \boldsymbol{D}')| \\ &= |\det(\lambda^i \boldsymbol{\omega}^i)||\det(\boldsymbol{D} - \boldsymbol{D}')| \\ &= |\det(\boldsymbol{D} - \boldsymbol{D}')|, \quad \text{since } |\det(\lambda^i \boldsymbol{\omega}^i)| = 1. \end{aligned} \tag{4.5}$$

Thus the minimum value of $d_{sc}(l, l')$ equals the minimum distance between two elements of $\mathcal{D}$. Hence, in order to have $d_{sc}(l, l') > 0$, it suffices to require the full diversity of the subgroup constellation $\mathcal{D}$.

ii) Distinct Coset (dc) Case

Suppose now that $\boldsymbol{V}_l, \boldsymbol{V}_{l'} \in \mathcal{V}$ lie in distinct cosets; say $\boldsymbol{V}_l = \lambda^k \boldsymbol{\omega}^k \boldsymbol{D}$ and $\boldsymbol{V}_{l'} = \lambda^j \boldsymbol{\omega}^j \boldsymbol{D}'$, $k < j$ for some $\boldsymbol{D}, \boldsymbol{D}' \in \mathcal{D}$. Then as above, we may restrict ourselves to the case where $\boldsymbol{V}_l \in \mathcal{D}$ and $\boldsymbol{V}_{l'} \in \lambda^i \boldsymbol{\omega}^i \mathcal{D}$, since

$$|\det(\lambda^k\boldsymbol{\omega}^k\boldsymbol{D}-\lambda^j\boldsymbol{\omega}^j\boldsymbol{D}')| = |\det(\lambda^k\boldsymbol{\omega}^k)||\det(\boldsymbol{D}-\lambda^{j-k}\boldsymbol{\omega}^{j-k}\boldsymbol{D}')| = |\det(\boldsymbol{D}-\lambda^{j-k}\boldsymbol{\omega}^{j-k}\boldsymbol{D}')|. \tag{4.6}$$

To compute d_{dc} explicitly, we proceed follows. Recall the decomposition of $\boldsymbol{\omega}^i$ into disjoint cycles given in (A.22), $\omega^i = \sigma_1 \, \sigma_2 \cdots \sigma_g$. Let $\tilde{S}_i$ be the set of all possible permutations which can be formed from the set of disjoint cycles $\{\sigma_1, \sigma_2, \ldots, \sigma_g\}$ using each cycle at most once. For example, in the symmetric group S_6 with $i = 2$, we have $\boldsymbol{\omega}^2 = (135)(246)$ so $\tilde{S}_{i=2} = \{I, (135), (246), (135)(246)\}$. Consequently, $|\tilde{S}_i| = 2^g$. For $\sigma \in \tilde{S}_i$, write $\sharp\sigma$ for the number of disjoint cycles occuring in σ, and let b represent the period of σ, which in this case equals the length of any of its cycles, and $b = N_t/g$.

Theorem 4.1.1. *The distance between $\boldsymbol{V}_l$ and $\boldsymbol{V}_{l'}$ in the distinct coset (dc) case is*

$$d_{dc}(l, l') = |\sum_{\sigma \in \tilde{S}_i} (-1)^{\sharp\sigma} \lambda^{\sharp\sigma \cdot i \cdot b} \prod_{j=1}^{n_T} d_j^{\sigma}| \tag{4.7}$$

where we define d_j^σ to be equal to d_j if $\sigma(j) = j$ and d'_j if $\sigma(j) \neq j$.

Proof. It is well known that for any $n_T \times n_T$ matrix $\boldsymbol{A} = (a_{ij})$:

$$\det(\boldsymbol{A}) = \sum_{\sigma \in S_{n_T}} (-1)^{\mathrm{sgn}(\sigma)} \prod_{j=1}^{n_T} a_{j\sigma(j)} \tag{4.8}$$

where $\prod_{j=1}^{n_T} a_{j\sigma(j)} = a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n_T\sigma(n_T)}$. In the case under consideration, $\boldsymbol{A} = \boldsymbol{D} - \lambda^i \boldsymbol{\omega}^i \boldsymbol{D}'$ where $\boldsymbol{D}, \boldsymbol{D}'$ are diagonal matrices, λ is a scalar and $\boldsymbol{\omega}$ is the full permutation $(12 \cdots M)$. Then we can see that

$$\begin{aligned} a_{kj} \neq 0 \Leftrightarrow \text{ either } j &= k && \text{in which case } a_{kk} = d_k \\ \text{or } j &= \boldsymbol{\omega}^i(k) && \text{in which case } a_{k\boldsymbol{\omega}^i(k)} = (-1)\lambda^i d'_{\omega^i(k)}. \end{aligned}$$

Thus the only permutations $\sigma \in S_{n_T}$ for which all $a_{k\sigma(k)} \neq 0$ are those for which either $\sigma(k) = k$ or $\sigma(k) = \boldsymbol{\omega}^i(k)$ for all $k = 1, \ldots, M$; that is, for $\sigma \in \tilde{S}_i$. Then since each disjoint cycle of $\boldsymbol{\omega}^i$ (and thus of σ) has period b, we get $\mathrm{sgn}(\sigma) = \sharp\sigma(b-1)$. Also, for each σ, the total number of elements $a_{k\sigma(k)}$ for $\sigma(k) \neq k$ is $\sharp\sigma b$. Thus

$$\begin{aligned}
(-1)^{\mathrm{sgn}(\sigma)} \prod_{j=1}^{n_T} a_{j\sigma(j)} &= (-1)^{\sharp\sigma(b-1)}((-1)\lambda^i)^{\sharp\sigma b} \prod_{j=1}^{n_T} d_j^\sigma \\
&= (-1)^{\sharp\sigma(2b-1)} \lambda^{\sharp\sigma i b} \prod_{j=1}^{n_T} d_j^\sigma \\
&= (-1)^{\sharp\sigma} \lambda^{\sharp\sigma i b} \prod_{j=1}^{n_T} d_j^\sigma
\end{aligned}$$

as required. From we have

$$\prod_{\text{some } j} d_j \times \prod_{\text{other } j} d_j' = \prod_j d_j^\sigma$$

since we have just permuted the indices with σ. □

We note that the term corresponding to $\sigma = 1$ is simply $\det(\boldsymbol{D}) = 1$, and the one corresponding to $\sigma = \boldsymbol{\omega}^i$ is $(-1)^g \lambda^{gib} \det(\boldsymbol{D}') = (-1)^g \lambda^{in_T}$. We need to ensure that the distance $d_{dc}(l, l')$ of (4.7) is strictly nonzero. For simplicity, we impose the condition that each $\boldsymbol{D} = \mathrm{diag}(d_1, d_2, \ldots, d_{n_T})$ satisfies

$$d_r \cdot d_{r\oplus i} \cdot d_{r\oplus 2i} \cdots d_{r\oplus(b-1)i} = 1 \tag{4.9}$$

for each $1 \leq r \leq g$. Here $\oplus$ denotes an additional modulo n_T. This ensures that the term $\prod_{j=1}^{n_T} d_j^\sigma = 1$ for all $\sigma \in \tilde{S}_i$. Hence (4.7) simplifies to

$$d_{dc}(l, l') = |\sum_{\sigma \in \tilde{S}_i} (-1)^{\sharp\sigma} \lambda^{\sharp\sigma i b}|. \tag{4.10}$$

For each value of k, $0 \leq k \leq g$, there are $\binom{g}{k}$ elements $\sigma \in \tilde{S}_i$ with $\sharp\sigma = k$. Thus to evaluate this expression,we may sum over k, to yield

$$\begin{aligned} d_{dc}(l,l') &= \left|\sum_{k=0}^{g} \binom{g}{k} (-1)^k \lambda^{kib}\right| & (4.11)\\ &= |(-1)^g(\lambda^{ib}-1)^g| & (4.12)\\ &= |\lambda^{ib}-1|^g. & (4.13)\end{aligned}$$

Since $i < n_T$ and $b = n_T/g < n_T$, we have that $ib < n_T^2$. Hence $\lambda^{ib} \neq 1$ for any i, and thus $d_{dc}(l,l') \neq 0$.

Example 4.1.1. *Set the number of transmitter antennas $n_T = 9$ and $\lambda = e^{2\pi j/81}$. Consider $i = 3$: the permutation $\boldsymbol{\omega}^3 = (147)(258)(369) = \sigma_1\sigma_2\sigma_3$ with $g = gcd(3,9) = 3$ and $b = 9/3 = 3$. We choose a subgroup $\mathcal{D}$ to consist of diagonal matrices $\boldsymbol{D} = diag(d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9)$ which satisfy $d_1d_4d_7 = d_2d_5d_8 = d_3d_6d_9 = 1$ (following from (4.9)). Clearly $\det(\boldsymbol{D}) = 1$ and from (4.13) we have the distance between any 2 elements of the distinct cosets $\mathcal{D}$ and $\boldsymbol{\omega}^3\lambda^3\mathcal{D}$ is $d_{dc}(l,l') = |\lambda^9 - 1|^3 = 0.3201$.*

Theorem 4.1.2. *Suppose the number of transmitter antennas n_T is prime. Then the choice of $\lambda = e^{2\pi j/n_T^2}$ maximizes the minimum value of $d_{dc}(l,l')$, and $\mathcal{D}$ may be taken to be any full-diversity subgroup such that $\det \boldsymbol{D} = 1$ for all $\boldsymbol{D} \in \mathcal{D}$.*

Proof: When the number of transmitter antennas n_T is prime, we have $g = \gcd(i, n_T) = 1$ for all $i = 1, 2, \ldots, n_T - 1$, so $b = n_T$. Hence from (4.13), we have $d_{dc}(l,l') = |\lambda^{in_T} - 1|$. This value is equal to the Euclidean distance between two points on a unit circle. It follows that the chosen value of $\lambda = e^{2\pi j/n_T^2}$ maximizes the minimum value of $d_{dc}(l,l')$ in this case, by ensuring the n_T points λ^{in_T} are equally spaced along the unit circle. Moreover, since the permutation $\boldsymbol{\omega}^i$ is a single cycle for each i, the equation (4.9) simplifies to nothing more than the requirement that $\det \boldsymbol{D} = 1$. □

Summary of Design Criterion (DC) of Full Diversity Bruhat Constellation

We now summarize the design criterion of a full diversity unitary Bruhat constellation $\mathcal{V}$ for any n_T transmitter antennas as follows:

DC1) Set $\lambda = e^{2\pi j/n_T^2}$.

DC2) Choose $\mathcal{D}$ to be a unitary cyclic diagonal subgroup $\{\boldsymbol{D}_l\}_{l=0}^{L_D-1}$, such that

$$\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2, \ldots, d_{n_T}) = \mathrm{diag}(e^{j2\pi u_1 l/L_D}, e^{j2\pi u_2 l/L_D}, \ldots, e^{j2\pi u_{n_T} l/L_D}) \tag{4.14}$$

where the values of $\{u_i\}_{i=1}^{n_T} \in \{1, 2, \ldots, L_D - 1\}$ must be chosen so that (DC2a) $\boldsymbol{D}_l$ satisfies (4.9) for each $i = 1, 2, \ldots, n_T - 1$, and also (DC2b) so that the minimum value of the distance $d_{sc}(l, l') = |\det(\boldsymbol{D}_l - \boldsymbol{D}_{l'})|$ is maximized.

In practice, when determining the constraints on a subgroup $\mathcal{D}$ imposed by (DC2a), one only needs to consider a very few values of i, by the following proposition.

Proposition 4.1.1. *Let $\{p_1, p_2, \ldots, p_n\}$ be the set of distinct primes dividing n_T. Then a subgroup $\mathcal{D}$ will satisfy the conditions of equation (4.9) for every $i \in \{1, 2, \ldots, n_T - 1\}$ if and only if it satisfies those conditions for $i \in \{n_T/p_1, n_T/p_2, \ldots, n_T/p_n\}$.*

Proof: We first prove that it suffices to consider values i which divide n_T, as follows. Choose any i and set $g = \gcd(i, n_T)$, $b = n_T/g$. Note that g is also the number of cycles in ω^i. We claim that the set $\{i, 2i, \ldots, (b-1)i\}$, which certainly consists of multiples of g, modulo n_T, is in fact the set of ALL multiples of g, modulo n_T. For suppose it was not. Then for some $1 \leq k < l < b$, we would have $ki \equiv li \mod n_T$. Dividing through by g and using that i/g is relatively prime to $b = n_T/g$, we deduce that b divides $k - l$; impossible. Consequently, for each $k \in \{1, 2, \ldots, g\}$, the sets of indices

$$\{k, k \oplus g, k \oplus 2g, \ldots, k \oplus (b-1)g\} \tag{4.15}$$

and

$$\{k, k \oplus i, k \oplus 2i, \ldots, k \oplus (b-1)i\} \tag{4.16}$$

are identical. This shows that the conditions imposed by equation (4.9) for $\boldsymbol{\omega}^i$ are identical to those for $\boldsymbol{\omega}^g$. The set of all such elements g is the set of all divisors of n_T.

Next, we show that if i divides j and j divides n_T, then the conditions imposed by (4.9) corresponding to $\boldsymbol{\omega}^j$ force those corresponding to $\boldsymbol{\omega}^i$ to hold automatically. This would in turn imply that it suffices to choose the largest divisors in any such chain of divisors, which is the statement of the theorem. So write $j = ni$, with j dividing n_T. Then (4.9) implies for this power j that

$$d_k d_{k \oplus j} \cdots d_{k \oplus (\frac{n_T}{j} - 1)j} = 1 \tag{4.17}$$

for each $1 \leq k \leq j$. Now note that

$$\prod_{k\in\{l,l+i,l+2i,\ldots,l+(n-1)i\}} d_k d_{k\oplus j}\cdots d_{k\oplus(n_T/j-1)j} = d_l d_{l\oplus i}\cdots d_{l\oplus(n_T/i-1)i} \tag{4.18}$$

whence the conclusion follows. □

For (DC2b) note that in particular each u_i must be relatively prime to L_D. If not, then for some power, $0 < l < L_D$, we would have $d_i = 1$, which coincides with a diagonal element of $\boldsymbol{I}_{n_T}$. This, in turn, implies $d_{sc}(l, l') = 0$ (for $l' = 0$) so the constellation $\mathcal{D}$, and hence $\mathcal{V}$ fails to have full diversity.

Example 4.1.2. *When the number of transmitter antennas $n_T = 3$, we must choose*

$$\boldsymbol{D}_l = diag(d_1, d_2, d_1^{-1}d_2^{-2}) = diag(e^{j2\pi u_1 l/L_D}, e^{j2\pi u_2 l/L_D}, e^{-j2\pi(u_1+u_2)l/L_D}). \tag{4.19}$$

This will give a full diversity constellation only if u_1, u_2 and $u_1 + u_2$ are relatively prime to L_D. For example, we can choose L_D to be prime.

Subject to these constraints (DC2a) and (DC2b), one chooses the values of u_1 and u_2 by exhausive search to maximize the minimum value of $d_{sc}(l, l')$.

Theorem 4.1.3. *If n_T has an odd prime factor, then the Bruhat constellation $\mathcal{V}$ has full diversity only if L_D is odd.*

Proof: Recall that we use the symbol $\oplus$ for addition modulo n_T. Suppose p is an odd prime factor of n_T. Taking $i = n_T/p$ in (4.9) as in Proposition 4.1.1, we see that each element $\boldsymbol{D} = \text{diag}(d_1, d_2, \ldots, d_{n_T})$ of the subgroup $\mathcal{D}$ must satisfy

$$d_j d_{j\oplus i} d_{j\oplus 2i}\cdots d_{j\oplus(p-1)i} = 1 \tag{4.20}$$

for each $1 \leq j \leq i$. Writing each $d_k = e^{2\pi j u_k/L_D}$ for some integer u_k, we may rephrase equation (4.20) as the condition

$$u_j + u_{j\oplus i} + \cdots + u_{j\oplus(p-1)i} \equiv 0 \mod L_D \tag{4.21}$$

for all j. In order to achieve full diversity, each u_k must be relatively prime to L_D. However, if L_D is even, then the equation (4.21) is an odd number of terms adding up to an even number, implying that at least one of the terms is even, and consequently not relatively prime to L_D. □

A partial converse to Theorem 4.1.3, about the existence of full diversity Bruhat constellations, is the following.

Theorem 4.1.4. *Suppose n_T is power of a prime number p. If $p \neq 2$, assume that L_D is relatively prime to $n_T - 1$. Then there exists a full diversity Bruhat constellation of order $n_T L_D$.*

Proof: Write $n_T = p^n$ is the power of a prime number. Then Proposition 4.1.1 implies that the constraint imposed by (4.9) for all $i < n_T$ is satisfied if we take $i = n_T/p = p^{n-1}$. In terms of the parameters u_i, what we require is

$$u_j + u_{j+p^{n-1}} + \cdots + u_{j+(p-1)p^{n-1}} \equiv 0 \mod L_D \tag{4.22}$$

for each $j < p^{n-1}$, with each u_i relatively prime to L_D. This may be satisfied as follows.

If $p = 2$, take $u_j = 1$ and $u_{j+n_T/2} = L_D - 1$.

If $p > 2$, we may by hypothesis choose $K < L_D$, $K > 0$ such that $K \equiv -(p-1)$ mod L_D. Then take

$$u_j = u_{j+p^{n-1}} = \cdots = u_{j+(p-2)p^{n-1}} = 1, \; u_{j+(p-1)p^{n-1}} = K. \tag{4.23}$$

Since $(n_T - 1)$ and L_D are relatively prime, so are K and L_D; since $n_T - 1 = p^n - 1 = (p-1)(p^{n-1} + \cdots + p + 1)$. □

4.1.1 Properties of Bruhat constellation

The order and the rate of the Bruhat constellation $\mathcal{V}$ are $L_D n_T$ and $\log_2(L_D n_T)/2$ bit/s, respectively. The following theorem gives a closed formula for the value of its diversity product in terms of the value of the diversity product of the subgroup $\mathcal{D}$.

Theorem 4.1.5. *If $n_T \neq 4$, and p is the smallest prime divisor of n_T, then the diversity product of the Bruhat constellation is given by*

$$\zeta_{\mathcal{V}} = \min\left\{\zeta_{\mathcal{D}}, \frac{1}{2}\left(2\sin\frac{\pi}{n_T}\right)^{1/p}\right\}, \tag{4.24}$$

where $\zeta_{\mathcal{D}}$ denotes the diversity product of the constellation consisting only of the subgroup $\mathcal{D}$. When $n_T = 4$, one has instead the formula

$$\zeta_{\mathcal{V}} = \min\left\{\zeta_{\mathcal{D}}, 2^{-7/8}\right\}. \tag{4.25}$$

Proof: Recall that for each i we define $g = \gcd(i, n_T)$ and $b = n_T/g$. From Section 4.1, we know that the diversity product of our constellation is computed as

$$\begin{aligned}\zeta_{\mathcal{V}} &= \frac{1}{2}\min_{l,l'}(d_{sc}(l,l'), d_{dc}(l,l'))^{\frac{1}{n_T}} &(4.26)\\ &= \min_i\left(\zeta_{\mathcal{D}}, \frac{1}{2}|\lambda^{ib}-1|^{\frac{g}{n_T}}\right). &(4.27)\end{aligned}$$

From $\lambda = e^{j2\pi/n_T^2}$, one can simplify

$$\begin{aligned}\frac{1}{2}|\lambda^{ib}-1|^{\frac{g}{n_T}} &= \frac{1}{2}|1-e^{j2\pi ib/n_T^2}|^{\frac{g}{n_T}}\\ &= \frac{1}{2}\left|\left(2-2\cos\frac{2\pi ib}{n_T^2}\right)^{\frac{1}{2}}\right|^{\frac{g}{n_T}}, \text{ from } e^{j\theta} = \cos\theta + j\sin\theta\\ &= \frac{1}{2}\left|\left(4\sin^2\frac{\pi ib}{n_T^2}\right)^{\frac{1}{2}}\right|^{\frac{g}{n_T}}, \text{ from } \sin^2 x = \frac{1}{2}(1-\cos 2x)\\ &= \frac{1}{2}\left(2\sin\frac{\pi ib}{n_T^2}\right)^{\frac{g}{n_T}}.\end{aligned}$$

Now note that if k is the integer such that $i = kg$, then $ib = kn_T$. Consequently, for each fixed value of g dividing n_T, the term in parentheses achieves its minimum value when $k = 1$, and that minimum value is $2\sin\frac{\pi}{n_T}$, independent of g. Thus we have

$$\min_i \frac{1}{2}\left(2\sin\frac{\pi ib}{n_T^2}\right)^{\frac{g}{n_T}} = \min_g \frac{1}{2}\left(2\sin\frac{\pi}{n_T}\right)^{\frac{g}{n_T}} \tag{4.28}$$

where now we are taking the minimum over all g which divide n_T.

If $n_T \geq 6$, then $2\sin\frac{\pi}{n_T} \leq 1$, and so this minimum occurs for the largest value of g, that is, when $g = n_T/p$, with p the least prime dividing n_T. Since then $g/n_T = 1/p$, the theorem is proven in this case.

If $n_T \leq 5$, then $2\sin\frac{\pi}{n_T} > 1$, so the minimum occurs instead when $g = 1$. However, since 2, 3 and 5 are prime, the formula is unchanged; in the case of $n_T = 4$, one has

$$\frac{1}{2}\left(2\sin\frac{\pi}{n_T}\right)^{1/M} = \frac{1}{2}\left(2\frac{1}{\sqrt{2}}\right)^{1/4} = 2^{-7/8} \tag{4.29}$$

as required. □

The methods of the proof of this theorem lead us to the following corollary.

Corollary 4.1.1. *A lower bound on the value of $\zeta_{\mathcal{D}}$, when a full diversity subgroup subject to the constraints of (17) exists, is*

$$\zeta_{\mathcal{D}} \geq \sin\frac{\pi}{L_D} \tag{4.30}$$

Proof: The term $\zeta_{\mathcal{D}}$ may be computed explicitly in terms of the parameters u_i defining the diagonal elements of $D \in \mathcal{D}$ as

$$\begin{aligned}
\zeta_{\mathcal{D}} &= \frac{1}{2}\min_{l',l''} d_{sc}(l',l'')^{\frac{1}{n_T}} = \frac{1}{2}\min_{0\leq l'<l''\leq L_D-1} |\det(D_{l'}-D_{l''})|^{\frac{1}{n_T}}, \qquad D_{l'}, D_{l''} \in \mathcal{D} \\
&= \frac{1}{2}\min_{0\leq l'<l''\leq L_D-1} \{|\det D_{l'}||\det(I-D_{l'}^{-1}D_{l''})|\}^{\frac{1}{n_T}} \\
&= \frac{1}{2}\min_{1\leq l\leq L_D-1} |\det(I_M - D_l)|^{\frac{1}{n_T}}, \qquad \text{since } D_{l'}^{-1}D_{l''} = D_l \in \mathcal{D} \\
&= \frac{1}{2}\min_{1\leq l\leq L_D-1} |\det(\mathrm{diag}(1-e^{j2\pi u_1 l/L_D}, 1-e^{j2\pi u_2 l/L_D}, \ldots, 1-e^{j2\pi u_{n_T} l/L_D})|^{\frac{1}{n_T}} \\
&= \frac{1}{2}\min_{1\leq l\leq L_D-1} \left|\prod_{i=1}^{n_T} |(1-e^{j2\pi u_i l/L_D})|\right|^{\frac{1}{n_T}} \\
&= \min_{1\leq l\leq L_D-1} \left|\prod_{i=1}^{n_T} \sin\frac{\pi u_i l}{L_D}\right|^{\frac{1}{n_T}}, \text{ from the same argument as above.}
\end{aligned} \tag{4.31}$$

If $\mathcal{D}$ has full diversity, then $u_i l$ is never 0 modulo L_D for $l \in \{1, 2, \ldots, L_D - 1\}$. Thus each term of the product in (4.31) is at least $\sin(\pi/L_D)$. □

4.1.2 Examples of Bruhat Constellation

$n_T = 2$ Transmitter Antennas

From (4.3), the Bruhat constellation for two transmitter antennas is

$$\mathcal{V}_2 = \mathcal{D} \cup \lambda\omega\mathcal{D} \tag{4.32}$$

where $\lambda = e^{j2\pi/4}$ and

$$\omega = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{4.33}$$

Using (4.13), we have $d_{dc}(l,l') = |\lambda^2 - 1| = |-1-1| = 2 > 0$. The elements $\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2) \in \mathcal{D}$ must satisfy $d_2 = d_1^{-1}$ by (4.9). Write $d_1 = e^{2\pi j u_1/L_D}$ then this constellation is

$$\begin{aligned} \mathcal{V}_2 &= \mathcal{D} \cup e^{j\frac{2\pi}{4}} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \mathcal{D} && (4.34) \\ &= \left\{ \begin{bmatrix} e^{j\frac{2\pi u_1 l}{L_D}} & 0 \\ 0 & e^{-j\frac{2\pi u_1 l}{L_D}} \end{bmatrix}_{l=0}^{L_D-1} \right\} \cup j \left\{ \begin{bmatrix} 0 & e^{-j\frac{2\pi u_1 l}{L_D}} \\ e^{j\frac{2\pi u_1 l}{L_D}} & 0 \end{bmatrix}_{l=0}^{L_D-1} \right\} && (4.35) \end{aligned}$$

where the value of $u_1 = \{1, 2, \ldots, L_D - 1\}$ is chosen to maximize $d_{sc}(l,l')$ for a given L_D. The order of this constellation is $2L_D$. (We note that our constellation in (4.35) is equivalent to the optimal dicyclic group constellation [37] for $n_T = 2$.)

$n_T = 3$ Transmitter Antennas

Our Bruhat constellation for three transmitter antennas is

$$\mathcal{V}_3 = \mathcal{D} \cup \lambda\omega\mathcal{D} \cup \lambda^2\omega^2\mathcal{D} \tag{4.36}$$

with $\lambda = e^{j2\pi/9}$ and

$$\omega = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}. \tag{4.37}$$

Using (4.13) with $g = 1$ and $b = 3$, the distance $d_{dc}(l,l')$ may be computed as:

for $i = 1$, $\boldsymbol{\omega} = (123)$, we have $d_{dc} = |\lambda^3 - 1| = 1.7321 > 0$; for $i = 2$, $\boldsymbol{\omega}^2 = (132)$, we have $d_{dc} = |\lambda^6 - 1| = 1.7321 > 0$. Each $\boldsymbol{D}_l \in \mathcal{D}$ must have $\det(\boldsymbol{D}_l) = 1$; so set $\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2, d_1^{-1}d_2^{-1})$. To obtain a cyclic subgroup, set each $d_i = e^{j2\pi u_i l/L_D}$, $i = 1, 2$ for some parameters $u_i \in \{1, 2, ..L_D - 1\}$ which are chosen to maximize the value of $d_{sc}(l, l')$ for a given L_D. Consequently, the constellation of order $3L_D$ is

$$\mathcal{V}_3 = \mathcal{D} \cup \begin{bmatrix} 0 & e^{j2\pi/9} & 0 \\ 0 & 0 & e^{j2\pi/9} \\ e^{j2\pi/9} & 0 & 0 \end{bmatrix} \mathcal{D} \cup \begin{bmatrix} 0 & 0 & e^{j4\pi/9} \\ e^{j4\pi/9} & 0 & 0 \\ 0 & e^{j4\pi/9} & 0 \end{bmatrix} \mathcal{D}. \tag{4.38}$$

$n_T = 4$ **Transmitter Antennas**

For four transmitter antennas, our proposed Bruhat constellation of order $4L_D$ is

$$\mathcal{V}_4 = \mathcal{D} \cup \lambda\boldsymbol{\omega}\mathcal{D} \cup \lambda^2\boldsymbol{\omega}^2\mathcal{D} \cup \lambda^3\boldsymbol{\omega}^3\mathcal{D}. \tag{4.39}$$

where $\lambda = e^{j2\pi/16}$ and

$$\boldsymbol{\omega} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \tag{4.40}$$

For $i = 1$, $\boldsymbol{\omega} = (1234)$, we have $d_{dc} = |\lambda^4 - 1|$ whenever $\det(\boldsymbol{D}_l) = 1$. For $i = 2$, $\boldsymbol{\omega}^2 = (13)(24)$, $g = \gcd(2, 4) = 2$, $b = 4/2 = 2$; from (4.13), we can have $d_{dc} = |\lambda^4 - 1|^2$ by setting $d_1 d_3 = d_2 d_4 = 1$. For $i = 3$, $\boldsymbol{\omega}^3 = (1432)$, we have $d_{dc} = |\lambda^{12} - 1|$. Thus the unitary diagonal matrices $\boldsymbol{D}_l$ can be chosen by

$$\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2, d_1^{-1}, d_2^{-1}) = \mathrm{diag}(e^{j2\pi u_1 l/L_D}, e^{j2\pi u_2 l/L_D}, e^{-j2\pi u_1 l/L_D}, e^{-j2\pi u_2 l/L_D}). \tag{4.41}$$

The values of $u_1, u_2 = \{1, 2, \ldots, L_D - 1\}$ are chosen to maximize $d_{sc}(l, l')$ for each given L_D.

Proposition 4.1.2. *Our proposed Bruhat constellations are superior to the optimal dicyclic group constellations [37] for large L and $n_T = 4$.*

Proof: We prove that the minimum value of $d(l, l')$ of our Bruhat constellation is higher than for constellation obtained from a dicyclic group when $n_T = 4$. The optimal dicyclic group constellation [37] of order $L_D M$ and n_T even is defined as

$$\mathcal{G}_d = \{\boldsymbol{G}_0^l \boldsymbol{G}_1^m : \ 0 \leq l < L_D n_T/2; \ m = 0, 1\} \tag{4.42}$$

where $\boldsymbol{G}_0 = \mathrm{diag}(g_1, g_2, \ldots, g_{n_T}) = \mathrm{diag}(e^{4\pi j v_1/L_D n_T}, e^{4\pi j v_2/L_D n_T}, \ldots, e^{4\pi j v_{n_T}/L_D n_T})$ and

$$\boldsymbol{G}_1 = \begin{bmatrix} 0 & -\boldsymbol{I}_{n_T/2} \\ \boldsymbol{I}_{n_T/2} & 0 \end{bmatrix}.$$

We can see that the structure of an optimal dicyclic group constellation is also generated from the Bruhat decomposition of a unitary diagonal subgroup $\boldsymbol{G}_0$ of order $L_D n_T/2$ with 2 distinct nonoverlapping cosets, $\boldsymbol{I}_{n_T}$ and $\boldsymbol{G}_1$ respectively. To achieve a full diversity dicyclic group constellation in (5.10), the elements of $\boldsymbol{G}_0$ must satisfy equations analogous of (4.9), with $i = n_T/2$.

When $n_T = 4$, these conditions on $\boldsymbol{G}_0$ coincide exactly with all the conditions (4.9) imposed upon the subgroup $\mathcal{D}$ of the proposed constellation. For both constellations, the distance between distinct cosets, d_{dc} is a constant, whereas the distance in the same coset d_{sc} varies inversely with L. Hence, when L is sufficiently large, the diversity product of each constellation depends only on $d_{sc}(l, l')$, and may be compared directly, as follows. For the optimal dicyclic group constellation, the distance within the subgroup $\boldsymbol{G}_0$ is given by

$$d_{sc}^{\boldsymbol{G}_0} = \min_{l=1,2,\ldots,L_D n_T/2-1} \left| \prod_{i=1}^{n_T} 2 \sin \frac{\pi v_i l}{L_D n_T/2} \right|. \tag{4.43}$$

The d_{sc} of proposed Bruhat constellation is

$$d_{sc} = \min_{l=1,2,\ldots,L_D-1} \left| \prod_{i=1}^{n_T} 2 \sin \frac{\pi u_i l}{L_D} \right|. \tag{4.44}$$

Since $L_D < L_D n_T/2$, the d_{sc} of Bruhat constellation is larger than the $d_{sc}^{\boldsymbol{G}_0}$. □

$n_T = 5$ Transmitter Antennas

A Bruhat constellation for five transmitter antennas is

$$\mathcal{V}_5 = \mathcal{D} \cup \lambda\boldsymbol{\omega}\mathcal{D} \cup \lambda^2\boldsymbol{\omega}^2\mathcal{D} \cup \lambda^3\boldsymbol{\omega}^3\mathcal{D} \cup \lambda^4\boldsymbol{\omega}^4\mathcal{D} \tag{4.45}$$

where $\lambda = e^{j2\pi/25}$. For this case, we have $g = \gcd(i, 5) = 1$ for all $i = 1, 2, 3, 4$. The choice of a subgroup of unitary diagonal matrices $\mathcal{D} = \{\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2, d_3, d_4, d_5 | d_1 d_2 d_3 d_4 d_5 = 1\}$ can be made by

$$\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2, d_3, d_4, d_1^{-1} d_2^{-1} d_3^{-1} d_4^{-1}) \tag{4.46}$$

where $d_i = e^{j2\pi u_i l / L_D}$, $i = 1, 2, 3, 4$. The values of $u_i = \{1, 2, \ldots, L_D - 1\}$ are chosen to maximize $d_{sc}(l, l')$ for a given L_D. The order of this constellation is $5L_D$.

$n_T = 6$ **Transmitter Antennas**

For six transmitter antennas, our proposed constellation is

$$\mathcal{V}_6 = \mathcal{D} \cup \lambda \boldsymbol{\omega} \mathcal{D} \cup \lambda^2 \boldsymbol{\omega}^2 \mathcal{D} \cup \lambda^3 \boldsymbol{\omega}^3 \mathcal{D} \cup \lambda^4 \boldsymbol{\omega}^4 \mathcal{D} \cup \lambda^5 \boldsymbol{\omega}^5 \mathcal{D} \tag{4.47}$$

where $\lambda = e^{j2\pi/36}$. For $i = 1$ and 5, $g = \gcd(i, 6) = 1$, the condition of (4.9) on the unitary diagonal matrix $\boldsymbol{D}_l$ is simply $d_1 d_2 d_3 d_4 d_5 d_6 = 1$. For $i = 2, 3, 4$, the conditions on $\boldsymbol{D}_l$ are listed below:

i	d_{dc}	Constraint on $\boldsymbol{D}_l$
2	$\lvert\lambda^6 - 1\rvert^2$	$d_1 d_3 d_5 = d_2 d_4 d_6 = 1$
3	$\lvert\lambda^6 - 1\rvert^3$	$d_1 d_4 = d_2 d_5 = d_3 d_6 = 1$
4	$\lvert\lambda^{12} - 1\rvert^2$	$d_1 d_3 d_5 = d_2 d_4 d_6 = 1$

Consequently we may choose a subgroup $\mathcal{D} = \{\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2, d_3, d_4, d_5, d_6)\}$ by

$$\boldsymbol{D}_l = \mathrm{diag}(d_1, d_2, d_1^{-1} d_2, d_1^{-1}, d_2^{-1}, d_1 d_2^{-1}) \tag{4.48}$$

where $d_1 = e^{j2\pi u_1 l / L_D}$ and $d_2 = e^{j2\pi u_2 l / L_D}$. The values of u_1 and u_2 are chosen to maximize $d_{sc}(l, l')$ for a given L_D. Here $6L_D$ is the order of this constellation.

4.2 Hamiltonian Bruhat Constellations

We improve the diversity product of a Bruhat constellation $\mathcal{V}$ in (4.3) for a case where the number of transmitter antennas is even by replacing the unitary cyclic diagonal subgroup $\mathcal{D}$ by a finite set of $n_T \times n_T$ block diagonal matrices, consisting of the direct sum of $n_T/2$ particularly suitable matrices of $SU(2)$: a *Hamiltonian constellation* $\mathcal{H} = \{H_l\}_{l=0}^{L_H-1}$ of order L_H as proposed in [57].

4.2.1 Hamiltonian Constellation

Let n_T be even. An $n_T \times n_T$ Hamiltonian space-time constellation can be constructed as the direct sum of 2×2 Hamiltonian matrices, $\mathcal{H}_{n_T \times n_T} = \{\boldsymbol{J}_l\}_{l=0}^{L_H-1}$. Each $\boldsymbol{J}_l$ has the block diagonal form

$$\boldsymbol{J}_l = \mathrm{diag}(\boldsymbol{H}_l^{k_1,k_2}, \boldsymbol{H}_l^{k_3,k_4}, \ldots, \boldsymbol{H}_l^{k_{n_T-1},k_{n_T}}) \tag{4.49}$$

where $\boldsymbol{H}_l^{k_m,k_n}$ is defined as

$$\boldsymbol{H}_l^{k_m,k_n} = \begin{bmatrix} \sqrt{x_1}e^{-j\frac{2\pi}{L_H}lk_m} & -\sqrt{x_2}e^{j\frac{2\pi}{L_H}lk_n} \\ \sqrt{x_2}e^{-j\frac{2\pi}{L_H}lk_n} & \sqrt{x_1}e^{j\frac{2\pi}{L_H}lk_m} \end{bmatrix} \tag{4.50}$$

where $x_1 + x_2 = 1$ and $x_1, x_2 > 0$.

Note we can write $\boldsymbol{H}_l^{k_m,k_n}$ in terms of $\boldsymbol{H}_{l=0}^{k_m,k_n} = \boldsymbol{H}_0$ as

$$\boldsymbol{H}_l^{k_m,k_n} = e^{j\frac{2\pi lk_m}{L_H}} \boldsymbol{R}_l^{k_m,k_n} \boldsymbol{H}_0 \boldsymbol{T}_l^{k_m,k_n} \tag{4.51}$$

where

$$\boldsymbol{R}_l^{k_m,k_n} = \begin{bmatrix} e^{-j\frac{2\pi}{L_H}lk_m} & 0 \\ 0 & e^{-j\frac{2\pi}{L_H}lk_n} \end{bmatrix}, \quad \boldsymbol{H}_0 = \begin{bmatrix} \sqrt{x_1} & -\sqrt{x_2} \\ \sqrt{x_2} & \sqrt{x_1} \end{bmatrix}$$

$$\text{and } \boldsymbol{T}_l^{k_m,k_n} = \begin{bmatrix} e^{-j\frac{2\pi}{L_H}lk_m} & 0 \\ 0 & e^{j\frac{2\pi}{L_H}lk_n} \end{bmatrix}.$$

4.2.2 Construction of Hamiltonian Bruhat Constellation

The idea of constructing the new proposed Hamiltonian Bruhat constellation $\mathcal{B}$ is to replace the nonzero elements in the matrices $\boldsymbol{\omega}^i$ and $\mathcal{D}$ of (4.3) by 2×2 matrices, that is, an identity matrix $\boldsymbol{I}_2$ and $\boldsymbol{H}_l^{m,n}$respectively. For example, we replace

$$\boldsymbol{\omega} = (12) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0 & \boldsymbol{I}_2 \\ \boldsymbol{I}_2 & 0 \end{bmatrix} = \boldsymbol{\rho} \tag{4.52}$$

$$\boldsymbol{D}_l = \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \leftrightarrow \begin{bmatrix} \boldsymbol{H}_l^{k_1,k_2} & 0 \\ 0 & \boldsymbol{H}_l^{k_3,k_4} \end{bmatrix} = \boldsymbol{J}_l. \tag{4.53}$$

Consequently the new proposed constellation is applicable when the number of transmitter antennas n_T is even and greater than 2. More specifically, define the matrices $\boldsymbol{J}_l$ as the direct sum (as in (4.53)) of $n_T/2$ copies of $H_l^{k_m,k_n}$ (with k_m and k_n varying). Setting $\mathcal{J} = \{\boldsymbol{J}_l\}_{l=0}^{L_H-1}$, we define our *Hamiltonian Bruhat constellation* (for n_T even and $n_T \geq 4$) by

$$\mathcal{B} = \bigcup_{i=0}^{n_T/2-1} \gamma^i \boldsymbol{\rho}^i \mathcal{J} \tag{4.54}$$

where we choose $\gamma = e^{2\pi j/(n_T/2)^2}$ and $\boldsymbol{\rho}$ is the $n_T \times n_T$ permutation matrix obtained from $\boldsymbol{\omega} = (12\cdots(M/2))$ by replacing each entry with a 2×2 identity matrix as in (4.52). The order of Hamiltonian Bruhat constellation is $L = L_H n_T/2$. The values of x_1 and $\{k_i\}_{i=1}^{n_T}$ are chosen to maximize the diversity product

$$\zeta_{\mathcal{B}} = \min_{\boldsymbol{B}_l, \boldsymbol{B}_{l'} \in \mathcal{B}} |\det(\boldsymbol{B}_l - \boldsymbol{B}_{l'})|^{\frac{1}{n_T}}. \tag{4.55}$$

Since a Hamiltonian Bruhat constellation $\mathcal{B}$ does not form a group, the optimization of the diversity product in (4.55) would in general require checking $L(L-1)$ pairs of matrices $\boldsymbol{B}_l, \boldsymbol{B}_{l'} \in \mathcal{B}$. The following lemma gives a condition on $\{k_i\}_{i=1}^{n_T}$ which reduces the number of comparisons required to optimize (4.55) to $L-1$ pairs – comparable with a group constellation.

Lemma 4.2.1. *Choose $\{k_i\}_{i=1}^{n_T}$ so that*

$$(k_1 - k_2) = (k_3 - k_4) = \cdots = (k_{n_T-1} - k_{n_T}). \tag{4.56}$$

Then

$$\zeta_{\mathcal{B}} = \min_{\boldsymbol{B}_l \in \mathcal{B}, \boldsymbol{B}_l \neq \boldsymbol{B}_0} |\det(\boldsymbol{B}_0 - \boldsymbol{B}_l)|^{1/n_T} \tag{4.57}$$

where $\boldsymbol{B}_0 = \boldsymbol{J}_0$ is a direct sum of $n_T/2$ copies of $\boldsymbol{H}_0$.

Proof: We prove that to compute the diversity product in (4.55) it suffices to fix $\boldsymbol{B}_l = \boldsymbol{B}_0$ and let $\boldsymbol{B}_{l'}$ range over all other matrices in the constellation. The proof uses the property given in (4.51), and is shown only for the case of $n_T = 4$. The case of general n_T follows immediately.

Define

$$\boldsymbol{M}(l, k_i, k_j) = \mathrm{diag}(1, e^{j\frac{2\pi l}{L_H}k_i}, 1, e^{j\frac{2\pi l}{L_H}k_j}).$$

Then we have $|\det(\boldsymbol{B}_l - \boldsymbol{B}_{l'})| =$

$$\begin{aligned}
&= |\det(\gamma^i \boldsymbol{\rho}^i \boldsymbol{J}_l - \gamma^j \boldsymbol{\rho}^j \boldsymbol{J}_{l'})| \\
&= |\det(\boldsymbol{J}_l - \gamma^k \boldsymbol{\rho}^k \boldsymbol{J}_{l'})|, \qquad \text{where } k = j - i \\
&= \left|\det\left(\boldsymbol{M}(l, k_1 - k_2, k_3 - k_4)\boldsymbol{J}_0\boldsymbol{T}_l - \gamma^k \boldsymbol{\rho}^k \boldsymbol{M}(l', k_1 - k_2, k_3 - k_4)\boldsymbol{J}_0\boldsymbol{T}_{l'}\right)\right| \\
&= \left|\det\left(\boldsymbol{J}_0 - \gamma^k \boldsymbol{M}(-l, k_1 - k_2, k_3 - k_4)\boldsymbol{\rho}^k \boldsymbol{M}(l', k_1 - k_2, k_3 - k_4)\boldsymbol{J}_0\boldsymbol{T}_{l'-l}\right)\right| \\
&= \left|\det\left(\boldsymbol{J}_0 - \gamma^k \boldsymbol{\rho}^k \boldsymbol{M}(-l, k_3 - k_4, k_1 - k_2)\boldsymbol{M}(l', k_1 - k_2, k_3 - k_4)\boldsymbol{J}_0\boldsymbol{T}_{l'-l}\right)\right| \\
&= \left|\det\left(\boldsymbol{J}_0 - \gamma^k \boldsymbol{\rho}^k \boldsymbol{M}(l' - l, k_1 - k_2, k_3 - k_4)\boldsymbol{J}_0\boldsymbol{T}_{l'-l}\right)\right|, \text{ assuming } k_1 - k_2 = k_3 - k_4 \\
&= |\det(\boldsymbol{J}_0 - \gamma^k \boldsymbol{\rho}^k \boldsymbol{J}_{l'-l})|
\end{aligned}$$

□

We give examples of constructing Hamiltonian Bruhat constellations for $n_T = 4$ and 6 as follows:

$n_T = 4$ Transmitter Antennas

For $n_T = 4$ transmitter antennas, we have

$$\mathcal{J} = \mathcal{H}_1 \oplus \mathcal{H}_2 = \left\{ \begin{bmatrix} \boldsymbol{H}_l^{k_1,k_2} & \\ & \boldsymbol{H}_l^{k_3,k_4} \end{bmatrix}_{l=0}^{L_H-1} \right\}. \tag{4.58}$$

Then the representation $\boldsymbol{\rho}$ of order $4/2 = 2$ is

$$\boldsymbol{\rho} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \tag{4.59}$$

Therefore this constellation of order $2L_H$ has a form as

$$\mathcal{B}_4 = \left\{ \begin{bmatrix} \boldsymbol{H}_l^{k_1,k_2} & \\ & \boldsymbol{H}_l^{k_3,k_4} \end{bmatrix}_{l=0}^{L_H-1} \right\} \cup e^{2\pi j/4} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \left\{ \begin{bmatrix} \boldsymbol{H}_l^{k_1,k_2} & \\ & \boldsymbol{H}_l^{k_3,k_4} \end{bmatrix}_{l=0}^{L_H-1} \right\}. \tag{4.60}$$

The values of x_1 and $\boldsymbol{k} = (k_1, k_2, k_3, k_4) \in \{1, 2, \ldots, L_H - 1\}$ satisfying Lemma 4.2.1 are chosen to maximize the diversity product.

