McMaster University
DigitalCommons@McMaster

Open Access Dissertations and Theses | Open Dissertations and Theses

10-1-2011

Full Diversity Noncoherent Space-Time Block Codes Designs via Unique Factorizations of Signals

Dong Xia
McMaster University, askxd@grads.ece.mcmaster.ca

Follow this and additional works at: http://digitalcommons.mcmaster.ca/opendissertations

Part of the Signal Processing Commons, and the Systems and Communications Commons

Recommended Citation
Xia, Dong, "Full Diversity Noncoherent Space-Time Block Codes Designs via Unique Factorizations of Signals" (2011). *Open Access Dissertations and Theses.* Paper 6008.

This Thesis is brought to you for free and open access by the Open Dissertations and Theses at DigitalCommons@McMaster. It has been accepted for inclusion in Open Access Dissertations and Theses by an authorized administrator of DigitalCommons@McMaster. For more information, please contact scom@mcmaster.ca.

Full Diversity Noncoherent Space-Time Block Codes Designs via Unique Factorizations of Signals

FULL DIVERSITY NONCOHERENT SPACE-TIME BLOCK CODES DESIGNS VIA UNIQUE FACTORIZATIONS OF SIGNALS

BY

DONG XIA, B.Sc.

A THESIS

SUBMITTED TO THE DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

AND THE SCHOOL OF GRADUATE STUDIES

OF MCMASTER UNIVERSITY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

© Copyright by Dong Xia, August 2011

All Rights Reserved

Master of Applied Science (2011) McMaster University

(Electrical & Computer Engineering) Hamilton, Ontario, Canada

TITLE:	Full Diversity Noncoherent Space-Time Block Codes Designs via Unique Factorizations of Signals
AUTHOR:	Dong Xia B.Eng., (Automation Engineering) University of Science and Technology of China, Hefei, China
SUPERVISOR:	Drs. Jian-Kang Zhang and Sorina Dumitrescu
NUMBER OF PAGES:	xi, 136

Abstract

In this thesis, a MISO wireless communication system having even transmitter antennas and a single receiver antenna is considered, where neither the transmitter nor the receiver knows channel state information. Particularly when the number of transmitter antennas is two, a novel concept called a *uniquely factorable constellation pair* (UFCP) is first proposed for the systematic design of a noncoherent full diversity collaborative unitary space-time block code by normalizing two Alamouti codes. It is proved that such a unitary UFCP code assures the unique identification of both channel coefficients and transmitted signals in a noise-free case as well as full diversity for the noncoherent maximum likelihood (ML) receiver in a noise case. To further improve error performance, an optimal unitary UFCP code is designed by appropriately and uniquely factorizing a pair of energy-efficient cross quadrature amplitude modulation (QAM) constellations to maximize the coding gain subject to a transmission bit rate constraint. After a deep investigation of the fractional coding gain function, a technical approach developed in this thesis to maximizing the coding gain is to carefully design an energy scale to compress the first three largest energy points in the corner of the QAM constellations in the denominator of the objective as well as carefully design a constellation triple forming two UFCPs, with one collaborating with the other two so as to make the accumulated minimum Euclidean distance along

the two transmitter antennas in the numerator of the objective as large as possible and at the same time, to avoid as many corner points of the QAM constellations with the largest energy as possible to achieve the minimum of the numerator. In other words, the optimal coding gain is attained by intelligent constellations collaboration and efficient energy compression.

Another contribution of this thesis is to generalize the design for the two transmitter antennas into that of the noncoherent system with any even number of transmitter antennas. Using the Alamouti coding scheme and the Toeplitz matrix structure, a novel noncoherent nonunitary space-time block code, which is called an Alamouti-based Toeplitz space-time block code, is proposed. By the fundamentals of Galois theory and algebraic number theory, two important properties on the two Alamouti codes generated from a pair of coprime phase shift keying (PSK) constellations, i.e., the uniqueness of factorization itself and the shift-invariant uniqueness of factorization, are first revealed and rigorously proved. Then, it is further shown that it is these two kinds of the unique factorizations that enable the unique blind identification of both the channel coefficients and the transmitted signals by only processing two block received signals as well as noncoherent full diversity with a generalized likelihood ratio test (GLRT) receiver. In addition, a full diversity unitary code design is also proposed by simply applying the QR decomposition to the full diversity nonunitary Alamouti-based Toeplitz space-time block code. Computer simulations demonstrate that error performance of both optimal unitary UFCP code and Alamouti-based Toeplitz code presented in this thesis outperform those of the differential code and the SNR-efficient training code, which is the best code in current literatures for the system.