$n_T = 6$ Transmitter Antennas

For $n_T = 6$ transmitter antennas, we have

$$\mathcal{J} = \mathcal{H}_1 \oplus \mathcal{H}_2 \oplus \mathcal{H}_3 = \left\{ \begin{bmatrix} \boldsymbol{H}_l^{k_1,k_2} & & \\ & \boldsymbol{H}_l^{k_3,k_4} & \\ & & \boldsymbol{H}_l^{k_5,k_6} \end{bmatrix}_{l=0}^{L_H-1} \right\}. \tag{4.61}$$

The representation $\boldsymbol{\rho}$ which has the order $6/2 = 3$ is

$$\boldsymbol{\rho} = \begin{bmatrix} 0 & \boldsymbol{I}_2 & 0 \\ 0 & 0 & \boldsymbol{I}_2 \\ \boldsymbol{I}_2 & 0 & 0 \end{bmatrix} \text{ and } \boldsymbol{\rho}^2 = \begin{bmatrix} 0 & 0 & \boldsymbol{I}_2 \\ \boldsymbol{I}_2 & 0 & 0 \\ 0 & \boldsymbol{I}_2 & 0 \end{bmatrix}. \tag{4.62}$$

The Hamiltonian Bruhat constellation of order $3L_H$ is

$$\mathcal{B}_6 = \mathcal{J} \cup \lambda\boldsymbol{\rho}\mathcal{J} \cup \lambda^2\boldsymbol{\rho}^2\mathcal{J} \tag{4.63}$$

where $\lambda = e^{2\pi j/9}$. The values of x_1 and $\boldsymbol{k} = (k_1, k_2, k_3, k_4, k_5, k_6) \in \{1, 2, \ldots, L_H - 1\}$ satisfying Lemma 4.2.1 are chosen to maximize the diversity product.

4.3 Results and Performance

Results

Table 4.1 shows some of the proposed constellations $\mathcal{V}$ and $\mathcal{B}$ with their best diversity products compared with different full diversity USTC designs from the literature. We can see that our proposed constellations have diversity products higher than constellations obtained from cyclic groups. Many of the proposed constellations have excellent diversity products; for example, for $n_T = 4$ the Hamiltonian Bruhat constellation $\mathcal{B}$ has $\zeta_{\mathcal{B}} = 0.5151$ which is higher than Konishi's constellation $\tilde{G}_4$ [47] at the same $R = 1.50$ bits/s. Also for $n_T = 6$ the Hamiltonian Bruhat constellation $\mathcal{B}$ at $R \approx 1.09$ bits/s has good diversity product $\zeta_{\mathcal{B}} = 0.5120$.

Our proposed Bruhat space-time constellation design has a simple structure for a case where the number of transmitter antennas is prime. Although our Bruhat constellation is not a group, we show that it is extremely symmetric in that the minimum value of $d(l, l')$ can be determined by checking only $L - 1$ distinct elements in $\mathcal{V}$ which is comparable to a group constellation. Furthermore, the optimization of the diversity product is not computationally intensive when the number of transmitters is a composite number, for example, when $n_T = 6$, since there are only two parameter values (u_1 and u_2) for searching, see (4.48).

Performance

The performance is considered by plotting the BLER against SNR in unknown Rayleigh flat fading channels, using DUSTM explained in Section 2.1. The fading coefficients and additive noise are independent $\mathcal{CN}(0, 1)$, and the channel matrix is assumed to be constant within two consecutive time periods. The ML decoder is used for decoding.

Figure 4.1 displays the BLER performance of our 3×3 Bruhat constellation $\mathcal{V}$ with $u_1 = 1, u_2 = 4$ at $R = 2.04$ bits/s compared with the cyclic group $u = (1, 11, 27)$ at $R = 2.00$ bits/s as given in Table 4.1 with the number of receiver antenna, $n_R = 1$. We can see that the proposed constellation outperforms the cyclic group. The gain improvement is ≈ 2 dB.

Figure 4.2 shows the BLER performance of a 4×4 proposed Bruhat constellation $\mathcal{V}$ (with $u_1 = 1$, $u_2 = 7$) and a Hamiltonian Bruhat constellation $\mathcal{B}$ (with $k = (1, 27, 21, 13)$) compared with the Konishi unitary constellation [47] as given in

n_T	L	R	$\zeta_{\mathcal{V}}$	Unitary space-time designs
3	9	1.06	0.6004	fixed-point free group $G_{9,1}$ [80]
3	9	1.06	0.6004	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 1$
3	57	1.94	0.4845	nongroup $\mathcal{S}_{19,3}, u = (1, 7, 11)$ [80]
3	57	1.94	0.4845	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 7$
3	63	1.99	0.3301	cyclic group $u = (1, 17, 26)$ [36]
3	63	1.99	0.3851	fixed-point free group $G_{21,4}$ [80]
3	63	1.99	0.3851	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 4$
3	64	2.00	0.2765	cyclic group $u = (1, 11, 27)$ [36]
3	69	2.04	0.3548	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 4$
3	513	3.00	0.1353	fixed-point free group $G_{171,64}$ [80]
3	513	3.00	0.1436	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 22$
3	4095	4.00	0.0361	fixed-point free group $G_{1365,16}$ [80]
3	4095	4.00	0.0471	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 121$
4	16	1.00	0.5453	cyclic group $u = (1, 3, 5, 7)$ [36]
4	16	1.00	0.6124	Hamiltonian Bruhat $\mathcal{B}$ $x_1 = 0.3232$, $k = (1, 5, 7, 3)$
4	64	1.50	0.3418	Konishi $\tilde{G}_4$ [47]
4	64	1.50	0.3827	Bruhat $\mathcal{V}$ $u = (1, 7)$
4	64	1.50	0.5151	Hamiltonian Bruhat $\mathcal{B}$ $x_1 = 0.4728$, $k = (1, 27, 21, 13)$
4	256	2.00	0.2208	cyclic group $u = (1, 25, 97, 107)$ [36]
4	256	2.00	0.3445	Hamiltonian Bruhat $\mathcal{B}$ $x_1 = 0.3606$, $k = (1, 89, 55, 143)$
5	32	1.00	0.4095	cyclic group $u = (1, 5, 7, 9, 11)$ [36]
5	33	1.01	0.5580	nongroup $\mathcal{S}_{11,3}$ $u = (1, 3, 4, 5, 9)$ [80]
5	35	1.03	0.5164	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 1, u_3 = 4, u_4 = 5$
6	64	1.00	0.3792	cyclic group $u = (1, 7, 15, 23, 25, 31)$ [36]
6	66	1.01	0.4865	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 3$
6	66	1.09	0.5120	Hamiltonian Bruhat $\mathcal{B}$ $x_1 = 0.4873$, $k = (1, 14, 11, 24, 6, 19)$
6	72	1.03	0.5000	nongroup $\mathcal{S}_{12,6}$ $u = (1, 1, 7, 7, 7, 1)$ [80]
6	72	1.03	0.5000	Hamiltonian Bruhat $\mathcal{B}$ $x = 0.5000$ $k = (1, 12, 8, 19, 4, 15)$
6	78	1.05	0.5000	Bruhat $\mathcal{V}$ $u_1 = 1, u_2 = 10$

Table 4.1: Comparison of different USTC designs. Our proposed designs are highlighted in grey.

Table 4.1 at the same rate $R = 1.50$ bits/s with $n_R = 1$ receiver antenna.

Figure 4.3 shows the BLER of our 5×5 Bruhat constellation $\mathcal{V}$ with $u_1 = 1, u_2 = 1, u_3 = 2$ at $R = 1.03$ bits/s compared with the cyclic group $u = (1, 5, 7, 9, 11)$ at $R = 1.00$ bits/s and the nongroup $\mathcal{S}_{11,3}$ at $R = 1.01$ bits/s as given in Table 4.1 with the number of receiver antenna, $n_R = 1$. We can see that our Bruhat constellation

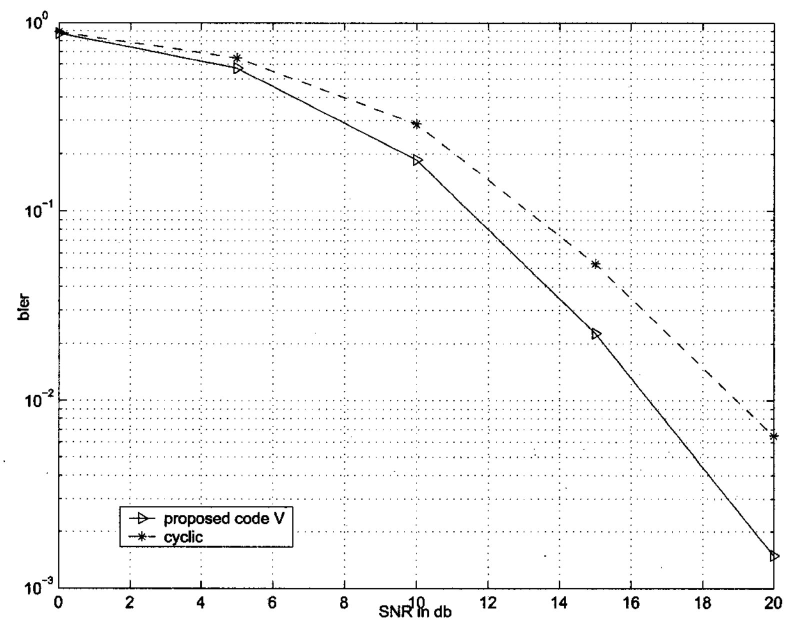

Figure 4.1: BLER performance for $n_T = 3, n_R = 1$ at $R \approx 2.00$ bits/s of a Bruhat constellation $\mathcal{V}$ and a cyclic group constellation

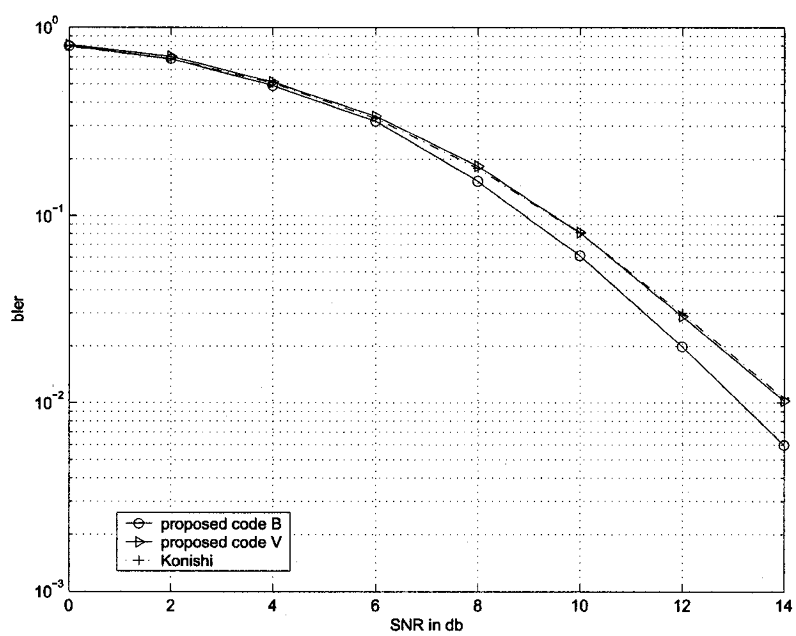

Figure 4.2: BLER performance for $n_T = 4, n_R = 1$ at $R = 1.50$ bits/s of our proposed constellation $\mathcal{B}$ and $\mathcal{V}$, and Konishi constellation

outperforms the cyclic group and compares well with the nongroup constellation.

Figure 4.4 displays the BLER performance of our 6×6 proposed constellation $\mathcal{V}$ with

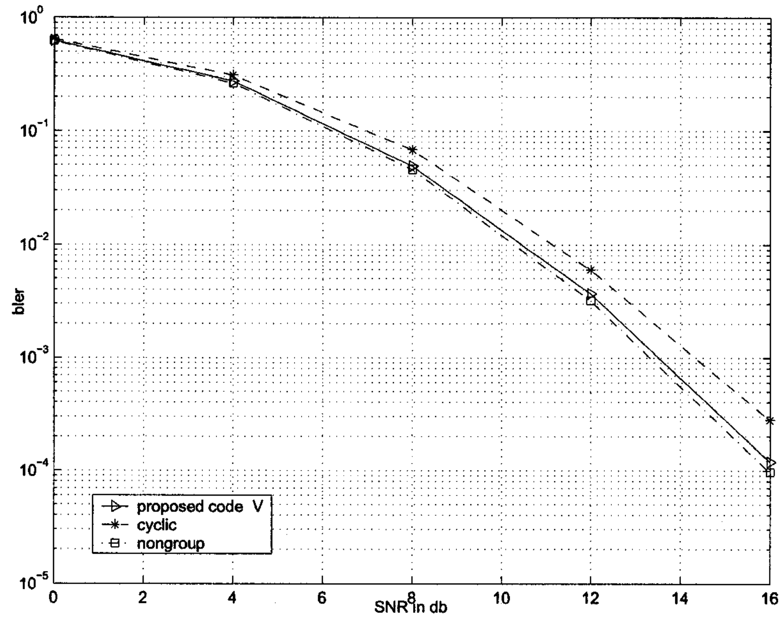

Figure 4.3: BLER performance for $n_T = 5, n_R = 1$ at $R \approx 1.00$ bit/s of our Bruhat constellation $\mathcal{V}$, cyclic group and nongroup

$u_1 = 1, u_2 = 3$ at $R = 1.01$ bits/s and $\mathcal{B}$ at $R = 1.09$ bits/s with $k = (1, 14, 11, 24, 6, 19)$ compared with the cyclic group $u = (1, 7, 15, 23, 25, 31)$ at $R = 1.00$ bits/s as given in Table 4.1 with the number of receiver antenna, $N = 1$. We can see that our proposed constellations $\mathcal{V}$ and $\mathcal{B}$ again outperform the cyclic group with ≈ 1 and ≈ 1.8 dB gain improvement respectively.

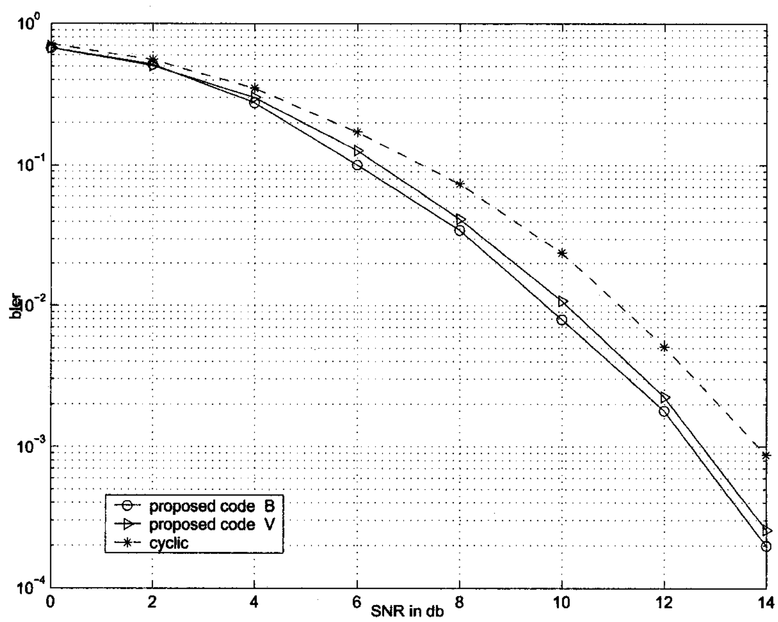

Figure 4.4: BLER performance for $n_T = 6, n_R = 1$ at $R \approx 1.00$ bit/s of our proposed constellation $\mathcal{B}$ and $\mathcal{V}$, and cyclic group

Chapter 5

Calculating the Diversity Sum From a Character Table

The finite simple unitary groups having full diversity (nonzero diversity product) are called *fixed-point free groups*, and have been classified in [80]. Fixed-point free group constellations with the best known diversity products were found by a computer search in [80]. Recently, Shokrollahi [79] has proposed a method to compute the diversity product of a unitary group constellation, using a characteristic polynomial which is derived from the *character table*[1] of the group.

In this chapter, we propose a method to compute the diversity sum of a unitary group constellation using a character table. The *diversity sum*, defined in (2.19), is calculated from the norm of the difference of two distinct elements in a signal constellation. It is the significant parameter to predict a USTC having a good performance in low SNR. We give some examples of using our method for different unitary groups: cyclic groups, dicyclic groups and the finite special linear groups. We also introduce the notion of a *faithful group constellation*, that is, one whose diversity sum is greater than 0. Faithful group constellations may be obtained from any nontrivial character of a group. We present in this chapter as an example the finite projective special linear group PSL_2.

We will call the unitary space-time group constellations having $\xi_{\mathcal{V}} > 0$, *faithful group constellations*, following the notion of faithful representations (as explained in Appendix A.2). Furthermore, we demonstrate with an example (the *special linear group*

[1]A review of group representations and character tables is summarized in Appendix A.2.

$SL_2(\mathbb{F}_q)$) how a constellation which is not faithful for a given group can be made into a faithful constellation for a quotient group (in this case, the *projective special linear group* $PSL_2(\mathbb{F}_q)$). We then show that non full diversity group constellations with high diversity sum outperform full diversity group constellations with low diversity sum in a specific range of low SNR.

5.1 Computing a Diversity Sum From Character Table

Let $\mathcal{V}$ be a unitary group constellation arising form an n_T-dimensional representation ρ of an abstract group $\mathcal{G}$. That is, $\mathcal{V}$ is a group of unitary $n_t \times n_T$ matrices representing the elements of $\mathcal{G}$. Let the character of ρ be χ (see the equation (A.4)). Recall the diversity sum is calculated via

$$\xi_{\mathcal{V}} = \frac{1}{2\sqrt{n_T}} \min_{\boldsymbol{V},\boldsymbol{V}' \in \mathcal{V}} \|\boldsymbol{V} - \boldsymbol{V}'\|. \tag{5.1}$$

We simplify the term $\|\boldsymbol{V} - \boldsymbol{V}'\|$ of the diversity sum $\xi_{\mathcal{V}}$ in (5.1) as follows:

$$\begin{aligned}
\|\boldsymbol{V} - \boldsymbol{V}'\|^2 &= \mathrm{tr}((\boldsymbol{V} - \boldsymbol{V}')(\boldsymbol{V} - \boldsymbol{V}')^\dagger) \\
&= \mathrm{Tr}(\boldsymbol{V}\boldsymbol{V}^\dagger - \boldsymbol{V}\boldsymbol{V}'^\dagger - \boldsymbol{V}'\boldsymbol{V}^\dagger + \boldsymbol{V}'\boldsymbol{V}'^\dagger) \\
&= \mathrm{Tr}(I - \boldsymbol{V}\boldsymbol{V}'^\dagger - (\boldsymbol{V}\boldsymbol{V}'^\dagger)^* + I) \quad \text{since } \boldsymbol{V}\boldsymbol{V}^\dagger = I \\
&= \mathrm{Tr}(I - \boldsymbol{V}'' - \boldsymbol{V}''^\dagger + I) \quad \text{from } \boldsymbol{V}\boldsymbol{V}'^\dagger = \boldsymbol{V}'' \in \mathcal{V} \\
&= \mathrm{Tr}[(I - \boldsymbol{V}'') + (I - \boldsymbol{V}'')^\dagger] \\
&= \mathrm{Tr}(I - \boldsymbol{V}'') + \mathrm{tr}(I - \boldsymbol{V}'')^\dagger \\
&= 2\mathrm{Re}\{\mathrm{tr}(I - \boldsymbol{V}'')\} \\
&= 2\mathrm{Re}\{\mathrm{tr}I - \mathrm{tr}\boldsymbol{V}''\} \\
&= 2(n_T - \mathrm{Re}\{\chi(\boldsymbol{V}'')\})
\end{aligned} \tag{5.2}$$

where $\mathrm{Re}\{x\}$ denotes the real part of the complex number x.

Let's say a group $\mathcal{G}$ has h conjugacy classes $\{\mathcal{C}_i\}_{i=1}^h$. From Appendix A.2, we know that the character is constant on conjugacy class. Consequently we can define the diversity sum in (5.1) in the terms of a character as

$$\xi_{\mathcal{V}} = \frac{1}{\sqrt{2n_T}} \min_{C_i \neq e} \sqrt{n_T - \mathrm{Re}\{\chi_{C_i}\}} \tag{5.3}$$

where $\chi_{C_i} = \chi(g)$ for any $g \in C_i$. Using the formula for the diversity sum given in (5.3), we now can choose a high performance group constellation at low SNR for any group by simply looking at its character table.

Proposition 5.1.1. *The value of a diversity sum is* $0 \leq \xi_{\mathcal{V}} \leq 1$.

Proof: From Appendix A.2, we know that $|\chi_C| \leq \chi(e) = n$ where n is the degree of the representation; here $n = n_T$. Thus $-n_T \leq \mathrm{Re}\{\chi_C\} \leq n_T$. Substituting this value in (5.3) completes the proof. □

Theorem 5.1.1. *If* $\chi_e \neq \chi_{C_i}$ *for any* $C_i \neq \{e\}$ *then* $\xi_{\mathcal{V}} > 0$.

Proof: From the property of a character, we know that $\chi_e = \chi(e) = n = n_T$. Our hypothesis is that $\chi_{C_i} \neq \chi_e$ for any $C_i \neq \{e\}$. This implies χ_{C_i} can not equal n_T. Hence, following the proof of Proposition 1, the right hand side of equation (5.3) can never be 0, and so the diversity sum $\xi_{\mathcal{V}}$ is always greater than zero. □

Remark: If $\chi_C = \chi_e = n_T$ when $C \neq \{e\}$ then $\xi_{\mathcal{V}} = 0$. Moreover if $\chi_C = n_T$ then necessarily $\rho(g) = \boldsymbol{I}_{n_T} = \rho(e)$ for all $g \in C$, so we see that the representation associated to χ is not faithful. In particularly, since $\rho : \mathcal{G} \to U(\mathbb{C}^{n_t})$ is not injective so $\rho(\mathcal{G}) = \mathcal{V}$ and $|\mathcal{V}| < |\mathcal{G}|$.

In particular, if $\mathcal{G}$ is not faithful then it is certainly not fixed-point free. This gives us the classification of all unitary group constellations based on the zero and nonzero terms of diversity product and diversity sum as shown in Figure 5.1. We can see that fixed-point free groups are a subset of the nonzero diversity sum groups, and some nonzero diversity sum groups do not have full diversity (the shaded area).

5.2 Faithful Unitary Group Constellation

Definition 5.2.1. *We say a finite unitary group constellation* $\mathcal{V}$ *is a* ***faithful group constellation*** *if it has* $\xi_{\mathcal{V}} > 0$.

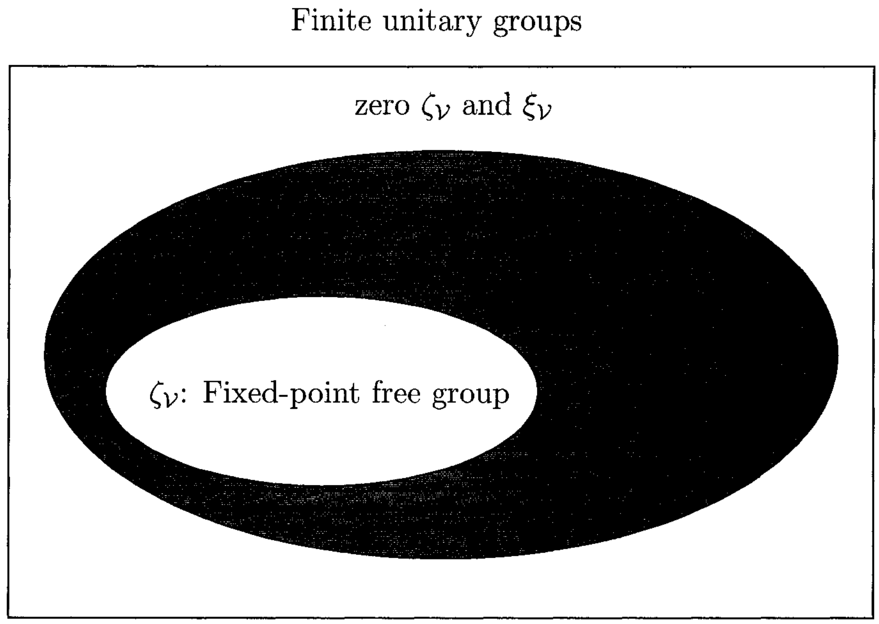

Figure 5.1: Classification of finite unitary groups

Example 5.2.1. *Consider the special linear group $SL_2(\mathbb{F}_5)$ over the finite field with 5 elements. The group $SL_2(\mathbb{F}_5)$ has 9 conjugacy classes which we denote by $e = I, B, C_1, D_1, D_2, E_1, E_{-1}, F_1$ and F_{-1}, and 9 irreducible characters $\{\chi_i\}_{i=1}^{9}$ (following [79]). Its character table is given in Table 5.1. The irreducible characters $\chi_2, \chi_3, \chi_5, \chi_6$ and χ_9 do not correspond to faithful representations because their $\chi_B = \chi_I$. The faithful constellations of $SL_2(\mathbb{F}_5)$ are χ_1, χ_4, χ_7 and χ_8. We note that, from computing the characteristic polynomials in [79], only the irreducible characters χ_7 and χ_8 correspond to fixed-point free groups ($\zeta_{\mathcal{V}} > 0$). Hence the irreducible characters χ_1 and χ_4 correspond to faithful constellations without full diversity which are in the shaded area in Figure 5.1.*

From Example 5.2.1, we see that the irreducible characters χ_2, χ_3, χ_5 and χ_6 do not give rise to faithful constellations. (We do not consider χ_9 because χ_9 is the trivial representation of degree 1, that is, $\chi_9(g) = 1$ for all $g \in \mathcal{G}$.) We deduce that the kernels of these unfaithful representations consist of all elements in the conjugacy classes I and B. The conjugacy class of B consists of exact one element of $SL_2(\mathbb{F}_5)$, namely $-I$. Hence to obtain a new faithful constellation, by group theory, we consider the quotient group

$$PSL_2(\mathbb{F}_5) = SL_2(\mathbb{F}_5)/\{\pm I\}, \tag{5.4}$$

	I	B	C_1	D_1	D_2	E_1	E_{-1}	F_1	F_{-1}
χ_1	6	-6	0	0	0	1	1	-1	-1
χ_2	5	5	1	-1	-1	0	0	0	0
χ_3	4	4	0	1	1	-1	-1	-1	-1
χ_4	4	-4	0	-1	1	-1	-1	1	1
χ_5	3	3	-1	0	0	$-\frac{(-1+j\sqrt{5})}{2}$	$\frac{-1-j\sqrt{5}}{2}$	$-\frac{(-1+j\sqrt{5})}{2}$	$\frac{-1-j\sqrt{5}}{2}$
χ_6	3	3	-1	0	0	$\frac{-1-j\sqrt{5}}{2}$	$-\frac{(-1+j\sqrt{5})}{2}$	$\frac{-1-j\sqrt{5}}{2}$	$-\frac{(-1+j\sqrt{5})}{2}$
χ_7	2	-2	0	1	-1	$-\frac{(-1-j\sqrt{5})}{2}$	$\frac{-1+j\sqrt{5}}{2}$	$\frac{-1-j\sqrt{5}}{2}$	$-\frac{(-1+j\sqrt{5})}{2}$
χ_8	2	-2	0	1	-1	$\frac{-1+j\sqrt{5}}{2}$	$-\frac{(-1-j\sqrt{5})}{2}$	$-\frac{(-1+j\sqrt{5})}{2}$	$\frac{-1-j\sqrt{5}}{2}$
χ_9	1	1	1	1	1	1	1	1	1

Table 5.1: The character table of $SL_2(\mathbb{F}_5)$

called the *projective special linear group.* These four representations will factor through $PSL_2(\mathbb{F}_5)$, giving faithful representations of $PSL_2(\mathbb{F}_5)$. Basically $PSL_2(\mathbb{F}_5)$ are the group of cosets of $\pm I$ in $SL_2(\mathbb{F}_5)$, with $|PSL_2(\mathbb{F}_5)| = \frac{1}{2}|SL_2(\mathbb{F}_5)|$. More properties of $PSL_2(\mathbb{F}_q)$ for an odd prime q are summarized in Appendix A.2.1.

Example 5.2.2. *We construct an irreducible faithful representation of $PSL_2(\mathbb{F}_5)$ from the irreducible character χ_3 of $SL_2(\mathbb{F}_5)$ (which corresponded to unfaithful constellation in Table 5.1). The group $PSL_2(\mathbb{F}_5)$ has 5 conjugacy classes and $120/2 = 60$ elements. The value of the faithful character $\bar{\chi}_3$ of $PSL_2(\mathbb{F}_5)$ can be read from Table 5.2. From (5.3), the diversity sum of this new 4-dimensional representation of $PSL_2(\mathbb{F}_5)$ is*

$$\xi_{\mathcal{V}} = \frac{1}{\sqrt{2\cdot 4}}\sqrt{4-1} = 0.6124. \tag{5.5}$$

The faithful $PSL_2(\mathbb{F}_5)$ constellation obtained from χ_2, χ_5 and χ_6 can be analyzed similarly.

5.3 Examples and Performance

We give some examples of computing the diversity sum using the character tables of different unitary groups. The performance is considered by plotting the BLER against SNR in dB, using DUSTM explained in Section 2.1. The fading coefficients

	$I = B$	C_1	$D_1 = D_2$	$E_1 = F_1$	$E_{-1} = F_{-1}$
$\bar{\chi}_2$	5	1	-1	0	0
$\bar{\chi}_3$	4	0	1	-1	-1
$\bar{\chi}_5$	3	-1	0	$-\frac{(-1+j\sqrt{5})}{2}$	$\frac{-1-j\sqrt{5}}{2}$
$\bar{\chi}_6$	3	-1	0	$\frac{-1-j\sqrt{5}}{2}$	$-\frac{(-1+j\sqrt{5})}{2}$

Table 5.2: The character table of $PSL_2(\mathbb{F}_5)$

and additive noise are independent $\mathcal{CN}(0,1)$, and the channel matrix is assumed to be constant within two consecutive time periods. The ML criterion is used for decoding.

5.3.1 Cyclic Group

An $n_T \times n_T$ cyclic group constellation of order L, $\mathcal{V} = \{\boldsymbol{V}_l\}_{l=0}^{L-1}$ is defined as [35, 36]

$$\boldsymbol{V}_l = \text{diag}(e^{j2\pi k_1 l/L}, e^{j2\pi k_2 l/L}, \ldots, e^{j2\pi k_{n_T} l/L}) \tag{5.6}$$

where $k_i \in \{1, 2, \ldots, L-1\}$. The character of this cyclic group constellation is

$$\chi_{\boldsymbol{V}_l} = \sum_{i=1}^{n_T} e^{j2\pi k_i l/L}. \tag{5.7}$$

Therefore

$$\text{Re}\{\chi_{\boldsymbol{V}_l}\} = \sum_{i=1}^{n_T} \cos\frac{2\pi k_i l}{L}. \tag{5.8}$$

The L conjugacy classes of a cyclic group each consist of only one element. Thus the diversity sum of a cyclic group of order L is

$$\xi_{\mathcal{V}} = \frac{1}{\sqrt{2n_T}} \min_{l=1,2,\ldots,L-1} \sqrt{n_T - \sum_{i=1}^{n_T} \cos\frac{2\pi k_i l}{L}}. \tag{5.9}$$

5.3.2 Dicyclic Group

The dicyclic group constellation [37] of order L and even n_T is defined as

$$\mathcal{V} = \{\boldsymbol{V}_0^l \boldsymbol{V}_1^m : \ 0 \le l < L/2; \ m = 0, 1\} \tag{5.10}$$

where

$$\boldsymbol{V}_0 = \mathrm{diag}(e^{j4\pi k_1/L}, e^{j4\pi k_2/L}, \ldots, e^{j4\pi k_{n_T}/L}) \text{ and } \boldsymbol{V}_1 = \begin{bmatrix} 0 & -I_{n_T/2} \\ I_{n_T/2} & 0 \end{bmatrix} \tag{5.11}$$

and $k_i \in \{1, 2, \ldots, L-1\}$. The character of $\{\boldsymbol{V}_0^l \boldsymbol{V}_1\}$ is 0 for every $l = 0, 1, \ldots, n_T/2$. So to compute a diversity sum, it is enough to consider only $\{\boldsymbol{V}_0^l\}_{l=0}^{n_T/2}$. Using a computation similar to the one in Section 5.3.1, the diversity sum of a dicyclic group of order L is

$$\xi_{\mathcal{V}} = \frac{1}{\sqrt{2n_T}} \min_{l=1,2,\ldots,L/2} \sqrt{n_T - \sum_{i=1}^{n_T} \cos\frac{4\pi k_i l}{L}}. \tag{5.12}$$

5.3.3 Performance of $SL_2(\mathbb{F}_q)$ For Odd Prime q

The character table of $SL_2(\mathbb{F}_q)$ for an odd prime q is given in Table II [79], so we can use the equation (5.3) to compute the diversity sum very easily. We give some examples for the group $SL_2(\mathbb{F}_5)$, and also show that their faithful non full diversity constellations outperform full diversity constellations in a specific range of low SNR. *Note*: χ_7 is a fixed-point free group [80].

The Group $SL_2(\mathbb{F}_5)$: $\mathcal{V}_{\chi_4}$ vs. $\mathcal{V}_{\chi_7 \oplus \chi_7}$, $n_T = 4$ transmitter antennas

The formulas to compute the 4-dimensional representation of irreducible character χ_4 (setting $\alpha(2^n) = e^{\pi j n/2}$) and the 2-dimensional representation of irreducible character χ_7 are given in Appendix A.2.2.

To compute the diversity sum in the equation (5.3), it is enough to consider only the term $n_T - \mathrm{Re}\{\chi_C\} = 4 - \mathrm{Re}\{\chi_C\}$. Table 5.3 shows the values of $4 - \mathrm{Re}\{\chi_C\}$ of χ_4 and $\chi_7 \oplus \chi_7$. We note that the character of $\chi_7 \oplus \chi_7 = \chi_7 + \chi_7$ from Section 5.2. We can see that the minimum values of $4 - \mathrm{Re}\{\chi\}$, over the conjugacy classes $C_i \neq I$, of χ_4 and $\chi_7 \oplus \chi_7$ are 3 and 2 respectively. Thus one can predict that the constellation $\mathcal{V}_{\chi_4}$ should outperform the constellation $\mathcal{V}_{\chi_7 \oplus \chi_7}$ at a low SNR. Simulation shows that this is true in the range of low SNR $\approx$ 0-17 dB as shown in Figure 5.2 with the number of receiver antenna $n_R = 1$.

	I	B	C_1	D_1	D_2	E_1	E_{-1}	F_1	F_{-1}
χ_4	4	-4	0	-1	1	-1	-1	1	1
$4 - \text{Re}\{\chi_4\}$	0	8	4	5	3	5	5	3	3
$\chi_7 \oplus \chi_7$	4	-4	0	2	-2	$1 + j\sqrt{5}$	$-1 + j\sqrt{5}$	$-1 - j\sqrt{5}$	$1 - j\sqrt{5}$
$4 - \text{Re}\{\chi_7 \oplus \chi_7\}$	0	8	4	2	6	3	5	5	3

Table 5.3: Comparison of χ_4 and $\chi_7 \oplus \chi_7$

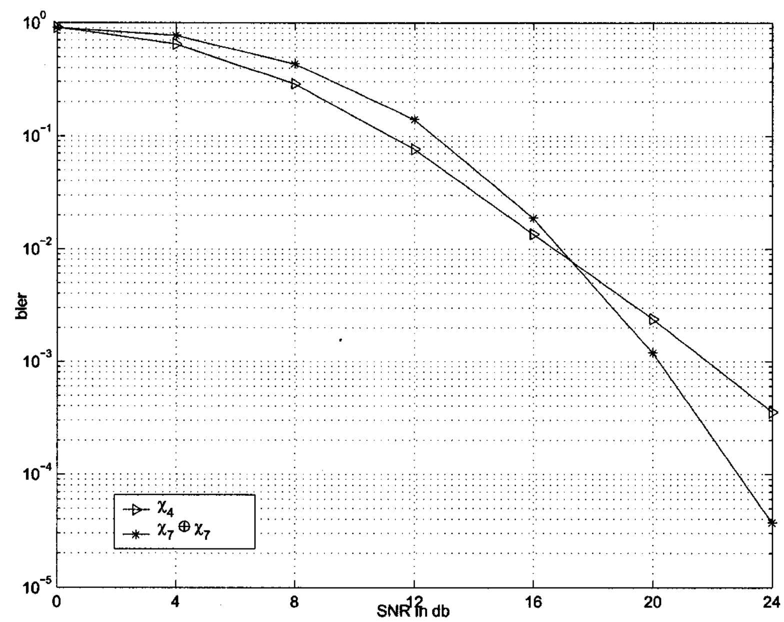

Figure 5.2: BLER performance of χ_4 vs. $\chi_7 \oplus \chi_7$. $n_T = 4, n_R = 1$ and $R = 1.73$ bits/s

The Group $SL_2(\mathbb{F}_5)$: $\mathcal{V}_{\chi_4 \oplus \chi_7}$ vs.$\mathcal{V}_{\chi_7 \oplus \chi_7 \oplus \chi_7}$, $n_T = 6$ Transmitter antennas

The values of $n_T - \text{Re}\{\chi_C\} = 6 - \text{Re}\{\chi_C\}$ for $\chi_4 \oplus \chi_7$ and $\chi_7 \oplus \chi_7 \oplus \chi_7$ are given in Table 5.4. Their minimum values are 5.5 and 3, respectively. From the simulation shown in Figure 5.3, we can see that the constellation $\mathcal{V}_{\chi_4 \oplus \chi_7}$ performs very well at low SNR 0-20 dB. It outperforms the constellation $\mathcal{V}_{\chi_7 \oplus \chi_7 \oplus \chi_7}$ by ≈ 3 dB.

5.3.4 Performance of $PSL_2(\mathbb{F}_q)$ For Odd Prime q

The group $PSL_2(\mathbb{F}_5)$: $\bar{\chi_3}$, $M = 4$ Transmitter Antennas

From Example 5.2.1, the constellation obtained from the irreducible character $\bar{\chi_3}$ of $PSL_2(\mathbb{F}_5)$ has $\xi_{\mathcal{V}} = 0.6124$. The rate is $R = \log_2(60)/4 = 1.48$ bits/s, using for 4

	I	B	C_1	D_1	D_2	E_1	E_{-1}	F_1	F_{-1}
$\chi_4 \oplus \chi_7$	6	-6	0	0	0	$\frac{-1+j\sqrt{5}}{2}$	$\frac{-3+j\sqrt{5}}{2}$	$\frac{1-j\sqrt{5}}{2}$	$\frac{3-j\sqrt{5}}{2}$
$6 - \mathrm{Re}\{\chi_4 \oplus \chi_7\}$	0	12	6	6	6	6.5	7.5	5.5	4.5
$\chi_7 \oplus \chi_7 \oplus \chi_7$	6	-6	0	3	-3	$\frac{3+j\sqrt{5}}{2}$	$\frac{-3+j\sqrt{5}}{2}$	$\frac{-3-j\sqrt{5}}{2}$	$\frac{3-j\sqrt{5}}{2}$
$6 - \mathrm{Re}\{\chi_7 \oplus \chi_7 \oplus \chi_7\}$	0	12	6	3	9	4.5	7.5	7.5	4.5

Table 5.4: Comparison of $\chi_4 \oplus \chi_7$ and $\chi_7 \oplus \chi_7 \oplus \chi_7$

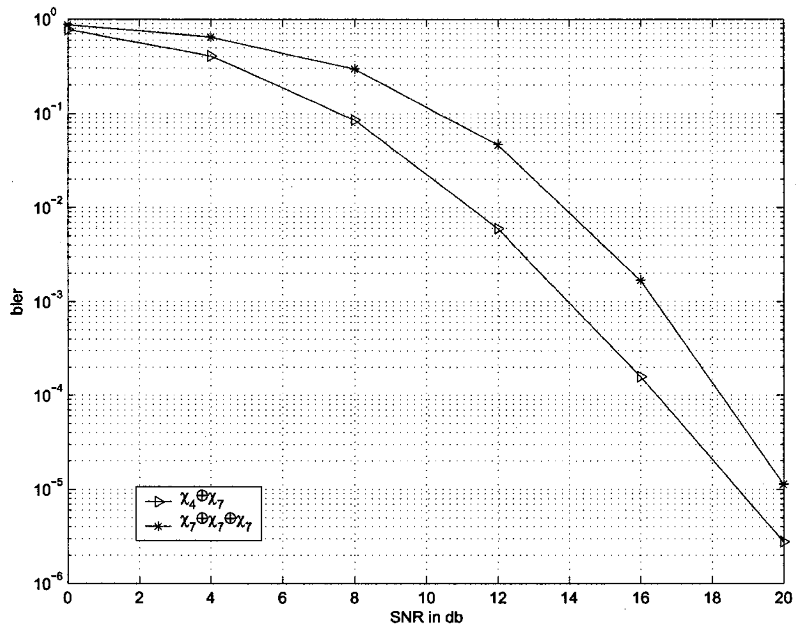

Figure 5.3: BLER performance of $\chi_4 \oplus \chi_7$ vs. $\chi_7 \oplus \chi_7 \oplus \chi_7$. $n_T = 6, n_R = 1$ and $R = 1.15$ bits/s

transmitter antennas. The 60 faithful representation matrices of $PSL_2(\mathbb{F}_5)$ can be generated from $(\boldsymbol{PQ})^j \boldsymbol{X}$ where $j = 0, 1, 2, 3, 4$ (see Appendix A.2.2, using $\alpha(2^n) = e^{\pi jn}$). Figure 5.4 shows the block error rate perfromance of $\mathcal{V}_{\bar{\chi}_4}$ for $n_R = 1, 2, 3$ receiver antennas. We can see that the performance is improved by increasing the number of receiver antennas.

The Group $PSL_2(\mathbb{F}_7)$, $M = 4$ Transmitter Antennas

From (A.7), the group $PSL_2(\mathbb{F}_7)$ has

$$3 + \left\lceil \frac{7-3}{4} \right\rceil + \left\lceil \frac{7-1}{4} \right\rceil = 3 + 1 + 2 = 6 \tag{5.13}$$

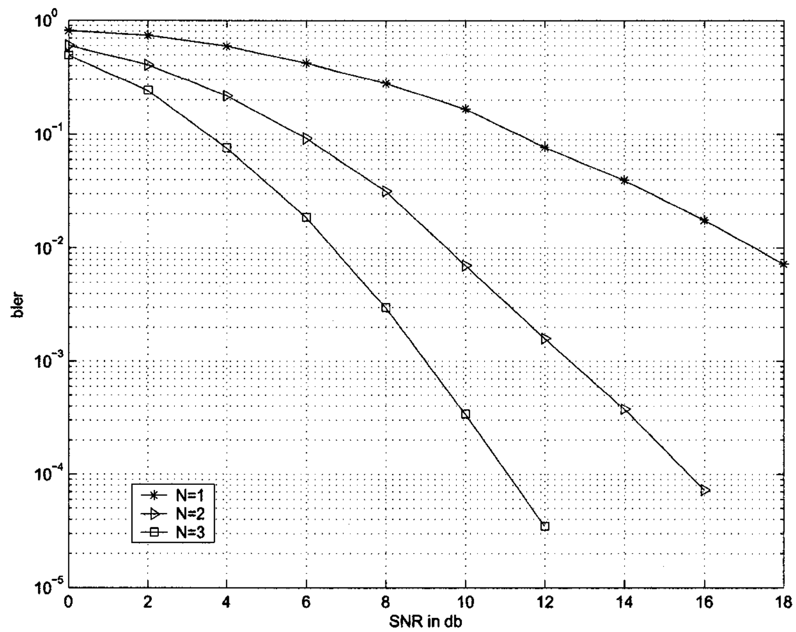

Figure 5.4: BLER performance of $PSL_2(\mathbb{F}_5)$

	$A=B$	$C_1=C_2$	$D_1=D_2$	D_3	$E_1=F_{-1}$	$E_{-1}=F_1$
$\bar{\chi_1}$	8	-1	0	0	1	1
$\bar{\chi_2}$	7	1	-1	-1	0	0
$\bar{\chi_3}$	6	0	0	2	-1	-1
$\bar{\chi_4}$	3	0	1	-1	$\frac{-1-j\sqrt{7}}{2}$	$\frac{-1+j\sqrt{7}}{2}$
$\bar{\chi_5}$	3	0	1	-1	$\frac{-1+j\sqrt{7}}{2}$	$\frac{-1-j\sqrt{7}}{2}$
$\bar{\chi_6}$	1	1	1	1	1	1

Table 5.5: The character table of $PSL_2(\mathbb{F}_7)$

conjugacy classes with $7(7^2-1)/2 = 168$ elements. The character table of $PSL_2(\mathbb{F}_7)$, as computed from Table A.1 (see also in [42, pp.314]) is shown in Table 5.5. Consider the irreducible character $\bar{\chi_4}$, using for 3 transmitter antennas with the rate $R = \log_2(168)/3 = 2.46$ bits/s. The value of diversity sum is

$$\xi_\mathcal{V} = \frac{1}{\sqrt{2\cdot 3}}\sqrt{3-1} = 0.557. \tag{5.14}$$

The main contribution of this chapter is to consider those nonzero diversity sum groups which have good performance at low SNR, as predicted by the upper bound on P_e in the equation (2.18). The advantage of using a character table to choose a good performance group constellation is that the character tables of finite groups are readily available, whereas their actual representations (that is, the constellations) are complicated and time-consuming to compute. Hence, using a character table, we can predict a good performance group constellation, and then compute its representation.

Another advantage of our proposed method is its fast computation of the diversity sum (2.19). While this would nominally require calculating the norms of $|\mathcal{V}| - 1$ matrices, our method computes $\xi_{\mathcal{V}}$ from $h-1$ values, where h is the number of conjugacy classes of a group $\mathcal{G}$; thus $h \leq |\mathcal{G}| = |\mathcal{V}|$. For example, the group $SL_2(\mathbb{F}_5)$ is of order $120 = |\mathcal{V}|$ yet to compute its diversity sum $\xi_{\mathcal{V}}$ we need to check only 8 values from its character table. Finally, in contrast to the case of computing the diversity product in [79], our method is very simple because it does not require the computation of characteristic polynomials, but only the values of the characters from the character table.

Chapter 6

Fast MSD for DUSTM Using a Stack Algorithm

This chapter presents a stack algorithm approach as a fast optimization of the MSD decision metric for DUSTM for any number of transmitter antennas. The proposed algorithm can be considered as the extension work of [10] as we use a stack to reduce the complexity for a large constellation of size L and the number of detected symbols N_d. The proposed stack algorithm can be used for any (diagonalizable and nondiagonalizable) USTC, and without requiring any knowledge of its algebraic structure.

Unlike most applications of using a *stack* algorithm [43] to reduce the complexity of a decoding problem (*i.e.* convolutional code), which are suboptimal, Theorem 6.2.1 shows that the proposed stack algorithm is equivalent to ML detection. Moreover, it has especially low complexity at high SNR, as shown in simulations. The complexity required to maximize the decision metric using the proposed stack algorithm is reduced from $O(L^{N_d}N_d^2)$ to $O(LN_d^2)$ at high SNR.

6.1 Literature Review

We give a summary of the literature on the use of MSD for DUSTM and also discuss their advantages and disadvantages as follows:

- The MSD was first presented for two transmitter antennas in [17], which allowed for the detection of two symbols by considering three consecutive blocks at the receiver.

- The decision metric of MSD for DUSTM was proposed in [22], for any number of transmitter antennas and any N_d (relating to $N_d + 1$ blocks, for the detection of N_d symbols). It further showed that the performance of MSD with 8 blocks gains approximately 1.5 dB compared to a conventional DUSTM in [35, 36] with two transmitter and one receiver antennas using BPSK. The complexity of the ML detection increases exponentially with N_d.

- Two reduced complexity MSD were presented in [88]: the feedback and reduced search detections. The paper derived the decision metric for a 2×2 OSTBC for two transmitter antennas [2]. The number of comparisons needed to optimize the decision metric using the reduced search detection is $LN_d + 2^{2N_d}$ where L is the size of a unitary space-time constellation.

- The approximation of a decision metric of general MSD for DUSTM was derived in [10]. This metric can be optimized using the Viterbi algorthm. The author uses a Per-Survivor Processing (PSP) method proposed in [74], which is suboptimal, to reduce the complexity of Viterbi decoding algorithm.

- Four reduced complexity detection algorithms for diagonal constellations, called bound-intersection detector (BID), were developed to optimize the decision metric of MSD in [15]. The first two are ML detections; the third is suboptimal and the fourth uses feedback detection. These algorithms have exceptionally low complexity, but do not apply to non-diagonalizable constellations. This paper pointed out that the BID algorithm can apply to signal constellations which are obtained from cyclic diagonal constellations by conjugation, meaning those of the form $\boldsymbol{U}^{\dagger}\boldsymbol{V}_l\boldsymbol{U}$ for $l = 0, 1, \cdots, L-1$ where $\{\boldsymbol{V}_0, \ldots, \boldsymbol{V}_{L-1}\}$ is a cyclic group of diagonal matrices. Since this group is abelian, so is any such non-diagonal constellation; it follows that any nonabelian fixed point free group [80], or any (nongroup) orthogonal constellation [91] does not fall into this category.

- The suboptimal MSD for DUSTM using a Fano algorithm was presented in [73]. The proposed on-demand bi-Fano algorithm has 3 dB degradation in power efficiency compared to the optimal sphere decoding but it has less complexity.

- The paper [72] presented three (outer) decoders, based on sphere decoding and

Fano algorithms, to reduce the complexity in N of MSD for DUSTM, in conjunction with another (inner) decoder, based on the algebraic structure of the given code, to reduce its complexity in L. Examples of this decoding scheme were given for 2x2 orthogonal and diagonal signal constellations. However, applying this inner decoding algorithm implies algebraically tailoring it to a given constellation, and it is not apparent that this is possible in general.

6.2 Proposed MSD Using a Stack Algorithm

We begin by rewriting the decision metric in (2.11) of MSD for DUSTM to detect N_d symbols with $N_d + 1$ blocks at the receiver to allow the best application of the stack algorithm. First note that the MSD decision metric (2.11) is the sum of terms of the form $\|\boldsymbol{Y}_k - \boldsymbol{U}\boldsymbol{Y}_l\|^2$, with $\boldsymbol{U}$ a unitary matrix. Since $\boldsymbol{U}$ is unitary, we can multiply through by $\boldsymbol{U}^{-1} = \boldsymbol{U}^\dagger$ to get

$$\|\boldsymbol{Y}_k - \boldsymbol{U}\boldsymbol{Y}_l\|^2 = \|\boldsymbol{U}^\dagger\boldsymbol{Y}_k - \boldsymbol{Y}_l\|^2 = \|\boldsymbol{Y}_k\|^2 - 2\langle \boldsymbol{U}^\dagger\boldsymbol{Y}_k, \boldsymbol{Y}_l\rangle + \|\boldsymbol{Y}_l\|^2 \tag{6.1}$$

where $\langle \boldsymbol{A}, \boldsymbol{B}\rangle = \mathrm{tr}(\boldsymbol{B}^\dagger\boldsymbol{A})$ is the inner product of $\boldsymbol{A}$ and $\boldsymbol{B}$. Minimizing this value, for fixed $\boldsymbol{Y}_k$ and $\boldsymbol{Y}_l$, over a selection of unitary matrices $\boldsymbol{U}$ is equivalent to maximizing

$$\|\boldsymbol{Y}_k\|^2 + 2\langle \boldsymbol{U}^\dagger\boldsymbol{Y}_k, \boldsymbol{Y}_l\rangle + \|\boldsymbol{Y}_l\|^2 = \|\boldsymbol{U}^\dagger\boldsymbol{Y}_k + \boldsymbol{Y}_l\|^2 = \|\boldsymbol{Y}_l + \boldsymbol{U}\boldsymbol{Y}_k\|^2. \tag{6.2}$$

This is equally true of any sum of such terms, so it follows that the minimization problem of the decision metric in (2.11) is equivalent to the maximization problem

$$\hat{\boldsymbol{z}}_{\tau N_d} = \arg \max_{\substack{\tau \le k \le \tau + N_d - 1 \\ 0 \le l_k \le L-1}} \sum_{i=1}^{N_d} \sum_{j=i+1}^{N_d+1} \|\boldsymbol{Y}_{\tau+i-1} + (\prod_{k=\tau+i-1}^{\tau+j-2} \boldsymbol{V}_{l_k}^\dagger)\boldsymbol{Y}_{\tau+j-1}\|^2. \tag{6.3}$$

For the purposes of our stack algorithm, we change the order of summation of MSD in (6.3) to obtain the equivalent expression

$$\hat{\boldsymbol{z}}_{\tau N_d} = \arg \max_{\substack{\tau \le k \le \tau + N_d - 1 \\ 0 \le l_k \le L-1}} \sum_{j=2}^{N_d+1} \sum_{i=1}^{j-1} \|\boldsymbol{Y}_{\tau+i-1} + (\prod_{k=\tau+i-1}^{\tau+j-2} \boldsymbol{V}_{l_k}^\dagger)\boldsymbol{Y}_{\tau+j-1}\|^2. \tag{6.4}$$

Note that when $N_d = 1$ (single symbol detection), the decision metric in (6.4) reduces to

$$\hat{z}_\tau = \arg \max_{l=0,\dots,L-1} \|\boldsymbol{Y}_\tau + \boldsymbol{V}_l^\dagger \boldsymbol{Y}_{\tau+1}\|^2 \tag{6.5}$$

which is the same decision metric for a conventional DUSTM (where the channel matrix is assumed constant over two consecutive blocks) as given in (21) in [35].

For the proposed stack algorithm, for each j we define the term

$$D_\tau(l_\tau, \cdots, l_{\tau+j-2}) = \sum_{i=1}^{j-1} \|\boldsymbol{Y}_{\tau+i-1} + (\prod_{k=\tau+i-1}^{\tau+j-2} \boldsymbol{V}_{l_k}^\dagger)\boldsymbol{Y}_{\tau+j-1}\|^2 \tag{6.6}$$

hence the decision metric of MSD for DUSTM given in (6.4) can be rewritten as

$$\hat{\boldsymbol{z}}_{\tau N_d} = \arg \max_{\substack{\tau \le k \le \tau+N_d-1 \\ 0 \le l_k \le L-1}} \sum_{j=2}^{N_d+1} D_\tau(l_\tau, \cdots, l_{\tau+j-2}). \tag{6.7}$$

Furthermore, we define

$$D'_\tau(j-1) = \sum_{i=1}^{j-1} (\|\boldsymbol{Y}_{\tau+i-1}\| + \|\boldsymbol{Y}_{\tau+j-1}\|)^2 . \tag{6.8}$$

Proposed Stack Algorithm

We are now ready to describe the proposed MSD algorithm using a stack as follows:

1. For each τ, collect the $N_d + 1$ received signal matrices $\boldsymbol{Y}_\tau, \boldsymbol{Y}_{\tau+1}, \cdots, \boldsymbol{Y}_{\tau+N_d}$.

2. Compute $D_\tau(l_\tau) = \|\boldsymbol{Y}_\tau + \boldsymbol{V}_{l_\tau}^\dagger \boldsymbol{Y}_{\tau+1}\|^2$, for all $\boldsymbol{V}_{l_\tau} \in \mathcal{V}$; store these L values in a stack. Sort the stack.

3. Let's say that $l_\tau = j$ corresponds to the maximum metric D_j. Compute $D_j + D_\tau(j, l_{\tau+1})$ for all $\boldsymbol{V}_{l_{\tau+1}} \in \mathcal{V}$ and store these in the stack, replacing D_j. To every other element of the stack, add $D'_\tau(3)$. Sort the stack.

4. If the maximal element is some $D_{j,k} = D_j + D_\tau(j,k)$, then proceed to the next index. In general terms, if the maximal element is of the form $D_{j_1,j_2,\cdots,j_k} = D_{j_1,j_2,\cdots,j_{k-1}} + D_\tau(j_1, \cdots, j_k)$, then replace $D_{j_1,j_2,\cdots,j_k}$ with the L terms $D_{j_1,j_2,\cdots,j_k} + D_\tau(j_1, j_2, \cdots, j_k, l)$, as $\boldsymbol{V}_l$ runs through $\mathcal{V}$, and add $D'_\tau(k+1)$ to the rest.

	Stack	Metric
1.	$\boldsymbol{V}_2$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+1}\\|^2$
	$\boldsymbol{V}_3$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+1}\\|^2$
	$\boldsymbol{V}_1$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+1}\\|^2$
2.	$\boldsymbol{V}_3$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + D'(\tau+1)$
	$\boldsymbol{V}_2\boldsymbol{V}_1$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_2\boldsymbol{V}_3$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_2\boldsymbol{V}_2$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_1$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + D'(\tau+1)$
3.	$\boldsymbol{V}_3\boldsymbol{V}_2$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_3\boldsymbol{V}_3$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_3\boldsymbol{V}_1$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_3^\dagger \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_2\boldsymbol{V}_1$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_2\boldsymbol{V}_3$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_3^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_2\boldsymbol{V}_2$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + \\|\boldsymbol{Y}_\tau + \boldsymbol{V}_2^\dagger \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+2}\\|^2 + \\|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_2^\dagger \boldsymbol{Y}_{\tau+2}\\|^2$
	$\boldsymbol{V}_1$	$\\|\boldsymbol{Y}_\tau + \boldsymbol{V}_1^\dagger \boldsymbol{Y}_{\tau+1}\\|^2 + D'(\tau+1)$

Table 6.1: Proposed MSD algorithm using a stack in Example 6.2.1

5. If instead the maximal element corresponds to some $D_\tau(j') + D'_\tau(2)$, then replace this element with the L terms $D_\tau(j') + D_\tau(j', l)$, as $\boldsymbol{V}_l$ runs through $\mathcal{V}$. More generally, replace $D'_\tau(k)$ with the corresponding $D_\tau(j_1, \cdots, j_{k-1}, l)$. Sort the stack.

6. Repeat the last two steps. Since the last step may be repeated at most L times, the algorithm will terminate. At that point, the top of the stack will be equal to the maximum decision metric for the received signals $\boldsymbol{Y}_\tau, \boldsymbol{Y}_{\tau+1}, \cdots, \boldsymbol{Y}_{\tau+N_d}$.

Example 6.2.1. *We illustrate the proposed MSD algorithm using a stack in Table 6.1. Let the unitary space-time constellation be $\mathcal{V} = \{\boldsymbol{V}_1, \boldsymbol{V}_2, \boldsymbol{V}_3\}$ and $L = 3$. We consider at $N_d + 1 = 3$ blocks which detect $N_d = 2$ symbols at the receiver. The top of stack has the maximum decision metric. Note that after Iteration 1, Step (3) of the algorithm was applied, whereas after Iteration 2, Step (5) was invoked. The final decoded message is $\hat{\boldsymbol{z}}_\tau = arg(\boldsymbol{V}_3, \boldsymbol{V}_2)$.*

Theorem 6.2.1. *The proposed stack algorithm to optimize the decision metric of MSD is equivalent to ML detection.*

Proof. Let $\boldsymbol{Y}_\tau$ and $\boldsymbol{V}_\tau$ be the received and transmitted signal matrices at time τ, respectively. For simplicity, we consider the case of detecting $N_d = 2$ symbols with $N_d + 1 = 3$ blocks; the proof generalizes to any $N_d > 2$.

The received signal matrices are $\boldsymbol{Y}_\tau$, $\boldsymbol{Y}_{\tau+1}$ and $\boldsymbol{Y}_{\tau+2}$. From (6.4), the ML decision metric is

$$\|\boldsymbol{Y}_\tau + \boldsymbol{V}_\tau^\dagger \boldsymbol{Y}_{\tau+1}\|^2 + \|\boldsymbol{Y}_\tau + \boldsymbol{V}_\tau^\dagger \boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|^2 + \|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|^2 \tag{6.9}$$

which can also be written as $D_\tau(\tau) + D_\tau(\tau, \tau+1)$.

The Step (2) of the stack algorithm is to compute $D_\tau(\tau) = \|\boldsymbol{Y}_\tau + \boldsymbol{V}_\tau^\dagger \boldsymbol{Y}_{\tau+1}\|^2$ for all $\boldsymbol{V}_\tau \in \mathcal{V}$. If $\boldsymbol{V}_j$ gives the maximum value, then the Step (3) has to compute

$$D_\tau(j)+D_\tau(j,\tau+1) = \|\boldsymbol{Y}_\tau+\boldsymbol{V}_j^\dagger \boldsymbol{Y}_{\tau+1}\|^2+\|\boldsymbol{Y}_\tau+\boldsymbol{V}_j^\dagger \boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|^2+\|\boldsymbol{Y}_{\tau+1}+\boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|^2, \tag{6.10}$$

for all $\boldsymbol{V}_{\tau+1} \in \mathcal{V}$, and to compare these values with the rest of the stack, whose entries are given as

$$D_\tau(i)+D'_\tau(3) = \|\boldsymbol{Y}_\tau+\boldsymbol{V}_i^\dagger \boldsymbol{Y}_{\tau+1}\|^2+(\|\boldsymbol{Y}_\tau\| + \|\boldsymbol{Y}_{\tau+2}\|)^2+(\|\boldsymbol{Y}_{\tau+1}\| + \|\boldsymbol{Y}_{\tau+2}\|)^2 \tag{6.11}$$

with $i \neq j$.

Therefore to prove Theorem 6.2.1, we need to show that if (6.10)(j) >(6.11)(i) for some $i \neq j$, then (6.10)(j) >(6.10)(i) as well, that is, $\boldsymbol{V}_i$ cannot give a larger decision metric in place of $\boldsymbol{V}_j$, for any choice of $\boldsymbol{V}_{\tau+1}$.

Applying the Cauchy-Schwarz inequality [48] to the term $D_\tau(i, \tau+1)$ in (6.10)(i), and using that each $\boldsymbol{V}_\tau$ is unitary, gives

$$\begin{aligned} D_\tau(i,\tau+1) &= \|\boldsymbol{Y}_\tau + \boldsymbol{V}_i^\dagger \boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|^2 + \|\boldsymbol{Y}_{\tau+1} + \boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|^2 \\ &\leq (\|\boldsymbol{Y}_\tau\| + \|\boldsymbol{V}_i^\dagger \boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|)^2 + (\|\boldsymbol{Y}_{\tau+1}\| + \|\boldsymbol{V}_{\tau+1}^\dagger \boldsymbol{Y}_{\tau+2}\|)^2 \\ &= (\|\boldsymbol{Y}_\tau\| + \|\boldsymbol{Y}_{\tau+2}\|)^2 + (\|\boldsymbol{Y}_{\tau+1}\| + \|\boldsymbol{Y}_{\tau+2}\|)^2 \text{ since } \boldsymbol{V} \text{ are unitary} \\ &= D'_\tau(3). \end{aligned} \tag{6.12}$$

Thus we have shown that this stack algorithm will produce the maximum metric. □

6.3 Simulation Results and Complexity Analysis

We discuss the complexity of the proposed stack algorithm, as compared to the brute-force maximization of the decision metric of MSD in (6.4). Simulation is done in MATLAB, using the DUSTM as explained in Section 2.1.1, where we assume the channel matrix is constant over $N_d + 1 = 4$ blocks and detect $N_d = 3$ decoded symbols. We consider the USTC from the cyclic group in [35, 36] at the data rate $R = 1.00$ bit/s with $n_T = 4$ transmitter antennas and $n_R = 1$ receiver antenna. The average number of flops per block of using the proposed stack algorithm to maximize the MSD decision metric compared to the brute-force method is given in Table 6.2. The brute-force maximization has 3.17×10^6 average flops per block for all SNR. It is clear that the stack algorithm has far lower complexity.

SNR (in dB)	0	5	10	15	20
Flops of brute force $\times 10^6$	3.17	3.17	3.17	3.17	3.17
Flops of stack $\times 10^3$	724.25	174.64	6.92	6.92	6.92

Table 6.2: The average number of flops per block at $n_T = 4, n_R = 1$ and $N_d = 3$

Complexity at High SNR

One interesting result from Table 6.2 is the number of average flops per block using the proposed stack algorithm is constant ($\approx 6.92 \times 10^3$) at high SNR ≥ 10 dB. The number of stack comparisons needed to maximize the decision metric is constant at high SNR. This implies that the Step (5) never happens in the stack algorithm.

At high SNR, the Step 4 is executed N_d times. At each iteration n, $1 \leq n \leq N_d$, one needs to calculate $D_\tau(j_1, \cdots, l)$, which involves n norm calculations, L times, and $D'_\tau(n)$ once. Assuming that the operation of calculating the square norm of a matrix is the most costly, and that one precomputes the norms of the N received signal matrices the cost of $D'_\tau(n)$ becomes negligible. Hence the complexity of the proposed algorithm at high SNR is $O(LN_d^2)$. On the other hand, a brute force algorithm implies calculating $N_d(N_d+1)/2$ matrix norms for each of L^{N_d} possible combinations, implying a complexity of approximately $O(N_d^2 L^{N_d})$.

Thus we reduce the number of comparisons required to maximize the decision metric from L^{N_d} candidates to $LN_d + (L-1)N_d(N_d-1)/2$.

Chapter 7

PEP of STC for a Keyhole Channel

In this chapter, we derive a tight upper bound on the average *pairwise error probability (PEP)* of full rank STCs for a keyhole channel, using a *Moment Generating Function (MGF)*-based approach. To obtain this upper bound, we use two closed-form upper bounds, denoted Q_1 and Q_2 in (7.3) and (7.4) respectively, of the *Q-function*, which is used in the exact conditional PEP for given fading channel coefficients as given in [89]. The two upper bounds are applicable everywhere but are especially tight in low and high SNR respectively.

The symbol error rate (SER) performance of STBC in a keyhole channel was studied in [78], using a MGF-based approach[1] to the conditional SER for a given instantaneous SNR. The proposed SERs in [78] are exact, but apply only to space-time block codes. More generally, the calculation of average PEP and a design criterion of STC in a keyhole channel have been presented in [87] (also in [56] for STTC only for two transmitter antennas and one receiver antenna). However when the (square moduli of the) eigenvalues of a codeword pair difference are not distinct, the PEPs proposed in [56, 87] do not apply; for example, in the 2×2 OSTBC in [90].

The advantage of our proposed bound on PEP is its closed form solution using *hypergeometric functions*[2], and its dependence only on the minimum eigenvalue of a codeword pair difference. This, in turn, implies a simple max-min eigenvalue computation which can be done by a power method [20].

Our proposed PEP applies more generally than does the SER of [78]; for example,

[1] We give a summary of the MGF-based approach in Appendix A.5.

[2] The definition of hypergeometric functions is given in Appendix A.4.

to STTC presented in [93]. Furthermore, our proposed PEP offers an improvement over the one suggested in [87], as it applies to all full rank STC for any number of antennas.

7.1 Proposed PEP for a Keyhole Channel

Consider a MIMO system with n_T transmitter and n_R receiver antennas in a Rayleigh flat fading channel with fading coefficients $\{\beta_i\alpha_j\}_{i=1,j=1}^{n_R,n_T}$. Let $\boldsymbol{H} = \boldsymbol{\beta}\boldsymbol{\alpha}^t$ denote the corresponding keyhole channel matrix (as explained in Section 2.1.4). Further, recall that the Q-function is defined by

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx. \tag{7.1}$$

Then the exact conditional PEP that the receiver antennas erroneously decodes $\boldsymbol{e}$ from a codeword $\boldsymbol{c}$ is given by [89]

$$P_{\text{PEP}}(\boldsymbol{c} \to \boldsymbol{e}|\beta_i\alpha_j) = Q\left(\sqrt{\frac{\rho}{2}\text{Tr}(\boldsymbol{H}\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger\boldsymbol{H}^\dagger)}\right) \tag{7.2}$$

where $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e}) = \boldsymbol{e} - \boldsymbol{c}$ is defined as the difference matrix of the codewords $\boldsymbol{c}$ and $\boldsymbol{e}$. Here, ρ is the SNR at each receiver antenna, and we assume that the expected value of the sum of all transmitted signal powers equals to one.

The STC achieves a *rank criterion* proposed in [93] if it has *full rank*, that is, $\text{rank}(\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})) = n_T$ for each codeword pair $(\boldsymbol{c},\boldsymbol{e})$. Since the codewords are in general $n_T \times l$ matrices, where l is the length of the codeword sequence, we must have $l \geq n_T$ for any full rank code.

To bound the value of P_{PEP} in (7.2), we define the two upper bounds of $Q(x)$ in (7.1) from

$$\begin{aligned} Q(x) &\leq Q_1(x) = \frac{1}{2}e^{-\frac{x^2}{2}}, && (7.3)\\ Q(x) &\leq Q_2(x) = \frac{1}{\sqrt{2\pi}x}e^{-\frac{x^2}{2}}. && (7.4) \end{aligned}$$

We plot $Q(x)$ compared with $Q_1(x)$ and $Q_2(x)$ in Figure 7.1. It is clear that when $x \leq \sqrt{\frac{2}{\pi}}$, $Q_1(x)$ gives the better upper bound of $Q(x)$, whereas when $x \geq \sqrt{\frac{2}{\pi}}$, $Q_2(x)$

gives the better upper bound. Hence we can approximate the Q-function by

$$Q(x) = \min(Q_1(x), Q_2(x)). \tag{7.5}$$

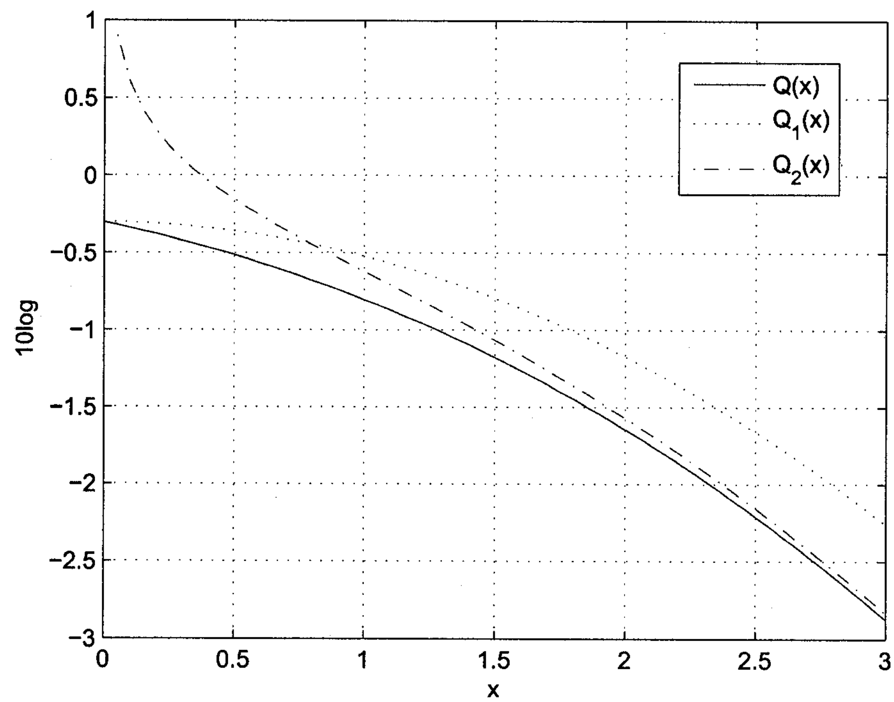

Figure 7.1: The Q-function

7.1.1 Using the Upper Bound $Q_1(x)$

Using the upper bound $Q_1(x)$ given in (7.3), the exact PEP in (7.2) is bounded by

$$P_{\text{PEP }1}(\boldsymbol{c} \rightarrow \boldsymbol{e}|\beta_i\alpha_j) \leq \frac{1}{2}\exp\left(-\frac{\rho}{4}\text{Tr}(\boldsymbol{H}\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger\boldsymbol{H}^\dagger)\right). \tag{7.6}$$

Recall that the $n_T \times n_T$ matrix $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger$ is hermitian and positive semi-definite. Hence it admits a singular value decomposition

$$\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger = \boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^\dagger, \tag{7.7}$$

where $\boldsymbol{U}$ is an $n_T \times n_T$ unitary matrix whose columns are eigenvectors of $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger$, and $\boldsymbol{D} = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_{n_T})$ is an $n_T \times n_T$ diagonal matrix whose diagonal entries, which are listed in decreasing order, are the corresponding eigenvalues of $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger$. In what follows, we will assume that the code is full rank, so that $\mathrm{rank}(\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})) = n_T$ and thus $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger$ is positive definite (not just positive semi-definite). It follows that $\lambda_i > 0$ for all i [93].

Consider now the specific case of a keyhole channel. Substituting $\boldsymbol{H} = \boldsymbol{\beta}\boldsymbol{\alpha}^t$ and $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger = \boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^\dagger$ in (7.6) gives

$$\begin{aligned} P_{\text{PEP 1}}(\boldsymbol{c} \to \boldsymbol{e}|\beta_i\alpha_j) &\le \frac{1}{2}\exp\left(-\frac{\rho}{4}\mathrm{Tr}(\boldsymbol{\beta}\boldsymbol{\alpha}^t\boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^\dagger(\boldsymbol{\beta}\boldsymbol{\alpha}^t)^\dagger)\right). \\ &= \frac{1}{2}\exp\left(-\frac{\rho}{4}\mathrm{Tr}(\boldsymbol{\beta}(\boldsymbol{\alpha}^t\boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^\dagger(\boldsymbol{\alpha}^t)^\dagger)\boldsymbol{\beta}^\dagger)\right). \end{aligned} \tag{7.8}$$

Set $\boldsymbol{\gamma} = \boldsymbol{\alpha}^t\boldsymbol{U} = [\gamma_1, \gamma_2, \ldots, \gamma_{n_T}]$; since $\boldsymbol{U}$ is unitary, it follows that $\|\boldsymbol{\gamma}\| = \|\boldsymbol{\alpha}\|$. Then we may write

$$\boldsymbol{\alpha}^t\boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^\dagger(\boldsymbol{\alpha}^t)^\dagger = \boldsymbol{\gamma}^t\boldsymbol{D}(\boldsymbol{\gamma}^t)^\dagger = \lambda_1|\gamma_1|^2 + \lambda_2|\gamma_2|^2 + \cdots + \lambda_{n_T}|\gamma_{n_T}|^2. \tag{7.9}$$

Recalling that $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_{n_T} > 0$, we may further simplify the above expression to deduce that

$$\begin{aligned} \boldsymbol{\alpha}^t\boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^\dagger(\boldsymbol{\alpha}^t)^\dagger &= \lambda_{n_T}\left(\frac{\lambda_1}{\lambda_{n_T}}|\gamma_1|^2 + \frac{\lambda_2}{\lambda_{n_T}}|\gamma_2|^2 + \cdots + |\gamma_{n_T}|^2\right) \\ &\ge \lambda_{n_T}(|\gamma_1|^2 + |\gamma_2|^2 + \cdots + |\gamma_{n_T}|^2) \\ &= \lambda_{n_T}\|\boldsymbol{\gamma}\|^2 \\ &= \lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}||\boldsymbol{\alpha}||^2 \end{aligned} \tag{7.10}$$

where we have defined $\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}} = \lambda_{n_T}$, the minimum eigenvalue of the matrix $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger$.

It now follows that the conditional PEP in the equation (7.8) is

$$\begin{aligned} P_{\text{PEP 1}}(\boldsymbol{c} \to \boldsymbol{e}|\beta_i\alpha_j) &\leq \frac{1}{2}\exp\left(-\frac{\rho}{4}(\mathrm{Tr}(\boldsymbol{\beta}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}||\boldsymbol{\alpha}||^2\boldsymbol{\beta}^\dagger)\right) \\ &= \frac{1}{2}\exp\left(-\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}||\boldsymbol{\alpha}||^2(\mathrm{Tr}(\boldsymbol{\beta}\boldsymbol{\beta}^\dagger)\right) \\ &= \frac{1}{2}\exp\left(-\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}||\boldsymbol{\alpha}||^2||\boldsymbol{\beta}||^2\right) \\ &= \frac{1}{2}\exp\left(-\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}Y\right), \end{aligned} \tag{7.11}$$

where we recall that $Y = UV = ||\boldsymbol{\alpha}||^2||\boldsymbol{\beta}||^2$, from Appendix A.5.

We note that the bound on conditional PEP determined in (7.11) has the form ke^{-sY}, with $k = 1/2$ and $s = \frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}$, and $Y = UV$ with U, V *Chi-square* random variables with $2n_T$ and $2n_R$ degrees of freedom, respectively. It follows that we may apply an MGF-based approach to bound the average probability of error. That is, we deduce from (A.29) through (A.33) that the average probability of error for STC on a keyhole channel is bounded by

$$\begin{aligned} P_{\text{PEP 1}} &\leq kM_Y(-s) \\ &= \frac{1}{2}\,{}_2F_0\left(n_T, n_R; ; -\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}\right) \qquad (7.12) \\ &= \frac{1}{2}(\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}})^{-n_T}\left(\frac{\rho}{4}\right)^{-n_T}\Psi\left(n_T, n_T - n_R + 1; \left(\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}\right)^{-1}\right). \qquad (7.13) \end{aligned}$$

7.1.2 Using the Upper Bound $Q_2(x)$

Using the upper bound $Q_2(x)$ as given in (7.4) to bound the exact conditional PEP in (7.2) gives the bound

$$P_{\text{PEP}}(\boldsymbol{c} \to \boldsymbol{e}|\beta_i\alpha_j) \leq \frac{\exp\left(-\frac{\rho}{4}\mathrm{Tr}(\boldsymbol{H}\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger\boldsymbol{H}^\dagger)\right)}{\sqrt{2\pi\cdot\frac{\rho}{2}\mathrm{Tr}(\boldsymbol{H}\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger\boldsymbol{H}^\dagger)}}. \tag{7.14}$$

Repeating the argument of the preceding section, with $\boldsymbol{H} = \boldsymbol{\beta}\boldsymbol{\alpha}^t$, we deduce that

$$\mathrm{Tr}(\boldsymbol{H}\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^\dagger\boldsymbol{H}^\dagger) = \boldsymbol{\alpha}^t\boldsymbol{U}\boldsymbol{D}\boldsymbol{U}^\dagger(\boldsymbol{\alpha}^t)^\dagger\mathrm{Tr}(\boldsymbol{\beta}\boldsymbol{\beta}^\dagger) \geq \lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}||\boldsymbol{\alpha}||^2||\boldsymbol{\beta}||^2. \tag{7.15}$$

Hence we may bound the numerator of (7.14) from above and the denominator of

(7.14) from below to obtain

$$P_{\text{PEP}}(\boldsymbol{c} \rightarrow \boldsymbol{e}|\alpha_i\beta_j) \leq \frac{\exp(-\frac{\varrho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}Y)}{\sqrt{2\pi \cdot \frac{\varrho}{2}Y\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}}} = \frac{\exp(-\frac{\varrho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}Y)}{\sqrt{\pi\rho\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}} \cdot \sqrt{Y}}. \tag{7.16}$$

Recall that Y is defined as $Y = UV = ||\boldsymbol{\alpha}||^2||\boldsymbol{\beta}||^2$ with U and V Chi-square random variables with $2n_T$ and $2n_R$ degrees of freedom respectively. Hence to compute the average probability of error from the bound on condition PEP given in (7.16), we define a new term called the *modified MGF* of Y as

$$M_Y'(s) \triangleq E\left[\frac{e^{-sY}}{\sqrt{Y}}\right] = \int_0^\infty \frac{e^{-sy}}{\sqrt{y}}\, p_Y(y)dy. \tag{7.17}$$

Using the pdf of Y given in (A.31), the modified MGF of Y can be computed by

$$\begin{aligned}
M_Y'(s) &= \int_0^\infty \int_0^\infty \frac{t^{n_T-n_R-1}e^{-t-(s+\frac{1}{t})y}y^{n_R-\frac{3}{2}}}{\Gamma(n_T)\Gamma(n_R)}dtdy \\
&= \frac{1}{\Gamma(n_T)\Gamma(n_R)}\int_0^\infty \int_0^\infty t^{n_T-\frac{3}{2}-(n_R-\frac{1}{2})}e^{-t}e^{-(s+\frac{1}{t})y}y^{n_R-\frac{3}{2}}dtdy \\
&= \frac{1}{\Gamma(n_T)\Gamma(n_R)}\int_0^\infty \frac{t^{n_T-\frac{3}{2}}e^{-t}}{t^{n_R-\frac{1}{2}}}\frac{\Gamma\left(n_R-\frac{1}{2}\right)}{\left(s+\frac{1}{t}\right)^{n_R-\frac{1}{2}}}dt \\
&\quad \text{from } \textstyle\int_0^\infty x^n e^{-ax}dx = \frac{\Gamma(n+1)}{a^{n+1}},\ n > -1 \text{ and } a > 0 \\
&= \frac{\Gamma\left(n_R-\frac{1}{2}\right)}{\Gamma(n_R)\Gamma(n_T)}\int_0^\infty \frac{e^{-t}t^{n_T-\frac{3}{2}}}{(1+st)^{n_R-\frac{1}{2}}}dt \\
&= \frac{\Gamma\left(n_R-\frac{1}{2}\right)}{\Gamma(n_R)\Gamma(n_T)}\int_0^\infty \frac{e^{-\frac{u}{s}}\left(\frac{u}{s}\right)^{n_T-\frac{3}{2}}}{(1+u)^{n_R-\frac{1}{2}}}\frac{du}{s} \qquad \text{from setting } u = st \rightarrow du = sdt \\
&= \frac{\Gamma\left(n_R-\frac{1}{2}\right)}{\Gamma(n_R)\Gamma(n_T)}s^{-(n_T-\frac{1}{2})}\frac{\Gamma\left(n_T-\frac{1}{2}\right)}{\Gamma\left(n_T-\frac{1}{2}\right)}\int_0^\infty e^{-\frac{u}{s}}u^{(n_T-\frac{1}{2})-1}(1+u)^{(n_T-n_R+1)-(n_T-\frac{1}{2})-1}du \\
&= \frac{\Gamma\left(n_R-\frac{1}{2}\right)\Gamma\left(n_T-\frac{1}{2}\right)}{\Gamma(n_R)\Gamma(n_T)}s^{-(n_T-\frac{1}{2})}\Psi(n_T-\frac{1}{2}, n_T-n_R+1; s^{-1}) \\
&= \frac{\Gamma\left(n_R-\frac{1}{2}\right)\Gamma\left(n_T-\frac{1}{2}\right)}{\Gamma(n_R)\Gamma(n_T)}\,{}_2F_0\left(n_T-\frac{1}{2}, n_R-\frac{1}{2};;-s\right).
\end{aligned} \tag{7.18}$$

Hence, using the modified MGF computed in (7.18) and the conditional PEP in (7.16), that is, setting $k = \left(\sqrt{\pi\rho\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}}\right)^{-1}$ and $s = \frac{\varrho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}$, we deduce that the average

PEP of STC using the upper bound Q_2 is

$$\begin{aligned} P_{\text{PEP }2} &\leq \int_0^\infty \frac{\exp(-\frac{\rho}{4}Y\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}})}{\sqrt{\pi\rho\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}}\cdot\sqrt{Y}}\cdot p_Y(y)dy = \frac{1}{\sqrt{\pi\rho\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}}}M_Y'(\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}) \\ &= \frac{1}{\sqrt{\pi\rho\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}}}\frac{\Gamma(n_R-\frac{1}{2})}{\Gamma(n_R)}\frac{\Gamma(n_T-\frac{1}{2})}{\Gamma(n_T)}\,{}_2F_0(n_T-\frac{1}{2},n_R-\frac{1}{2};;-\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}). \end{aligned} \tag{7.19}$$

It is also written in the terms of the degenerate hypergeometric function as

$$P_{\text{PEP }2} \leq \frac{1}{\sqrt{\pi}}\frac{\Gamma(n_R-\frac{1}{2})}{\Gamma(n_R)}\frac{\Gamma(n_T-\frac{1}{2})}{\Gamma(n_T)}(\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}})^{-n_T}\left(\frac{\rho}{4}\right)^{-n_T}\Psi\left(n_T-\frac{1}{2},n_T-n_R+1;\left(\frac{\rho}{4}\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}}\right)^{-1}\right). \tag{7.20}$$

Consequently, we can summarize our proposed bound on the average PEP of erroneously decoding $\boldsymbol{e}$ for $\boldsymbol{c}$ over a keyhole channel as

$$P_{\text{PEP}} = \min(P_{\text{PEP }1}, P_{\text{PEP }2}) \tag{7.21}$$

where $P_{\text{PEP }1}$ and $P_{\text{PEP }2}$ are as defined in (7.12) and (7.19) respectively.

7.2 BLER and Union Bound Performance

Let $\mathcal{V}$ be a signal constellation, $\mathcal{V} = \{\boldsymbol{V}_l\}_{l=0}^{L-1}$, where the number of columns of V_l is equal to n_T, the number of transmitter antennas. The average PEP for a given transmitted V_l is

$$P_{\text{PEP}|V_l} \leq \sum_{l'=0,l'\neq l}^{L-1} P_{\text{PEP}}(l,l') \tag{7.22}$$

where $P_{\text{PEP}}(l,l')$ is defined in (7.21). We may assume that all codewords occur with the same probability, hence, the BLER of STC of order L for a keyhole channel is computed by

$$P_{\text{BLER}} = \frac{1}{L}\sum_{l=0}^{L-1} P_{\text{PEP}|V_l} \leq \frac{1}{L}\sum_{l=0}^{L-1}\sum_{l'=0,l'\neq l}^{L-1} P_{\text{PEP}}(l,l'). \tag{7.23}$$

In the case that $\mathcal{V}$ is suitably symmetric, *e.g.* $\mathcal{V}$ is a unitary group constellation, the BLER given in (7.23) is reduced to

$$P_{\text{BLER}} \leq \sum_{l=1}^{L-1} P_{\text{PEP}}(l, 0). \tag{7.24}$$

We note that a union bound on the block error rate of STC of order L can be approximated by

$$PU_{\text{BLER}} \leq (L-1) P_{\text{PEP}}(l, l'). \tag{7.25}$$

where l, l' are chosen so that $\lambda_{\min}^{\boldsymbol{c},\boldsymbol{e}} = \lambda_{\min} = \min(\lambda_{\min}^{l,l'})$ for all $l, l' = \{0, 1, \ldots, L-1\}$ and $l \neq l'$.

7.2.1 Simulation

We compare simulation results with the analytical BLER performance from (7.23) using the proposed bound on PEPs in (7.21), for a 2×2 OSTBC in [90]. Since this code is a group (in fact a subgroup of the special unitary group of rank 2, $SU(2)$), we can compute its BLER using (7.24). The eigenvalues of a codeword pair difference of 2×2 OSTBC are not distinct so the PEP and the rank and determinant design criterion of the equation (11) and (12) in [87] can not be applied.

The performance is considered by plotting BLER against SNR in dB, using the assumption of a keyhole channel described in Section 2.1.4. Figure 7.2 shows the BLER performance of 2×2 OSTBC using BPSK (which has $L = 4$ so the data rate is $R = 1.00$ bit/s) for $n_R = 1$, 2 and 3 receiver antennas. The analytical curves in Figure 7.2 are the function $\min(P_{\text{PEP }1}, P_{\text{PEP }2})$, as defined in (7.12) and (7.19). The generalized hypergeometric function ${}_2F_0(a, b; ; -z)$ is computed using the MATLAB with the built-in command `hypergeom([a,b],[],-z)`.

Using the upper bounds of the Q-function which arises in the expression for the exact conditional PEP yields a gap between the analytical curves and the simulations. However we can see that the proposed PEP will give a particularly tight upper bound on the simulation at high SNR.

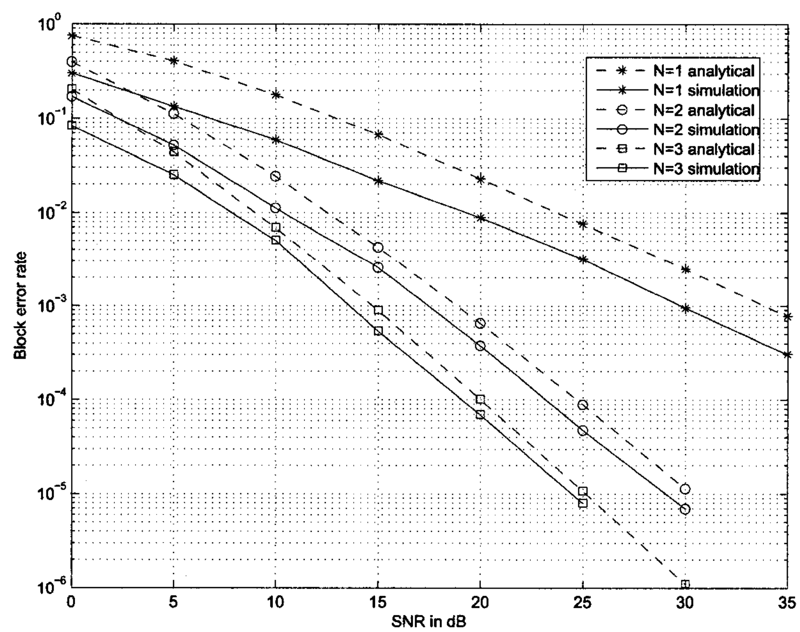

Figure 7.2: BLER performance of 2×2 OSTBC at $R = 1.00$ bit/s for $n_R = 1$, 2 and 3

Chapter 8

Affine Reflection Group Codes

This chapter presents a construction of *affine reflection group codes (ARGCs)*. The solution to the *initial vector* $\boldsymbol{x}_0$ and the *nearest-neighbour distance* $d_{\min}$ problem is presented for all irreducible affine reflection groups of rank $n \geq 2$, for varying stabilizer subgroups. Theorem 8.1.1 gives a closed-form solution for $\boldsymbol{x}_0$ as well as a formula for $d_{\min}$ of the corresponding ARGCs. In Corollary 8.1.1, we solve the initial vector problem also for the case that the stabilizer subgroup of $\boldsymbol{x}_0$ is nontrivial. The solutions to the initial vector problem, together with the corresponding nearest distance, for the corresponding irreducible affine reflection groups are summarized in Table 8.1.

In Section 8.2.1 we define the *bounded codeword regions*. These are designed to be maximally symmetric. We give examples of the size of these codes for irreducible affine reflection groups with bounded codeword regions in Table 8.2, together with the data relevant to their construction. We use a detailed analysis of the geometry of affine reflection groups to produce a decoding algorithm which is equivalent to the ML decoder, yet whose complexity depends only on the dimension of the vector space containing the codewords, and not on the number of codewords.

We note that other group codes have provided alternatives to ML decoders. In particular, the length-reduction algorithm which is proposed in [53, Section IV] for finite reflection groups can be adapted directly for use with ARGCs, but it would have high complexity for the case that the group code is large, or when the received vector lies very far from the fundamental domain.

A decoding algorithm for the corresponding group code is proposed in Section 8.2.2. The complexity of the proposed decoding algorithm depends only the rank n of the

ARG(that is, on the dimension of the space spanned by the roots), and not on the size L of the group code; this is in sharp contrast with the ML decoder. Consequently, when L is large relative to n, our decoding algorithm is more efficient.

We summarize the decoding algorithm briefly in Section 8.2.2 and Figure 8.3, showing how to efficiently reduce the decoding of a distant vector to one adjacent to the origin, where decoding techniques for finite reflection groups, such as the length-reduction algorithm of [53] may be applied effectively. We then proceed to describe the algorithm in detail, including proofs of correctness, in Section 8.2.2. The final step of the algorithm is illustrated in detail for the irreducible affine reflection groups $\mathcal{A}_2$, $\mathcal{B}_2$ and $\mathcal{A}_3$; in the first two of these we further optimize the algorithm by exploiting the many symmetries of the rank 2 groups.