Acknowledgements

First and foremost, I would like to show my deepest gratitude to my supervisor, Dr. Jian-Kang Zhang, a respectable, responsible and resourceful scholar, who has provided me with valuable guidance in every stage of the writing of this thesis. Without his enlightening instruction, impressive kindness and patience, I could not have completed my thesis. His keen and vigorous academic observation enlightens me not only in this thesis but also in my future study.

I shall extend my thanks to my co-supervisor Dr. Sorina Dumitrescu, for all her kindness and help in my Master program. I would also like to thank Drs. Kon Max Wong and Dongmei Zhao for taking their time to be a part of my defence committee and sharing their valuable comments and critiques on my thesis. Besides, I am also deeply indebted to Drs. Jun Chen and Steve Hranilovic who have taught me or helped me develop the fundamental and essential academic competence. My sincere appreciation also goes to all my friends, especially the classmates in Signal Processing Laboratory and my two lovely housemates Li Xiong and Jiayi Xu.

Last and the most important, I' d like to thank my parents and girlfriend Yinghan Wan for their encouragement and support.

Notation and abbreviations

e.g. $\mathbf{a}$	column vectors are denoted by lowercase boldface characters
e.g. $\mathbf{A}$	matrices are denoted by uppercase boldface characters
$(\cdot)^T$	the transpose of a vector or matrix
$(\cdot)^*$	the complex conjugate of a vector or matrix
$(\cdot)^H$	the Hermitian of a vector or matrix
$\mathrm{Tr}(\cdot)$	the trace operator
$\det(\cdot)$	the determinant operator
$\lVert \cdot \rVert_F$	the Frobenius norm of a vector or matrix
$\mathbf{I}_N$	$N \times N$ identity matrix
Φ	empty set
$f(x) = o(g(x))$	$\lim_{x \leftarrow \infty} \frac{f(x)}{g(x)} = 0$
$\phi(n)$	the Euler totient function
$\mathbb{Z}$	ring of rational integers
$\mathbb{Q}$	field of rational numbers

$\mathbb{R}$	field of real numbers
$\mathbb{C}$	field of complex numbers
ζ_p	$\exp(\frac{j2\pi}{p})$
$\mathbb{Z}[\zeta_p]$	cyclotomic ring generated by $\mathbb{Z}$ and ζ_p
$\mathbb{Q}(\zeta_p)$	the field generated by $\mathbb{Q}$ and ζ_p
$\gcd(m, n)$	the greatest common divisor of positive integers m and n
$\mathrm{lcm}(m, n)$	the least common multiple of positive integers m and n
MIMO	multi-input multi-output
MISO	multi-input single-output
STBC	space-time block code
ML	maximum likelihood
GLRT	generalized likelihood ratio test
UFCP	uniquely factorable constellation pair
QAM	quadrature amplitude modulation
PSK	phase-shift keying
SNR	signal-to-noise ratio

Contents

Abstract **iii**

Acknowledgements **v**

Notation and abbreviations **vi**

1 Introduction **1**

1.1 Two Transmitter Antennas System 3

1.2 Arbitrary Even Number of Transmitter Antennas System 5

2 Channel Model and Space-Time Block Coding **7**

2.1 Channel Model 7

2.2 Collaborative Unitary Space-Time Block Code 8

2.3 Alamouti-based Toeplitz Code 12

3 Uniquely Factorable Constellation Pair **16**

3.1 UFCP 16

3.2 Unique Factorizations of The Modified Cross QAM Constellation . . 19

4 Collaborative Unitary UFCP Space-Time Block Code **29**

4.1 Signal Designs and Unique Identification 29
4.2 Full Diversity 33

5 Optimal Designs of Collaborative Unitary UFCP Space-Time Block Code 38

5.1 Problem Formulation 38
5.2 The Solution to Problem 3 40
5.2.1 $\delta = 0$ 43
5.2.2 $\delta = 1$ 50
5.2.3 $\delta = 2$ 61
5.2.4 One Optimal Solution to Problem 3 67