We then illustrate the complete algorithm with several examples from $\mathcal{A}_2$ and $\mathcal{B}_2$ in Section 8.3, it may be further streamlined by exploiting additional symmetries of the group. The ARGCs presented in this thesis are in general not lattices, since the zero vector is not a codeword. They are however intimately related to the root lattices discussed in [13]. Namely, our ARGCs are certain unions of cosets of the corresponding coroot lattice, where the number of these cosets is at most the number of elements of the corresponding finite reflection group. This perspective offers yet another approach to the decoding problem considered in this paper. We compare our approach to this one in Section 8.3.4.

We let $\mathcal{G}_a$ be an (infinite) irreducible ARG of rank $n \geq 2$, which has a natural irreducible action on $\mathbb{R}^n$ by orthogonal affine transformations. The action of $\mathcal{G}_a$ restricted to any bounded portion of $\mathbb{R}^n$ (a **codeword region**) may be considered a nonlinear Slepian group code, in the sense that: the group acts by isometries; the codewords are generated by acting on $\boldsymbol{x}_0$ with the elements of the group; and, for a suitable choice of $\boldsymbol{x}_0$, they satisfy the nearest-neighbour equidistance property.

8.1 An Initial Vector and Nearest Distance

For a given irreducible ARG $\mathcal{G}_a$ of rank n with the simple system $\Delta = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_n\}$ and highest long root $\boldsymbol{\rho} = \sum_{i=1}^{n} a_i \boldsymbol{r}_i$ (see Section 2.2), we define the *fundamental* *domain* D_Δ of ARGC associated to the simple system Δ as

$$D = \{\boldsymbol{x} \in \mathbb{R}^n \colon \boldsymbol{x} \cdot \boldsymbol{r}_i \geq 0 \text{ for all } \boldsymbol{r}_i \in \Delta, \text{ and } \boldsymbol{x} \cdot \boldsymbol{\rho} \leq 1\}. \tag{8.1}$$

This is a compact region of $\mathbb{R}^n$, consisting of exactly one representative of each orbit of the action of $\mathcal{G}_a$ on $\mathbb{R}^n$. The boundary of the fundamental domain D_Δ is formed by the linear hyperplanes $H_{\boldsymbol{r}_i,0}$, $i = 1, \dots, n$, corresponding to the simple roots, together with the affine hyperplane $H_{\boldsymbol{\rho},1}$. The image of the fundamental domain under any element of the group is called a chamber; by construction, the chambers tessellate $\mathbb{R}^n$. Geometrically, each chamber is the closure of a connected component of the set obtained from $\mathbb{R}^n$ by deleting all the reflection hyperplanes, that is, of $\mathbb{R}^n \setminus \cup_{\boldsymbol{r}\in\Phi,\, k\in\mathbb{Z}} H_{\boldsymbol{r},k}$ where Φ is a root system of $\mathcal{G}_a$.

We next prove that the nearest neighbours in the orbit of a vector $\boldsymbol{x} \in D_\Delta$ under $\mathcal{G}_a$ are those in directly adjacent chambers.

Lemma 8.1.1. *Let $\boldsymbol{x} \in D_\Delta$ and consider the set $\mathcal{V} = \{g\boldsymbol{x} \colon g \in \mathcal{G}_a\}$. The nearest neighbours in $\mathcal{V}$ to $\boldsymbol{x}$ are in the set $\{S_{\boldsymbol{\rho},1}\boldsymbol{x}\} \cup \{S_{\boldsymbol{r}_i,0}\boldsymbol{x} \colon \boldsymbol{r}_i \in \Phi\}$.*

Proof. Since $\{S_{\boldsymbol{r},0} \colon \boldsymbol{r} \in \Delta\} \cup \{S_{\boldsymbol{\rho},1}\}$ is a generating set of $\mathcal{G}_a$, every $g \in \mathcal{G}_a$ can be written as a word in these generators (not necessarily uniquely). Choose a reduced expression for g (that is, a word of minimal length representing g); write it as $g = sg'$ for some s in the generating set and an element $g' = s^{-1}g \in \mathcal{G}_a$ of shorter length. We shall prove that $\|\boldsymbol{x} - g\boldsymbol{x}\| \geq \|\boldsymbol{x} - g'\boldsymbol{x}\|$, from which the desired result follows by induction.

If $g' = 1$ there is nothing to show; assume then that $g' \neq 1$. Since g has a reduced expression $g = sg'$ beginning with s, it follows from [39, Theorem 4.5] that the vectors $\boldsymbol{x}$ and $g'\boldsymbol{x}$ lie on the same side of the hyperplane H_s corresponding to the reflection s, with their images under s (that is, $s\boldsymbol{x}$ and $g\boldsymbol{x}$) symmetrically opposite. These four points form a nondegenerate trapezoid. The sides joining $g'\boldsymbol{x}$ to $g\boldsymbol{x}$, and $\boldsymbol{x}$ to $s\boldsymbol{x}$, are orthogonal to H_s and are bisected by H_s. The other two sides are congruent since

$$\|s\boldsymbol{x} - g\boldsymbol{x}\| = \|s(\boldsymbol{x} - g'\boldsymbol{x})\| = \|\boldsymbol{x} - g'\boldsymbol{x}\|.$$

As at least one of the interior angles opposite the diagonal from $\boldsymbol{x}$ to $g\boldsymbol{x}$ is obtuse, it follows by the law of cosines that the congruent sides are shorter than this diagonal.

This is the desired inequality $\|\boldsymbol{x} - g\boldsymbol{x}\| \geq \|\boldsymbol{x} - g'\boldsymbol{x}\|$. □

Let us now derive a formula for the best initial vector $\boldsymbol{x}_0 \in D_\Delta$. Set $\{\boldsymbol{\lambda}_i\}_{i=1}^n$ to be the dual basis to Δ, defined by $\boldsymbol{\lambda}_i \cdot \boldsymbol{r}_j = \delta_{ij}$. Then any initial vector $\boldsymbol{x}_0$ which lies in the fundamental domain D_Δ can be expressed in coordinates with respect to $\{\boldsymbol{\lambda}_i\}_{i=1}^n$ as

$$\boldsymbol{x}_0 = \sum_{i=1}^n b_i \boldsymbol{\lambda}_i \tag{8.2}$$

where, by (8.1), we have $b_i \geq 0$ for each $i \in \{1, 2, \ldots, n\}$ and $\sum_{i=1}^n a_i b_i \leq 1$. Using the affine reflection defined in (2.29), the distance between the initial vector $\boldsymbol{x}_0$ and its (affine) reflection $S_{\boldsymbol{r},k}\boldsymbol{x}_0$ can be computed via

$$\begin{aligned}
d(\boldsymbol{x}_0, S_{\boldsymbol{r},k}\boldsymbol{x}_0) &= \|\boldsymbol{x}_0 - S_{\boldsymbol{r},k}\boldsymbol{x}_0\| \\
&= \|\boldsymbol{x}_0 - \{\boldsymbol{x}_0 - ((\boldsymbol{x}_0, \boldsymbol{r}) - k)\frac{2\boldsymbol{r}}{(\boldsymbol{r}, \boldsymbol{r})}\}\| \\
&= |(\sum_{i=1}^n b_i \boldsymbol{\lambda}_i, \boldsymbol{r}) - k| \, \frac{2\|\boldsymbol{r}\|}{(\boldsymbol{r}, \boldsymbol{r})} \\
&= \frac{2}{\|\boldsymbol{r}\|} |\sum_{i=1}^n b_i (\boldsymbol{\lambda}_i, \boldsymbol{r}) - k|.
\end{aligned} \tag{8.3}$$

Now if $\boldsymbol{r}$ is the simple root $\boldsymbol{r}_i$, and $k = 0$, then since $\boldsymbol{\lambda}_j \cdot \boldsymbol{r}_i = 0$ unless $i = j$, and $\boldsymbol{\lambda}_i \cdot \boldsymbol{r}_i = 1$, the distance computed in (8.3) reduces to

$$d_i = \frac{2b_i}{\|\boldsymbol{r}_i\|}, \tag{8.4}$$

for $i = 1, 2, \ldots, n$. On the other hand, if $\boldsymbol{r} = \boldsymbol{\rho} = \sum_{i=1} a_i \boldsymbol{r}_i$, the highest long root, and $k = 1$, then we have

$$d_{\text{long}} = \frac{2}{\|\rho\|} \left(1 - \sum_{i=1}^n a_i b_i\right). \tag{8.5}$$

The optimal initial vector is the point in the fundamental domain D_Δ for which all nearest neighbours are equidistant. By Lemma 8.1.1 we deduce it is a vector for which

$$d_1 = \cdots = d_n = d_{\text{long}} = d. \tag{8.6}$$

We consequently have, from (8.4) and (8.5), $n + 1$ linear equations in the $n + 1$

unknowns $b_1, \ldots, b_n, d$. The system is consistent, and solving it yields the following theorem.

Theorem 8.1.1. *Let $\mathcal{G}_a$ be an irreducible ARG with simple roots $\{\boldsymbol{r}_i\}_{i=1}^n$ and highest long root $\boldsymbol{\rho} = \sum_{i=1}^n a_i \boldsymbol{r}_i$. Set*

$$d = \frac{2}{\|\boldsymbol{\rho}\| + \sum_{i=1}^n a_i \|\boldsymbol{r}_i\|}; \tag{8.7}$$

then

$$\boldsymbol{x}_0 = \sum_{i=1}^n \frac{d\|\boldsymbol{r}_i\|}{2} \boldsymbol{\lambda}_i \tag{8.8}$$

is the optimal initial vector for the ARGC for $\mathcal{G}_a$. The resulting nearest neighbour distance is d.

Proof: The proof follows from (8.4) and (8.5), setting of (8.6). This gives

$$\begin{aligned} d &= \frac{2}{\|\boldsymbol{\rho}\|}\left(1 - \sum_{i=1}^n a_i \frac{d\|\boldsymbol{r}_i\|}{2}\right) \\ &= \frac{2}{\|\boldsymbol{\rho}\|} - \frac{d}{\|\boldsymbol{\rho}\|}\sum_{i=1}^n a_i \|\boldsymbol{r}_i\| \\ d\left(1 + \frac{\sum_{i=1}^n a_i \|\boldsymbol{r}_i\|}{\|\boldsymbol{\rho}\|}\right) &= \frac{2}{\|\boldsymbol{\rho}\|} \\ d &= \frac{2}{\|\boldsymbol{\rho}\| + \sum_{i=1}^n a_i \|\boldsymbol{r}_i\|}. \end{aligned}$$

The initial vector $\boldsymbol{x}_0$ is then found by substituting (8.4), $b_i = d\|\boldsymbol{r}_i\|/2$, in (8.2). □

Theorem 8.1.1 addresses the case that the stabilizer of $\boldsymbol{x}_0$ is trivial. More generally, $\boldsymbol{x}_0$ could be chosen to lie on one or more of the walls of the fundamental domain, and thus be stabilized by the subgroup of $\mathcal{G}_a$ generated by the reflections in the corresponding hyperplanes; in Corollary 8.1.1 below, we give the solution to the initial vector problem, and calculate $d_{\min}$, in this more general case as well. We first require some notation.

Let $\Delta_p \subsetneq \Delta \cup \{\boldsymbol{\rho}\}$; we call Δ_p a set of *passive roots*, following the terminology of [54]. An initial vector for $\mathcal{G}_a$ with passive roots Δ_p is a vector $\boldsymbol{x}_0$ in the fundamental domain such that for all $\boldsymbol{r}_i \in \Delta$, $S_{\boldsymbol{r}_i,0}\boldsymbol{x}_0 = \boldsymbol{x}_0$ if and only if $\boldsymbol{r}_i \in \Delta_p$, and such that $S_{\boldsymbol{\rho},1}\boldsymbol{x}_0 = \boldsymbol{x}_0$ if and only if $\boldsymbol{\rho} \in \Delta_p$. In other words, the stabilizer of $\boldsymbol{x}_0$ is generated by the reflections (in the walls of the fundamental domain) corresponding to the roots in Δ_p. Denote by $\Delta \setminus \Delta_p = \{\boldsymbol{r} \in \Delta \colon \boldsymbol{r} \notin \Delta_p\}$ the complement of Δ_p in Δ.

Corollary 8.1.1. *The solution to the initial vector problem for a given set $\Delta_p \subsetneq \Delta \cup \{\boldsymbol{\rho}\}$ of passive roots is*

$$\boldsymbol{x}_0 = \sum_{\boldsymbol{r}_i \in \Delta \setminus \Delta_p} \frac{d\|\boldsymbol{r}_i\|}{2} \boldsymbol{\lambda}_i \tag{8.9}$$

where the minimum distance d is given by

$$d = \begin{cases} 2\left(\|\boldsymbol{\rho}\| + \sum_{\boldsymbol{r}_i \in \Delta\setminus\Delta_p} a_i \|\boldsymbol{r}_i\|\right)^{-1} & \text{if } \boldsymbol{\rho} \notin \Delta_p; \\ 2\left(\sum_{\boldsymbol{r}_i \in \Delta\setminus\Delta_p} a_i \|\boldsymbol{r}_i\|\right)^{-1} & \text{if } \boldsymbol{\rho} \in \Delta_p. \end{cases}$$

Proof. This is obtained by setting $d_i = 0$ if $\boldsymbol{r}_i \in \Delta_p$, and $d_{long} = 0$ if $\boldsymbol{\rho} \in \Delta_p$, and then equating the remaining distance values, as in the proof of Theorem 8.1.1. Note that in the special case $\Delta_p = \Delta$, we have $\boldsymbol{x}_0 = \boldsymbol{0}$ and the codewords are generated by strictly affine reflections of $\boldsymbol{0}$; these points form the *coroot lattice* of $\mathcal{G}_a$ [39, Prop 4.2]. □

Example 8.1.1. *Consider the irreducible ARG $\mathcal{B}_2$. From Table 2.2, the simple roots are $\boldsymbol{r}_1 = (1,0)$, $\boldsymbol{r}_2 = (-1,1)$ and the highest long root is $\boldsymbol{\rho} = (1,1) = 2\boldsymbol{r}_1 + \boldsymbol{r}_2$. Consequently the fundamental domain D_Δ is the shaded region shown in Figure 8.1. From Theorem 8.1.1 we calculate the nearest distance to be*

$$d = \frac{1}{1+\sqrt{2}}. \tag{8.10}$$

Thus we have $b_1 = \frac{1}{2+2\sqrt{2}}$ and $b_2 = \frac{1}{2+\sqrt{2}}$. The dual basis to $\{\boldsymbol{r}_1, \boldsymbol{r}_2\}$ is $\{\boldsymbol{\lambda}_1 = (1,1), \boldsymbol{\lambda}_2 = (0,1)\}$. Hence we conclude from (8.2) that the best initial vector is

$$\boldsymbol{x}_0 = b_1\boldsymbol{\lambda}_1 + b_2\boldsymbol{\lambda}_2 = \frac{1}{2+2\sqrt{2}}(1,1) + \frac{1}{2+\sqrt{2}}(0,1) = \left(\frac{1}{2+2\sqrt{2}}, \frac{1}{2}\right). \tag{8.11}$$

This vector points to the interior of the shaded region in Figure 8.1.

Example 8.1.2. *Consider $\mathcal{B}_2$ as in Example 8.1.1, but now $\Delta_p = \{\boldsymbol{r}_1\}$. By Corollary 8.1.1, the minimum distance is*

$$d = \frac{2}{\sqrt{2} + 1 \times \sqrt{2}} = \frac{1}{\sqrt{2}} \tag{8.12}$$

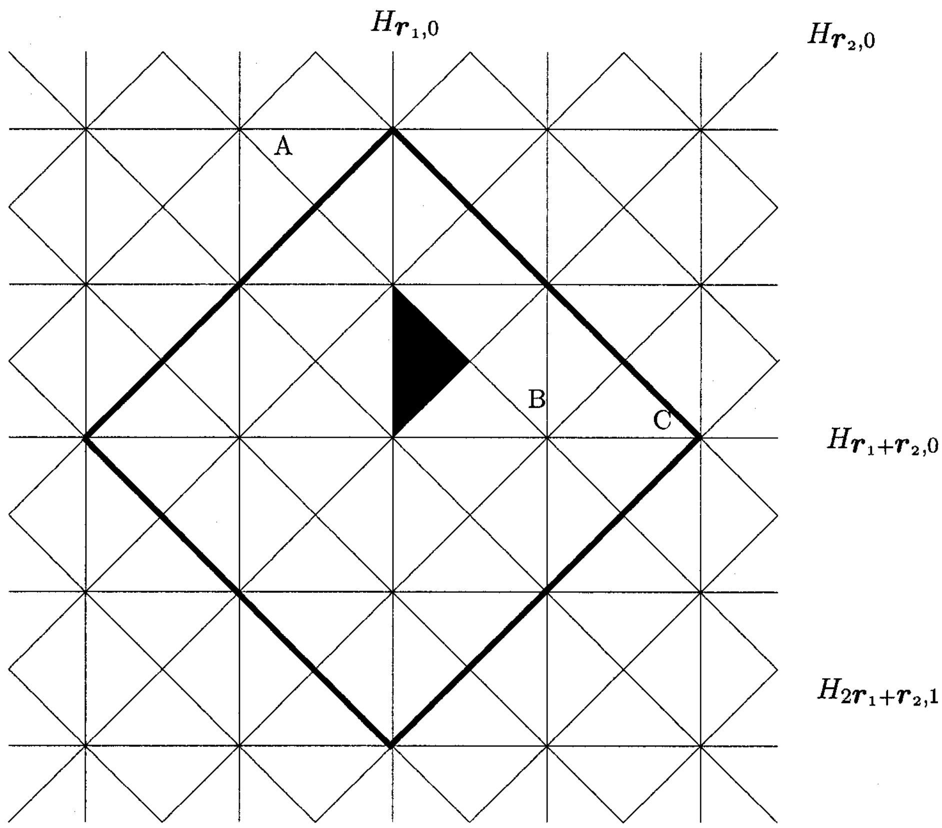

Figure 8.1: Hyperplanes and chambers of the ARG code $\mathcal{B}_2$. Each line is orthogonal to the corresponding root. The horizontal and vertical lines are at unit intervals. The shaded region is the fundamental domain; the heavy outline corresponds to the bounded codeword region $\mathcal{R}_2$ of Section 8.3.1.

and the optimal initial vector is

$$\boldsymbol{x}_0 = (0, \frac{1}{2}) \in H_{\boldsymbol{r}_1,0} \cap D_\Delta. \tag{8.13}$$

Example 8.1.3. *Consider $\mathcal{B}_2$ as in the preceding example, but now $\Delta_p = \{\boldsymbol{\rho}\}$. From Corollary 8.1.1, we have the minimum distance*

$$d = \frac{2}{2\|\boldsymbol{r}_1\| + 1\|\boldsymbol{r}_2\|} = \frac{2}{2+\sqrt{2}} \tag{8.14}$$

and the optimal initial vector is

$$\boldsymbol{x}_0 = \frac{d}{2}\boldsymbol{\lambda}_1 + \frac{d}{2}\sqrt{2}\boldsymbol{\lambda}_2 = (1 - \frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}), \tag{8.15}$$

which is the point on $H_{\boldsymbol{\rho},1}$ such that the line from the origin to $\boldsymbol{x}_0$ bisects the angle between the two linear hyperplanes $H_{\boldsymbol{r}_1,0}$ and $H_{\boldsymbol{r}_2,0}$.

Example 8.1.4. *Consider the irreducible ARG $\mathcal{G}_2$. From Table 2.2, the simple roots of $\mathcal{G}_2$ are $\boldsymbol{r}_1 = (1, 0)$ and $\boldsymbol{r}_2 = (-\frac{3}{2}, \frac{\sqrt{3}}{2})$. Its highest long root is $\boldsymbol{\rho} = 3\boldsymbol{r}_1 + 2\boldsymbol{r}_2 = (0, \sqrt{3})$. The hyperplanes and chambers are illustrated in Figure 8.2. (Note how the geometry of the hyperplanes and chambers is obtained from the root diagram: the short roots have length 1 so the corresponding hyperplanes $H_{\boldsymbol{r},1}$ contain the endpoint of $\boldsymbol{r}$ (and have $\boldsymbol{r}$ as normal vector); since the long roots have length $\sqrt{3}$, their corresponding hyperplanes $H_{\boldsymbol{r},k}$ are at a distance of $(\sqrt{3})^{-1}$ apart.)*

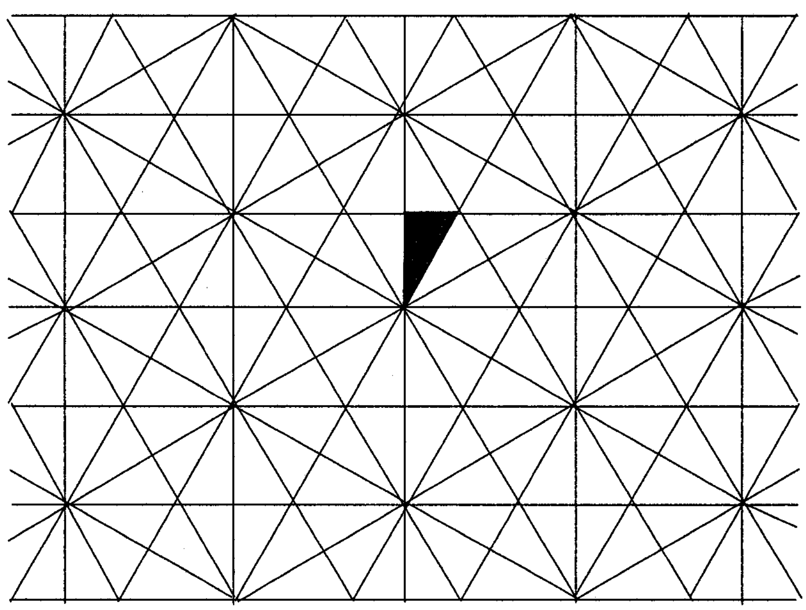

Figure 8.2: Hyperplanes and chambers for $\mathcal{G}_2$. The vertical lines are at unit intervals; the horizontal lines are $1/\sqrt{3}$ units apart. The shaded region is the fundamental domain.

Using Theorem 8.1.1, we find the nearest distance is

$$d = \frac{2}{\sqrt{3} + (3 \times 1 + 2 \times \sqrt{3})} = \frac{2}{3(\sqrt{3}+1)}. \tag{8.16}$$

Hence we have $b_1 = \frac{1}{3(\sqrt{3}+1)}$ and $b_2 = \frac{1}{\sqrt{3}+3}$. The dual basis to $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ are

$\boldsymbol{\lambda}_1 = (1, \sqrt{3})$ *and* $\boldsymbol{\lambda}_2 = (0, 2/\sqrt{3})$. *Therefore the best initial vector is*

$$\begin{aligned} \boldsymbol{x}_0 &= \frac{1}{3(\sqrt{3}+1)}(1, \sqrt{3}) + \frac{1}{\sqrt{3}+3}\left(0, \frac{2}{\sqrt{3}}\right) \\ &= \left(\frac{1}{3(\sqrt{3}+1)}, \frac{\sqrt{3}+2}{3(\sqrt{3}+1)}\right). \end{aligned} \tag{8.17}$$

A summary of the best initial vectors and the minimum distance $d_{\min}$ for each of the irreducible affine reflection groups is given in Table 8.1. The details of the remaining calculations are included in Appendix B.

Group	$\boldsymbol{x}_0$	$d_{\min}$
$\mathcal{A}_2$	$\left(\frac{1}{3}, \frac{1}{\sqrt{3}}\right)$	$\frac{2}{3}$
$\mathcal{A}_3$	$\frac{1}{4}\left(1, \sqrt{3}, \frac{\sqrt{3}(1+\sqrt{2})}{2}\right)$	$\frac{1}{2}$
* $\mathcal{A}_n$ $(n\geq 2)$	$\frac{\sqrt{2}}{(n+1)^2}(-1,-1,\ldots,-1,n) \in \mathbb{R}^{n+1}$	$\frac{2}{n+1}$
$\mathcal{B}_2$	$\left(\frac{1}{2+2\sqrt{2}}, \frac{1}{2}\right)$	$\frac{1}{1+\sqrt{2}}$
$\mathcal{B}_3$	$\left(\frac{1}{2+4\sqrt{2}}, \frac{1+\sqrt{2}}{2+4\sqrt{2}}, \frac{1}{2}\right)$	$\frac{1}{1+2\sqrt{2}}$
$\mathcal{B}_n$ $(n\geq 2)$	$\frac{1}{2(1+(n-1)\sqrt{2})}(1, 1+\sqrt{2}, 1+2\sqrt{2}, \ldots, 1+(n-1)\sqrt{2})$	$\frac{1}{1+(n-1)\sqrt{2}}$
$\mathcal{C}_n$ $(n\geq 3)$	$\frac{1}{2(2+(n-1)\sqrt{2})}(1, 1+\sqrt{2}, 1+2\sqrt{2}, \ldots, 1+(n-1)\sqrt{2})$	$\frac{1}{2+(n-1)\sqrt{2}}$
$\mathcal{D}_4$	$\frac{1}{6}(0,1,2,3)$	$\frac{1}{3\sqrt{2}}$
$\mathcal{D}_n$ $(n\geq 4)$	$\frac{1}{2(n-1)}(0,1,2,\ldots,n-1)$	$\frac{1}{(n-1)\sqrt{2}}$
$\mathcal{F}_4$	$\frac{1}{6(1+\sqrt{2})}(3\sqrt{2}+5, 2\sqrt{2}+1, \sqrt{2}+1, 1)$	$\frac{1}{3(1+\sqrt{2})}$
$\mathcal{G}_2$	$\left(\frac{1}{3(\sqrt{3}+1)}, \frac{\sqrt{3}+2}{3(\sqrt{3}+1)}\right)$	$\frac{2}{3(\sqrt{3}+1)}$
* $\mathcal{E}_6$	$\frac{1}{12}(0,1,2,3,4,-4,-4,4)$	$\frac{1}{6\sqrt{2}}$
* $\mathcal{E}_7$	$\frac{1}{18}(0,1,2,3,4,5,-\frac{17}{2},\frac{17}{2})$	$\frac{1}{9\sqrt{2}}$
$\mathcal{E}_8$	$\frac{1}{30}(0,1,2,3,4,5,6,23)$	$\frac{1}{15\sqrt{2}}$

Table 8.1: Initial vector and nearest distance of ARGCs. Here, * indicates that the initial vector is given in coordinates with respect to the ambient space used for the definition of the root vectors; see also the remarks preceding Table 2.2.

8.2 Decoding Algorithm

8.2.1 Bounded Codeword Regions

If no bounds are imposed, an infinite ARG will generate an infinite number of codewords. Thus, to restrict to the case of a finite set of codewords, we will define a bounded codeword region as follows.

Choose a root in the root system Φ. For $l \in \mathbb{R}$, such that $\exists \boldsymbol{r} \in \Phi$ and $\|\boldsymbol{r}\| = l$, let $\Phi(l) = \{\boldsymbol{r}^1, \boldsymbol{r}^2, \ldots, \boldsymbol{r}^k\} \subseteq \Phi$ denote the set of **all** roots of length l. In particular, for any $\boldsymbol{r} \in \Phi(l)$, it follows that $-\boldsymbol{r} \in \Phi(l)$ as well.[1] Choose a positive integer M; then we define the codeword region $\mathcal{R} = \mathcal{R}_M$ of *radius*[2] M by

$$\mathcal{R} = \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{r}^i \cdot \boldsymbol{x} \leq M \ \forall i \in \{1, 2, \ldots, k\}\}. \tag{8.18}$$

Several examples are given in Table 8.2, together with the number of codewords in $\mathcal{R}_M$. This number is calculated by noting that in the region of radius $M = 1$ for the long roots, the number of chambers equals the order of the corresponding Weyl group; as M increases, the volume of the region (and consequently the number of chambers, and hence codewords) increases by the factor M^n, where n is the rank of the group.

Group	Root Length l	$\#\ \Phi(l)$	Number of codewords in $\mathcal{R}_M$
$\mathcal{A}_n$	1	$n(n+1)$	$(n+1)!\ M^n$
$\mathcal{B}_n$	$\sqrt{2}$	$2n(n-1)$	$2^n n! M^n$
$\mathcal{C}_n$	2	$2n$	$2^n n! M^n$
$\mathcal{D}_n$	$\sqrt{2}$	$2n(n-1)$	$2^{n-1} n! M^n$
$\mathcal{E}_6$	$\sqrt{2}$	72	$51840 M^6$
$\mathcal{F}_4$	$\sqrt{2}$	24	$1152 M^4$
$\mathcal{G}_2$	1	6	$36 M^2$
$\mathcal{G}_2$	$\sqrt{3}$	6	$12 M^2$

Table 8.2: Some sample ARGCs with the number of codewords in a bounded codeword region $\mathcal{R}_M$.

[1] Consequently, for implementation purposes of the algorithm in Section 8.2.2, it suffices to consider $\Phi(l) \cap \Phi^+$ and then keep track of signs.

[2] The term "radius" is a misnomer in the case that $l \neq 1$, but we hope it will not cause confusion.

8.2.2 Proposed Decoding Algorithm

For a given received vector $\boldsymbol{y}$ and group code C, the problem of decoding is to search for the codeword vector $\boldsymbol{c} \in C$ which gives the closest distance $\|\boldsymbol{y} - \boldsymbol{c}\|$ over all $\boldsymbol{c} \in C$. This is the ML decoder. Consider now a group code generated from an ARG via $\boldsymbol{c}_g = g\boldsymbol{x}_0$ for all $g \in \mathcal{G}_a$.

Lemma 8.2.1. *The maximum-likelihood decoder is equivalent to finding the codeword vector $\boldsymbol{c}_g$ in the chamber containing the received vector $\boldsymbol{y}$.*

Proof. First note that since each chamber contains exactly one representative of each orbit of the group acting on $\mathbb{R}^n$, each chamber contains exactly one codeword. This codeword lies in the interior of the chamber, unless the stabilizer (and Δ_p) is nontrivial, in which case it lies on the boundary of the chamber.

The same geometric argument as was used in the proof of Lemma 8.1.1 now applies. Namely, given any codeword $\boldsymbol{c}$, if there exists some hyperplane H separating $\boldsymbol{y}$ and $\boldsymbol{c}$, then by the law of cosines, $\boldsymbol{y}$ is closer to the reflection $\boldsymbol{c}'$ of $\boldsymbol{c}$ in H than to $\boldsymbol{c}$; by construction, $\boldsymbol{c}'$ is another codeword. Consequently the closest codeword must be the unique codeword in the same chamber as $\boldsymbol{y}$. □

Summary of the Decoding Algorithm

The proposed decoding algorithm described in Figure 8.3 works as follows. If the codeword region $\mathcal{R}$ is all of $\mathbb{R}^n$, then Steps 1 and 2 are ignored. Let us assume that $\Delta_p = \emptyset$, for simplicity.

Step 1 consists of checking if the received vector $\boldsymbol{y}$ is outside of the bounds determined by $\mathcal{R}$. If so, then we find the closest point to $\boldsymbol{y}$ on the boundary of the region $\mathcal{R}$ using Proposition 8.2.1, and use this to identify a point $\boldsymbol{u}$ on the boundary of the *chamber* closest to $\boldsymbol{y}$, using Proposition 8.2.2. We then rename $\boldsymbol{y} = \boldsymbol{u}$.

Step 2 checks to see if $\boldsymbol{y}$ is exactly on the boundary of $\mathcal{R}$. If so, then using Proposition 8.2.3 it is scaled so that it lies on the interior of the corresponding chamber.

Finally, given a point $\boldsymbol{y}$ in the interior of $\mathcal{R}$, lying in a chamber D', **Step 3** decodes to the codeword on the interior of D' as follows. First identify a vertex $\boldsymbol{v} \in D'$ which is of the same *type* as the origin, that is, for which translation $T_{\boldsymbol{v}}$ by $\boldsymbol{v}$ is an isometry of the tessalated space. Then $T_{(-\boldsymbol{v})}D'$ is a chamber adjacent to the origin. If the codeword it contains is $\boldsymbol{c}$, then the closest codeword to $\boldsymbol{y}$ is $T_{\boldsymbol{v}}(\boldsymbol{c})$; this is Proposition 8.2.4.

To find the codeword $\boldsymbol{c}$, one may apply decoding algorithms from the corresponding *finite* reflection group, such as the length reduction algorithm of [53], or the permutation decoding algorithms of [54]. Alternatively, where the the geometry of the group is well understood (for example, in low rank cases) one can set up a decision tree. This latter novel method is illustrated in detail in Sections 8.2.3 and 8.2.4, below; the complete Step 3 is illustrated in Sections 8.2.3 through 8.2.6.

Proposed Decoding Algorithm

Input

Denote the received vector by $\boldsymbol{y} \in \mathbb{R}^n$. Recall the set of roots of length l was $\Phi(l) = \{\boldsymbol{r}^1, \ldots, \boldsymbol{r}^k\}$ and the codeword region $\mathcal{R} = \mathcal{R}_M$ is defined as in (8.18).

Step 1: Is $\boldsymbol{y}$ out of bounds?

Evaluate $\boldsymbol{r}^1 \cdot \boldsymbol{y} = a^1, \boldsymbol{r}^2 \cdot \boldsymbol{y} = a^2, \ldots, \boldsymbol{r}^k \cdot \boldsymbol{y} = a^k$. If each a^i satisfies $a^i < M$, then the received vector $\boldsymbol{y}$ is already in the interior of the codeword region; go to Step 3. If $a^i = M$ for some i, and $a^j \leq M$ for all j, then $\boldsymbol{y}$ is on the boundary; proceed to Step 2. But if any $a^i > M$, then $\boldsymbol{y}$ is out of bounds; we correct it as follows.

We first remark that if $\mathcal{R}$ were an n-dimensional ball of radius M, then the closest point in $\mathcal{R}$ to $\boldsymbol{y}$ would be $(M/\|\boldsymbol{y}\|)\boldsymbol{y}$. However, the codeword region $\mathcal{R}$ is an n-dimensional convex "polygon", so the closest point is found instead using the orthogonal projection of $\boldsymbol{y}$ onto the boundary of $\mathcal{R}$.

To simplify the notation, write $H_i = H_{\boldsymbol{r}^i, M}$, for each $i \in \{1, 2, \ldots, k\}$, for the boundary hyperplanes of $\mathcal{R}$, and let $H_{i_1 i_2 \ldots i_m} = H_{i_1} \cap H_{i_2} \cap \ldots \cap H_{i_m}$. Then by construction, the intersections $\mathcal{R} \cap H_i$ are nonempty; these are the *faces* of the boundary of $\mathcal{R}$. For each $j_1, j_2, \cdots, j_m$ such that $\mathcal{R} \cap H_{ij_1 \cdots j_m} \neq \emptyset$, we have that $\mathcal{R} \cap H_{ij_1 \cdots j_m}$ is a *corner* on the boundary of the i^{th} face $\mathcal{R} \cap H_i$, of dimension at least $n - (m+1)$.

The point of $\mathcal{R}$ closest to $\boldsymbol{y}$ will be a point on some $\mathcal{R} \cap H_{i_1 \cdots i_m}$. To find it we proceed as follows.

Lemma 8.2.2. *Find $i \in \{1, 2, \cdots, k\}$ so that $\boldsymbol{r}^i \cdot \boldsymbol{y}$ is maximal. Then the i^{th} face $\mathcal{R} \cap H_i$ is the one closest to $\boldsymbol{y}$.*

Proof. Set $t = \boldsymbol{r}^i \cdot \boldsymbol{y}$. By the maximality of $t > M$, we know that $\frac{M}{t}\boldsymbol{y}$ satisfies $\boldsymbol{r}^j \cdot \frac{M}{t}\boldsymbol{y} \leq M$ for all $j \in \{1, 2, \ldots, k\}$; hence $\frac{M}{t}\boldsymbol{y} \in \mathcal{R} \cap H_i$. The maximality of t

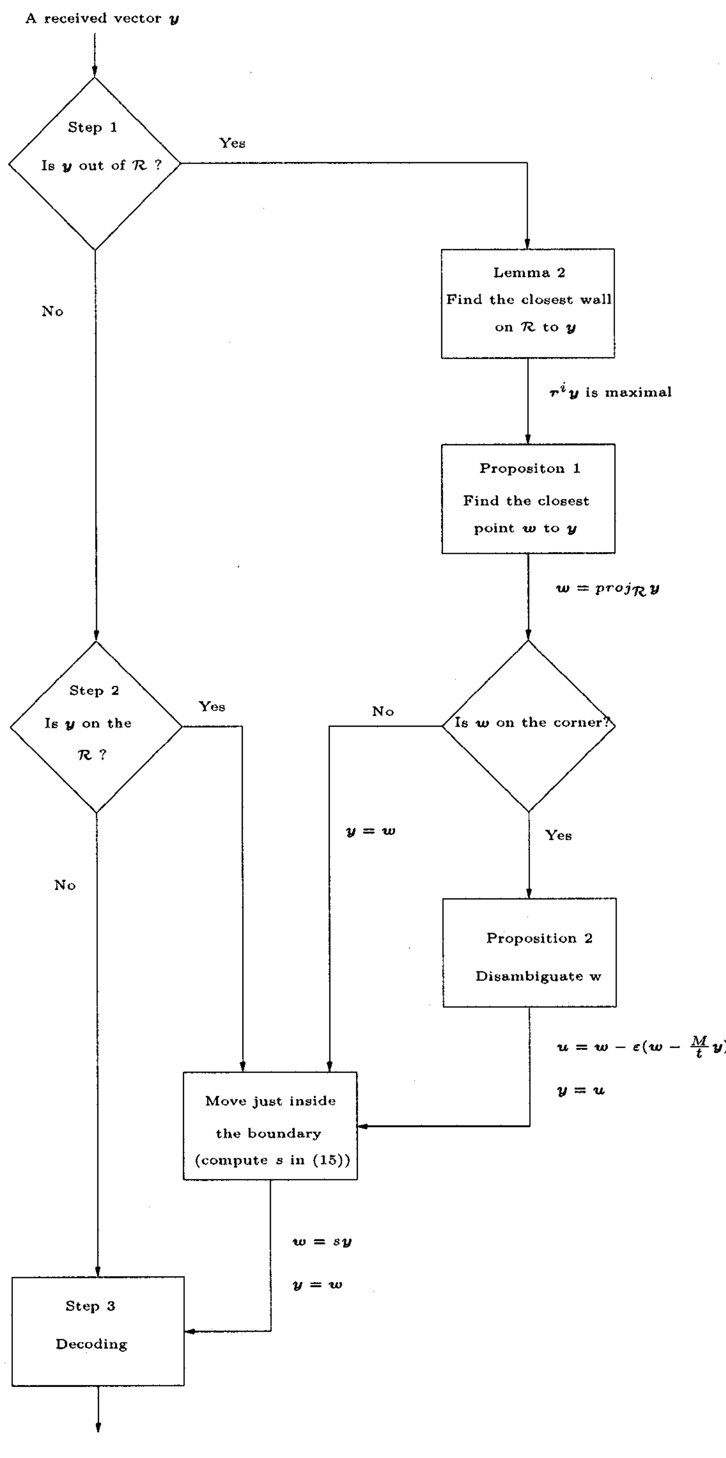

Figure 8.3: Proposed decoding algorithm

furthermore ensures that $s\boldsymbol{y} \notin \mathcal{R}$ for all $s > \frac{M}{t}$. We claim that this implies that $\boldsymbol{y}$ is itself closest to the ith face, as follows.

For any $j \neq i$, consider the linear hyperplane H_j^i defined by $(\boldsymbol{r}^i - \boldsymbol{r}^j) \cdot \boldsymbol{x} = 0$. Since $\|\boldsymbol{r}^i\| = \|\boldsymbol{r}^j\|$, we have that $(\boldsymbol{r}^i - \boldsymbol{r}^j) \cdot \boldsymbol{r}^i = \|\boldsymbol{r}^i\|^2 - \boldsymbol{r}^i \cdot \boldsymbol{r}^j = -(\boldsymbol{r}^i - \boldsymbol{r}^j) \cdot \boldsymbol{r}^j$. We conclude that H_j^i bisects the angle between H_i and H_j; it also contains H_{ij}. Hence, H_j^i divides $\mathbb{R}^n$ into those points closer to the ith face and those closer to the jth face. Since the line through $\boldsymbol{y}$ and the origin cannot meet the linear hyperplane H_j^i unless it is contained in it, we conclude that $\boldsymbol{y}$ and $\frac{M}{t}\boldsymbol{y}$ lie on the same side of H_j^i, and thus are both closer to $\mathcal{R} \cap H_i$. □

We can now state the algorithm.

Proposition 8.2.1. *Identify i, the index of the closest face, from Lemma 8.2.2. Calculate $proj_{H_i}\boldsymbol{y}$. If this is in $\mathcal{R}$, then $\boldsymbol{w} = proj_{H_i}\boldsymbol{y}$. Otherwise, proceed inductively with $m \geq 1$: given that $proj_{H_{ii_1\cdots i_{m-1}}}\boldsymbol{y} \notin \mathcal{R}$ for all $m-1$-element subsets $\{\boldsymbol{r}_{i_1}, \ldots, \boldsymbol{r}_{i_{m-1}}\} \subset \Phi(l)$, calculate $proj_{H_{ii_1\cdots i_m}}\boldsymbol{y}$ for every m-element subset $\{\boldsymbol{r}_{i_1}, \ldots, \boldsymbol{r}_{i_m}\} \subseteq \Phi(l)$. If any of these projections is in $\mathcal{R}$, then the closest such is $\boldsymbol{w}$; otherwise, proceed to $m+1$. This algorithm yields $\boldsymbol{w}$, the closest point on the boundary of $\mathcal{R}$ to $\boldsymbol{y}$.*

Proof. We first note that the process described in the Proposition will terminate after at most n steps, since any vertex $\boldsymbol{v}$ of $\mathcal{R} \cap H_i$ arises as $H_{ij_1\cdots j_{n-1}} = \{\boldsymbol{v}\}$ for some choice of $j_1, \ldots j_{n-1} \in \{1, 2, \ldots, k\}$, and the projection $\text{proj}_{H_{ij_1\cdots j_{n-1}}}\boldsymbol{y}$ gives $\boldsymbol{v} \in \mathcal{R}$, which is in range.

Furthermore, since $U \subset V$ implies that the distance between a vector $\boldsymbol{y}$ and the subset U is greater than or equal to the distance between $\boldsymbol{y}$ and V, and that the orthogonal projection identifies these closest points, we conclude that the inductive nature of this algorithm will correctly identify $\boldsymbol{w}$. □

Remark 8.2.1. *Since any corner of the ith face is defined by intersections of higher-dimensional corners, the calculations of Proposition 8.2.1 can be limited to those $i_1, i_2, \ldots i_m$ such that $i_j \neq i$ and $H_i \cap H_{i_j} \cap \mathcal{R} \neq \emptyset$, that is, to those i_j which define the $n-2$-dimensional corners of the ith face.*

Remark 8.2.2. *To apply the Proposition more concretely, given an* orthonormal *basis $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ of the linear subspace parallel to $H_{i_1 i_2\cdots i_m}$, and numbers $M_1, M_2, \ldots, M_m$*

such that

$$H_{i_1 i_2 \cdots i_m} = \{\boldsymbol{x} \in \mathbb{R}^n \colon \alpha_i \cdot \boldsymbol{x} = M_i, i \in \{1, 2, \ldots, m\}\}, \tag{8.19}$$

we calculate the orthogonal projection of $\boldsymbol{y}$ *onto* $H_{i_1 i_2 \cdots i_m}$ *via*

$$proj_{H_{i_1 i_2 \cdots i_m}} \boldsymbol{y} = \boldsymbol{y} - \sum_{i=1}^{m} (\alpha_i \cdot \boldsymbol{y} - M_i)\alpha_i. \tag{8.20}$$

In general the roots in $\Phi(l)$ *are not themselves orthogonal, and hence cannot be used for this formula. An important exception follows below.*

Corollary 8.2.1. *If* $\mathcal{G}_a = \mathcal{B}_n$ *with* $l = 1$ *and the bounded codeword region* $\mathcal{R} = \mathcal{R}_M$*, or if* $\mathcal{G}_a = \mathcal{C}_n$ *with* $l = 2$ *and the bounded codeword region* $\mathcal{R} = \mathcal{R}_{2M}$*, then the closest point on the boundary of* $\mathcal{R}$ *to the received word* $\boldsymbol{y} = (y_1, y_2, \cdots, y_n)$ *is*

$$\boldsymbol{w} = (y_1^*, y_2^*, \cdots, y_n^*) \tag{8.21}$$

where for each $i \in \{1, 2, \ldots, n\}$ *we define*

$$y_i^* = \begin{cases} y_i & \text{if } -M \leq y_i \leq M; \\ M & \text{if } y_i > M; \\ -M & \text{if } y_i < -M. \end{cases} \tag{8.22}$$

Proof. In $\mathcal{B}_n$, $\Phi(1)$ consists of the orthonormal standard basis of $\mathbb{R}^n$, so orthogonal projection, as per Remark 8.2.2, amounts to independently projecting each coordinate to the interval $[-M, M]$. The case for $\mathcal{C}_n$ is similar, where $\Phi(2)$ consists of the standard basis vectors scaled by a factor of 2. □

Now Proposition 8.2.1 gives the point $\boldsymbol{w}$ on $\mathcal{R}$ closest to $\boldsymbol{y}$; but unless $\boldsymbol{w}$ is simply equal to $proj_{H_i}\boldsymbol{y}$, (in which case, decoding $\boldsymbol{w}$ yields the codeword closest to $\boldsymbol{y}$), our construction has chosen $\boldsymbol{w}$ on a corner, and hence on the boundary of at least one other hyperplane, and thus chamber, which is *not* the closest.

To disambiguate $\boldsymbol{w}$, we recall that the closest chamber meets the i^{th} face $\mathcal{R} \cap H_i$. Thus translating $\boldsymbol{w}$ a small amount in the direction of the point of intersection $\mathbb{R}\boldsymbol{y} \cap H_i = \frac{M}{\boldsymbol{r}^i \cdot \boldsymbol{y}} \boldsymbol{y} \in H_i$ will identify the correct chamber to decode to, as in the following proposition. Let $\lceil a \rceil$ denote the least integer greater than or equal to a; we also later use $\lfloor a \rfloor$ to denote the greatest integer less than or equal to a.