6 Unique Identification and Full Diversity for Alamouti-based Toeplitz Code 70

6.1 Some Basic Definitions and Properties in Algebraic Theory 71
6.1.1 The Greatest Common Factor, The Least Common Multiple and Euler's Totient Function 71
6.1.2 Galois Theory 72
6.1.3 Cyclotomic Polynomials and Cyclotomic Extension 74
6.2 Two Kinds of Unique Factorizations for Alamouti Codes 76
6.3 Unique Identification 77
6.4 Full Diversity 83

7 Detection and Simulations 86

7.1 Detection and Simulations for Collaborative Unitary UFCP Code . . 86
7.2 Detection and Simulations for Alamouti-based Toeplitz Code 90

8 Conclusion and Discussions **95**

A Appendix **100**

A.1 Proof of Proposition 5 100

A.2 Proof of Lemma 3 104

A.3 Proof of Lemma 4 105

A.4 Proof of Lemma 5 107

A.5 Proof of Theorem 3 108

A.6 Proof of Lemma 6 112

A.7 Proof of Proposition 6 114

A.8 Proof of Proposition 7 117

List of Figures

3.1 The optimal UFCP selections from the square 64QAM and cross 128QAM constellations in Proposition 5 28

5.1 The optimal coding gains versus transmission bit rates 69

7.1 Performance comparison of unitary UFCP codes with currently available noncoherent codes 89

7.2 Error performance comparison of Alamouti-based Toeplitz codes with differential codes and training scheme 94

A.1 Nine corner points in the cross QAM constellation 102

Chapter 1

Introduction

At present, the technology intelligently combing multiple antennas [1–3] with space-time block coding [4–25] has been well developed to improve the spectral efficiency of a coherent wireless communication system. Lately, simple space-time block code designs with low complexity decoding [24–39] have attracted much attention. In this thesis, we are specifically interested in a flat fading wireless communication system with even transmitter antennas and a single receiver antenna. This system is often encountered in mobile down-link communications for which the mobile receiver may not be able to deploy multiple antennas. For such a system, if the exact knowledge of the channel coefficients is available at the receivers, full diversity linear space-time block codes [24] based on the Toeplitz matrix structure and full diversity overlapped space-time block codes [25] based on the Alamouti code have been proposed with linear receivers enabling the optimal tradeoff between diversity and multiplexing gain. Especially when the number of transmitter antenna is two, the orthogonal Alamouti [26] space-time block code is particularly appealing, since it enables the coherent ML receiver to extract full diversity not only with linear processing complexity, but with

information losslessness as well [40]. Unfortunately, perfect channel state information at the receiver, in practice, is not easily obtainable. If the channel changes slowly, then, the transmitter may have sufficiently long channel coherence time and send training signals enabling the channel coefficients to be estimated accurately. However, the fading coefficients in mobile wireless communications may vary rapidly and the coherence time may be too short to allow reliable estimation of the coefficients. Therefore, the time cost on sending training signals cannot be ignored since more training signals need sending for the accurate estimation of the channel [41–43]. In this thesis, we consider the communication scenario with even number of transmitter antennas where channel fading changes promptly, assuming that the channel gains are completely unknown at the destination, but remain unchanged within a certain amount of transmission time slots called coherent time, after which they change to new independent values that are fixed for next coherent time, and so on. When the coherent time is small, such fast varying channel with flat fading for a single transmitter and single receiver antenna was first considered for determining the capacity-achieving input distribution [44–48]. In order to make communication as reliable as possible under this severe environment and avoid sending the training signals for estimation of the channel, using differential space-time block coding [49–59] is one of solutions. Unfortunately, this approach results in an approximate loss of 3dB in performance compared to coherent detection. Recently, some techniques of blind signal processing such as the subspace method based on the second order statistics have been utilized to blindly identify the space-time block coded channel [60–64]. However, phase ambiguity incurs the channel not being able to be identified uniquely, even in the noise-free case. In addition, even if there were no phase ambiguity, the subspace method could