Proposition 8.2.2. *Let $\mathcal{R} \cap H_i$ be the closest face to $\boldsymbol{y}$ and set $t = \boldsymbol{r}^i \cdot \boldsymbol{y}$ (as in Lemma 8.2.2) and $\boldsymbol{w}$ as in Proposition 8.2.1. Define the direction vector $\boldsymbol{d} = \boldsymbol{w} - \frac{M}{t}\boldsymbol{y}$. Let $\Phi_{\boldsymbol{y}}$ be the set of all root vectors $\boldsymbol{r} \in \Phi$ with the property that $\boldsymbol{r} \cdot \boldsymbol{d} > 0$. Then define*

$$\varepsilon = \frac{1}{2} \min \left\{ \left(\frac{\boldsymbol{r} \cdot \boldsymbol{w} - \lceil \boldsymbol{r} \cdot \boldsymbol{w} \rceil + 1}{\boldsymbol{r} \cdot \boldsymbol{d}} \right) : \boldsymbol{r} \in \Phi_{\boldsymbol{y}} \right\} > 0 \tag{8.23}$$

and set

$$\boldsymbol{u} = \boldsymbol{w} - \varepsilon \boldsymbol{d}. \tag{8.24}$$

This is a vector on the boundary of $\mathcal{R}$ which will decode to the closest codeword to $\boldsymbol{y}$.

Proof. Note that the direction vector $\boldsymbol{d}$ lies parallel to H_i. Recall from Lemma 8.2.2 that $\frac{M}{t}\boldsymbol{y}$ lies in some H_{ij} if and only if $\boldsymbol{y}$ is equidistant from both the ith and jth faces. Hence when i is unique (the generic case), $-\boldsymbol{d}$ points towards the interior of the ith face, thus choosing the side on which lies the chamber closest to $\boldsymbol{y}$.

More precisely, let us first verify that $\boldsymbol{u}$ shares a chamber in common with $\boldsymbol{w}$. We need to show that for *every* root $\boldsymbol{r} \in \Phi$, $\boldsymbol{u}$ and $\boldsymbol{w}$ lie between the same pair of walls defined by $\boldsymbol{r}$; or in other words, that the numbers $\boldsymbol{r} \cdot \boldsymbol{u}$ and $\boldsymbol{r} \cdot \boldsymbol{w}$ lie between the same pair of consecutive integers.

For each $\boldsymbol{r} \in \Phi$, one of two cases holds:

- First case: one of $\pm \boldsymbol{r}$ lies in $\Phi_{\boldsymbol{y}}$. Without loss of generality, suppose it is $\boldsymbol{r}$. Then $\boldsymbol{r} \cdot \boldsymbol{u} < \boldsymbol{r} \cdot \boldsymbol{w}$ by the definition of $\Phi_{\boldsymbol{y}}$ and

$$\begin{aligned}
\boldsymbol{r} \cdot \boldsymbol{u} &= \boldsymbol{r} \cdot \boldsymbol{w} - \varepsilon(\boldsymbol{r} \cdot \boldsymbol{d}) \\
&\geq \boldsymbol{r} \cdot \boldsymbol{w} - \frac{1}{2}(\boldsymbol{r} \cdot \boldsymbol{w} - \lceil \boldsymbol{r} \cdot \boldsymbol{w} \rceil + 1) \\
&= \frac{1}{2}(\boldsymbol{r} \cdot \boldsymbol{w} + \lceil \boldsymbol{r} \cdot \boldsymbol{w} \rceil - 1) \\
&> \lceil \boldsymbol{r} \cdot \boldsymbol{w} \rceil - 1.
\end{aligned}$$

  Thus $\lceil \boldsymbol{r} \cdot \boldsymbol{w} \rceil \geq \boldsymbol{r} \cdot \boldsymbol{w} > \boldsymbol{r} \cdot \boldsymbol{u} > \lceil \boldsymbol{r} \cdot \boldsymbol{w} \rceil - 1$ which implies that $\boldsymbol{u}$ and $\boldsymbol{w}$ lie on the same side of each hyperplane $H_{\boldsymbol{r},l}$, $l \in \mathbb{Z}$.

- Second case: $\boldsymbol{r} \cdot \boldsymbol{d} = 0$, so $\boldsymbol{r} \cdot \boldsymbol{w} = \boldsymbol{r} \cdot (\frac{M}{t}\boldsymbol{y})$. In this case, the vector $\boldsymbol{d}$ is parallel to the walls $H_{\boldsymbol{r},l}$, so $\boldsymbol{u}$ and $\boldsymbol{w}$ will lie between the same pairs of walls, whatever the value of ε.

Now suppose that $\boldsymbol{w}$ was on a corner H_{ij} of the ith face but that $\frac{M}{t}\boldsymbol{y}$ was not. Then we have $\boldsymbol{r}_j \cdot \boldsymbol{w} = M > \boldsymbol{r}_j \cdot (\frac{M}{t}\boldsymbol{y})$, which implies $\boldsymbol{r}_j \cdot \boldsymbol{d} > 0$ and $\boldsymbol{r}_j \cdot \boldsymbol{u} < M$, by construction. Thus $\boldsymbol{u}$ is not on the corner of the i face.

Hence we have shown that ε is an amount sufficient to remove the ambiguity of $\boldsymbol{w}$ but not large enough to allow $\boldsymbol{u}$ to cross any interior walls of $\mathcal{R}$. □

We rename $\boldsymbol{y} = \boldsymbol{u}$, and continue.

Step 2: Is $\boldsymbol{y}$ on the boundary of $\mathcal{R}$?

Now, given a vector $\boldsymbol{y}$ on the boundary of the codeword region $\mathcal{R}$ (in particular, as arises from the result of Step 1) we would be equally likely to decode inside as outside the region. Hence we scale the vector by a factor of $0 < s < 1$ to put it in the interior of $\mathcal{R}$. As in Proposition 8.2.2, the scaling factor s must be chosen carefully so that $\boldsymbol{y}$ and $\boldsymbol{w} = s\boldsymbol{y}$ lie on the same side of all internal walls of the codeword region, that is, in the same chamber, and hence decode to the same element.

Proposition 8.2.3. *For each root $\boldsymbol{r}$ in Φ^+, set $a_{\boldsymbol{r}} = \boldsymbol{r} \cdot \boldsymbol{y}$ and define*

$$s = \frac{1}{2}\max\left\{\frac{\lceil |a_{\boldsymbol{r}}| \rceil + |a_{\boldsymbol{r}}| - 1}{|a_{\boldsymbol{r}}|} : \boldsymbol{r} \in \Phi^+, a_{\boldsymbol{r}} \neq 0\right\} < 1. \tag{8.25}$$

Then $\boldsymbol{w} = s\boldsymbol{y}$ is a vector in the same chamber as $\boldsymbol{y}$ and in the interior of the bounded codeword region $\mathcal{R}$.

Proof. Since for $a > 0$, $\frac{1}{2}(\lceil a \rceil + a - 1) \geq \lceil a \rceil - 1$, we have for each $\boldsymbol{r} \in \Phi^+$ such that $a_{\boldsymbol{r}} \neq 0$ that $\lceil |a_{\boldsymbol{r}}| \rceil \geq |a_{\boldsymbol{r}}| > s|a_{\boldsymbol{r}}| \geq \lceil |a_{\boldsymbol{r}}| \rceil - 1$. Noting that $a_{\boldsymbol{r}} = \boldsymbol{r} \cdot \boldsymbol{y}$ and $sa_{\boldsymbol{r}} = \boldsymbol{r} \cdot \boldsymbol{w}$, we conclude that $\boldsymbol{w}$ and $\boldsymbol{y}$ lie between the same two adjacent affine hyperplanes corresponding to $\boldsymbol{r}$. On the other hand, if $a_{\boldsymbol{r}} = 0$, then $\boldsymbol{y} \in H_{\boldsymbol{r},0}$, which is a linear subspace, and so $s\boldsymbol{y} \in H_{\boldsymbol{r},0}$ as well. We conclude that $\boldsymbol{w}$ and $\boldsymbol{y}$ lie in the same chamber; moreover, if $\boldsymbol{y}$ was on the boundary of the codeword region $\mathcal{R}$ then, since $s < 1$, we have that $\boldsymbol{w}$ is in its interior. □

We rename $\boldsymbol{y} = \boldsymbol{w}$, and continue.

Step 3: Decoder for elements on the interior of the codeword region

Now suppose (by renaming as necessary) that $\boldsymbol{y}$ is a received codeword on the interior of the codeword region. For each root $\boldsymbol{r} \in \Phi^+$, define $a_{\boldsymbol{r}} = \boldsymbol{r} \cdot \boldsymbol{y}$. Then the chamber containing $\boldsymbol{y}$ is uniquely identified as the set of points $\boldsymbol{x}$ such that for all $\boldsymbol{r} \in \Phi^+$, $\lfloor a_{\boldsymbol{r}} \rfloor \leq \boldsymbol{r} \cdot \boldsymbol{x} \leq \lfloor a_{\boldsymbol{r}} \rfloor + 1$, since the chambers are defined by the hyperplanes $H_{\boldsymbol{r},k}$ with $k \in \mathbb{Z}$. To decode $\boldsymbol{y}$, we need to find the codeword in this chamber. We present the general solution first, and then illustrate it, together with some decision tree optimizations of it, below.

We first note that if $\boldsymbol{r}(1), \cdots, \boldsymbol{r}(n)$ are n linearly independent roots and $\boldsymbol{p} = [p_1\ p_2\ \ldots\ p_n]^T \in \mathbb{Z}^n$, then the intersection of the n corresponding hyperplanes consists of a single point, a vertex of a chamber

$$H_{\boldsymbol{r}(1),p_1} \cap H_{\boldsymbol{r}(2),p_2} \cap \cdots \cap H_{\boldsymbol{r}(n),p_n} = \{\boldsymbol{v}\},$$

whose coordinates are given by

$$\boldsymbol{v} = \boldsymbol{P}^{-1}\boldsymbol{p}, \tag{8.26}$$

where $\boldsymbol{P}$ is the matrix with row vectors $\boldsymbol{r}(1)$, $\boldsymbol{r}(2)$, ..., $\boldsymbol{r}(n)$.

Now suppose that we choose a vertex $\boldsymbol{v}$ of the chamber containing $\boldsymbol{y}$ which has the property that translation by $\boldsymbol{v}$ is an element of the ARG $\mathcal{G}_a$; it then clearly induces an isometry on the tessalated space[3]. Such a vertex $\boldsymbol{v}$ may be determined as follows.

The translations contained in the ARG $\mathcal{G}_a$ are generated by elements of the form $S_{\boldsymbol{r},1}S_{\boldsymbol{r}}$ with $\boldsymbol{r} \in \Delta$, which act on $\boldsymbol{x} \in \mathbb{R}^n$ via the translation:

$$S_{\boldsymbol{r},1}S_{\boldsymbol{r}}(\boldsymbol{x}) = \boldsymbol{x} + \frac{2}{\|\boldsymbol{r}\|^2}\boldsymbol{r},$$

Hence the vertices in question are those of the form

$$\boldsymbol{v} = \sum_{i=1}^{n} \frac{2c_i}{\|\boldsymbol{r}_i\|^2}\boldsymbol{r}_i, \tag{8.27}$$

for some $c_i \in \mathbb{Z}$, $1 \leq i \leq n$, and $\boldsymbol{r}_i \in \Delta$. From Chapter 2, we can see that this is the coroot lattice. We note also that while some vertices of the chambers may be defined by

[3]Such vectors are elements of the coroot lattice of $\mathcal{G}_a$; more generally one may use any vertex belonging to the coweight lattice [39, Prop 4.2].

the intersection of hyperplanes corresponding to only a subset of the positive roots (as occurs in $\mathcal{B}_2$, for example; see Figure 8.1), those vertices of the same type as the origin are defined by common intersections of linear hyperplanes corresponding to *every one* of the roots.

Since, by transitivity, every chamber contains a vertex of the same type as the origin, there must be at least one choice of values $\boldsymbol{p} = (p_{\boldsymbol{r}})_{\boldsymbol{r}\in\Phi}$, with $p_{\boldsymbol{r}} \in \{\lfloor a_{\boldsymbol{r}} \rfloor, \lfloor a_{\boldsymbol{r}} \rfloor + 1\}$, such that the corresponding vertex $\boldsymbol{v}$ as determined by (8.26) satisfies (8.27) for some choice of $c_i \in \mathbb{Z}$.

Proposition 8.2.4. *Given a received vector $\boldsymbol{y} \in D_1$ and a vertex $\boldsymbol{v}$ of D_1 of the same type as the origin, as above, the vector $\boldsymbol{y} - \boldsymbol{v}$ lies in a chamber D_2 adjacent to the origin. If $\boldsymbol{x}'$ is the codeword in D_2, then $\boldsymbol{x} = \boldsymbol{x}' + \boldsymbol{v}$ is the codeword in D_1.*

Proof. These statements follow from the choice of $\boldsymbol{v} \in D_1$ such that translation by $\boldsymbol{v}$ is an element of $\mathcal{G}_a$. □

The decoding to $\boldsymbol{x}'$ may be done using any number of fast decoding techniques (including the length-reduction algorithm of [53]), and may often be simplified by exploiting the geometry of the tessalation generated by the affine reflection group. Note that the number of chambers adjacent to the origin is the order of the finite Weyl group, which depends on the dimension n (see Table 8.2), and is independent of the radius M of $\mathcal{R}$.

Let us now illustrate Step 3 with a number of varied examples.

8.2.3 Step 3 for $\mathcal{A}_2$

Let $\mathcal{G}_a = \mathcal{A}_2$. Following the calculation in the Appendix, the simple roots are given by $\boldsymbol{r}_1 = (1, 0)$ and $\boldsymbol{r}_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$, as vectors in $\mathbb{R}^2$; see Figure 8.4. Set $\boldsymbol{r}_3 = \boldsymbol{r}_1 + \boldsymbol{r}_2$ for ease of notation. Given the initial vector $\boldsymbol{x}_0 = (\frac{1}{3}, \frac{1}{\sqrt{3}})$ (from Table 8.1), we calculate $\boldsymbol{x}_1 = S_{\boldsymbol{r}_1}\boldsymbol{x}_0 = (-\frac{1}{3}, \frac{1}{\sqrt{3}})$. Then, as can be seen from the symmetry of Figure 8.4, and the corresponding tessalation of $\mathbb{R}^2$ in Figure 8.5, all codewords are given by adding either $\boldsymbol{x}_0$ or $\boldsymbol{x}_1$ to a vertex of the tessalation.

Choosing $\boldsymbol{r}_2$ and $\boldsymbol{r}_3$ as the linearly independent roots, it follows from (8.26) that for any $p_2, p_3 \in \mathbb{Z}$,

$$\boldsymbol{v}(p_2, p_3) = \begin{bmatrix} -1 & 1 \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \end{bmatrix} \begin{bmatrix} p_2 \\ p_3 \end{bmatrix} \tag{8.28}$$

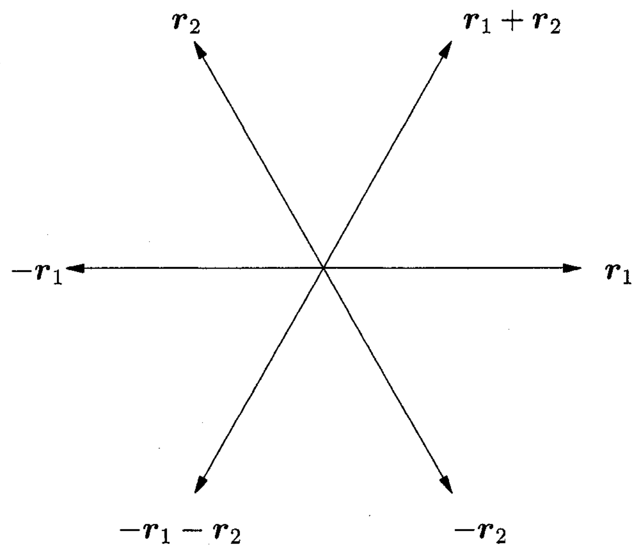

Figure 8.4: The set Φ of all roots of $\mathcal{A}_2$

is a vector pointing to the vertex $H_{\boldsymbol{r}_2,p_2} \cap H_{\boldsymbol{r}_3,p_3}$. In particular, let $\boldsymbol{y}$ be a received codeword, and for each $i \in \{1, 2, 3\}$, set $p_i = \lfloor \boldsymbol{r}_i \cdot \boldsymbol{y} \rfloor$. Then the lower corner of the simplex containing $\boldsymbol{y}$ is exactly $\boldsymbol{v}(p_2, p_3)$.

If $p_1 + p_2 = p_3$, then we are the on the right side of the corner, and we decode

$$\boldsymbol{v}(p_2, p_3) + \boldsymbol{x}_0 \tag{8.29}$$

whereas if $p_1 + p_2 < p_3$ then we are on the left side and should instead decode

$$\boldsymbol{v}(p_2, p_3) + \boldsymbol{x}_1. \tag{8.30}$$

8.2.4 Step 3 for $\mathcal{B}_2$

Recall that our irreducible ARG $\mathcal{B}_2$ has simple roots $\boldsymbol{r}_1 = (1, 0)$ and $\boldsymbol{r}_2 = (-1, 1)$; see Figure 8.1. Set $\boldsymbol{r}(1) = 2\boldsymbol{r}_1 + \boldsymbol{r}_2$ and $\boldsymbol{r}(2) = \boldsymbol{r}_2$, and calculate

$$p_1 = \lfloor (2\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot \boldsymbol{y} \rfloor \qquad \text{and} \qquad p_2 = \lfloor \boldsymbol{r}_2 \cdot \boldsymbol{y} \rfloor. \tag{8.31}$$

Then the vector

$$\boldsymbol{v} = P^{-1}\boldsymbol{p} = \frac{p_1}{2}(2\boldsymbol{r}_1 + \boldsymbol{r}_2) + \frac{p_2}{2}\boldsymbol{r}_2 \tag{8.32}$$

points to the bottom corner of the unit square containing $\boldsymbol{y}$, while the vector

$$\boldsymbol{v}' = \boldsymbol{v} + \frac{1}{2}\boldsymbol{r}_2 \tag{8.33}$$

points to the left corner of that square. Exactly one of these is a vertex of the same type as the origin; which one depends on the relative parity of p_1 and p_2. In each square there are two chambers, separated by $H_{\boldsymbol{r}_1, \frac{1}{2}(p_1-p_2)}$ in the first case and $H_{\boldsymbol{r}_1+\boldsymbol{r}_2, \frac{1}{2}(p_1+p_2+1)}$ in the second. Translating this to the origin yields the following decision tree for the decoding of $\mathcal{B}_2$:

- if $p_1 - p_2$ is even then
  - if $2\lfloor \boldsymbol{r}_1 \cdot y \rfloor = p_1 - p_2$, then decode $\boldsymbol{x} = \boldsymbol{v} + \boldsymbol{x}_0$;
  - else decode $\boldsymbol{x} = \boldsymbol{v} + S_{\boldsymbol{r}_1}\boldsymbol{x}_0$;
- else
  - if $2\lfloor (\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot y \rfloor = p_1 + p_2 + 1$, then decode $\boldsymbol{x} = \boldsymbol{v}' + S_{\boldsymbol{r}_2}\boldsymbol{x}_0$;
  - else decode $\boldsymbol{x} = \boldsymbol{v}' + S_{\boldsymbol{r}_2}S_{\boldsymbol{r}_1}\boldsymbol{x}_0$.

8.2.5 Step 3 for $\mathcal{G}_2$

From Table 2.2, the simple roots are $\boldsymbol{r}_1 = (1, 0)$ and $\boldsymbol{r}_2 = (-\frac{3}{2}, \frac{\sqrt{3}}{2})$. Set $\boldsymbol{r}_3 = (0, \sqrt{3}) = 3\boldsymbol{r}_1 + 2\boldsymbol{r}_2$, $\boldsymbol{r}_4 = (\frac{3}{2}, \frac{\sqrt{3}}{2}) = 3\boldsymbol{r}_1 + \boldsymbol{r}_2$ and $\boldsymbol{x}_0 = \left(\frac{1}{3(\sqrt{3}+1)}, \frac{\sqrt{3}+2}{3(\sqrt{3}+1)}\right)$. We compute $p_i = \lfloor \boldsymbol{r}_i \cdot \boldsymbol{y} \rfloor$ for all $i = 1, 2, 3, 4$.

- if $p_2 + p_3 \equiv 0 \mod 3$ then $\boldsymbol{v} = (-\frac{2}{3}p_2 + \frac{1}{3}p_3, -\frac{1}{\sqrt{3}}p_3)$.
- elseif $p_2 + p_3 \equiv 1 \mod 3$ then $\boldsymbol{v} = (-\frac{2}{3}(p_2 + 1) + \frac{1}{3}(p_3 + 1), -\frac{1}{\sqrt{3}}(p_3 + 1))$.
- elseif $p_4 + p_3 \equiv 0 \mod 3$ then $\boldsymbol{v} = (\frac{2}{3}p_4 - \frac{1}{3}p_3, \frac{1}{\sqrt{3}}p_3)$.
- else $\boldsymbol{v} = (\frac{2}{3}(p_4 + 1) - \frac{1}{3}(p_3 + 1), \frac{1}{\sqrt{3}}(p_3 + 1))$.

Then we compute

$$\boldsymbol{w} = (w_1, w_2) = \boldsymbol{y} - \boldsymbol{v} \text{ and } \boldsymbol{A} = \operatorname{diag}(\operatorname{sgn}(w_1), \operatorname{sgn}(w_2)). \tag{8.34}$$

- if $\left|\frac{w_2}{w_1}\right| \geq \sqrt{3}$ then decode $\boldsymbol{x} = \boldsymbol{v} + \boldsymbol{A}\boldsymbol{x}_0$.
- elseif $\frac{1}{\sqrt{3}} \leq \left|\frac{w_2}{w_1}\right| < \sqrt{3}$ then decode $\boldsymbol{x} = \boldsymbol{v} + \boldsymbol{A}\boldsymbol{S}_{\boldsymbol{r}_2}\boldsymbol{x}_0$.
- else decode $\boldsymbol{x} = \boldsymbol{v} + \boldsymbol{A}\boldsymbol{S}_{\boldsymbol{r}_1+\boldsymbol{r}_2}\boldsymbol{S}_{\boldsymbol{r}_2}\boldsymbol{x}_0$.

8.2.6 Step 3 for $\mathcal{A}_3$

Here, each chamber is a 3-dimensional irregular tetrahedron. There are fewer symmetries to exploit, so we apply Step 3 directly.

From Appendix B, we have that $\boldsymbol{r}_1 = (1,0,0)$, $\boldsymbol{r}_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2}, 0)$, and $\boldsymbol{r}_3 = (0, -\frac{1}{\sqrt{3}}, \sqrt{\frac{2}{3}})$. The remaining positive roots are $\boldsymbol{r}_4 = \boldsymbol{r}_1 + \boldsymbol{r}_2$, $\boldsymbol{r}_5 = \boldsymbol{r}_2 + \boldsymbol{r}_3$, and $\boldsymbol{r}_6 = \boldsymbol{\rho} = \boldsymbol{r}_1 + \boldsymbol{r}_2 + \boldsymbol{r}_3$. We note that each root has length 1.

If $p_1, p_2, p_3 \in \mathbb{Z}$, then we may calculate explicitly that the vertex $H_{\boldsymbol{r}_1,p_1} \cap H_{\boldsymbol{r}_2,p_2} \cap H_{\boldsymbol{r}_3,p_3}$ is equal to $\boldsymbol{v} = 2c_1\boldsymbol{r}_1 + 2c_2\boldsymbol{r}_2 + 2c_3\boldsymbol{r}_3$ (from (8.27)) for some choice of $c_1, c_2, c_3 \in \mathbb{Z}$ if and only if

$$c_2 = p_2 + \frac{1}{2}(p_1 + p_3); \quad c_1 = \frac{1}{2}(p_1 + c_2); \quad c_3 = \frac{1}{2}(p_3 + c_2), \tag{8.35}$$

and if it is also in the intersection $H_{\boldsymbol{r}_4,p_4} \cap H_{\boldsymbol{r}_5,p_5} \cap H_{\boldsymbol{r}_6,p_6}$, where

$$p_4 = p_1 + p_2; \quad p_5 = p_2 + p_3; \quad p_6 = p_1 + p_2 + p_3. \tag{8.36}$$

Define $a_i = \boldsymbol{r}_i \cdot \boldsymbol{y}$, for $1 \leq i \leq 6$. Then a vertex of the chamber containing $\boldsymbol{y}$ of the same type as the origin is defined by a set of choices of $p_i \in \{\lfloor a_i \rfloor, \lfloor a_i \rfloor + 1\}$. Solve (8.35) and (8.36) from among these available choices. Since each chamber contains a vertex of the same type as the origin (since all chambers are obtained by group actions on the fundamental chamber), this system is consistent. For $\mathcal{A}_3$, the solution is unique. It follows that the vertex $\boldsymbol{v}$ corresponding to this solution is of the same type as the origin, so that translation by $\boldsymbol{v}$ is an isometry of the chambers. Consequently $\boldsymbol{y} - \boldsymbol{v}$ is in a chamber adjacent to the origin; there are $|W| = 24$ of these, which is a number independent of the radius of $\mathcal{R}$. We find the closest codeword $\boldsymbol{c}$ to $\boldsymbol{y} - \boldsymbol{v}$ using a lookup table (on parities of the values $\lfloor (\boldsymbol{y} - \boldsymbol{c}) \cdot \boldsymbol{r}_i \rfloor$, for example) or with the length-reduction algorithm of [53], which now applies since we have reduced the problem to the finite reflection group case. Finally, we decode to $\boldsymbol{v} + \boldsymbol{c}$.

8.3 Examples and Performance

We now illustrate the steps of this algorithm with a variety of examples.

8.3.1 Affine Reflection Group Code $\mathcal{B}_2$

The root system for $\mathcal{B}_2$ was explored in Example 8.1.1. The best initial vector is $\boldsymbol{x}_0 = (\frac{1}{2\sqrt{2}+2}, \frac{1}{2}) = (0.207, 0.5)$, from Table 8.1. Consider the codeword region with 32 codewords defined by the root vectors of length $\sqrt{2}$ and $M = 2$:

$$\mathcal{R} = \{|\boldsymbol{r}_2 \cdot x| \leq 2 \text{ and } |\boldsymbol{\rho} \cdot x| \leq 2\}. \tag{8.37}$$

This is represented with the solid line in Figure 8.1.

Example 8.3.1. *Consider the received vector* $\boldsymbol{y} = B = (0.95, 0.25)$ *in Figure 8.1. This lies in* $\mathcal{R}$*, so we proceed to apply Step 3 (as described in Section 8.2.4) to* B*. We evaluate* $(2\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot \boldsymbol{y} = 1.2$ *and* $\boldsymbol{r}_2 \cdot \boldsymbol{y} = -0.7$*. Thus we have* $p_1 = 1$ *and* $p_2 = -1$*. The difference* $p_1 - p_2 = 2$ *is even, from which we deduce that the chamber containing* $\boldsymbol{y} = B$ *is oriented with its long side parallel to* $(0, 1)$*. Now calculate* $2\boldsymbol{r}_1 \cdot \boldsymbol{y} = 1.9 < 2$*; we are thus in the second of the four cases. We have*

$$\boldsymbol{v} = \frac{1}{2}(2\boldsymbol{r}_1 + \boldsymbol{r}_2) - \frac{1}{2}\boldsymbol{r}_2 = \frac{1}{2}(1,1) - \frac{1}{2}(-1,1) = (1,0).$$

Thus the decoded word is

$$\boldsymbol{x} = \boldsymbol{v} + S_{\boldsymbol{r}_1}\boldsymbol{x}_0 = (1,0) + \left(-\frac{1}{2\sqrt{2}+2}, \frac{1}{2}\right) = \left(\frac{2\sqrt{2}+1}{2\sqrt{2}+2}, \frac{1}{2}\right) = (0.793, 0.5).$$

Example 8.3.2. *Consider the received vector* $\boldsymbol{y} = C = (1.75, 0.05)$ *in Figure 8.1; this again lies inside* $\mathcal{R}$*, so we proceed directly to Step 3. We evaluate* $(2\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot \boldsymbol{y} = 1.8$ *and* $\boldsymbol{r}_2 \cdot \boldsymbol{y} = -1.7$*. Hence* $p_1 = 1$ *and* $p_2 = -2$*, so* $p_1 - p_2 = 3$ *is odd, which indicates that the chamber containing* $\boldsymbol{y} = C$ *is oriented with long side parallel to* $(0, 1)$*. Since* $2(\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot \boldsymbol{y} = 0.1 > 1 + (-2) + 1 = 0$*, we are in the third of four cases of Section 8.2.4.*

Thus we should decode

$$\begin{aligned}
\boldsymbol{x} &= \boldsymbol{v}' + S_{\boldsymbol{r}_2}\boldsymbol{x}_0 \\
&= \left(\frac{1}{2}(2\boldsymbol{r}_1 + \boldsymbol{r}_2) + \frac{-2+1}{2}\boldsymbol{r}_2\right) + \left(\boldsymbol{x}_0 - \frac{2\boldsymbol{r}_2 \cdot \boldsymbol{x}_0}{\boldsymbol{r}_2 \cdot \boldsymbol{r}_2}\boldsymbol{r}_2\right) \\
&= (1,0) + \boldsymbol{x}_0 - (\boldsymbol{r}_2 \cdot \boldsymbol{x}_0)\boldsymbol{r}_2 \\
&= \left(\frac{3}{2}, \frac{1}{2\sqrt{2}+2}\right) = (1.5, 0.207).
\end{aligned}$$

Example 8.3.3. *Now let us illustrate Steps 1 and 2. Consider the received vector* $\boldsymbol{y} = A = (-0.75, 1.8)$*. By Step 1, we compute* $\boldsymbol{r}_2 \cdot \boldsymbol{y} = 2.55 > 2$ *and* $\boldsymbol{\rho} \cdot \boldsymbol{y} = 1.05 < 2$*; note that this implies also that* $(-\boldsymbol{r}_2) \cdot \boldsymbol{y} = -2.55 < 2$ *and* $(-\boldsymbol{\rho}) \cdot \boldsymbol{y} = -1.05 < 2$*. Thus* $\boldsymbol{y} \notin \mathcal{R}$*, and the closest face (by Lemma 8.2.2) is the one corresponding to* $\boldsymbol{r}_2$*. We compute*

$$\begin{aligned}
\boldsymbol{w} &= proj_{H_{\boldsymbol{r}_{2,2}}}\boldsymbol{y} \\
&= \boldsymbol{y} - \frac{\boldsymbol{r}_2 \cdot \boldsymbol{y} - 2}{\|\boldsymbol{r}_2\|^2}\boldsymbol{r}_2 \\
&= (-0.75, 1.8) - \frac{0.55}{2}(-1, 1) \\
&= (-0.475, 1.525).
\end{aligned}$$

Since this point is in range by the conditions (8.37)*, we conclude that it is the closest projection to* $\boldsymbol{y} = A$*. Since we did not proceed to a further intersection of boundary hyperplanes (that is, to corners), we do not need to disambiguate* $\boldsymbol{w}$*.*

As $\boldsymbol{w}$ *is by construction on the boundary of* $\mathcal{R}$*, we apply Step 2 to shrink* $\boldsymbol{w}$ *inside the region; compute the factor* s *as follows. We have* $\boldsymbol{r}_1 \cdot \boldsymbol{w} = -0.475$*,* $(\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot \boldsymbol{w} = 1.525$*,* $\boldsymbol{r}_2 \cdot \boldsymbol{w} = 2$ *and* $(2\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot \boldsymbol{w} = 1.05$*. Thus*

$$s = \frac{1}{2}\max\left\{1, \frac{2.525}{1.525}, \frac{3}{2}, \frac{2.05}{1.05}\right\} = 0.976,$$

hence we take $\boldsymbol{z} = 0.976(-0.475, 1.525) = (-0.464, 1.488)$ *which is now on the interior of the codeword region, and in the same chamber as* $\boldsymbol{w}$*.*

Finally, for Step 3, we evaluate $p_1 = \lfloor(2\boldsymbol{r}_1 + \boldsymbol{r}_2) \cdot \boldsymbol{z}\rfloor = 1$ *and* $p_2 = \lfloor \boldsymbol{r}_2 \cdot \boldsymbol{z}\rfloor = 1$*. The difference* $p_1 - p_2 = 0$ *is even, and* $2\lfloor \boldsymbol{r}_1 \cdot \boldsymbol{z}\rfloor = -2 < 0 = p_1 - p_2$*, so we are in the* *second case of Section 8.2.4. We have that* $\boldsymbol{v} = \boldsymbol{r}_1 + \boldsymbol{r}_2 = (0, 1)$ *and hence the decoded message is*

$$\boldsymbol{x} = \boldsymbol{v} + S_{\boldsymbol{r}_1}\boldsymbol{x}_0 = (-0.207, 1.5).$$

8.3.2 Affine Reflection Group Code $\mathcal{A}_2$

Take the root system $\mathcal{A}_2$ with simple roots $\boldsymbol{r}_1 = (1, 0)$ and $\boldsymbol{r}_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$. The long root is $\boldsymbol{r}_3 = \boldsymbol{r}_1 + \boldsymbol{r}_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$. The best initial root vector is $\boldsymbol{x}_0 = (\frac{1}{3}, \frac{1}{\sqrt{3}})$, from Table 8.1.

Consider the codeword region defined by

$$\mathcal{R} = \mathcal{R}_3 = \{\boldsymbol{x} \colon |\boldsymbol{r}_1 \cdot \boldsymbol{x}| \leq 3, |\boldsymbol{r}_2 \cdot \boldsymbol{x}| \leq 3, |\boldsymbol{r}_3 \cdot \boldsymbol{x}| \leq 3.\} \tag{8.38}$$

This region is indicated by a solid line in Figure 8.5; the shaded region represents the fundamental chamber. It contains $6(3)^2 = 54$ codewords, by Table 8.2.

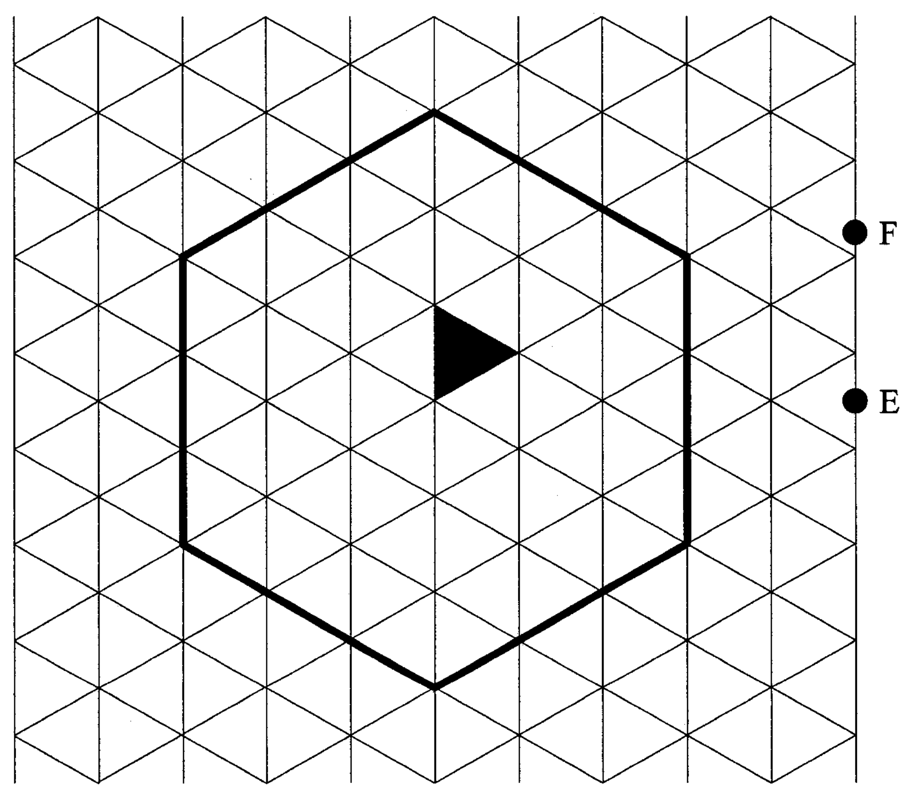

Figure 8.5: Hyperplanes and chambers for $\mathcal{A}_2$. The fundamental domain is shaded, and the outline defines the bounded codeword region $\mathcal{R}_3$; see Section 8.3.2.

Example 8.3.4. *Consider the received vector $\boldsymbol{y} = E = (5,0)$. By Step 1, we calculate*

$$\boldsymbol{r}_1 \cdot \boldsymbol{y} = 5, \quad \boldsymbol{r}_2 \cdot \boldsymbol{y} = -2.5, \quad \boldsymbol{r}_3 \cdot \boldsymbol{y} = 2.5;$$

considering these values (and also their negatives), we conclude that $\boldsymbol{y} \notin \mathcal{R}$ and that the closest face, by Lemma 8.2.2, is the one contained in $H_{\boldsymbol{r}_1,3}$. The projection of $\boldsymbol{y}$ onto $H_{\boldsymbol{r}_1,3}$ is

$$\boldsymbol{w} = \boldsymbol{y} - (\boldsymbol{r}_1 \cdot \boldsymbol{y} - 3)\boldsymbol{r}_1 = (3,0),$$

which already lies on the boundary of $\mathcal{R}$; hence we proceed to Step 2.

We compute: $\boldsymbol{r}_1 \cdot \boldsymbol{w} = 3$, $\boldsymbol{r}_2 \cdot \boldsymbol{w} = -\frac{3}{2}$ and $\boldsymbol{\rho} \cdot \boldsymbol{w} = \frac{3}{2}$. Thus the scaling factor s defined in (8.25) *is*

$$s = \frac{1}{2}\max\{\frac{5}{3}, \frac{2.5}{1.5}, \frac{2.5}{1.5}\} = \frac{5}{6}.$$

so $\boldsymbol{z} = s\boldsymbol{w} = (\frac{5}{2}, 0)$.

Finally, to decode $\boldsymbol{z}$ using Step 3, we note that $p_1 = 2$, $p_2 = -2$ and $p_3 = 1$, so $p_1 + p_2 \neq p_3$ and we decode

$$\boldsymbol{x} = \boldsymbol{v}(-2,1) + S_{\boldsymbol{r}_1}\boldsymbol{x}_0 = (\frac{8}{3}, 0).$$

Example 8.3.5. *Consider the received vector $\boldsymbol{y} = F = (5,2)$. Then by Step 1, we calculate:*

$$\boldsymbol{r}_1 \cdot \boldsymbol{y} = 5, \quad \boldsymbol{r}_2 \cdot \boldsymbol{y} = -0.768, \quad \boldsymbol{r}_3 \cdot \boldsymbol{y} = 4.232;$$

thus $\boldsymbol{y} \notin \mathcal{R}$ and by Lemma 8.2.2, the closest wall is the one contained in $H_{\boldsymbol{r}_1,3}$. The first projection is

$$proj_{H_{\boldsymbol{r}_1,3}}\boldsymbol{y} = \boldsymbol{y} - (\boldsymbol{r}_1 \cdot \boldsymbol{y} - 3)\boldsymbol{r}_1 = (3,2),$$

which this time is not in $\mathcal{R}$ since $\boldsymbol{r}_3 \cdot (3,2) = 3.232 > 3$. Thus we proceed as per Proposition 8.2.1, computing the projections onto the boundaries of the closest face. In this case, the boundaries are

$$H_{\boldsymbol{r}_1,3} \cap H_{\boldsymbol{r}_3,3} = (3, \sqrt{3}) \text{ and } H_{\boldsymbol{r}_1,3} \cap H_{-\boldsymbol{r}_2,3} = (3, -\sqrt{3}).$$

Since these are points, the projection of $\boldsymbol{y}$ onto each is just the point, and both are in $\mathcal{R}$. The closest is $\boldsymbol{w} = (3, \sqrt{3})$. Since $\boldsymbol{w}$ is the projection of $\boldsymbol{y}$ onto the intersection of *two walls, not both equally close to* $\boldsymbol{y}$, *we must disambiguate* $\boldsymbol{w}$ *using Proposition 8.2.2. We have*

$$\boldsymbol{d} = (3, \sqrt{3}) - \frac{3}{5}(5, 2) = (0, 0.532)$$

so $\Phi_{\boldsymbol{y}} = \{\boldsymbol{r}_2, \boldsymbol{r}_3\}$. *Since* $\boldsymbol{r}_2 \cdot \boldsymbol{w} = 0$ *and* $\boldsymbol{r}_3 \cdot \boldsymbol{w} = 3$, *we calculate*

$$\varepsilon = \frac{1}{2}\min\left\{\left(\frac{0 - 0 + 1}{0 - \frac{3}{5}(-0.768)}\right), \left(\frac{3 - 3 + 1}{3 - \frac{3}{5}(4.232)}\right)\right\} = 1.085.$$

We conclude that $\boldsymbol{u} = \boldsymbol{w} - \varepsilon\boldsymbol{d} = (3, 1.155)$ *is a point on the face of the chamber in* $\mathcal{R}$ *closest to* $\boldsymbol{y}$.

This point is by construction on the boundary of $\mathcal{R}$. *Since* $\boldsymbol{r}_1 \cdot \boldsymbol{u} = 3$, $\boldsymbol{r}_2 \cdot \boldsymbol{u} = -0.5$ *and* $\boldsymbol{r}_3 \cdot \boldsymbol{u} = 2.5$, *the scaling factor* s *of* (8.25) *is* $s = \frac{1}{2}\max\{\frac{5}{3}, 1, \frac{4.5}{2.5}\} = 0.9$. *Hence Step 2 applied to* $\boldsymbol{u}$ *yields* $\boldsymbol{z} = s\boldsymbol{u} = (2.7, 1.0395)$, *which lies in the interior of* $\mathcal{R}$.

We are finally in Step 3; since $p_1 = \lfloor \boldsymbol{r}_1 \cdot \boldsymbol{w} \rfloor = 2$, $p_2 = -1$ *and* $p_3 = 2$, *our codeword is*

$$\boldsymbol{x} = \boldsymbol{v}(-1, 2) + S_{\boldsymbol{r}_1}\boldsymbol{x}_0 = (2.667, 1.155).$$

8.3.3 Performance

We further illustrate the correctness of our proposed decoding algorithm, as compared to the ML decoder, in Figures 8.6 and 8.7, for some ARGCs of dimension $n = 2, 3$ and 4. The simulation was done by plotting symbol error rate (SER) versus SNR in dB, under the assumption that the noise is Gaussian distributed with zero mean. We applied the proposed decoding algorithm in Section 8.2.2 for decoding.

Figure 8.6 shows the SER performance of ARGC $\mathcal{A}_3$ for the codeword regions of radius $M = 1$ and $M = 2$; the length-reduction method in [53] was applied in Step 3 for this case. Figure 8.7 shows the SER performance of the affine reflection groups $\mathcal{B}_n$ of rank $n = 2, 3$ and 4 at the same radius $M = 1$. We use the proposed Step 3 described in Section 8.2.4 to decode $\mathcal{B}_2$ and the length-reduction method to decode $\mathcal{B}_3$ and $\mathcal{B}_4$.

We can see that the proposed algorithm achieves the same correctness as the ML decoder. We claim that for cases in which n is small relative to M, our decoding algorithm is more efficient. Namely, the ML decoder must compare the received vector $\boldsymbol{y}$ with each of the L codewords, where L is as in Table 8.2. This is at least exponential in n and is polynomial in M. For our algorithm, the complexity in n will also be at least exponential (due to the iterative procedure in Step 1, as well as in some cases the decoding in Step 3); it will vary depending on the group chosen and the implementation used. That said, significant gains are made in that the complexity of our decoding algorithm is *independent of* M.

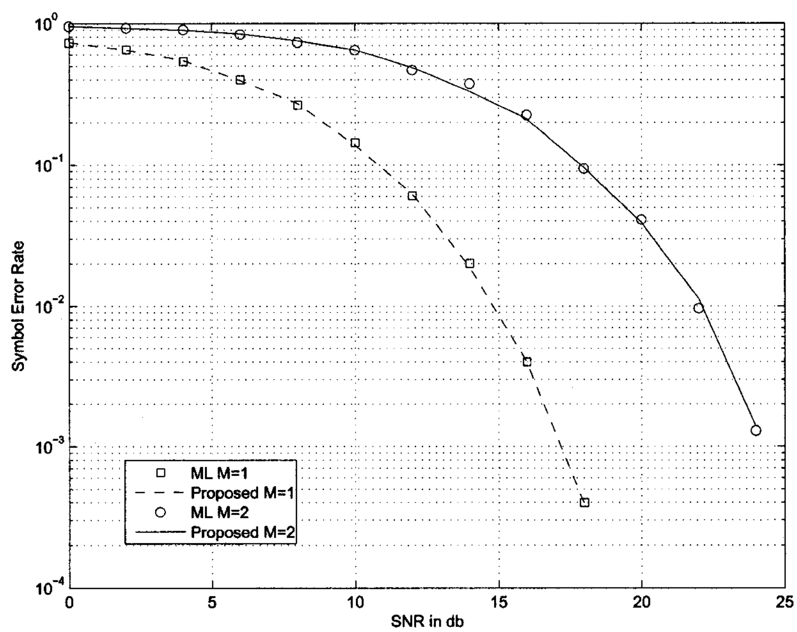

Figure 8.6: SER performance of $\mathcal{A}_3$ for $M = 1$ and 2

8.3.4 Comparison with Lattice Decoding

In the context of lattice (as in Section 2.2.4), we consider an unbounded codeword region and compare Step 3 of our proposed algorithm of ARGC $\mathcal{A}_2$ and $\mathcal{A}_3$ against the coset decoding method [23].

The coroot lattices of $\mathcal{A}_2$ and $\mathcal{A}_3$ are each two cosets of rectangular lattices [3, 13]. The ARGC $\mathcal{A}_2$ is in turn given as the union of two cosets of this lattice (represented by $\boldsymbol{x}_0$ and $\boldsymbol{x}_1$ as in Section 8.2.3), giving a total of 4 iterations of the fast trellis decoding algorithm of [3].

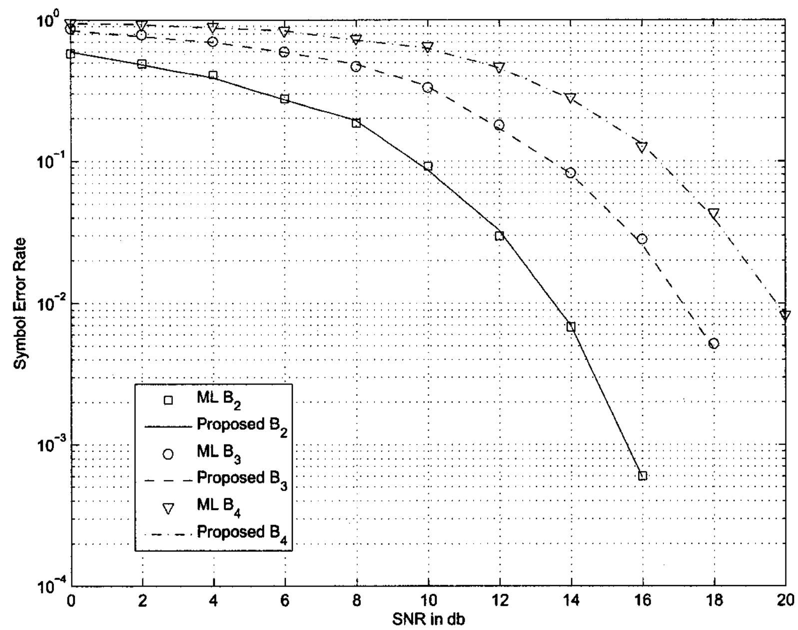

Figure 8.7: SER performance of $\mathcal{B}_n$ of rank $n = 2, 3$ and 4 at $M = 1$

Consider 4 cosets (C_1, C_2, C_3 and C_4) as shown in Figure 8.8, we can express

$$\begin{aligned}\mathcal{A}_2 &= \{\boldsymbol{x}_0 + \Lambda_L\} \cup \{\boldsymbol{x}_0 + \boldsymbol{z} + \Lambda_L\} \cup \{\boldsymbol{x}_1 + \Lambda_L\} \cup \{\boldsymbol{x}_1 + \boldsymbol{z} + \Lambda_L\} &(8.39)\\ &= C_1 \cup C_2 \cup C_3 \cup C_4 &(8.40)\end{aligned}$$

where $\boldsymbol{x}_0 = (\frac{1}{3}, \frac{1}{\sqrt{3}})$ and $\boldsymbol{x}_1 = (-\frac{1}{3}, \frac{1}{\sqrt{3}})$ and Λ_L is a rectangular lattice. Hence we have 4 candidate vectors (one from each coset). We use the algorithm of finding the closest point for an integer lattice as described in Section III [12] to compute the candidate vector from each coset. Then we choose one vector which is closest to the received vector.

On the other hand, the ARG $\mathcal{A}_3$ has far less symmetrical chambers, with the result that this group code is 24 ($= 4!$) distinct cosets of the coroot lattice, giving a total of 48 iterations of the trellis decoding algorithm.

In Table 8.3, we compare our algorithm (as specified for $\mathcal{A}_2$ in Section 8.2.3, and for $\mathcal{A}_3$ in Section 8.2.6, choosing a table lookup for the final step) against this coset decoding algorithm. The performance is considered by counting the average number of flops per symbol using MATLAB. We can see that the proposed algorithms outperform the coset decoding in these cases.

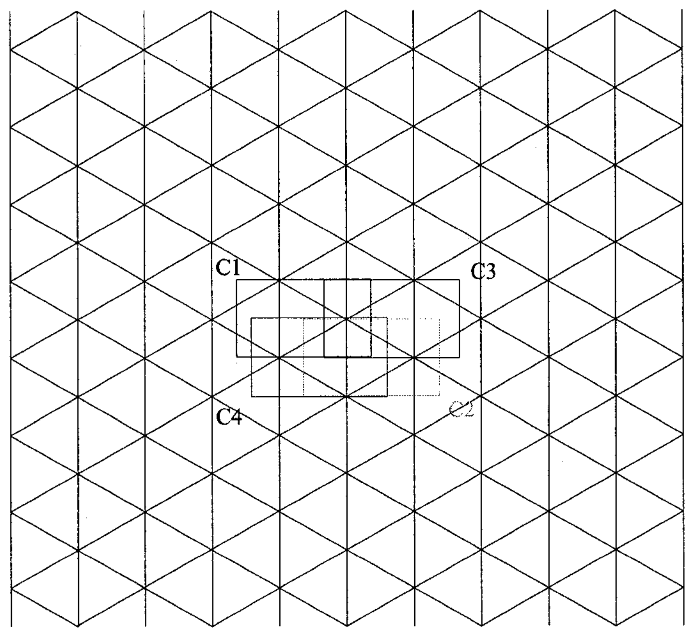

Figure 8.8: The 4 cosets of $\mathcal{A}_2$

Algorithm	$\mathcal{A}_2$	$\mathcal{A}_3$
Proposed decision tree	16	186
Coset decoding	52	1104

Table 8.3: The comparison of average number of flops per symbol

Chapter 9

Trellis Representation and Decoding Methods

Decoding algorithms of some ARGCs have been proposed in the step 3 in Section 8.3, using the analysis of the geometry of the affine reflection group. These decision trees have been shown to have less complexity and be faster compared to the lattice decoding. However these decision trees are provided only for some affine reflection groups and for low dimension, *i.e.* $\mathcal{A}_2, \mathcal{B}_2, \mathcal{G}_2$ and $\mathcal{A}_3$. Moreover the geometry of affine reflection groups is not easy to analyze for high dimensions, that is, $n \geq 3$.

In this chapter, we show that ARGCs are also generalizations of lattice codes [13] and use this to produce two efficient decoding methods. From Theorem 2.2.1 given in Section 2.2.5, for a given initial vector $\boldsymbol{x}_0$, every element of an ARGC $\mathcal{G}_a\boldsymbol{x}_0$ can be obtained by applying some elements in crystallographic finite reflection group $\mathcal{G}$ and then translating by a coroot lattice vector $\boldsymbol{v} \in \Lambda(\Phi^\vee)$, that is,

$$\mathcal{G}_a\boldsymbol{x}_0 = \bigcup_{g\in\mathcal{G}} \left(g\boldsymbol{x}_0 + \Lambda(\Phi^\vee)\right). \tag{9.1}$$

Thus if Λ_L is a rectangular sublattice of $\Lambda(\Phi^\vee)$, with quotient $Q = \Lambda(\Phi^\vee)/\Lambda_L$, then the ARGC $\mathcal{G}_a\mathbf{x}_0$ is a union of cosets of Λ_L given by

$$\mathcal{G}_a\mathbf{x}_0 = \bigcup_{g\in\mathcal{G},\mathbf{v}\in Q} \left(g\mathbf{x}_0 + \mathbf{v} + \Lambda_L\right). \tag{9.2}$$

There is a well known method to represent a lattice by a trellis diagram and to decode it using the Viterbi algorithm [4, 24], which we recalled in Section 2.4.2. Thus we can use the idea of trellis diagram representations as a possible solution to the problem of decoding ARGCs. This leads us to develop two efficient decoding methods for any ARGC in any dimension. (We note that the conventional derivation of the trellis diagram of a lattice, as originally proposed in [24], does not apply to ARGCs since these codes do not have an additive group structure.)

Section 9.1 presents the first proposed decoding method which is developed from the fact that affine reflection groups are infinite groups given by combining crystallographic finite reflection groups and their coroot lattices in a semi-direct product, see (2.2.1). Decoding Method I (hybrid) combines the Viterbi algorithm on the trellis diagram of the coroot lattice $\Lambda(\Phi^\vee)$ and the length-reduction method as explained in Section 2.3.3 (or the fast permutation-decoding algorithm [54]) on the crystallographic finite reflection group $\mathcal{G}$.

The second proposed decoding method is given in Section 9.2. In Decoding Method II (lattice cosets), we consider an ARGC as itself a union of cosets of the coroot lattice. The comparison in decoding complexity as well as the trade-off of these two decoding methods are discussed in Section 9.3.

We conclude in Section 9.4 with an application of ARGCs, with the proposed decoding methods, as a tone injection constellation to improve an PAPR reduction of OFDM system.

9.1 Decoding Method I: Hybrid

The proposed Decoding Method I is developed from Theorem 2.2.1 as mentioned above. We summarize the decoding algorithm as follows:

1. For a given ARG $\mathcal{G}_a$ with root system Φ (listed in Table 2.2), consider the coroot lattice $\Lambda(\Phi^\vee)$. (The definitions of coroots and the coroot lattice are given in (2.24) and in Section 2.2.4 respectively.)

2. Compute the closest coroot lattice vector $\boldsymbol{v} \in \Lambda(\Phi^\vee)$ to the received vector $\boldsymbol{y}$, using the Viterbi algorithm on the trellis diagram of $\Lambda(\Phi^\vee)$. We do this as follows. Since the trellis coordinate system of the trellis diagram of the coroot lattice $\Lambda(\Phi^\vee)$ is $\boldsymbol{w}_i$, $i = 1, 2, \ldots, n$ (see Section 2.4), we need to transform the received vector $\boldsymbol{y}$ into

coordinates with respect to $\boldsymbol{w}_i$ via

$$\boldsymbol{y}' = \left(\frac{(\boldsymbol{y}, \boldsymbol{w}_1)}{\|\boldsymbol{w}_1\|^2}, \frac{(\boldsymbol{y}, \boldsymbol{w}_2)}{\|\boldsymbol{w}_2\|^2}, \cdots, \frac{(\boldsymbol{y}, \boldsymbol{w}_n)}{\|\boldsymbol{w}_n\|^2} \right). \tag{9.3}$$

Using the Viterbi algorithm on $\boldsymbol{y}'$ gives $\boldsymbol{v}' = (v_1', v_2', \ldots, v_n')$, the coordinates of $\boldsymbol{v}$ with respect to $\boldsymbol{w}_i$. (The decision metric for the Viterbi algorithm to decode $\boldsymbol{y}'$ is given in Section 2.4.2.) Then $\boldsymbol{v}$ can be computed from

$$\boldsymbol{v} = v_1' \boldsymbol{w}_1 + v_2' \boldsymbol{w}_2 + \cdots + v_n' \boldsymbol{w}_n \tag{9.4}$$

3. Translate the received vector $\boldsymbol{y}$ to the first shell[1] of ARG $\mathcal{G}_a$ by $\boldsymbol{y} - \boldsymbol{v}$.

4. Apply the length reduction algorithm in Section 2.3.3 (or fast permutation-decoding algorithm) on $\boldsymbol{y} - \boldsymbol{v}$ (relative to the group code $\{g\boldsymbol{x}_0,\ g \in \mathcal{G}\}$) which gives $\boldsymbol{x}_{\mathcal{R}_1}$. Then the decoded message is

$$\hat{\boldsymbol{x}} = \boldsymbol{x}_{\mathcal{R}_1} + \boldsymbol{v}. \tag{9.5}$$

We illustrate Decoding Method I for the ARGC $\mathcal{A}_2$ in Example 9.1.1 and Figure 9.1.

Example 9.1.1. *Consider the coroot lattice $\mathcal{A}_2$ with its trellis diagram in Figure 2.6 (as explained in Example 2.4.2). Let $\boldsymbol{y}$ be the received codeword. See Figure 9.1. The solid circles represent the coroot lattice. From step 2 in Decoding Method I, using the Viterbi algorithm on its trellis diagram gives the closet coroot lattice vector $\boldsymbol{v} \in \Lambda(\Phi^\vee)$. We translate this received vector $\boldsymbol{y}$ to the first shell (the bold line in the same figure) by $\boldsymbol{y} - \boldsymbol{v}$. Let's say we get $\boldsymbol{x}_{\mathcal{R}_1}$ from the decoding the vector $\boldsymbol{y} - \boldsymbol{v}$ using the length reduction algorithm (or this can also be done by the decision tree of $\mathcal{A}_2$ explained in Section 8.2.3) then the decoded message is $\hat{\boldsymbol{x}} = \boldsymbol{x}_{\mathcal{R}_1} + \boldsymbol{v}$.*

9.2 Decoding Method II: Lattice Cosets

For the proposed Decoding Method II, we first compute the trellis diagram representing a given ARG $\mathcal{G}_a$ and then use the Viterbi algorithm on this trellis diagram for decoding.

[1]The region of the first shell is defined from $\bigcup_{g \in \mathcal{G}} \{gD\}$ where D is a fundamental domain for $\mathcal{G}_a$; as defined in Section 8.2.1

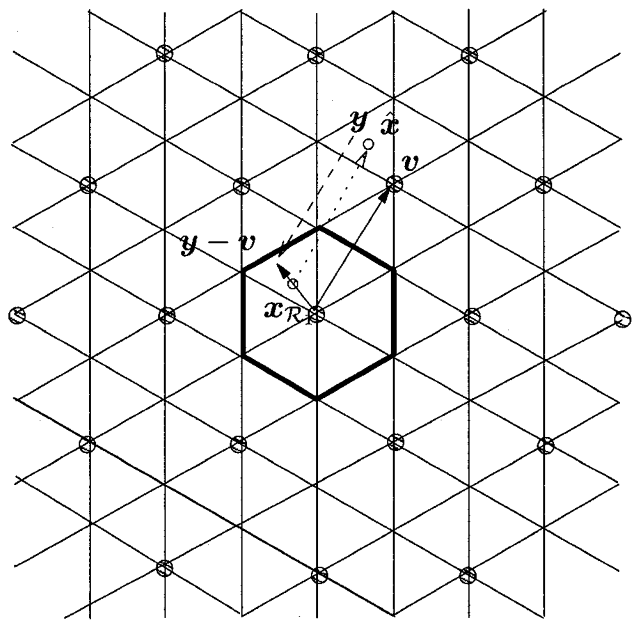

Figure 9.1: Decoding method I of the ARGC $\mathcal{A}_2$

Hence the main work in Decoding Method II lie in computing the trellis diagram for a given $\mathcal{G}_a$.

The result from Theorem 2.2.1, as expressed in (9.1), implies that $\mathcal{G}_a\boldsymbol{x}_0$ is the union of cosets of $\Lambda(\Phi^\vee)$. The trellis diagram for $\Lambda(\Phi^\vee)$ expresses $\Lambda(\Phi^\vee)$ as a union of cosets of a rectangular sublattice Λ_L. So $\mathcal{G}_a\boldsymbol{x}_0$ is the union of cosets of Λ_L as well and each coset (of Λ_L) corresponds to a path on the trellis diagram of $\mathcal{G}_a$.

We present the method to compute the trellis diagram of any ARGC as follows:

1. For a given ARG $\mathcal{G}_a$ with root system Φ, consider the trellis diagram of the coroot lattice $\Lambda(\Phi^\vee)$ with the trellis coordinate system $\boldsymbol{w}_i$, $i = 1, 2, \ldots, n$. Let $\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{N_p-1}$ be the path labels where $\boldsymbol{v}_0$ is the label of the lattice vector at the origin and N_p is the number of paths of the trellis diagram.

2. Generate the finite reflection group codewords in the first shell ($\mathcal{R}_1$); these are just the vectors in $\mathcal{G}\boldsymbol{x}_0$. Label them $\{\boldsymbol{x}_0, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_{R_1-1}\}$, where $R_1 = |\mathcal{G}|$. The number of codewords in the first shell R_1 is given in Table 9.1.

3. Calculate the path labels (coordinates) for these first shell codewords with respect to $\boldsymbol{w}_i$ by

$$\boldsymbol{x}_i' = \left(\frac{(\boldsymbol{x}_1, \boldsymbol{w}_1)}{\|\boldsymbol{w}_1\|^2}, \frac{(\boldsymbol{x}_1, \boldsymbol{w}_2)}{\|\boldsymbol{w}_2\|^2}, \cdots, \frac{(\boldsymbol{x}_1, \boldsymbol{w}_n)}{\|\boldsymbol{w}_n\|^2}\right) \tag{9.6}$$

for all $i = 0, 1, \ldots, R_1 - 1$.

Group	$\|\Phi\|$	R_1
$\mathcal{A}_n$	n^2+n	$(n+1)!$
$\mathcal{B}_n$	$2n^2$	$2^n n!$
$\mathcal{D}_n$	$2n(n-1)$	$2^{n-1}n!$
$\mathcal{E}_6$	72	51840
$\mathcal{F}_4$	48	$2^7 \cdot 3^2$
$\mathcal{G}_2$	12	36

Table 9.1: The order of the root systems and R_1 of affine reflection groups [54, Table II]

4. The complete set of path labels is

$$\{\boldsymbol{x}'_i + \boldsymbol{v}_j \mid i = 0, \ldots, R_1 - 1,\ j = 0, \ldots, N_p - 1\} \tag{9.7}$$

which corresponds to $R_1 N_p$ paths.

5. To draw the trellis diagram, we rearrange and regroup the path labels in (9.7) by the same repeat, that is, modulo Λ_L as described in Section 2.4. This gives the trellis diagram representing the ARGC. We note that the labels of the resulting trellis diagram depend on the choice of $\boldsymbol{w}_i$.

We illustrate the Decoding Method II for the different ARGCs as followings:

Example 9.2.1. *From Example 2.4.2, the generator matrix of the coroot lattice $\mathcal{A}_2$ is*

$$\boldsymbol{G} = \begin{bmatrix} 2 & 0 \\ -1 & \sqrt{3} \end{bmatrix},$$

and its trellis diagram representation is shown in Figure 2.6 which is with respect to the trellis coordinate system $\boldsymbol{w}_1 = (2,0)$ and $\boldsymbol{w}_2 = (0,2)$.

The six codewords in the first shell of the ARG are $\boldsymbol{x}_0 = (2/3, 0)$, $\boldsymbol{x}_1 = (1/3, 1/\sqrt{3})$, $\boldsymbol{x}_2 = (-1/3, 1/\sqrt{3})$, $\boldsymbol{x}_3 = (-2/3, 0)$, $\boldsymbol{x}_4 = (-1/3, -1/\sqrt{3})$ and $\boldsymbol{x}_5 = (1/3, -1/\sqrt{3})$ (we compute these codewords from Section 8.3, using the simple roots $\boldsymbol{r}_1 = (1,0)$ and $\boldsymbol{r}_2 = (-1/2, \sqrt{3}/2)$). From (9.6), computing the path labels of these codewords with respect to $\boldsymbol{w}_1 = (2,0)$ and $\boldsymbol{w}_2 = (0,2)$ gives $\boldsymbol{x}'_0 = (1/3, 0)$, $\boldsymbol{x}'_1 = (1/6, 1/2\sqrt{3})$, $\boldsymbol{x}'_2 = (-1/6, 1/2\sqrt{3})$, $\boldsymbol{x}'_3 = (-1/3, 0)$, $\boldsymbol{x}'_4 = (-1/6, -1/2\sqrt{3})$ and $\boldsymbol{x}'_5 = (1/6, -1/2\sqrt{3})$. From its trellis diagram shown in Figure 2.6, we know that it has $N_p = 2$ paths.

Therefore we need to generate another $6 \times (2-1) = 6$ *label paths by adding the vector* $\boldsymbol{v}_1 = (1/2, \sqrt{3}/2)$ *corresponding to the nontrivial path in Figure 2.6, that is,*

$$\{\boldsymbol{x}'_i\}_{i=0}^{R_1-1} + \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right).$$

Thus, writing $\boldsymbol{x}'_{i+6} = \boldsymbol{x}'_i + \boldsymbol{v}_1$ *for* $i = 0, 1, \ldots, 5$, *the complete 12 path labels are*

$$\begin{array}{llll}
\boldsymbol{x}'_0 = \left(\frac{1}{3}, 0\right), & \boldsymbol{x}'_1 = \left(\frac{1}{6}, \frac{1}{2\sqrt{3}}\right), & \boldsymbol{x}'_2 = \left(-\frac{1}{6}, \frac{1}{2\sqrt{3}}\right), & \boldsymbol{x}'_3 = \left(-\frac{1}{3}, 0\right), \\
\boldsymbol{x}'_4 = \left(-\frac{1}{6}, -\frac{1}{2\sqrt{3}}\right), & \boldsymbol{x}'_5 = \left(\frac{1}{6}, -\frac{1}{2\sqrt{3}}\right), & \boldsymbol{x}'_6 = \left(\frac{5}{6}, \frac{\sqrt{3}}{2}\right), & \boldsymbol{x}'_7 = \left(\frac{2}{3}, \frac{2}{\sqrt{3}}\right), \\
\boldsymbol{x}'_8 = \left(\frac{1}{3}, \frac{2}{\sqrt{3}}\right), & \boldsymbol{x}'_9 = \left(\frac{1}{6}, \frac{\sqrt{3}}{2}\right), & \boldsymbol{x}'_{10} = \left(\frac{1}{3}, \frac{1}{\sqrt{3}}\right), & \boldsymbol{x}'_{11} = \left(\frac{2}{3}, \frac{1}{\sqrt{3}}\right).
\end{array}$$

From Figure 2.6, we also know that the first and the second coordinate repeat at 1 (or mod $\mathbb{Z}$*) and at* $\sqrt{3}$ *(or mod* $\sqrt{3}\mathbb{Z}$*) respectively. Now we note additional symmetry, which allows us to collapse the trellis diagram further. For example, consider* $\boldsymbol{x}'_0, \boldsymbol{x}'_8$ *and* $\boldsymbol{x}'_{10}$*. These 3 path labels share the same first coordinate, that is,* $\frac{1}{3}$ *mod* $\mathbb{Z}$*, and their second coordinate are*

$$\left\{0, \frac{2}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right\} \textit{ mod } \sqrt{3}\mathbb{Z} \equiv \left\{\frac{3}{\sqrt{3}}, \frac{2}{\sqrt{3}}, \frac{1}{\sqrt{3}}\right\} \textit{ mod } \sqrt{3}\mathbb{Z} \equiv 0 \textit{ mod } \frac{\mathbb{Z}}{\sqrt{3}}.$$

The other triplet path labels ($\{\boldsymbol{x}'_1, \boldsymbol{x}'_5, \boldsymbol{x}'_9\}$, $\{\boldsymbol{x}'_2, \boldsymbol{x}'_4, \boldsymbol{x}'_6\}$ *and* $\{\boldsymbol{x}'_3, \boldsymbol{x}'_7, \boldsymbol{x}'_{11}\}$*) can be proceeded in the same manner, by using*

$$\begin{aligned}
\left\{-\frac{1}{3}, \frac{2}{3}\right\} \textit{ mod } \mathbb{Z} &\equiv -\frac{1}{3} \textit{ mod } \mathbb{Z}, \\
\left\{-\frac{1}{6}, \frac{5}{6}\right\} \textit{ mod } \mathbb{Z} &\equiv -\frac{1}{6} \textit{ mod } \mathbb{Z},
\end{aligned}$$

$$\left\{\frac{1}{2\sqrt{3}}, -\frac{1}{2\sqrt{3}}, \frac{3}{2\sqrt{3}}\right\} \textit{ mod } \sqrt{3}\mathbb{Z} \equiv \left\{\frac{7}{2\sqrt{3}}, \frac{5}{2\sqrt{3}}, \frac{3}{2\sqrt{3}}\right\} \textit{ mod } \sqrt{3}\mathbb{Z} \equiv \frac{1}{2\sqrt{3}} \textit{ mod } \frac{\mathbb{Z}}{\sqrt{3}}.$$

This gives the minimal trellis diagram shown in Figure 9.2, where now the repeat on the second coordinate is more dense than for the coroot lattice, due to the symmetry of the group. The trellis diagram of ARGC A_2 *in Figure 9.2 is with respect to* $\boldsymbol{w}_1 = (2, 0)$ *and* $\boldsymbol{w}_2 = (0, 2)$ *and has 4 paths.*

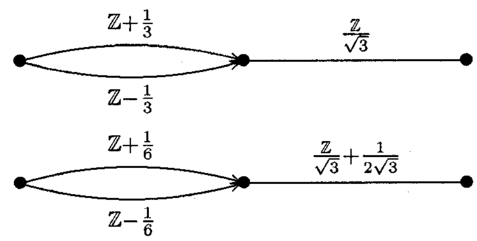

Figure 9.2: The trellis diagram of the ARGC $\mathcal{A}_2$

Example 9.2.2. *From Example 2.4.3, the generator matrix of the coroot lattice* $\mathcal{A}_3$ *is*

$$\boldsymbol{G} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & -\frac{2}{\sqrt{3}} & 2\sqrt{\frac{2}{3}} \\ -1 & \sqrt{3} & 0 \end{bmatrix}. \tag{9.8}$$

The trellis diagram of the coroot lattice $\mathcal{A}_3$ *is shown in Figure 2.7 which is with respect to* $\boldsymbol{w}_1 = (2,0,0)$, $\boldsymbol{w}_2 = \left(0, -\frac{2}{\sqrt{3}}, 2\sqrt{\frac{2}{3}}\right)$ *and* $\boldsymbol{w}_3 = \left(0, 2\sqrt{\frac{2}{3}}, \frac{2}{\sqrt{3}}\right)$.

The 24 codewords in the first shell of an ARG $\mathcal{A}_3$ *are shown in Table 9.2. These codewords are computed from Section 8.3 using the simple roots* $\boldsymbol{r}_1 = (1,0,0)$, $\boldsymbol{r}_2 = (-1/2, \sqrt{3}/2, 0)$ *and* $\boldsymbol{r}_3 = (0, -1/\sqrt{3}, \sqrt{2/3})$*).*

(−0.6768,−0.1021, 0.2340),	(−0.2500,−0.4330, 0.5227),	(0.2500,−0.4330, 0.5227)
(−0.6768, 0.1866,−0.1742),	(−0.2500, 0.3485,−0.5825),	(0.2500, 0.4330, 0.5227)
(−0.5000, 0.0000, 0.5227),	(−0.1768,−0.6794,−0.1742),	(0.4268,−0.5351, 0.2340)
(−0.5000, 0.4928,−0.1742),	(−0.1768,−0.3907,−0.5825),	(0.4268, 0.0423,−0.5825)
(−0.4268,−0.5351, 0.2340),	(0.1768,−0.3907,−0.5825),	(0.5000, 0.0000, 0.5227)
(−0.4268, 0.0423,−0.5825),	(0.1768,−0.6794,−0.1742),	(0.5000, 0.4928,−0.1742)
(−0.2500, 0.4330, 0.5227),	(0.2500, 0.6371, 0.2340),	(0.6768,−0.1021, 0.2340)
(−0.2500, 0.6371, 0.2340),	(0.2500, 0.3485,−0.5825),	(0.6768, 0.1866,−0.1742)

Table 9.2: The 24 codeword from the first shell of the ARG $\mathcal{A}_3$

The path labels of these codewords with respect to $\boldsymbol{w}_i$, $i = 1,2,3$ *using the formula in (9.6) are listed in Table 9.3.*

The trellis diagram of the coroot lattice shown in Figure 2.7 has $N_p = 2$ *paths (cosets of* Λ_L*) thus we need to generate another* $(2-1) \times 24 = 24$ *path labels, by adding the vector* $(1/2, 1/2, 1/\sqrt{2})$ *corresponding the bottom path of the same figure. This gives a total of 48 codewords, and we rearrange these path labels by mod* $\mathbb{Z}$*, mod* $\mathbb{Z}$ *and mod* $\sqrt{2}$ *for the first, second and third coordinates respectively. We list the complete 48*

(−0.3384, 0.1250, 0.0259),	(−0.1250, 0.3384,−0.0259),	(0.1250, 0.3384,−0.0259)
(−0.3384,−0.1250, 0.0259),	(−0.1250,−0.3384,−0.0259),	(0.1250, 0.0884, 0.3277)
(−0.2500, 0.2134, 0.1509),	(−0.0884, 0.1250,−0.3277),	(0.2134, 0.2500,−0.1509)
(−0.2500,−0.2134, 0.1509),	(−0.0884,−0.1250,−0.3277),	(0.2134,−0.2500,−0.1509)
(−0.2134, 0.2500,−0.1509),	(0.0884,−0.1250,−0.3277),	(0.2500, 0.2134, 0.1509)
(−0.2134,−0.2500,−0.1509),	(0.0884, 0.1250,−0.3277),	(0.2500,−0.2134, 0.1509)
(−0.1250, 0.0884, 0.3277),	(0.1250,−0.0884, 0.3276),	(0.3384, 0.1250, 0.0259)
(−0.1250,−0.0884, 0.3276),	(0.1250,−0.3384,−0.0259),	(0.3384,−0.1250, 0.0259)

Table 9.3: The 24 path labels from the first shell of the ARG $\mathcal{A}_3$, respected to $\{\boldsymbol{w}_i\}_{i=1}^3$

(0.1616, 0.3750,−0.6812),	(0.3750, 0.4116,−0.3795),	(−0.2134,−0.2500,−0.1509)
(−0.1616, 0.3750,−0.6812),	(−0.3750, 0.4116,−0.3795),	(0.2134,−0.2500,−0.1509)
(0.1616,−0.3750,−0.6812),	(0.3750,−0.4116,−0.3795),	(−0.2134, 0.2500,−0.1509)
(−0.1616,−0.3750,−0.6812),	(−0.3750,−0.4116,−0.3795),	(0.2134, 0.2500,−0.1509)
(0.2500, 0.2866,−0.5560),	(−0.0884,−0.1250,−0.3277),	(−0.1250,−0.3384,−0.0259)
(−0.2500, 0.2866,−0.5560),	(0.0884,−0.1250,−0.3277),	(0.1250,−0.3384,−0.0259)
(0.2500,−0.2866,−0.5560),	(−0.0884, 0.1250,−0.3277),	(−0.1250, 0.3384,−0.0259)
(−0.2500,−0.2866,−0.5560),	(0.0884, 0.1250,−0.3277),	(0.1250, 0.3384,−0.0259)
(−0.3384,−0.1250, 0.0259),	(−0.1250,−0.0884, 0.3276),	(0.2866, 0.2500, 0.5562)
(0.3384,−0.1250, 0.0259),	(0.1250,−0.0884, 0.3276),	(−0.2866, 0.2500, 0.5562)
(−0.3384, 0.1250, 0.0259),	(−0.1250, 0.0884, 0.3277),	(0.2866,−0.2500, 0.5562)
(0.3384, 0.1250, 0.0259),	(0.1250, 0.0884, 0.3277),	(−0.2866,−0.2500, 0.5562)
(−0.2500,−0.2134, 0.1509),	(0.4116, 0.3750, 0.3795),	(0.3750, 0.1616, 0.6812)
(0.2500,−0.2134, 0.1509),	(−0.4116, 0.3750, 0.3795),	(−0.3750, 0.1616, 0.6812)
(−0.2500, 0.2134, 0.1509),	(0.4116,−0.3750, 0.3795),	(0.3750,−0.1616, 0.6812)
(0.2500, 0.2134, 0.1509),	(−0.4116,−0.3750, 0.3795),	(−0.3750,−0.1616, 0.6812)

Table 9.4: The 48 path lables of the ARGC $\mathcal{A}_3$, with respect to $\{\boldsymbol{w}_i\}_{i=1}^3$

path labels in Table 9.4. Consequently, the trellis diagram of ARGC $\mathcal{A}_3$ is shown in Figure 9.3.

Example 9.2.3. *From Example 2.4.6, the trellis diagram of the coroot lattice of $\mathcal{B}_2$ is shown in Figure 2.10 which is with respect to $\boldsymbol{w}_1 = (-1,1)$ and $\boldsymbol{w}_2 = (1,1)$. The 8 codewords in the first shell of the ARG $\mathcal{B}_2$, using the simple roots $\boldsymbol{r}_1 = (1,0)$ and $\boldsymbol{r}_2 = (-1,1)$, are given in Table 9.5. (Note that $0.2071 = 1/(2+2\sqrt{2})$).*

The path labels from these codewords with respect to $\boldsymbol{w}_1 = (-1,1)$ and $\boldsymbol{w}_2 = (1,1)$ are listed in Table 9.6. Since the trellis diagram in Figure 2.10 has only one path, these 8 path labels in Table 9.6 are also the complete path labels of ARGC $\mathcal{B}_2$. From Figure 2.10, we know that these 8 path labels are repeated at mod $\mathbb{Z}$ for both coordinates. In this case, each trellis diagram of the ARGC $\mathcal{B}_2$ is shown in Figure 9.4; it has 8 paths with 2 subtrellises.

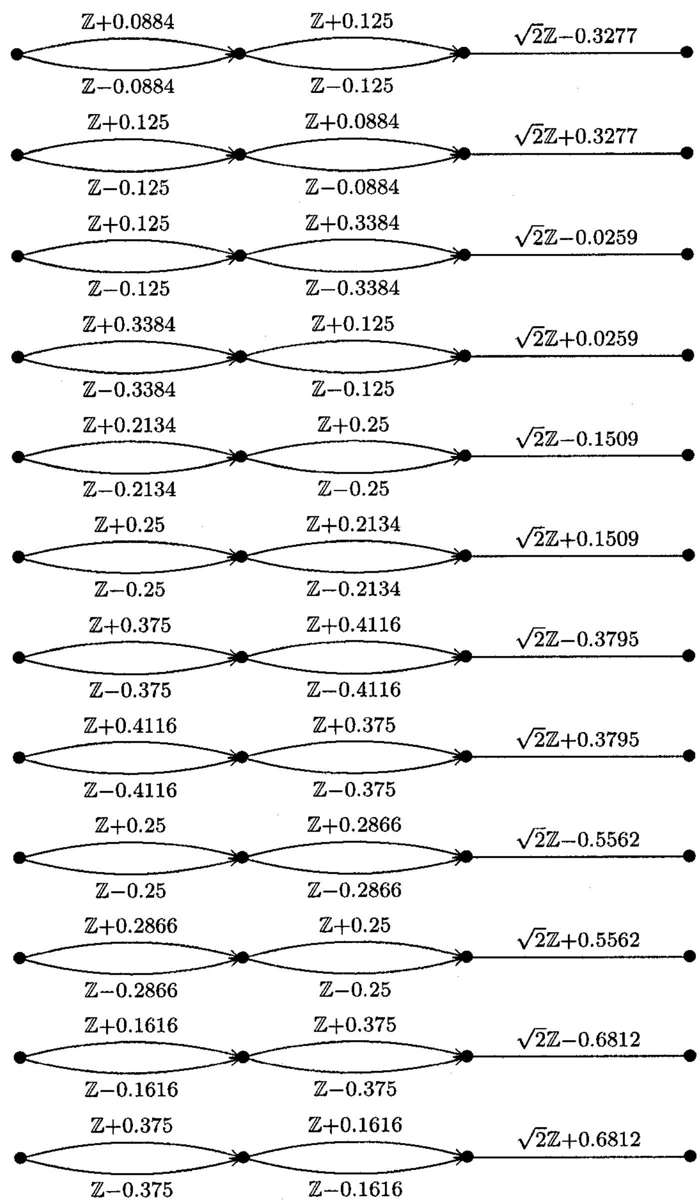

Figure 9.3: The trellis diagram of the ARGC $\mathcal{A}_3$

(0.2071,0.5000),	(0.2071,−0.5000),	(−0.2071,0.5000),	(−0.2071,−0.5000)
(0.5000,0.2071),	(0.5000,−0.2071),	(−0.5000,0.2071),	(−0.5000,−0.2071)

Table 9.5: The 8 codewords from the first shell of the ARG $\mathcal{B}_2$

Example 9.2.4. *From Table 2.2, the simple roots of* $\mathcal{D}_4$ *(which coincide with the simple coroots, by Example 2.2.4), are* $\boldsymbol{r}_1 = (1,1,0,0)$, $\boldsymbol{r}_2 = (-1,1,0,0)$, $\boldsymbol{r}_3 = (0,-1,1,0)$

(0.1464,0.3536),	(−0.3536,−0.1465),	(0.3536, 0.1465),	(−0.1464,−0.3536)
(−0.1464,0.3536),	(−0.3536, 0.1465),	(0.3536,−0.1465),	(0.1465,−0.3536)

Table 9.6: The 8 path labels of ARGC $\mathcal{B}_2$, with respect to $\boldsymbol{w}_1 = (-1, 1)$ and $\boldsymbol{w}_2 = (1, 1)$

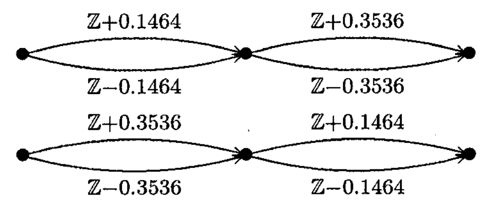

Figure 9.4: The trellis diagram of the ARGC $\mathcal{B}_2$, with respect to $\boldsymbol{w}_1 = (-1, 1)$ and $\boldsymbol{w}_2 = (1, 1)$

and $\boldsymbol{r}_4 = (0, 0, -1, 1)$, *on these simple roots to choose the generator matrix of* $\Lambda(\Phi^\vee)$ *as*

$$G' = \begin{bmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & -1 & 1 & 0 \end{bmatrix}. \tag{9.9}$$

Follow the well known method in [24, 3], the trellis diagram of the root lattice $\mathcal{D}_4$ *is shown in Figure 9.5 with respect to the trellis coordinate system*

$$\boldsymbol{w}_1 = (1, 1, 0, 0), \boldsymbol{w}_2 = (-1, 1, 0, 0), \boldsymbol{w}_3 = (0, 0, -1, 1), \boldsymbol{w}_4 = (0, 0, 1, 1). \tag{9.10}$$

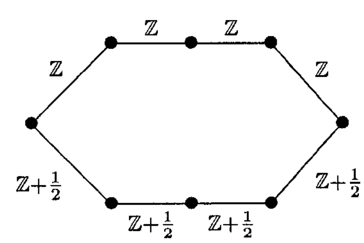

Figure 9.5: The trellis diagram of the root lattice $\mathcal{D}_4$

1. From Figure 9.5, the (co)root lattice $\mathcal{D}_4$ *has* $N_p = 2$ *distinct paths. It is clear from the label paths on the trellis diagram that representatives for the two cosets are*

$\boldsymbol{v}_0 = (0,0,0,0)$ *and* $\boldsymbol{v}_1 = \left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$.

2. From Table 9.1, the FRG of $\mathcal{D}_4$ *has* $2^{4-1}\cdot 4! = 192$ *codewords at the first shell* $\mathcal{R}_1$. *Let* $\boldsymbol{X} = \{\boldsymbol{x}_0,\ldots,\boldsymbol{x}_{191}\}$ *be these 192 codewords.*

3. Calculate $\boldsymbol{X}'$*, that is,* $\boldsymbol{X}$ *with respect to the trellis coordinate system* $\boldsymbol{w}_i$ *via*

$$\boldsymbol{x}'_j = \left(\frac{(\boldsymbol{x}_j,\boldsymbol{w}_1)}{\|\boldsymbol{w}_1\|^2},\frac{(\boldsymbol{x}_j,\boldsymbol{w}_2)}{\|\boldsymbol{w}_2\|^2},\frac{(\boldsymbol{x}_j,\boldsymbol{w}_3)}{\|\boldsymbol{w}_3\|^2},\frac{(\boldsymbol{x}_j,\boldsymbol{w}_4)}{\|\boldsymbol{w}_4\|^2}\right) \tag{9.11}$$

for all $j = 0,1,\ldots,191$ *and* $\{\boldsymbol{w}_i\}_{i=1}^4$ *are defined in (9.10).*

4. Then the complete set of label paths of the trellis diagram of ARGC of $\mathcal{D}_4$ *is*

$$\left\{\boldsymbol{X}',\boldsymbol{X}'+\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)\right\} \tag{9.12}$$

which have $192\times 2 = 384$ *label paths.*

5. Using the knowledge from the trellis diagram of the root lattice $\mathcal{D}_4$ *in Figure 9.5, we can see that all coordinates repeat at 1* $(\bmod\ \mathbb{Z})$. *We rearrange and group these label paths.*

This gives 24 subtrellis diagrams. Each subtrellis diagram has 16 paths (so $24\times 16 = 384$ *label paths). The 24 subtrellis diagrams are*

$$\begin{aligned}
&(\pm 0.4167,\pm 0.0834,\pm 0.0834,\pm 0.0834)^\pi, && (\pm 0.0834,\pm 0.4167,\pm 0.4167,\pm 0.4167,)^\pi,\\
&(\pm 0.4167,\pm 0.2500,\pm 0.2500,\pm 0.2500)^\pi && (\pm 0.0834,\pm 0.2500,\pm 0.2500,\pm 0.2500,)^\pi,\\
&(\pm 0.3334,\pm 0.1667,\pm 0.1667,\pm 0.1667)^\pi, && (\pm 0.1667,\pm 0.3334,\pm 0.3334,\pm 0.3334,)^\pi,
\end{aligned} \tag{9.13}$$

where π *denotes the set of all possible permutations. For example,*

$$(\pm 0.4167,\pm 0.0834,\pm 0.0834,\pm 0.0834)^\pi = \{(\pm 0.4167,\pm 0.0834,\pm 0.0834,\pm 0.0834),$$

$$(\pm 0.0834,\pm 0.4167,\pm 0.0834,\pm 0.0834),(\pm 0.0834,\pm 0.0834,\pm 0.4167,\pm 0.0834),$$

$$(\pm 0.0834,\pm 0.0834,\pm 0.0834,\pm 0.4167)\}.$$

The trellis diagram of $(\pm 0.4167,\pm 0.0834,\pm 0.0834,\pm 0.0834)$ *which has 16 paths is shown in Figure 9.6. The remaining 23 subtrellis diagrams also have the same trellis diagram as shown in Figure 9.6 with the different path labels given in (9.13).*

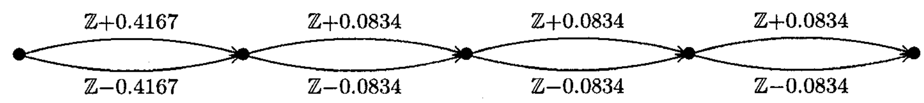

Figure 9.6: One of 24 subtrellis diagrams of ARGC $\mathcal{D}_4$

9.3 Discussion of Complexity

In this section, we compare the complexity of Decoding Methods I and II. The result gives us the trade-off to choose the appropriate decoding algorithm with low complexity for general ARGC.

9.3.1 Complexity of Proposed Trellis Diagram

An upper bound of the number of paths N_{pa} of a trellis diagram representing an ARGC using the Decoding Method II in Section 9.2 is

$$N_{pa} \leq R_1 N_p \tag{9.14}$$

where R_1 is the number of the codewords in the first shell related to $\mathcal{G}$ and N_p is the number of distinct paths in the trellis diagram of the coroot lattice $\Lambda(\Phi^\vee)$.

When the trellis coordinate system is chosen so that for $i = 1, \ldots, r \leq n$, $\boldsymbol{w}_i$ coincides, up to scaling, with a root $\boldsymbol{r}_i \in \Phi$, then the first r coordinates of the ARGC label paths will arise in $\pm$ pairs. This happens because the reflection in $\boldsymbol{w}_i$ is the same as that in $\boldsymbol{r}_i$, and so permutes the codewords, but simply changes the sign of the ith coordinate.

Since the label paths occur in $\pm$ pairs, this reduces the number of survivor paths for the Viterbi algorithm by a factor of 2^r, so we deduce that

$$N_{sp} \leq \frac{N_{pa}}{2^r} \leq \frac{R_1 N_p}{2^r}. \tag{9.15}$$

However, note that since the $\boldsymbol{w}_i$ are orthogonal, r is at most the maximum number of mutually orthogonal roots in Φ. From [39], one knows that there are at least $n/2$ mutually orthogonal *simple* roots, we deduce that in general $n/2 \leq r \leq n$. Consequently, we can predict the number of distinct paths N_{pa} and the number of survivor paths N_{sp} of the trellis diagram of an ARGC, using the value of $R_1 = |\mathcal{G}|$ listed in

Table 9.1, the number of N_p given in [4, 3], and the maximum number of mutually orthogonal roots.

Example 9.3.1. *From Example 9.2.4, the trellis diagram of ARGC of $\mathcal{D}_4$ has 24 subtrellis diagrams (one of them is shown in Figure 9.6). Each subtrellis diagram corresponds to one survivor path in the Viterbi algorithm. To compare with the upper bound given in (9.15), note that for the ARGC $\mathcal{D}_4$, we have $R_1 = 192$, $N_p = 2$ and $r = 4$ hence*

$$N_{sp} = 24 \leq \frac{192 \cdot 2}{2^4} = 24 \tag{9.16}$$

which shows our upper bound in (9.15) is tight.

9.3.2 Comparison of Decoding Complexity

The decoding complexity of the length-reduction and Viterbi algorithms are summarized in Section 2.3.3 and 2.4.2. For the length-reduction algorithm of FRGC, the number of iterations required in the algorithm depends on the location of the received codeword, but in the worst case, the inner loop will repeat no more than $|\Phi|/2$ times (corresponding to the number of reflections for the furthest element). Thus on average, one expect $|\Phi|/4$ iterations.

The comparison of the decoding complexity of the Decoding Methods I and II of general ARGC of dimension n is given in Table 9.7. For Decoding Method I, the numbers of theoretical complexity are from the Viterbi algorithm and the length-reduction method (where the number of iterations for the worst and the best case are $|\Phi|/2$ and 1 respectively). For Decoding Method II, we may relate the number of survivor paths N_{sp} to the number of paths N_p of the trellis diagram of the coroot lattice and R_1, the number of codewords in the first shell, using (9.15), knowing that in general $n/2 \leq r \leq n$. And we assume that $\pm$ pairs occur for all coordinate as discussed in Section 9.3.1.