not be successfully applicable to our case, since the coherence time slots might be too short to allow the second-order statistics to be estimated accurately. Therefore, in order to attain a more satisfactory solution, noncoherent space-time block coding techniques [49, 65–69] have been developed. It has been proved that either at high signal-to-noise ratio (SNR) or for long coherence time, the unitary code is optimal [43,49,70,71]. Hence, most of the noncoherent space-time block code designs have been primarily concentrated on unitary designs [49,58,65–69,72]. The Cayley [54,58] transform and the exponential transform [69] are now two well-established transforms which convert a linear dispersion code and a linear space-time block code into unitary codes. The exponential transform [69] requires that the number of the receiver antennas is greater than or equal to that of the transmitter antennas. In general, it cannot assure full diversity for the noncoherent ML receiver. The unitary design using the Cayley transform aimed mainly at differential modulation and a differential receiver. Recently, the original non-full diversity design [54,58] based on the Cayley transform has been improved into a full diversity design utilizing division algebra and algebraic number theory [73].

1.1 Two Transmitter Antennas System

The first contribution of this thesis [**?**] is to design a full diversity unitary space-time block code for the system with two transmitter antennas by using the two Alamouti codes and the energy-efficient cross QAM constellations such that the noncoherent coding gain is maximized subject a transmission bit rate constraint. For such system, the phase ambiguity and full diversity issue for the noncoherent Alamouti space-time block code has been completely resolved using a pair of coprime PSK

constellations [74, 75]. However, the PSK constellation is not as energy-efficient as the QAM constellation. In addition, despite the fact that recent research on coherent MIMO communications has told us that the Alamouti code enables coherent full diversity for any constellations and with any receivers, this is no longer true for noncoherent communications, even if the commonly-used QAM constellations are transmitted and even if the noncoherent ML receiver is employed, since the likelihood function is invariant under certain rotation of some QAM constellation points [64,76]. Hence, signals must be carefully designed to combat against fading. In the noncoherent wireless communication scenario, the unknown of the fading channel at both the transmitter and the receiver requires that the transmitted signals emitting from different time slots must be more correlated than in the coherent environment so that reliable communications with noncoherent full diversity are made possible under a maximum allowable transmission rate.

All the aforementioned factors greatly motivate us to proposing a novel concept, a uniquely factorable constellation pair (UFCP), for the systematic design of an optimal unitary constellation for the system. The main idea of the UFCP design essentially comprises the following two major steps.

1. *Intelligent constellations collaboration*: From a pair of the energy-efficient cross QAM constellations, a constellation triple constituting two UFCPs will be carefully designed, with the one collaboratively shared with the other two through the two transmitter antennas, so that the minimum of the numerator in the factional objection function is made as large as possible and at the same time, the largest energy points of the QAM constellations as many as possible are avoided to reach the minimum of the denominator.

2. *Efficient energy compression*: An energy scale will be carefully designed to compress the first three largest energy points of the QAM constellations in the denominator of the objective.

1.2 Arbitrary Even Number of Transmitter Antennas System

The second contribution of this thesis [**?**] is to generalize the noncoherent space-time block coding techniques [74, 75] for the two transmitter antennas system into a design for the MISO system with arbitrary even number of transmitter antennas. For such system, we consider the systematic design of nonunitary and unitary space-time block codes by taking advantage of the Alamouti code and the Toeplitz matrix structure. The main idea of achieving this goal is to thoroughly reveal and rigorously prove two important unique factorization properties on the two Alamouti codes generated by a pair of coprime PSK constellations.

1. Unique factorization itself: The multiplication of any two codeword matrices from the one code is uniquely distinguishable from the other;

2. Shift-invariant unique factorization: The multiplication of any codeword matrix and the difference between any two codeword matrices from the one code is uniquely distinguishable from the other.