The comparison of the decoding complexity of the two proposed decoding methods on the ARGC $\mathcal{D}_4$ is shown in Table 9.8. The theoretical complexity is computed from Table 9.7 where $R_1 = 192$, $|\Phi| = 24$ $N_p = 2$ and $N_{sp} = 24$. *Note*: the complexity is given for both general a and for $a = 1$, where the decision metric in (20) is significantly simpler to compute (it has just 1 multiplication and 2 additions).

Method.	Comparisons	Multiplications
I	$n + N_p$ to $\frac{\lvert\Phi\rvert}{2}n + N_p$	$n^2 + 3n(1 + N_p)$ to $\frac{\lvert\Phi\rvert}{2}(n^2 + 3n) + 3nN_p$
II	$nN_{sp} + N_{sp}$	$6nN_{sp}$

Method	Additions
I	$n^2 + n(3N_p + 2) - (N_p + 1)$ to $\frac{\lvert\Phi\rvert}{2}(n^2 + 2n - 1) + (3n - 1)N_p$
II	$(5n - 1)N_{sp}$

Table 9.7: Decoding (theoretical) complexity of Decoding Methods I and II for general ARGCs

The decoding algorithms were also implemented in MATLAB, where simulation results were used to determine their actual average decoding complexity. For simulation decoding complexity, we use MATLAB for implementations. We can see that the decoding complexity of Decoding Method II is higher than the complexity of Decoding Method I. However, the 24 subtrellis diagrams have the permutation structure as shown in (9.13) which can reduce the overall complexity as shown in the last row (highlighted in grey) in the same table.

The optimization based on the permutation structure can be done as follows. For example, first we compute ± 0.4167 and ± 0.0834 for all 4 coordinates. This gives 8 comparisons, 16 multiplications and 32 additions. Then the 4 candidates from $(\pm 0.4167, \pm 0.0834, \pm 0.0834, \pm 0.0834)^{\pi}$ need only 12 more additions. Since ± 0.4167 and ± 0.0834 are computed before for all 4 coordinates, the 4 candidates from $(\pm 0.0834, \pm 0.4167, \pm 0.4167, \pm 0.4167)^{\pi}$ also need 12 additions only. We can see that we reduce the number of multiplications, which have high cost in hardware implementations, from 192 to 64. This is a great improvement over Decoding Method I; furthermore, the number of comparisons and additions required for the optimized Method II remain comparable to Method I.

9.3.3 Summary of Three Decoding Methods

We can conclude the use and the tradeoff of three decoding methods as follows:

1. For ARGCs of low rank (*e.g.* $\mathcal{A}_2, \mathcal{B}_2, \mathcal{G}_2$ and $\mathcal{A}_3$), we choose the decision tree presented in Chapter 8 for decoding.

Method	Comparisons	Multiplications	Additions
I (theoretical, a)	6 to 50	52 to 360	47 to 298
I (theoretical, $a = 1$)	6 to 50	36 to 342	47 to 298
I (simulation)	28	190	171
II (theoretical, a)	216	576	456
II (theoretical, $a = 1$)	120	192	456
II (simulation)	120	192	456
II (optimized)	56	64	200

Table 9.8: The comparison of complexity of two decoding methods on the ARGC of $\mathcal{D}_4$

2. In general, the Decoding Method I which combines two decoding algorithms (trellis decoding and the length-reduction method) has less complexity than the Decoding Method II since $R_1 \gg |\Phi|$ for large n. However the number of survivor paths from Decoding Method II can be reduced by a factor of 2^r from (9.15). Furthermore, it is well-known that all the finite reflection groups which arise in affine reflection groups have a permutation structure, like the structure in $\mathcal{D}_4$. Hence similar optimization methods as those employed for $\mathcal{D}_4$ could be applied to reduce the complexity of Decoding Method II for any ARGC.

3. The advantage of Decoding Method II is its simple implementation because it uses only one decoding algorithm (trellis decoding).

9.4 Application to PAPR Reduction of an OFDM system

Lattices (or high dimensional constellations) with good minimum nearest-neighbour distance and low decoding complexity have been studied widely for problems in communication systems. From Chapter 8, we showed that ARGCs are cosets of (coroot) lattice codes and also have good performance in a Gaussian channel with low complexity in decoding. In this section, we give an application of ARGCs with the proposed decoding methods as a signal constellation of OFDM system. We apply a TI method [95] on an affine reflection $\mathcal{A}_2$ constellation to reduce the PAPR.

As we mentioned in Section 2.5.2, the improvement of PAPR reduction of the TI method comes from the large degree of freedom of a new (larger) constellation. The TI method on a hexagonal (HEX) constellation (the root lattice of $\mathcal{A}_2$) was first introduced in [29]. It also illustrates the example of TI signal mapping for a 91-HEX with 64 signals (at $M = 5$). The advantages of ARGC $\mathcal{A}_2$ over the hexagonal constellation are:

- For a given (same) radius M, the number of signal points of $\mathcal{A}_2$ and the hexagonal constellation are $6M^2$ and $3M(M+1)+1$ respectively. Hence the ARGC of $\mathcal{A}_2$ is more dense and consequently has more degrees of freedom to allow the TI method to reduce the PAPR.

- The ARGC of $\mathcal{A}_2$ has a low complexity ML decoding algorithm. Although a fast decoding algorithm of a hexagonal constellation was provided in [30, Appendix], it cannot decode any received vectors which are outside the bounds of constellation and therefore is not ML. The algorithm also cannot work with the Modified 73-HEX in [29]. On other hand, the Step 1 and 2 of ARGC's decoding algorithm in Chapter 8 are specifically proposed to solve this problem.

Let K be the number of points in q-QAM which have more than one representation. The TI mapping from q-QAM to an ARGC of rank 2 at radius M with L codewords ($q < L$) is done as follows. For $i = 1$ to $L - 2K$, we map a codeword vector $\boldsymbol{x}_i$ of an ARGC by $f(\boldsymbol{x}_i) = q_i$ where $q_i = 1, 2, \ldots, L - 2K \in$ QAM. For the remaining vectors, we map $f(\boldsymbol{x}_i) = q_i A$ and $f(-\boldsymbol{x}_i) = q_i B$ (notation as Figure 9.7) where $i = L - 2K + 1, \ldots, q$. This symmetric mapping allows one to use the TI efficiently to reduce the PAPR and total power of the system. We note that this TI mapping can be easily modified if we have more than two representations for some points.

Example 9.4.1. *Figure 9.7 shows the TI signal mapping from 64-QAM to the ARGC $\mathcal{A}_2$ with $L = 96$ (at the radius $M = 4$). Here we set $K = 32$. Then the 32 points in 64-QAM have one representation and the remain 32 points in 64-QAM have two representations (A and B). For example, the 44th point of 64-QAM can be chosen from either the vector $\boldsymbol{x}_i$=44A or $-\boldsymbol{x}'_i$=44B in Figure 9.7 to transmit. Also, at the receiver, both the received vectors 44A and 44B are decoded as the same symbol. We note that the power $|\boldsymbol{x}_i|^2 = |-\boldsymbol{x}'_i|^2$ for all $i = 33, 34, \ldots, 64$.*

We use a (suboptimal) reduced complexity algorithm [46] to search appropriate $\pm\boldsymbol{x}_i$ to reduce the PAPR of a TI signal constellation. This searching algorithm reduces the

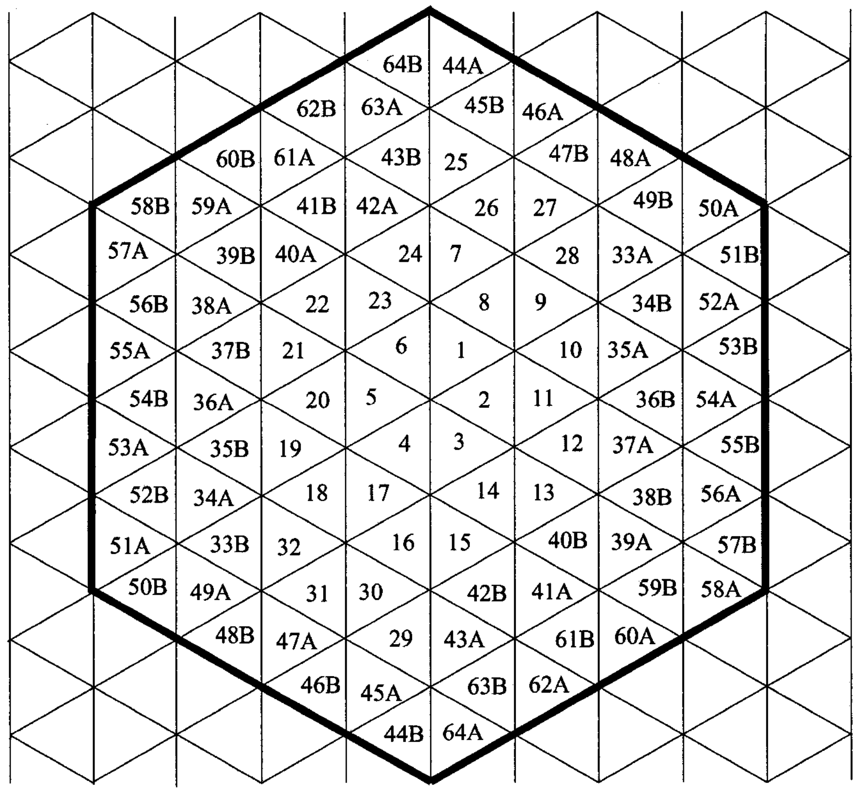

Figure 9.7: The TI method on an ARG $\mathcal{A}_2$ with 64 signal points

complexity from $(N_{ct})^J$ (for the optimal searching algorithm) to $N_{ct}J$ where N_{ct} is the number of subcarriers whose signals have more than one representation and J is the number of representations (for example, $J = 2$ in Example 9.4.1). A summary of the reduced complexity searching algorithm [46] is given as follows.

1. Given a symbol q. Let $I = \{i_1, i_2, \ldots\}$ be the subcarrier indices such that $q(i_j)$ has more than one representation. Start $j = 0$, compute the PAPR from the first representation for all subcarriers in I.

2. Increase j by 1. At the subcarrier i_j, calculate the PAPR of the remaining $J-1$ representation and choose that representation which gives the lowest PAPR. (We note that we can skip the first representation in J since since its PAPR was already computed in Step 1.)

3. If $j < |I|$, go to Step 2. Otherwise terminate.

The complementary cumulative density function (CCDF) of PAPR from the TI signal constellation of the ARGC $\mathcal{A}_2$ with 64 signals in Example 9.4.1 is shown in

Figure 9.8. We compare it with the 91-HEX constellation [29] and the (square) 64-QAM at the same $N_c = 64$ subcarriers of OFDM system. The CCDF simulation is done with 10,000 random OFDM blocks with the sampling factor $W = 4$ (see Section 2.5.2). We can see that our ARG A_2 improves the PAPR reduction. For example, we improve ≈ 3.5 dB and ≈ 0.2 dB over the 64-QAM and the 91-HEX at the same PAPR of 0.01%. The reason is our ARGC $\mathcal{A}_2$ has more two representations (more degrees of freedom) than the 91-HEX; we have 32 points with two representations and the 91-HEX has 27 points with two representations.

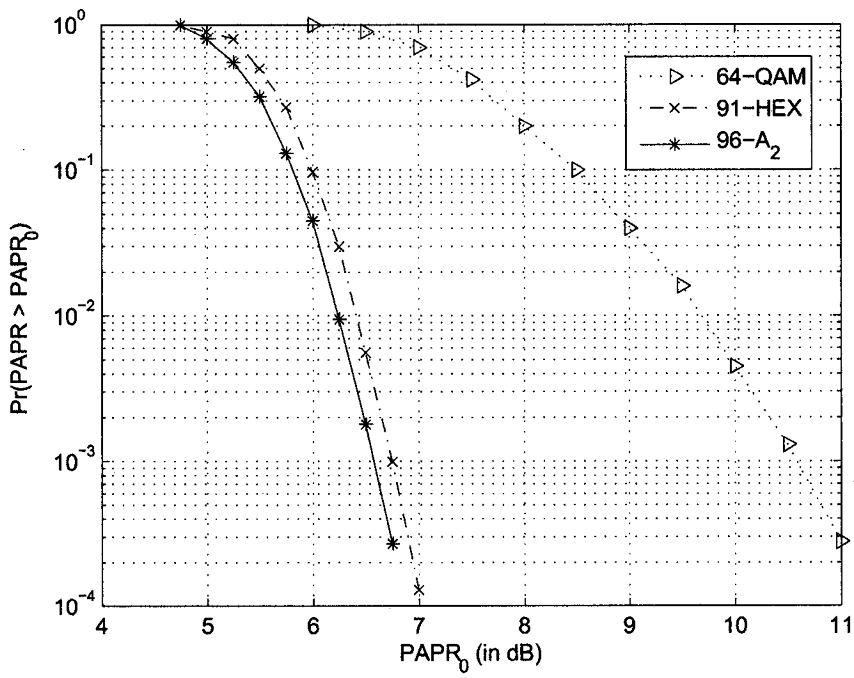

Figure 9.8: The PAPR comparison of 96-$\mathcal{A}_2$, 91-HEX and 64-QAM for an OFDM system with $N_c = 64$ subscarriers

Figure 9.9 shows the SER performance of an OFDM system with $N_c = 64$ subcarriers in a Rayleigh fading channel, using the 96-$\mathcal{A}_2$ (in Example 9.4.1) and 64-QAM constellations. The simulation is done from (2.74). We can see that the SER performance of our proposed 96-$\mathcal{A}_2$ is inferior to 64-QAM ≈ 2 dB however the significant improvement over the 64-QAM is a huge PAPR reduction as shown in Figure 9.8.

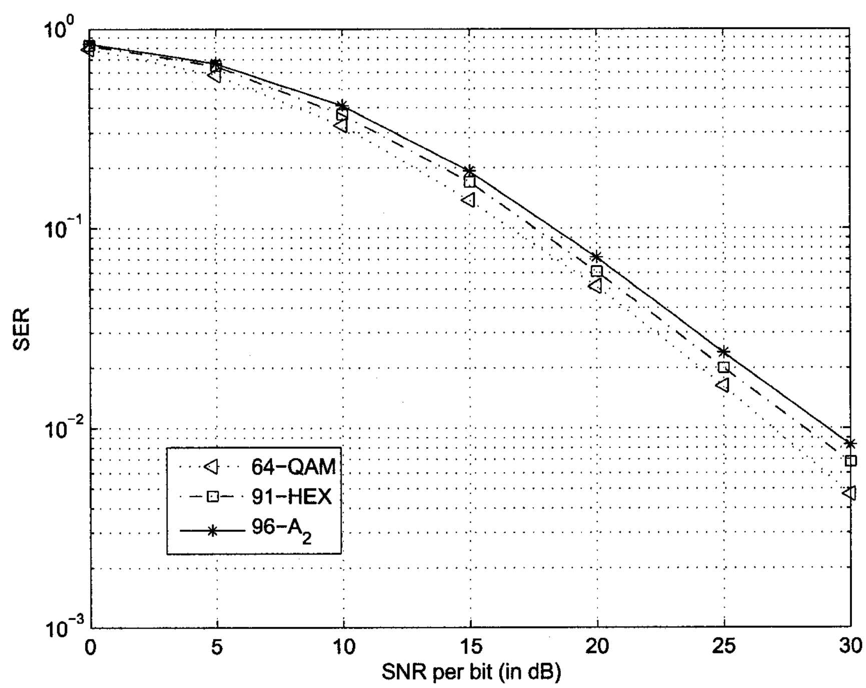

Figure 9.9: The SER performance of an OFDM system with $N_c = 96$ subcarriers in a Rayleigh fading channel

Chapter 10

Conclusion

10.1 Summary

We have presented designs of full diversity USTCs with high coding gain, using group codes generated from permutation codes variant II and finite reflection group codes for two transmitter antennas, and using the Bruhat decomposition for any number of transmitter antennas. We have shown that our proposed constellations have excellent diversity products and, from simulations, they perform well without the information of channel, and outperform some designs in literature. We have introduced the notion of a faithful unitary space-time group constellation, as one which has a diversity sum greater than zero, and have also presented a method to compute the diversity sum of a group constellation from its character table.

We have also developed a fast algorithm to optimize the decision metric of MSD for DUSTM, using a stack. This allows us to consider a greater number of blocks, and consequently to increase the decoding performance, with low additional complexity. The proposed algorithm is equivalent to the ML detection and can be used for any USTC and for any number of transmitter antennas.

We have derived a simple closed form solution for the average PEP of space-time codes over a keyhole channel, which applies to all full rank constellations. We have shown that the BLER performance obtained from our proposed PEP gives a good tight upper bound compared to simulation.

For the problem of affine reflection group codes, we have derived a formula for its best initial vector, as well as for its best nearest-neighbour distance, for group codes generated from irreducible affine reflection groups of any rank. We have also proposed a general decoding algorithm (from the analysis of group's geometry) for all irreducible affine reflection groups which is equivalent to the ML decoder and which is more efficient than ML when the rank of the group is low and the number of codewords is large, that is, for low rank but large boundary region.

We have also presented Decoding Method I (hybrid) and II (lattice cosets) as well as a method to draw the trellis diagram of affine reflection group code of any rank. The decoding complexity of the proposed algorithms has been analyzed so one could choose the proper decoding algorithm with fast and low complexity for a given group. Finally, we have given an application of affine reflection group code of $\mathcal{A}_2$ using the proposed decoding methods as an OFDM signal constellation for improved PAPR reduction.

10.2 Discussion of Future Work

We discuss the possible work and development of this thesis in this section.

Bit-Mapping Assignment of USTC

In this thesis, we assign the bit-mapping (from a message z_i to a matrix $\boldsymbol{V}_i$ of the signal constellation $\mathcal{V}$) of USTC randomly. No computer search (by the optimization of bit error rate (BER)) was done. The efficient and systematic bit mapping could be applied to the proposed USTC from finite reflection groups in Chapter 3. A gray code mapping for finite reflection groups has been presented in [14]. This systematical mapping method could improve the BER performance of proposed USTC, without a computer search.

Bruhat USTCs

- We have given the condition of $\{d_i\}_{i=1}^{n_T}$ for a full diversity Bruhat constellation $\mathcal{V}$ (see (4.9)), but not given how to make the right choice of d_i for a given n_T and L_D. We have shown only for a case of an odd prime n_T. Therefore the case where n_T is a general number is an open problem.

- The analysis of the choice of parameters $\{k_i\}_{i=1}^{n_T}$ for a full diversity Hamiltonian Bruhat constellation $\mathcal{B}$ can be considered as an another possible extension work.

Pursuing this could give us a better understanding of the structure of these constellations, and also give fast optimization methods.

PEP of STC in a Keyhole Channel

- The key upper bound (7.10) would not be tight in the case that there is a large disparity in the sizes of the eigenvalues. Hence future work should consider tightening the bound in this case, as well as extending to rank deficient codes.
- From the proposed average PEPs presented in (7.12) and (7.19) and given that the generalized hypergeometric function ${}_2F_0$ is an increasing function, a design criterion of robust codes for a keyhole channel might be to maximize the $\lambda_{\min}$ of $\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})\boldsymbol{B}(\boldsymbol{c},\boldsymbol{e})^{\dagger}$ for all distinct codewords $\boldsymbol{c}$ and $\boldsymbol{e}$. An extension work would be to find a method to construct space-time codes which meet this design criterion; this is a max-min eigenvalue problem that can be done by the power method using the POWER software [20].
- The same analysis of PEP, using a MGF-based approach and geometric functions can be extended to a case of keyhole channel with non-identical m distribution Nakagami fading [55, 100].

Fast MSD for MS-DUSTM

The BID algorithm in [15] has far less complexity, on diagonal constellations in Chapter 6, than our proposed stack algorithm. Hence a possible extension work of this paper is to find a reduced complexity MSD for general (nondiagonal) constellations by combining the BID and stack algorithms. Moreover, it would be also interesting to explore applying the ideas of outer decoder in [72] to see if it can help to further optimize the stack algorithm in the general case.

Affine Reflection Group Codes

- Step 1 in Section 8.2.2 can be made more efficient, but suboptimal, by replacing Step 1 with the simple scaling $\boldsymbol{w} = (M/t)\boldsymbol{y}$ (notation as in Proposition 8.2.2); the resulting decoding fails to be ML because $\mathcal{R}_M$ is not spherical.

- Linear programming can be considered as another possible approach to approximating the projection onto the boundary to optimize the inner product with the receiver vector subject to the constraints of code region.
- Affine reflection group codes of rank 2 can be used as a signal constellation of quasi-OSTBC, with no requirement of rotation [16, 76, 85].

The lines of enquiry in this doctoral work have included all aspects of the design and analysis of space-time codes and affine reflection group codes. In addition to the extensions of this work discussed over the preceding paragraphs, this work opens up a number of exciting new directions of research– from implementation of the proposed systems, to the analysis of new communications paradigms (for improved error rate performance and decoding complexity), to the further application of group and representation theory to the development of these systems.

Appendix A

Mathematical Background

A.1 Semi-Direct Product

We use a semi-direct product to express an affine reflection group in (2.32) and a Bruhat decomposition in (A.24). Let $\mathcal{G}$ and $\mathcal{H}$ be groups. We define a *semi-direct product* $\mathcal{G} \ltimes \mathcal{H}$ as the set of all pairs (g, h), from $g \in \mathcal{G}$ and $h \in \mathcal{H}$ with multiplication defined as

$$(g, h) \cdot (g', h') = (gg', (g'^{-1}hg')h^{-1}) \tag{A.1}$$

for all $g, g' \in \mathcal{G}$ and $h, h' \in \mathcal{H}$.

A.2 Representation Theory and Character Table

An excellent reference on groups, representation theory and character tables can be found on [42]. They are used in Chapters 3 and 5.

Let $\mathcal{G}$ be a group. A representation φ of a group $\mathcal{G}$ is a group homomorphism $\varphi : \mathcal{G} \longmapsto GL_n(\mathbb{C})$ where $GL_n(\mathbb{C})$ is the general linear group consisting of $n \times n$ invertible matrices with complex entries. We call n the *degree* of the representation. A representation is irreducible if the only subspaces of $\mathbb{C}^n$ preserved by all $\varphi(g)$, $g \in \mathcal{G}$, are the zero subspace and $\mathbb{C}^n$ itself; it is reducible otherwise. Define the direct sum of two representations φ and φ', of degrees n and n', respectively, to be the representation

$\varphi \oplus \varphi' \colon \mathcal{G} \to GL_{n+n'}(\mathbb{C})$ given by

$$(\varphi \oplus \varphi')(g) = \begin{bmatrix} \varphi(g) & 0 \\ 0 & \varphi'(g) \end{bmatrix} \tag{A.2}$$

for each $g \in \mathcal{G}$. It has been proven that any reducible representation of a finite group may be written as a direct sum of two or more irreducible representations (with respect to a suitable choice of basis of $\mathbb{C}^n$).

The *character* χ of representation φ of a group $\mathcal{G}$ is a mapping $\chi : G \to \mathbb{C}$ defined as

$$\chi(g) = \operatorname{tr} \varphi(g) = \sum_{i=1}^{n} \lambda_i \tag{A.3}$$

where $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the eigenvalues of $\varphi(g)$. We call χ an *irreducible character* or a *reducible character* if φ is an irreducible or a reducible representation respectively. We also call n the *degree* of χ. Let φ and φ' be two representations of a group $\mathcal{G}$ with characters χ and χ', respectively. Then the character of $\varphi \oplus \varphi'$ is the function $\chi + \chi'$. This allows us to easily compute the character of a new reducible group constellation which is constructed by a direct sum of irreducible representations.

Two elements $g, g' \in \mathcal{G}$ are *conjugate* if there is an element $h \in \mathcal{G}$ such that $g = hg'h^{-1}$. It follows that if χ is a character of $\mathcal{G}$, then $\chi(g) = \chi(g')$ whenever g and g' are conjugate. The *conjugacy class* of g is the set of all elements in $\mathcal{G}$ which are conjugate to g. It has been shown that the number of irreducible representations of a group $\mathcal{G}$ equals the number of conjugacy classes of $\mathcal{G}$. Hence the set of all irreducible characters can be described by an $h \times h$ matrix called a *character table* where h is a number of conjugacy classes of a group $\mathcal{G}$. The rows represent irreducible characters $\{\chi_i\}_{i=1}^{h}$, and the columns represent the values of these characters on elements of the distinct conjugacy classes $\{\mathcal{C}_i\}_{i=1}^{h}$. Let the first column correspond to the conjugacy class $\{e\}$ of the identity element of $\mathcal{G}$. Note that for any irreducible character of $\mathcal{G}$, $\chi(e) =$ degree of $\varphi = n$ and $|\chi(g)| \leq \chi(e)$ for all $g \in \mathcal{G}$. Moreover $|\mathcal{G}| = \sum_{i=1}^{h} \chi_i(e)^2$ and $\chi_i(e)$ divides $|\mathcal{G}|$ [42].

We let $n = n_T$ be the number of transmitter antennas, and we consider only *unitary representations*, that is, representation φ such that $\varphi(g)\varphi(g)^* = I_{n_T}$ for all $g \in \mathcal{G}$. (This is no restriction, since all representations of a finite group are unitary with respect to a suitable choice of basis.) We say that a group constellation $\mathcal{V}$, coming from a unitary representation φ, is a set of unitary representation matrices $\varphi(g)$ for all $g \in \mathcal{G}$:

$$\mathcal{V} = \{\varphi(g) \text{ for all } g \in \mathcal{G}\}. \tag{A.4}$$

We say φ is a *faithful representation* if φ is a one-to-one mapping between g and $\varphi(g)$ for all $g \in \mathcal{G}$. Thus if there exist $g \neq h \in \mathcal{G}$ such that $\varphi(g) = \varphi(h)$ then φ is not faithful. We use this to define a nonzero diversity sum unitary constellation in Definition 5.2.1.

A.2.1 The Group $PSL_2(\mathbb{F}_q)$ For Odd Prime q

We use the description of the group $SL_2(\mathbb{F}_q)$, for odd prime q, given in [79]. Let us summarize the number and the sizes of the conjugacy classes and the character table of $PSL_2(\mathbb{F}_q)$ for an odd prime q below.

Let φ denote a representation of $SL_2(\mathbb{F}_q)$. If $\varphi(I) = \varphi(-I)$ then by the group homomorphism property, $\varphi(g) = \varphi(-g)$ for all $g \in SL_2(\mathbb{F}_q)$. Hence φ may be thought of as a representation of $PSL_2(\mathbb{F}_q) = SL_2(\mathbb{F}_q)/\{\pm I\}$, denoted $\bar{\varphi}$ for clarity. The order of $PSL_2(\mathbb{F}_q)$ is one half of the order of $SL_2(\mathbb{F}_q)$ (where $|SL_2(\mathbb{F}_q)| = q(q^2-1)$), that is

$$|PSL_2(\mathbb{F}_q)| = \frac{1}{2}q(q^2-1). \tag{A.5}$$

The group $SL_2(\mathbb{F}_q)$ has $q+4$ conjugacy classes which are denoted A, B, $C_1, \ldots, C_{(q-3)/2}$, $D_1, \ldots, D_{(q-1)/2}$, E_1,E_{-1},F_1 and F_{-1}. Since we are quotienting out by the center of $SL_2(\mathbb{F}_q)$, the conjugacy classes of $PSL_2(\mathbb{F}_q)$ are formed by taking the union of conjugacy classes of $SL_2(\mathbb{F}_q)$. Namely, if $g \in \mathcal{C}_i$ and $-g \in \mathcal{C}_j$ then $\mathcal{C}_i \cup \mathcal{C}_j$ lifts to a single conjugacy class of $PSL_2(\mathbb{F}_q)$. It can be shown that the conjugacy classes of $SL_2(\mathbb{F}_q)$

lift as follows to form conjugacy classes of $PSL_2(\mathbb{F}_q)$:

$$
\begin{aligned}
&A = B \\
&\begin{cases} C_1 = C_2, C_3 = C_4, \ldots, C_{(q-3)/2-1} = C_{(q-3)/2} \text{ if } (q-3)/2 \text{ is an even number or} \\ C_1 = C_2, C_3 = C_4, \ldots, C_{(q-3)/2} \text{ if } (q-3)/2 \text{ is an odd number} \end{cases} \\
&\begin{cases} D_1 = D_2, D_3 = D_4, \ldots, D_{(q-1)/2-1} = D_{(q-1)/2} \text{ if } (q-1)/2 \text{ is an even number} \quad \text{or} \\ D_1 = D_2, D_3 = D_4, \ldots, D_{(q-1)/2} \text{ if } (q-1) \text{ is an odd number} \end{cases} \\
&E_1 = F_{-1} \\
&E_{-1} = F_1.
\end{aligned}
\tag{A.6}
$$

Consequently the number of conjugacy classes of the group $PSL_2(\mathbb{F}_q)$ is

$$
3 + \left\lceil \frac{q-3}{4} \right\rceil + \left\lceil \frac{q-1}{4} \right\rceil \tag{A.7}
$$

where $\lceil\ \rceil$ denotes the upper floor integer. The sizes of those conjugacy classes in $PSL_2(\mathbb{F}_q)$ are

$$
\begin{aligned}
&|A| = |B| = 1 \\
&|C_i| = q(q+1) \text{ , and } |C_{(q-3)/2}| = q(q+1)/2 \text{ if } (q-3)/2 \text{ is an odd number} \\
&|D_i| = q(q-1) \text{ , and } |D_{(q-1)/2}| = q(q-1)/2 \text{ if } (q-1)/2 \text{ is an odd number} \\
&|E_1| = |F_{-1}| = (q^2-1)/2 \\
&|E_{-1}| = |F_1| = (q^2-1)/2.
\end{aligned}
\tag{A.8}
$$

The character table of $PSL_2(\mathbb{F}_q)$ can then be computed from the character table of $SL_2(\mathbb{F}_q)$ (Table II in [79]). For example, the irreducible character $\chi = R_T^G(\alpha)$ of $SL_2(\mathbb{F}_q)$ has $\chi(A) = q+1$ and $\chi(B) = \alpha(-1)(q+1)$. Hence to have $\chi(A) = \chi(B)$ and hence a representation of $PSL_2(\mathbb{F}_q)$, we need to restrict to the case $\alpha(-1) = 1$. The remaining irreducible characters can be defined in the same way. The character table of $PSL_2(\mathbb{F}_q)$ is given in Table A.1 where ω is a generator of $\mathbb{F}_q^\times$ and θ is a primitive $(q+1)$st root of unity over $\mathbb{F}_{q^2}$. The α and β are multiplicative mappings from $\mathbb{F}_q^\times$ and $\mathbb{F}_{q^2}$ to complex numbers respectively (a homomorphism from $\mathbb{F}_q^\times$ or $\mathbb{F}_q$ to $\mathbb{C}$ is also called a character). We define α_0 and β_0 by mapping squares in their fields to 1, and nonsquares to -1.

	$A = B$	C_i	D_i	$E_1 = F_{-1}$	$E_{-1} = F_1$
Id	1	1	1	1	1
$R_T^G(\alpha)$	$q+1$	$\alpha(\omega^i) + \alpha(\omega^{-i})$	0	1	1
St	q	1	-1	0	0
$R_T^G(\beta)$	$q-1$	0	$-\beta(\theta^i) - \beta(\theta^{-i})$	-1	-1
$\chi_{\alpha_0}^{\epsilon}$	$(q+1)/2$	$\alpha_0(\omega^i)$	0	$\frac{1+j\sqrt{q}}{2}$	$\frac{1-j\sqrt{q}}{2}$
$\chi_{\beta_0}^{\epsilon}$	$(q-1)/2$	0	$-\beta_0(\theta^i)$	$\frac{-1+j\sqrt{q}}{2}$	$\frac{-1-j\sqrt{q}}{2}$

Table A.1: The character table of the group $PSL_2(\mathbb{F}_q)$

A.2.2 Explicit 4-Dimensional Representations of $SL_2(\mathbb{F}_5)$

We compute some 4-dimensional representations of $SL_2(\mathbb{F}_5)$ following the construction in [81]. We first choose an additive character Φ of $\mathbb{F}_5$ via $\Phi(u) = e^{2\pi j \frac{u}{5}}$ for $u \in \{0, 1, 2, 3, 4\}$. Secondly we choose a multiplicative character α of $\mathbb{F}_5^*$, from among four possible choices:

i) $\alpha(z) = 1$ for all $z \in \{1, 2, 3, 4\}$, the trivial character.

ii) $\alpha(1) = \alpha(2^2) = 1$, $\alpha(2) = \alpha(2^3) = -1$.

iii) $\alpha(1) = 1, \alpha(2) = j, \alpha(4) = -1, \alpha(3) = -j$.

iv) $\alpha(1) = 1, \alpha(2) = -j, \alpha(4) = -1, \alpha(3) = j$.

We note that (iii) and (iv) are inverses of one another. Thirdly, consider the field $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{2}) = \{c + d\sqrt{2} | c, d \in F_5\}$. $\mathbb{F}_{25}^*$ is cyclic, with generator $\epsilon = 2 + 4\sqrt{2}$. We choose a character Π of $\mathbb{F}_{25}^*$; there are $24 = |\mathbb{F}_{25}^*|$ possible choices.

To get *discrete series representations* (such as χ_3, see Table 5.1 in Chapter 5) however, there is a condition. Let N^1 denote those elements in $\mathbb{F}_{25}^*$ whose *norm* is equal to 1. The norm of an element of $\mathbb{F}_{25}^*$ is defined by $N(c + d\sqrt{2}) = (c + d\sqrt{2})(c - d\sqrt{2}) = c^2 - 2d^2$. From direct calculations, we deduce that $N^1 = \{1, \epsilon^4, \epsilon^8, \ldots, \epsilon^{20}\}$. The condition on Π is that its restriction to N^1 is not allowed to be trivial. Moreover, if two choices of Π give the same restriction to N^1, or restrictions to N^1 which are exactly inverses of each other, then the resulting discrete series representations will be the same.

Finally, there is a condition relating Π and α. Namely, one must have $\Pi(2) = \alpha(2)$ (so that Π and α agree on $\mathbb{F}_5^*$). Since $2 = \epsilon^6$, this implies we have the following choices:

i) $\Pi(\epsilon^n) = e^{\pi j n/12}$, $\alpha(2^n) = e^{\pi j n/2}$.

ii) $\Pi(\epsilon^n) = e^{\pi j n/6}$, $\alpha(2^n) = e^{\pi j n}$.

iii) $\Pi(\epsilon^n) = e^{\pi jn/4}$, $\alpha(2^n) = e^{\pi j3n/2}$.

The first two will give irreducible discrete series (characters χ_4 and χ_3, respectively) and the last will be reducible, with two inequivalent 2-dimensional components.

We need one technical definition, which will simplify the notation in what follows. For each $n \in \{0, 1, \ldots, 23\}$, write $\epsilon^n = c_n + d_n\sqrt{2}$ with $c_n, d_n \in \{0, 1, 2, 3, 4\}$. Thus, for example, $c_0 = 1$, $c_1 = 2$, $c_2 = 1$, $c_3 = 0$, $c_4 = 3$, $c_5 = 2$. Since multiplication by ϵ^6 is multiplication by a number in $\mathbb{F}_5^*$, we deduce that $c_{6+n} = 2c_n$, $c_{12+n} = 4c_n$ and $c_{18+n} = 3c_n$, and so the rest are easily computed. For each $N \in \{0, 1, 2, 3\}$, define a complex number $F(N)$ as follows:

$$F(N) = \sum_{0 \le n \le 23, n \equiv N \mod 4} \Pi(\epsilon^n)\Phi(2c_n).$$

So for example, for χ_4, if $N = 0$ and we take $\Pi(\epsilon^n) = e^{\pi jn/12}$, then $F(0) = e^{2\pi j\frac{2}{5}} + e^{2\pi j\frac{4}{24}}e^{2\pi j\frac{1}{5}} + e^{2\pi j\frac{8}{24}}e^{2\pi j\frac{4}{5}} + e^{2\pi j\frac{12}{24}}e^{2\pi j\frac{8}{5}} + e^{2\pi j\frac{16}{24}}e^{2\pi j\frac{4}{5}} + e^{2\pi j\frac{20}{24}}e^{2\pi j\frac{6}{5}}$.

Each element of $SL_2(\mathbb{F}_5)$ is either of the form

$$\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & au \\ 0 & a^{-1} \end{bmatrix} \tag{A.9}$$

with $a \in \mathbb{F}_5^* = \{1, 2, 3, 4\}$ and $u \in \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, or of the form

$$\begin{bmatrix} 1 & v \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -av & -auv + a^{-1} \\ -a & -au \end{bmatrix} \tag{A.10}$$

with $a \in \mathbb{F}_5^*$, and $u, v \in \mathbb{F}_5$. Thus there are 20 elements of the first kind and 100 of the second kind.

For elements in g of the first kind (A.9), the (i, k)th element of the representation matrix $\varphi(g)$ is given by

$$\varphi(g)_{i,k} = \alpha(a)\Phi(ku) \quad \text{if } ki^{-1} = a^2 \tag{A.11}$$

and is zero otherwise. The formula for the (i, k)th matrix coefficient of $\varphi(g)$, when g

is of the form (A.10), is

$$\varphi(g)_{i,k} = -\frac{1}{5}\Phi(iv + ku)\alpha(ai^{-1})F(\log_2(ika^{-2})) \tag{A.12}$$

where $N = \log_2(ika^{-2}) \in \{0, 1, 2, 3\}$ is the number so that $2^N \equiv ika^{-2} \mod 5$.

The group $SL_2(\mathbb{F}_5)$ has two generators $\boldsymbol{P}$ and $\boldsymbol{Q}$ [80]. The 120 elements are given by $(PQ)^j X$, where $j = 0, 1, \ldots, 9$ and X runs over $\{\boldsymbol{I}_2, \boldsymbol{P}, \boldsymbol{Q}, \boldsymbol{QP}, \boldsymbol{QPQ}, \boldsymbol{QPQP}, \boldsymbol{QPQ}^2, \boldsymbol{QPQPQ}, \boldsymbol{QPQPQ}^2, \boldsymbol{QPQPQ}^2 P, \boldsymbol{QPQPQ}^2\boldsymbol{PQ}, \boldsymbol{QPQPQ}^2\boldsymbol{PQP}\}$. We deduce from calculations that the two generators P and Q belong to elements of the second kind (A.10), namely

$$\boldsymbol{P} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ when } a = 1, u = 0, v = 0$$

and

$$\boldsymbol{Q} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \text{ when } a = 1, u = -1, v = 0.$$

(Note that $(\boldsymbol{PQ})^5 = \boldsymbol{I}$, which shows that $PSL_2(\mathbb{F}_q)$ is generated using only $j \in \{0, 1, 2, 3, 4\}$, above.) Using the formula (A.12), the 4-dimensional representation corresponding to χ_4 of P is

$$\varphi(P)_{i,k} = -\frac{1}{5}\alpha(i^{-1})F(\log_2(ik)) \tag{A.13}$$

for $i, k = 1, 2, 3, 4$. This gives

$$\varphi(\boldsymbol{P}) = -\frac{1}{5}\begin{bmatrix} F(0) & F(1) & F(3) & F(2) \\ -jF(1) & -jF(2) & -jF(0) & -jF(3) \\ jF(3) & jF(0) & jF(2) & jF(1) \\ -F(2) & -F(3) & -F(1) & -F(0) \end{bmatrix}, \tag{A.14}$$

where

$$
\begin{aligned}
F(0) &= e^{2\pi j\frac{2}{5}} + e^{2\pi j\frac{4}{24}}e^{2\pi j\frac{1}{5}} + e^{2\pi j\frac{8}{24}}e^{2\pi j\frac{4}{5}} + e^{2\pi j\frac{12}{24}}e^{2\pi j\frac{8}{5}} + e^{2\pi j\frac{16}{24}}e^{2\pi j\frac{4}{5}} + e^{2\pi j\frac{20}{24}}e^{2\pi j\frac{6}{5}} && \text{(A.15)}\\
F(1) &= e^{2\pi j\frac{1}{24}}e^{2\pi j\frac{4}{5}} + e^{2\pi j\frac{5}{24}}e^{2\pi j\frac{4}{5}} + e^{2\pi j\frac{9}{24}} + e^{2\pi j\frac{13}{24}}e^{2\pi j\frac{6}{5}} + e^{2\pi j\frac{17}{24}}e^{2\pi j\frac{6}{5}} + e^{2\pi j\frac{21}{24}} && \text{(A.16)}\\
F(2) &= e^{2\pi j\frac{2}{24}}e^{2\pi j\frac{2}{5}} + e^{2\pi j\frac{6}{24}}e^{2\pi j\frac{4}{5}} + e^{2\pi j\frac{10}{24}}e^{2\pi j\frac{2}{5}} + e^{2\pi j\frac{14}{24}}e^{2\pi j\frac{8}{5}} + e^{2\pi j\frac{18}{24}}e^{2\pi j\frac{6}{5}} + e^{2\pi j\frac{22}{24}}e^{2\pi j\frac{8}{5}} && \text{(A.17)}\\
F(3) &= e^{2\pi j\frac{3}{24}} + e^{2\pi j\frac{7}{24}}e^{2\pi j\frac{8}{5}} + e^{2\pi j\frac{11}{24}}e^{2\pi j\frac{8}{5}} + e^{2\pi j\frac{15}{24}} + e^{2\pi j\frac{19}{24}}e^{2\pi j\frac{2}{5}} + e^{2\pi j\frac{23}{24}}e^{2\pi j\frac{2}{5}}. && \text{(A.18)}
\end{aligned}
$$

The 4-dimensional representation corresponding to χ_4 of Q (also using a formula (A.12)) is

$$\varphi(\boldsymbol{Q})_{i,k} = -\frac{1}{5}e^{-j2\pi k/5}\alpha(i^{-1})F(\log_2(ik)) = e^{-2\pi j\frac{k}{5}}\varphi(\boldsymbol{P}) \tag{A.19}$$

for $i, k = 1, 2, 3, 4$. This gives

$$\varphi(\boldsymbol{Q}) = -\frac{1}{5}\begin{bmatrix} e^{-2\pi j\frac{1}{5}}F(0) & e^{-2\pi j\frac{2}{5}}F(1) & e^{-2\pi j\frac{3}{5}}F(3) & e^{-2\pi j\frac{4}{5}}F(2) \\ -je^{-2\pi j\frac{1}{5}}F(1) & -je^{-2\pi j\frac{2}{5}}F(2) & -je^{-2\pi j\frac{3}{5}}F(0) & -je^{-2\pi j\frac{4}{5}}F(3) \\ je^{-2\pi j\frac{1}{5}}F(3) & je^{-2\pi j\frac{2}{5}}F(0) & je^{-2\pi j\frac{3}{5}}F(2) & je^{-2\pi j\frac{4}{5}}F(1) \\ -e^{-2\pi j\frac{1}{5}}F(2) & -e^{-2\pi j\frac{2}{5}}F(3) & -e^{-2\pi j\frac{3}{5}}F(1) & -e^{-2\pi j\frac{4}{5}}F(0) \end{bmatrix}. \tag{A.20}$$

For the 2-dimensional representations (χ_7), we have more directly from [80] that

$$\varphi(\boldsymbol{P}) = \frac{1}{\sqrt{5}}\begin{bmatrix} \eta^2-\eta^3 & \eta-\eta^4 \\ \eta-\eta^4 & \eta^3-\eta^2 \end{bmatrix}, \quad \varphi(\boldsymbol{Q}) = \frac{1}{\sqrt{5}}\begin{bmatrix} \eta-\eta^2 & \eta^2-1 \\ 1-\eta^3 & \eta^4-\eta^3 \end{bmatrix} \tag{A.21}$$

where $\eta = e^{j2\pi/5}$.

A.3 Bruhat Decomposition

One excellent reference on *Bruhat decomposition* is [9]. The purpose of using Bruhat decomposition is to construct a set of unitary matrices in Chapter 4. Let S_M denote the symmetric group of order M, that is, the group consisting of all permutations of M elements. We use the notation (123) to denote the cycle sending $1 \to 2 \to 3 \to 1$; every element of S_M may be decomposed uniquely into a product of disjoint cycles. Of particular interest is cycle $\omega = (12\cdots M)$. For $i > 1$, the permutation $\omega^i = \omega \cdot \cdots \cdot \omega$

(i times) need not be a single cycle. Set $g = \gcd(i, M)$ and $b = M/g$. Then we may decompose

$$\omega^i = \sigma_1\, \sigma_2 \cdots \sigma_g \tag{A.22}$$

where σ_r is the cycle $(r, r\oplus i, r\oplus 2i, \cdots, r\oplus(b-1)i)$ where we write $r\oplus k$ for the result of adding k to r mod M. For example, if $\omega = (123456)$ and $i = 4$, then $g = \gcd(4, 6) = 2$ and $b = 6/2 = 3$. So we have $\omega^4 = (153)(264)$ is a product of 2 disjoint cycles of length 3.

The group S_M has a natural representation on $\mathbb{C}^M$, called the permutation representation, in which each element $\boldsymbol{\tau} \in S_M$ is realized as the $M \times M$ matrix of the linear transformation which permutes the standard basis vectors $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, ... $\boldsymbol{e}_M$ of $\mathbb{C}^M$ according to $\boldsymbol{\tau}$. For example, in S_3, the permutation $\boldsymbol{\tau} = (123)$ sends $\boldsymbol{e}_1$ to $\boldsymbol{e}_2$, $\boldsymbol{e}_2$ to $\boldsymbol{e}_3$ and $\boldsymbol{e}_3$ to $\boldsymbol{e}_1$. Hence under the natural representation, we identify $\boldsymbol{\tau}$ with the (unitary) matrix

$$\boldsymbol{\tau} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

The symmetric group has a special relationship with the general linear group $GL(M)$ (that is, the group of all invertible $M \times M$ matrices) defined by the *Bruhat decomposition.* The Bruhat decomposition of $GL(M)$ is the disjoint union of double cosets

$$GL(M) = \bigcup_{\boldsymbol{\tau}\in S_M} \mathcal{B}\boldsymbol{\tau}\mathcal{B} \tag{A.23}$$

where $\mathcal{B}$ denotes the subgroup of all invertible upper triangular matrices, and $\boldsymbol{\tau}$ is written in its natural representation. More generally, any reductive Lie group admits a Bruhat decomposition, relative to a Borel subgroup $\mathcal{B}$ and its Weyl group $\mathcal{W}$ (in place of S_M).

Since the group $\mathcal{B}$ in (A.23) is not unitary, we need to consider a subgroup of $\mathcal{B}$, the diagonal unitary matrices $\mathcal{T}$ where $\mathcal{T}$ is the subgroup of all unitary matrices in $\mathcal{B}$. A quick calculation reveals that the double coset $\mathcal{T}\boldsymbol{\tau}\mathcal{T}$ is equal to the left coset $\boldsymbol{\tau}\mathcal{T}$ for any $\boldsymbol{\tau} \in S_M$. Restricting to $\mathcal{T}$ in equation (A.23) defines a unitary subgroup of

$GL(M)$. This defines an infinite unitary subgroup of $GL(M)$ as:

$$S_M \ltimes \mathcal{T} = \bigcup_{\tau \in S_M} \mathcal{T}\tau\mathcal{T} = \bigcup_{\tau \in S_M} \tau\mathcal{T}. \tag{A.24}$$

The multiplication in this group respects this decomposition, and is given by $(\tau_1 t_1) \cdot (\tau_2 t_2) = (\tau_1\tau_2) \cdot [(\tau_2^{-1} t_1 \tau_2) t_2]$.

A.4 Hypergeometric Functions

All definitions of hypergeometric functions are from [27]. We use the hypergeometric functions to express the closed form PEP of STC in keyhole channel in Chapter 7. The generalized hypergeometric function is given by

$${}_pF_q(a_1, \ldots, a_p; b_1, \ldots, b_q; z) = \sum_{k=0}^{\infty} \frac{(a_1)_k (a_2)_k \cdots (a_p)_k}{(b_1)_k (b_2)_k \cdots (b_q)_k} \frac{z^k}{k!} \tag{A.25}$$

where $(a)_k = a(a+1)\cdots(a+k-1)$ is called a rising factorial.

The degenerate hypergeometric function is defined as

$$\Psi(a, b; z) = \frac{1}{\Gamma(a)} \int_0^{\infty} e^{-zt} t^{a-1} (1+t)^{b-a-1} dt, \quad \mathrm{Re}\{a\} > 0 \tag{A.26}$$

where $\Gamma(\cdot)$ denotes a gamma function. Of particular interest, we define

$${}_2F_0(a, b; ; -z^{-1}) = z^a \Psi(a, a-b+1; z). \tag{A.27}$$

A.5 Moment Generating Function (MGF)-Based Approach

In this appendix, we give necessary background on probability density functions (pdfs) which is used in Chapter 7 to analyze the average PEP starting from the conditional PEP, starting with a given product of two random variables; see (7.11). The reference of pdf and Moment Generating Function (MGF)-based approach is from [82].

Let $P(E|Y = y)$ be the conditional probability of error for a given nonnegative random variable Y, and let $p_Y(y)$ be the probability density function (pdf) of Y. The average probability of error is computed by $P(E) = \int_0^\infty P(E|Y = y)p_Y(y)dy$, whereas the MGF of Y is defined as

$$M_Y(s) = E[e^{sY}] = \int_0^\infty e^{sy} p_Y(y)dy. \tag{A.28}$$

Suppose the conditional probability of error for a given Y is of the form $P(E|Y = y) = ke^{-sy}$ where k and s are positive constants. Then the average probability of error is computed as

$$P(E) = \int_0^\infty ke^{-sy} p_Y(y)dy = kM_Y(-s). \tag{A.29}$$

Now consider a keyhole channel whose channel matrix is $\boldsymbol{H} = \boldsymbol{\beta}\boldsymbol{\alpha}^T$ and set $Y = ||\boldsymbol{H}||^2$. Then $Y = ||\boldsymbol{H}||^2 = ||\boldsymbol{\alpha}||^2||\boldsymbol{\beta}||^2 = UV$, where now U and V are Chi-square random variables with $2M$ and $2N$ degrees of freedom respectively. For $y \geq 0$, the pdf of $Y = UV$ is computed by [78]

$$\begin{aligned} p_Y(y) &= \int_{-\infty}^{\infty} \frac{1}{|u|} p_U(u) p_V\left(\frac{y}{u}\right) du & \text{(A.30)} \\ &= \int_0^\infty \frac{t^{M-N-1} e^{-t-\frac{y}{t}} y^{N-1}}{\Gamma(M)\Gamma(N)} dt & \text{(A.31)} \end{aligned}$$

where $\Gamma(\cdot)$ is the gamma function.

To express its MGF, we recall the degenerate hypergeometric function $\Psi(a, b; z)$ and the generalized hypergeometric function ${}_pF_q$ in Appendix A.4. It is shown in [78] that the MGF of $Y = UV$ is given by

$$\begin{aligned} M_Y(s) &= s^{-M} \Psi(M, M - N + 1; s^{-1}) & \text{(A.32)} \\ &= {}_2F_0(M, N; ; -s). & \text{(A.33)} \end{aligned}$$

Appendix B

Computation of Initial Vectors

Recall from Theorem 8.1.1 that the nearest distance between codewords in affine reflection group code is computed from

$$d = \frac{2}{\|\boldsymbol{\rho}\| + \sum_{i=1}^{n} a_i \|\boldsymbol{r}_i\|}; \tag{B.1}$$

and the initial vector is

$$\boldsymbol{x}_0 = \sum_{i=1}^{n} \frac{d\|\boldsymbol{r}_i\|}{2} \boldsymbol{\lambda}_i \tag{B.2}$$

where $\Delta = \{\boldsymbol{r}_i\}$ is the simple system, $\{\boldsymbol{\lambda}_i\}$ is the dual basis of Δ and $\boldsymbol{\rho} = \sum_{i=1}^{n} a_i \boldsymbol{r}_i$ is the highest long root, see Table 2.2. In the following, we compute the values in Table 8.1.

For $\mathcal{A}_2$

The two 3-dimensional simple roots of $\mathcal{A}_2$ are $\boldsymbol{r}_1 = \frac{1}{\sqrt{2}}(-1, 1, 0)$ and $\boldsymbol{r}_2 = \frac{1}{\sqrt{2}}(0, -1, 1)$. Using the Gram-Schmidt method to obtain an orthonormal basis for the space spanned by these roots yields coordinates for these simple roots in 2 dimensional space as $\boldsymbol{r}_1 = (1, 0)$ and $\boldsymbol{r}_2 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. The highest long root is $\boldsymbol{\rho} = \boldsymbol{r}_1 + \boldsymbol{r}_2 = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. Hence the nearest distance is

$$d = \frac{2}{1 + (1 + 1)} = \frac{2}{3}. \tag{B.3}$$

The dual basis to the simple roots is the set

$$\boldsymbol{\lambda}_1 = \left(1, \frac{1}{\sqrt{3}}\right), \quad \text{and} \quad \boldsymbol{\lambda}_2 = \left(0, \frac{2}{\sqrt{3}}\right).$$

Since $\frac{d\|\boldsymbol{r}_i\|}{2} = \frac{1}{3}$ for all $i = 1, 2$, we have the initial vector

$$\boldsymbol{x}_0 = \frac{1}{3}\left(1, \sqrt{3}\right). \tag{B.4}$$

For $\mathcal{A}_3$

The three 4-dimensional simple roots of $\mathcal{A}_3$ are $\boldsymbol{r}_1 = \frac{1}{\sqrt{2}}(-1,1,0,0)$, $\boldsymbol{r}_2 = \frac{1}{\sqrt{2}}(0,-1,1,0)$ and $\boldsymbol{r}_3 = \frac{1}{\sqrt{2}}(0,0,-1,1)$. Using the Gram-Schmidt method to obtain an orthonormal basis for the space spanned by these roots yields coordinates for these simple roots in 3 dimensional space as

$$\boldsymbol{r}_1 = (1,0,0), \boldsymbol{r}_2 = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}, 0\right) \text{ and } \boldsymbol{r}_3 = \left(0, -\frac{1}{\sqrt{3}}, \sqrt{\frac{2}{3}}\right).$$

The highest long root is

$$\boldsymbol{\rho} = \boldsymbol{r}_1 + \boldsymbol{r}_2 + \boldsymbol{r}_3 = \left(\frac{1}{2}, \frac{1}{2\sqrt{3}}, \sqrt{\frac{2}{3}}\right).$$

Hence the nearest distance is

$$d = \frac{2}{1 + (1+1+1)} = \frac{1}{2}. \tag{B.5}$$

The dual basis to the simple roots is the set

$$\boldsymbol{\lambda}_1 = \left(1, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{6}}\right), \boldsymbol{\lambda}_2 = \left(0, \frac{2}{\sqrt{3}}, \sqrt{\frac{2}{3}}\right) \text{ and } \boldsymbol{\lambda}_3 = \left(0, 0, \frac{\sqrt{3}}{2}\right).$$

Since $\frac{d\|\boldsymbol{r}_i\|}{2} = \frac{1}{4}$ for all $i = 1, 2, 3$, we have the initial vector

$$\boldsymbol{x}_0 = \frac{1}{4}\left(1, \sqrt{3}, \frac{\sqrt{3}(1+\sqrt{2})}{2}\right). \tag{B.6}$$

For $\mathcal{A}_n$

Since $\|\boldsymbol{\rho}\| = \|\boldsymbol{r}_i\| = 1$ for all $i = 1, 2, \ldots, n$, we have

$$d = \frac{2}{1 + \sum_{i=1}^{n}(1)} = \frac{2}{n+1}. \tag{B.7}$$

The n-dimensional subspace of $\mathbb{R}^{n+1}$ spanned by the simple roots $\boldsymbol{r}_i = \frac{1}{\sqrt{2}}(e_i - e_{i-1})$, $2 \le i \le n$, of $\mathcal{A}_n$ is the hyperplane orthogonal to the vector $(1, 1, \ldots, 1)$. Hence, using the coordinates of the ambient space $\mathbb{R}^{n+1}$, we have that the dual basis is given by, for $1 \le i \le n$,

$$\boldsymbol{\lambda}_i = \frac{\sqrt{2}}{n+1}\left(\sum_{j \ne i} e_j - n e_i\right).$$

It now follows that

$$\boldsymbol{x}_0 = \frac{\sqrt{2}}{(n+1)^2}\left(n e_{n+1} - \sum_{i=1}^{n} e_i\right). \tag{B.8}$$

For $\mathcal{B}_3$

The simple roots are $\boldsymbol{r}_1 = (1, 0, 0), \boldsymbol{r}_2 = (-1, 1, 0)$ and $\boldsymbol{r}_3 = (0, -1, 1)$. The highest long root is

$$\boldsymbol{\rho} = 2\boldsymbol{r}_1 + 2\boldsymbol{r}_2 + \boldsymbol{r}_3 = (0, 1, 1).$$

So the nearest distance is

$$d = \frac{2}{\sqrt{2} + (2 + 2\sqrt{2} + \sqrt{2})} = \frac{1}{1 + 2\sqrt{2}}. \tag{B.9}$$

The dual basis to the basis of simple roots is the set of vectors $\boldsymbol{\lambda}_1 = (1, 1, 1), \boldsymbol{\lambda}_2 = (0, 1, 1)$ and $\boldsymbol{\lambda}_3 = (0, 0, 1)$. Hence the initial vector is

$$\boldsymbol{x}_0 = \left(\frac{1}{2 + 4\sqrt{2}}, \frac{1 + \sqrt{2}}{2 + 4\sqrt{2}}, \frac{1 + 2\sqrt{2}}{2 + 4\sqrt{2}}\right). \tag{B.10}$$

For $\mathcal{B}_n$

From Table 2.2, we deduce that $\|\boldsymbol{r}_i\|$ is 1 if $i = 1$ and $\sqrt{2}$ otherwise. Since all roots are obtained from the simple roots by orthogonal reflections, we deduce that the highest long root has length $\|\boldsymbol{\rho}\| = \sqrt{2}$ as well. Hence

$$d = \frac{2}{\sqrt{2} + 2 + \sum_{i=2}^{n-1} 2\sqrt{2} + \sqrt{2}} = \frac{1}{1 + (n-1)\sqrt{2}}. \tag{B.11}$$

The dual basis to the simple root basis is given by $\boldsymbol{\lambda}_i = \sum_{j=i}^{n} e_j$. Thus

$$\begin{aligned} \boldsymbol{x}_0 &= \frac{d}{2}\sum_{i=1}^{n} \|\boldsymbol{r}_i\|\boldsymbol{\lambda}_i \\ &= \frac{d}{2}(\boldsymbol{\lambda}_1 + \sqrt{2}\sum_{i=2}^{n} \boldsymbol{\lambda}_i) \\ &= \frac{1}{2(1+(n-1)\sqrt{2})}(1, 1+\sqrt{2}, 1+2\sqrt{2}, \ldots, 1+(n-1)\sqrt{2}). \end{aligned} \tag{B.12}$$

For $\mathcal{C}_n$

From Table 2.2, we deduce that $\|\boldsymbol{r}_i\|$ is 2 if $i = 1$ and $\sqrt{2}$ otherwise. Since all roots are obtained from the simple roots by orthogonal reflections, we deduce that the highest long root has length $\|\boldsymbol{\rho}\| = 2$ as well. Hence

$$d = \frac{2}{2 + 2 + \sum_{i=2}^{n} 2\sqrt{2}} = \frac{1}{2 + (n-1)\sqrt{2}}. \tag{B.13}$$

The dual basis to the simple root basis is given by $\boldsymbol{\lambda}_1 = \frac{1}{2}\sum_{j=1}^{n} e_j$ and $\boldsymbol{\lambda}_i = \sum_{j=i}^{n} e_j$ for $2 \le i \le n$. Thus

$$\begin{aligned} \boldsymbol{x}_0 &= \frac{d}{2}\sum_{i=1}^{n} \|\boldsymbol{r}_i\|\boldsymbol{\lambda}_i \\ &= \frac{d}{2}(2\boldsymbol{\lambda}_1 + \sqrt{2}\sum_{i=2}^{n} \boldsymbol{\lambda}_i) \\ &= \frac{1}{2(2+(n-1)\sqrt{2})}(1, 1+\sqrt{2}, 1+2\sqrt{2}, \ldots, 1+(n-1)\sqrt{2}). \end{aligned} \tag{B.14}$$

For $\mathcal{D}_4$

The simple roots are $\boldsymbol{r}_1 = (1,1,0,0), \boldsymbol{r}_2 = (-1,1,0,0), \boldsymbol{r}_3 = (0,-1,1,0)$ and $\boldsymbol{r}_4 = (0,0,-1,1)$. The highest long root is $\boldsymbol{\rho} = \boldsymbol{r}_1 + \boldsymbol{r}_2 + 2\boldsymbol{r}_3 + \boldsymbol{r}_4 = (0,0,1,1)$. The minimum distance is

$$d = \frac{2}{\sqrt{2} + (\sqrt{2} + 1\sqrt{2} + 2\sqrt{2} + \sqrt{2})} = \frac{1}{3\sqrt{2}}. \tag{B.15}$$

The dual basis are $\boldsymbol{\lambda}_1 = (1/2, 1/2, 1/2, 1/2)$, $\boldsymbol{\lambda}_2 = (-1/2, 1/2, 1/2, 1/2)$, $\boldsymbol{\lambda}_3 = (0, 0, 1, 1)$ and $\boldsymbol{\lambda}_4 = (0, 0, 0, 1)$. From $\frac{d\|\boldsymbol{r}_i\|}{2} = \frac{1}{6}$ for all $i = 1, 2, 3, 4$ so we have

$$\boldsymbol{x}_0 = \frac{1}{6}(0, 1, 2, 3). \tag{B.16}$$

For $\mathcal{D}_n$

Each root has length $\sqrt{2}$, and so it follows that

$$d = \frac{2}{\sqrt{2} + 3\sqrt{2} + \sum_{i=2}^{n-2} 2\sqrt{2}} = \frac{1}{(n-1)\sqrt{2}}. \tag{B.17}$$

As the roots are given by $\boldsymbol{r}_1 = e_1 + e_2$ and $\boldsymbol{r}_i = e_i - e_{i-1}$ for $i \geq 2$, we see that the dual basis is given by $\boldsymbol{\lambda}_1 = \frac{1}{2}\sum_{i=1}^{n} e_i$, $\boldsymbol{\lambda}_2 = \frac{1}{2}(\sum_{i=2}^{n} e_i - e_1)$, and $\boldsymbol{\lambda}_i = \sum_{j=i}^{n} e_j$. It follows that

$$\boldsymbol{x}_0 = \frac{d\sqrt{2}}{2}\sum_{i=1}^{n} \boldsymbol{\lambda}_i = \frac{1}{2(n-1)}(0, 1, 2, \ldots, n-1). \tag{B.18}$$

For $\mathcal{F}_4$

The simple roots of $\mathcal{F}_4$ are $\boldsymbol{r}_1 = (0, 1, -1, 0)$, $\boldsymbol{r}_2 = (0, 0, 1, -1)$, $\boldsymbol{r}_3 = (0, 0, 0, 1)$ and $\boldsymbol{r}_4 = \frac{1}{2}(1, -1, -1, -1)$. The highest long root is $\boldsymbol{\rho} = 2\boldsymbol{r}_1 + 3\boldsymbol{r}_2 + 4\boldsymbol{r}_3 + 2\boldsymbol{r}_4 = (1, 1, 0, 0)$. The nearest distance is

$$d = \frac{2}{\sqrt{2} + (2\sqrt{2} + 3\sqrt{2} + 4 + 2)} = \frac{1}{3(1 + \sqrt{2})}. \tag{B.19}$$

The dual basis vectors are $\boldsymbol{\lambda}_1 = (1, 1, 0, 0)$, $\boldsymbol{\lambda}_2 = (2, 1, 1, 0)$, $\boldsymbol{\lambda}_3 = (3, 1, 1, 1)$ and $\boldsymbol{\lambda}_4 = (2, 0, 0, 0)$. So the initial vector is

$$\boldsymbol{x}_0 = \frac{1}{6(1 + \sqrt{2})}(3\sqrt{2} + 5, 2\sqrt{2} + 1, \sqrt{2} + 1, 1). \tag{B.20}$$

For $\mathcal{E}_8$

The simple roots of $\mathcal{E}_8$ are

$$
\begin{aligned}
\boldsymbol{r}_1 &= \frac{1}{2}(1,-1,-1,-1,-1,-1,-1,1), & \boldsymbol{r}_2 &= (1,1,0,0,0,0,0,0),\\
\boldsymbol{r}_3 &= (-1,1,0,0,0,0,0,0), & \boldsymbol{r}_4 &= (0,-1,1,0,0,0,0,0),\\
\boldsymbol{r}_5 &= (0,0,-1,1,0,0,0,0), & \boldsymbol{r}_6 &= (0,0,0,-1,1,0,0,0),\\
\boldsymbol{r}_7 &= (0,0,0,0,-1,1,0,0), & \boldsymbol{r}_8 &= (0,0,0,0,0,-1,1,0). \qquad \text{(B.21)}
\end{aligned}
$$

The highest long root of $\mathcal{E}_8$ is $\boldsymbol{\rho} = 2\boldsymbol{r}_1 + 3\boldsymbol{r}_2 + 4\boldsymbol{r}_3 + 6\boldsymbol{r}_4 + 5\boldsymbol{r}_5 + 4\boldsymbol{r}_6 + 3\boldsymbol{r}_7 + 2\boldsymbol{r}_8 = (0,0,0,0,0,0,1,1)$. Each root has length $\sqrt{2}$, so it follows that the nearest distance is

$$d = \frac{2}{\sqrt{2} + \sum_{i=1}^{8} a_i\sqrt{2}} = \frac{1}{15\sqrt{2}}. \qquad \text{(B.22)}$$

The dual basis is

$$
\begin{aligned}
\boldsymbol{\lambda}_1 &= (0,0,0,0,0,0,0,2), & \boldsymbol{\lambda}_2 &= \frac{1}{2}(1,1,1,1,1,1,1,5),\\
\boldsymbol{\lambda}_3 &= \frac{1}{2}(-1,1,1,1,1,1,1,7), & \boldsymbol{\lambda}_4 &= (0,0,1,1,1,1,1,5),\\
\boldsymbol{\lambda}_5 &= (0,0,0,1,1,1,1,4), & \boldsymbol{\lambda}_6 &= (0,0,0,0,1,1,1,3),\\
\boldsymbol{\lambda}_7 &= (0,0,0,0,0,1,1,2), & \boldsymbol{\lambda}_8 &= (0,0,0,0,0,0,1,1).
\end{aligned}
$$

Since $\frac{d\|\boldsymbol{r}_i\|}{2} = \frac{1}{30}$ for all $i = 1, 2, \ldots, 8$, the best initial vector of $\mathcal{E}_8$ is

$$\boldsymbol{x}_0 = \frac{1}{30}(0,1,2,3,4,5,6,23). \qquad \text{(B.23)}$$

For $\mathcal{E}_7$

The 7 simple roots of $\mathcal{E}_7$ in $\mathbb{R}^8$ are $\Delta = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_7\}$ of (B.21); the span of these roots is the 7-dimensional subspace W_7 upon which $\mathcal{E}_7$ acts irreducibly by affine reflections. Each root has length $\sqrt{2}$ and, by Table 2.2, the highest long root is $\boldsymbol{\rho} = 2\boldsymbol{r}_1 + 2\boldsymbol{r}_2 + 3\boldsymbol{r}_3 + 4\boldsymbol{r}_4 + 3\boldsymbol{r}_5 + 2\boldsymbol{r}_6 + \boldsymbol{r}_7 = (0,0,0,0,0,0,-1,1)$. Hence the optimal nearest neighbour distance is

$$d = \frac{2}{\sqrt{2} + \sum_{i=1}^{7} a_i\sqrt{2}} = \frac{1}{9\sqrt{2}} \qquad \text{(B.24)}$$

From [38, Table 13.1], we have that the dual basis to Δ, that is, the set of vectors $\boldsymbol{\lambda}_i \in W_7 \subset \mathbb{R}^8$ with the property that $\boldsymbol{\lambda}_i \cdot \boldsymbol{r}_j = \delta_{ij}$ for all $i, j \in \{1, 2, \ldots, 7\}$, is given by

$$\begin{aligned}
\boldsymbol{\lambda}_1 &= (0,0,0,0,0,0,-1,1), & \boldsymbol{\lambda}_2 &= \frac{1}{2}(1,1,1,1,1,1,-2,2),\\
\boldsymbol{\lambda}_3 &= \frac{1}{2}(-1,1,1,1,1,1,-3,3), & \boldsymbol{\lambda}_4 &= (0,0,1,1,1,1,-2,2),\\
\boldsymbol{\lambda}_5 &= \frac{1}{2}(0,0,0,2,2,2,-3,3), & \boldsymbol{\lambda}_6 &= (0,0,0,0,1,1,-1,1),\\
\boldsymbol{\lambda}_7 &= \frac{1}{2}(0,0,0,0,0,2,-1,1).
\end{aligned}$$

It now follows from (8.8) that the best initial vector is

$$\boldsymbol{x}_0 = \frac{1}{18}(0,1,2,3,4,5,-\frac{17}{2},\frac{17}{2}), \tag{B.25}$$

which is in the subspace W_7 as well.

Note that to realize W_7 directly one should apply Gram-Schmidt to Δ to find an orthonormal basis $\mathbb{B}$ of W_7, and then express Δ, the $\boldsymbol{\lambda}_i$s, and $\boldsymbol{x}_0$ in coordinates relative to $\mathbb{B}$. (An orthonormal basis is required in order to preserve the geometry of the reflection group.)

For $\mathcal{E}_6$

The 6 simple roots of $\mathcal{E}_6$ in $\mathbb{R}^8$ are $\Delta = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_6\}$ of (B.21); the span of these roots is the 6-dimensional subspace W_6 upon which $\mathcal{E}_6$ acts irreducibly by affine reflections. Each root has length $\sqrt{2}$ and, by Table 2.2, the highest long root is $\boldsymbol{\rho} = \boldsymbol{r}_1 + 2\boldsymbol{r}_2 + 2\boldsymbol{r}_3 + 3\boldsymbol{r}_4 + 2\boldsymbol{r}_5 + \boldsymbol{r}_6 = \frac{1}{2}(1,1,1,1,1,-1,-1,1)$. The optimal nearest neighbour distance (8.7) is

$$d = \frac{2}{\sqrt{2} + \sum_{i=1}^{6} a_i\sqrt{2}} = \frac{1}{6\sqrt{2}}. \tag{B.26}$$

From [38, Table 13.1], we have that the dual basis to Δ in W_6 is given by

$$\begin{aligned}
\boldsymbol{\lambda}_1 &= \frac{2}{3}(0,0,0,0,0,-1,-1,1), & \boldsymbol{\lambda}_2 &= \frac{1}{2}(1,1,1,1,1,-1,-1,1),\\
\boldsymbol{\lambda}_3 &= \frac{1}{6}(-3,3,3,3,3,-5,-5,5), & \boldsymbol{\lambda}_4 &= (0,0,1,1,1,-1,-1,1),\\
\boldsymbol{\lambda}_5 &= \frac{1}{3}(0,0,0,3,3,-2,-2,2), & \boldsymbol{\lambda}_6 &= \frac{1}{3}(0,0,0,0,3,-1,-1,1).
\end{aligned}$$

It now follows from (8.8) that the best initial vector is

$$\boldsymbol{x}_0 = \frac{1}{12}(0, 1, 2, 3, 4, -4, -4, 4), \tag{B.27}$$

which is in the subspace W_6 as well.

As noted above, one may realize Δ and $\boldsymbol{x}_0$ as vectors with 6 coordinates by choosing an isometry $W_6 \simeq \mathbb{R}^6$.

Appendix C

List of Publications

Refereed Journals

1. T. Niyomsataya, A. Miri and M. Nevins, "*Unitary space-time group codes: diversity sums from character tables,*" IEEE Transactions on Information Theory, vol.54, no. 11, pp. 5203-5210, Nov 2008.
2. T. Niyomsataya, A. Miri and M. Nevins, "*Trellis Representation And Decoding Methods of Affine Reflection Group Codes,*" submitted to IEEE Transactions on Information Theory, Oct 2008.
3. T. Niyomsataya, A. Miri and M. Nevins, "*On application of the Bruhat decomposition to the design of full diversity unitary space-time codes,*" to appear in IEEE Transactions on Information Theory, accepted on Sep 2008.
4. T. Niyomsataya, A. Miri and M. Nevins,"*Affine reflection group codes,*" IEEE Transactions on Information Theory, vol.54, no.1, pp.441-454, Jan 2008.
5. T. Niyomsataya, A. Miri and M. Nevins, "*Pairwise error probability of space-time codes for a keyhole channel,*" IEE Proc. Communications, vol.1, pp.101-105, Feb 2007.
6. T. Niyomsataya, A. Miri and M. Nevins,"*Applications of finite reflection groups to wireless communications,*" Designs, Codes and Cryptography Journal, vol.41, no.3, pp. 307-318, Dec 2006.

Refereed Conference Proceedings

7. T. Niyomsataya, A. Miri and M. Nevins, "*Fast multiple-symbol differential unitary space-time decoding using stack algorithm,*" in the proceedings of the 24th Biennial

Symposium Communications, Kingston, Canada, June 2008, pp.374-377.

8. T. Niyomsataya, A. Miri and M. Nevins, "*Efficient decoding algorithms for affine reflection group codes of rank 2*," in the proceedings of the 24th Biennial Symposium Communications, Kingston, Canada, June 2008, pp.72-75 .

9. T. Niyomsataya, A. Miri and M. Nevins, "*Unitary space-time constellations based on finite reflection group codes*," in the proceedings of Canadian Workshop in Information Theory, CWIT 2005, Montreal, Canada, June 2005, pp.264-267.

10. T. Niyomsataya, A. Miri and M. Nevins, "*Full diversity unitary space-time Bruhat constellations*," in the proceedings of IEEE Information Theory Workshop, ITW 2004, Texas, USA, Oct 2004, pp.370-374.

11. T. Niyomsataya, A. Miri and M. Nevins, "*New space-time code design for prime number of transmitter antennas*," in the proceedings of the 22nd Biennial Symposium on Communications, Kingston, Canada, June 2004, pp.12-14.

12. T. Niyomsataya, A. Miri and M. Nevins, "*Unitary space-time codes from group codes: permutation code variant II*," in the proceedings of IEEE Canadian Conference on Electrical and Computer Engineering, CCECE 2004, Niagara Falls, Canada, May 2004, vol.1, pp.597-600.

Bibliography

[1] "Groups, algorithms, programming (GAP) – a system for computational discrete algebra," http://www.gap-system.org/gap.html.

[2] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Area Comm.*, vol. 16, pp. 1451–1458, Oct 1998.

[3] A. H. Banihashemi and I. F. Blake, "Trellis complexity and minimal trellis diagrams of lattices," *IEEE Trans. on Information Theory*, vol. 44, no. 5, pp. 1829–1847, Sept. 1998.

[4] A. Banihashemi, "Decoding complexity and trellis structure of lattices," Ph.D. dissertation, University of Waterloo, 1997.

[5] C. T. Benson and L. C. Grove, *Finite Reflection Groups.* Bogden & Quigley Inc. Publishers, 1971.

[6] E. Biglieri and M. Elia, "Cyclic-group codes for the Gaussian channel," *IEEE Trans. Info. Theory*, vol. 22, pp. 624–629, Sept 1976.

[7] J. A. C. Bingham, "Multicarrier modulation for data transmission: an idea whose time has come," *IEEE Comm. Mag.*, pp. 5–14, May 1990.

[8] I. F. Blake, "Distance properties of group codes for the Gaussian channel," *SIAM J.Appl. Math*, vol. 23, pp. 312–324, Nov 1972.

[9] M. Burrow, *Representation Theory of Finite Groups.* Academic press, 1965.

[10] E. Chiavaccini and G. M. Vitetta, "Further results on different space-time modulations," *IEEE Trans. Comm.*, vol. 51, pp. 1093–1101, July 2003.

[11] D. Chizhik, G. J. Foschini, M. J. Gans, and R. A. Valenzuela, "Keyhole, correlations, and capacities of multi-element transmit and receive antennas," *IEEE Trans. Wireless Comm.*, vol. 1, pp. 361–368, April 2002.

[12] J. H. Conway and N. J. A. Sloane, "Fast quantizing and decoding algorithm for lattice quantizers and codes," *IEEE Trans. on Information Theory*, vol. IT-28, no. 2, pp. 227–232, Mar. 1982.

[13] ——, *Sphere Packings, Lattices and Groups*, 2nd ed. Springer-Verlag, 1993.

[14] J. H. Conway, N. J. A. Sloane, and A. R. Wilks, *Gray codes for reflection groups.* Springer-Verlag, 1989, vol. 5, pp. 315–325.

[15] T. Cui and C. Tellambura, "Bound intersection detection for multiple-symbol differential unitary space-time modulation," *IEEE Trans. on Comm.*, vol. 53, no. 12, pp. 2114–2123, Dec 2005.

[16] L. A. Dalton and C. N. Georghiades, "A full-rate, full-diversity four-antenna quasi-orthogonal space-time blcok code," *IEEE Trans. on Wireless Comm.*, vol. 4, no. 2, pp. 363–366, Mar 2005.

[17] P. Fan, "Multiple-symbol detection for transmit diversity with differential encoding scheme," *IEEE Trans. Consumer Electronics*, vol. 47, pp. 96–100, 2001.

[18] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs. Tech. Journal*, vol. 1, pp. 41–59, 1996.

[19] G. J. Foschini and M. J. Gans, "On limits of wireless communication in a fading environment when using multiple antennas," *Wireless Personal Comm.*, Mar 1998.

[20] J. B. Fraleigh and R. A. Beauregard, *Linear Algebra*, 2nd ed. Addison-Wesley Publishing Company, 1990.

[21] H. E. Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Info. Theory*, vol. 49, pp. 1097–1119, May 2003.

[22] C. Gao and A. M. Haimovich, "Multiple-symbol differential detection for space-time block codes," in *Conf. Information Sciences and Systems.* Princeton University, Mar 2002.

[23] J. G.D. Forney, "Codet codes– part II: binary lattices and related codes," *IEEE Trans. on Information Theory*, vol. 34, no. 5, pp. 1152–1182, Nov 1988.

[24] ——, "Density/length profiles and trellis complexity of lattices," *IEEE Trans. on Info. Theory*, vol. 40, pp. 1753–1772, Nov 1994.

[25] D. Gesbert, H. Bolcshkei, D. A. Gore, and A. J. Paulraj, "Outdoor MIMO wireless channels: models and performance prediction," *IEEE Trans. Comm.*, vol. 50, pp. 1962–1934, Dec 2002.

[26] A. Goldsmith, *Wireless Communications.* Cambridge University Press, 2005.

[27] I. S. Gradshteyn and I. M.Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. San Diego, CA: Academic, 2000.

[28] G. Han and J. Rosenthal, "A numerical approach for designing unitary space time codes with large diversity product and diversity sum," in *IEEE Int. Symp. Information Theory, ISIT 2003*, 2003, p. 178.

[29] S. H. Han and J. M. C. anf J. H. Lee, "Tone injection with hexagonal constellation for peak-to-average power ratio reduction in OFDM," *IEEE Comm. Letters*, vol. 10, no. 9, pp. 646–648, Sept. 2006.

[30] S. H. Han, J. M. Cioffi, and J. H. Lee, "On the use of hexagonal constellation for peak-to-average power ratio reduction of an OFDM signal," *IEEE Trans. Wireless Comm.*, vol. 7, no. 3, pp. 781–786, Mar 2008.

[31] S. H. Han and J. Lee., "An overview of peak-to-average power ratio reduction techniques for multiuser transmission," *IEEE Trans. Wireless Comm.*, vol. 12, no. 2, pp. 56–65, Apr 2005.

[32] L. Hanzo and T. Keller, *OFDM and MC-CDMA: A Primer.* John Wiley & Sons Ltd., 2006.

[33] B. Hassibi and B. M. Hochwald, "Cayley differential unitary space-time codes," *IEEE Trans. Info. Theory*, vol. 48, pp. 1485–1503, June 2002.

[34] B. Hassibi and M. Khorrami, "Fully-diverse multiple antenna signal constellations and fixed-point free Lie groups," in *IEEE International Symposium on Info. Theory*, June 2001, p. 199.

[35] B. M. Hochwald and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Info. Theory*, vol. 48, pp. 2041–2052, Dec 2000.

[36] B. L. Hughes, "Differential space-time modulation," *IEEE Trans. Info. Theory*, vol. 46, pp. 2567–2578, Nov 2000.

[37] ——, "Optimal space-time constellations from groups," *IEEE Trans. Info. Theory*, vol. 49, pp. 401–410, Feb 2003.

[38] J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory.* Springer-Verlag, 1987.

[39] ——, *Reflection Groups and Coxeter Groups*, ser. Cambridge studies in advanced mathematics. Cambridge Univ. Press, 1990, vol. 29.

[40] I. Ingemarsson, "Group codes for the Gaussian channel," in *Topics in Coding Theory.* Springer-Verlag, 1989, vol. 128, pp. 73–108.

[41] H. Jafarkhani and V. Tarokh, "Multiple transmit antenna differential detection from generalized orthogonal designs," *IEEE Trans. Info. Theory*, vol. 47, pp. 2626–2631, Sept 2001.

[42] G. James and M. Liebeck, *Representations and Characters of Groups.* Cambridge University Press, 1993.

[43] F. Jelinel, "A fast sequential decoding algorithm using a stack," *IBM Journal of Research and Development*, vol. 13, pp. 675–685, Nov 1969.

[44] Y. Jing and B. Hassibi, "Design of fully-diverse multiple-antenna codes based on $Sp(2)$," *IEEE Trans. Info. Theory*, vol. 50, pp. 2639–2656, Nov 2004.

[45] ——, "Three-transmit-antenna space-time codes based on $SU(3)$," *IEEE Trans. Signal Processing*, vol. 53, pp. 3688– 3702, Oct 2005.

[46] J. M. C. Jr. and N. R. Sollenberger, "Peak-to-average power ratio redcution of an OFDM signal using partial tranmsit sequences," *IEEE Comm. Letters*, vol. 4, pp. 86–88, Mar 2000.

[47] T. Konishi, "Unitary subgroup space-time codes using Bruhat decomposition and Weyl groups," *IEEE Trans. Info. Theory*, vol. 49, pp. 2713–2717, Oct 2003.

[48] D. C. Lay, *Linear Algebra and Its Applications*, 3rd ed. Addison Wesley, 2002.

[49] X. B. Liang and X. G. Xia, "Unitary signal constellations for differential space-time modulation with two transmit antennas: Parametric codes, optimal designs, and bounds," *IEEE Trans. Info. Theory*, vol. 48, pp. 2291–2322, Aug 2002.

[50] S. Litsyn, *Peak power control in multicarrier communications.* Cambridge University Press, 2007.

[51] Z. Liu, Y. Xin, and G. B. Giannakis, "Space-time-frequency coded ofdm over frequency-selective fading channels," *IEEE Trans. Signal Processing*, vol. 50, no. 10, pp. 2465–2476, Oct 2002.

[52] S. Loyka and A. Kouki, "On MIMO channel capacity, and keyholes: analysis of degenerate channels," *IEEE Comm. Letters*, vol. 20, pp. 1886–1888, Dec 2002.

[53] T. Mittelholzer, "Construction and decoding of optimal group codes from finite reflection groups," in *Communications and Cryptography: Two Sides of One Tapestry*, R. Blahut, J. D.J. Costello, U. Maurer, and T. Mittelholzer, Eds. Eds. Norwell, MA: Kluwer, 1996.

[54] T. Mittelholzer and J. Lahtonen, "Group codes generated by finite reflection groups," *IEEE Trans. Info. Theory*, vol. 42, pp. 519–528, Mar 1996.

[55] A. Muller and J. Speidel, "Bit error analysis of orthogonal space-time block codes in Nakagami-m keyhole channels," in *IEEE Wireless Communications and Networking Conf., WCNC 2007*, 2007, pp. 2184–2189.

[56] A. M. N. Nasrabadi, H. R. Bahrami, and S. H. Jamali, “Space-time trellis codes for keyhole channel: performance criterion and code design,” *IEE Electronics Letters*, vol. 40, no. 1, pp. 53–55, Jan 2004.

[57] T. Niyomsataya, “New unitary space-time codes with high diversity products,” Master’s thesis, University of Ottawa, Canada, March 2004.

[58] T. Niyomsataya, A. Miri, and M. Nevins, “On an application of the Bruhat decomposition to the design of full diversity unitary space-time codes,” to appear in *IEEE Trans. on Info. Theory*, accepted in Sept 2008.

[59] ——, “Full diversity unitary space-time Bruhat constellations,” in *IEEE Information Theory Workshop, ITW 2004, Texas, USA*, Oct 2004, pp. 370–374.

[60] ——, “New space-time code design for prime number of transmitter antennas,” in *22nd Biennial Symposium on Communications, Kingston, Canada*, June 2004, pp. 12–14.

[61] ——, “Unitary space-time codes from group codes: permutation code variant II,” in *IEEE Canadian Conference on Electrical and Computer Engineering, CCECE 2004, Niagara Falls, Canada*, May 2004, pp. 597–600.

[62] ——, “Unitary space-time constellations based on finite reflection group codes,” in *Canadian Workshop in Information Theory, CWIT 2005, Montreal, Canada*, June 2005, pp. 264–267.

[63] ——, “Applications of finite reflection groups to wireless communications,” *Designs, Codes and Cryptography Journal*, vol. 41, pp. 307–318, Dec 2006.

[64] ——, “Pairwise error probability of space-time codes for a keyhole channel,” *IEE Proc. Communications*, vol. 1, pp. 101–105, Feb 2007.

[65] ——, “Unitary space-time constellation designs from group codes,” *IEEE Trans. on Information Theory*, vol. 53, no. 11, pp. 4322–4329, Nov 2007.

[66] ——, “Affine reflection group codes,” *IEEE Trans. Info. Theory*, vol. 54, no. 1, pp. 441–454, Jan 2008.

[67] ——, "Efficient decoding algorithms for affine reflection group codes of rank 2," in *24th Biennial Symposium Communications, Kingston, Canada*, June 2008, pp. 72–75.

[68] ——, "Fast multiple-symbol differential unitary space-time decoding using stack algorithm," in *24th Biennial Symposium Communications, Kingston , Canada*, June 2008, pp. 374–377.

[69] ——, "Unitary space-time group codes: diversity sums from character tables," *IEEE Trans. on Information Theory*, vol. 54, no. 11, pp. 5203–5210, Nov 2008.

[70] F. Oggier and E. Lequeu, "Families of unitary matrices achieving full diversity," in *IEEE International Symposium on Information Theory,, ISIT 2005, Adelaide, Australia*, 2005, pp. 1173–1177.

[71] F. Oggier, G. Rekaya, J. C. Belfiore, and E. Viterbo, "Perfect space time block codes," *IEEE Trans. Info. Theory*, vol. 52, pp. 3885 – 3902, Sept 2006.

[72] V. Pauli and L. Lampe, "Tree-search multiple-symbol differential decoding for unitary space-time modulation," *IEEE Trans. Info. Theory*, vol. 55, no. 8, pp. 1567–1576, Aug 2007.

[73] P. K. M. Pun and P. K. M. Ho, "Fano multiple-symbol differential detectors for differential unitary space-time modulation," *IEEE Trans. on Comms.*, vol. 55, no. 3, pp. 540–550, Mar 2007.

[74] R. Raheli and A. Polydoros, "Per-survivor processing: a general approach to MLSE in uncertain environment," *IEEE Trans. Comm.*, vol. 43, Feb-Apr 1995.

[75] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Info. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct 2003.

[76] N. Sharma and c. B. Papadias, "Improved quasi-orthogonal codes through constellation rotation," *IEEE Trans. on Comm.*, vol. 51, pp. 332–335, Mar 2003.

[77] H. Shin and J. H. Lee, "Capacity of multiple-antenna fading channels: spatial fading correlation, double scattering, and keyhole," *IEEE Trans. Info. Theory*, vol. 49, no. 10, pp. 2636–2647, Oct 2003.

[78] ——, "Performance analysis of space-time block codes over keyhole Nakagami-m fading channels," *IEEE Trans. Vehicular Tech.*, vol. 53, no. 2, pp. 351–362, Mar 2004.

[79] A. Shokrollahi, "Computing the performance of unitary space-time group codes from their character table," *IEEE Trans. Info. Theory*, vol. 48, pp. 1355–1371, June 2002.

[80] A. Shokrollahi, B. Hassibi, B. M. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code designs," *IEEE Trans. Info. Theory*, vol. 47, pp. 2335–2367, Sept 2001.

[81] A. Silberger, "An elementary construction of the representations of $SL(2, GF(q))$," *Osaka J. Math.*, vol. 6, pp. 329–338, 1969.

[82] M. Simon and M. Alouini, *Digital Communication Over Fading Channels: A Unified Approach to Performance Analysis.* New York: Wiley, 2000.

[83] D. Slepian, "Permutation modulation," *Proc. IEEE*, vol. 53, pp. 228–236, March 1965.

[84] ——, "Group codes for the Gaussian channel," *The Bell system Technical Journal*, vol. 47, pp. 575–602, April 1968.

[85] D. B. Smith, "Improved quasi-orthogonal space-time block codes with hexagonal lattice modulation," in *IEEE 8th Workshop on Signal Processing Advances in Wireless Comm., SPAWC 2007*, June 2007, pp. 1–5.

[86] A. Song, G. Wang, W. Su, and X. G. Xia, "Unitary space-time codes from Alamouti's scheme with APSK signals," *IEEE Trans. Wireless Comm.*, vol. 3, pp. 2374–2384, Nov 2004.

[87] S.Sanayei, A. Hedayat, and A. Nosratinia, "Space-time codes in keyhole channels: analysis and design," in *IEEE Globecom'04, Dallas*, Nov 2004, pp. 3768–3772.

[88] P. Tarasak and V. K. Bhargava, "Reduced complexity multiple-symbol differential detection of space-time block code," in *IEEE Conf. Wireless Comm. and Networking, Florida, USA*, vol. 1, Mar 2002, pp. 505 – 509.

[89] G. Taricco and E. Biglieri, "Exact pairwise error probability of space-time codes," *IEEE Trans. Info. Theory*, vol. 48, no. 2, pp. 510–513, Feb 2002.

[90] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE J. Sel. Area Comm.*, vol. 18, pp. 1169–1174, July 2000.

[91] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Info. Theory*, vol. 45, pp. 1456–1474, July 1999.

[92] V. Tarokh, H. Jafarkhani, and A. Calderbank, "Space-time block coding for wireless communications: performance results," *IEEE J. Sel. Area Comm.*, vol. 17, pp. 451–460, Mar 1999.

[93] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. Info. Theory*, vol. 44, pp. 744–765, March 1998.

[94] I. E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecomm.*, vol. 10, pp. 585–598, Nov 1999.

[95] J. Tellado, "Peak to average power reduction for multicarrier modulation," Ph.D. dissertation, Standford University, 2000.

[96] C. Tellambura, "Computation of the continuous-time PAR of an OFDM signal with BPSK subcarriers," *IEEE Comm. Letter*, vol. 5, no. 5, pp. 185–187, May 2001.

[97] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space-time block codes for complex signal constellations," *IEEE Trans. Info. Theory*, vol. 48, pp. 384–395, Feb 2002.

[98] Z. Wang, X. Ma, and G. B. Giannakis, "OFDM or single-carrier block transmissions?" *IEEE Trans. on Comm.*, vol. 52, pp. 380–394, Mar 2004.

[99] G. Xingxin, L. Mingquan, and F. Zhenming, "Asymmetric hexagonal QAM based OFDM system." IEEE Int. Conf. on Comm., Circuits and Systems and West Sino Expositions, June 2002, pp. 299–302.

[100] H. Zhao, Y. Gong, Y. L. Guan, C. L. Law, and Y. Tang, "Space-time block codes in Nakagami fading channels with non-identical m-distributions," in *IEEE Wireless Comm. and Networking Conf.*, Mar 2007, pp. 536–540.