In fact, the first unique factorization is nothing but the extension of UFCP concept onto the Alamouti code and the second one is a variant of such extension. It will be

seen from the proofs of Theorems 4 and 5 that it is these two kinds of the unique factorizations that enable the unique blind identification of both the channel coefficients and the transmitted signals by only processing two block received signals as well as noncoherent full diversity with the GLRT receiver.

As mentioned before, the PSK constellation is not energy-efficient as the QAM constellation. However, the two Alamouti codes generated by the QAM constellation pairs cannot satisfy the unique factorizations, the proof of which using an counterexample was given in [76]. In fact, the likelihood function of the optimal noncoherent ML receiver is rotation-invariant for some QAM constellation points [64,76], resulting in the channel and the transmitted signals not being capable of being distinguished uniquely.

Chapter 2

Channel Model and Space-Time Block Coding

In this chapter, we first briefly review the channel model in which we are interested in this thesis. Then, we propose our transmission schemes and unitary code structures.

2.1 Channel Model

Let us consider a wireless communication system having M transmitter antennas and a single receiver antenna, M is a positive even integer. The transmitted symbols from the M transmitter antennas arrive at the receiver via M different channels h_1, h_2, $\cdots$, h_M. Then, the discrete baseband received signal r can be represented as

$$r = h_1 s_1 + h_2 s_2 + \cdots + h_M s_M + \xi. \tag{2.1}$$

Throughout this thesis we assume h_i, $i = 1, 2, \cdots, M$ are samples of independent circularly symmetric zero-mean complex white Gaussian random variables with unit variances and remain constant for the first T time slots, after which they change to new independent values that are fixed for the next T time slots, and so on, the explanation for which will be given in the ensuing section. s_i, $i = 1, 2, \cdots, M$ are corresponding transmitted symbols from these M antennas, and ξ is a circularly symmetric complex Gaussian noise with zero mean and variance σ^2.

2.2 Collaborative Unitary Space-Time Block Code

First, we consider the system with two transmitter antennas, i.e., $M = 2$. Let $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ be three constellations to be designed. Then, our unitary space-time block code for the channel model (2.1) is basically generated by normalizing two Alamouti codes and is described as follows: First, randomly, independently and equally likely choose three symbols $a \in \mathcal{A}, b_1 \in \mathcal{B}_1$ and $b_2 \in \mathcal{B}_2$ and then, transmit their normalized version from the two transmitter antennas within four time slots. During the first time slot, we transmit the signals $s_1 = a/\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}$ and $s_2 = 0$ in (2.1) at the same time from the respective Antennas 1 and 2. During the second time slot, the signals $s_1 = 0$ and $s_2 = a^*/\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}$, are simultaneously transmitted from Antennas 1 and 2, respectively. Collecting these two received signals yields

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \frac{1}{\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}} \begin{pmatrix} a & 0 \\ 0 & a^* \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} + \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix}, \tag{2.2a}$$

or equivalently,

$$\mathbf{r}_a = \frac{1}{\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}} \mathbf{A}\mathbf{h} + \boldsymbol{\xi}_a, \tag{2.2b}$$

where $\mathbf{r}_a = (r_1, r_2)^T, \mathbf{A} = \text{diag}(a, a^*), \mathbf{h} = (h_1, h_2)^T$ and $\boldsymbol{\xi}_a = (\xi_1, \xi_2)^T$. In the rest two time slots, the second and third symbols are transmitted using the Alamouti coding scheme, i.e.,

$$\begin{pmatrix} r_3 \\ r_4 \end{pmatrix} = \frac{1}{\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}} \begin{pmatrix} b_1 & b_2 \\ -b_2^* & b_1^* \end{pmatrix} \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} + \begin{pmatrix} \xi_3 \\ \xi_4 \end{pmatrix}, \tag{2.2c}$$

or equivalently,

$$\mathbf{r}_b = \frac{1}{\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}} \mathbf{B}\mathbf{h} + \boldsymbol{\xi}_b, \tag{2.2d}$$

where $\mathbf{r}_b = (r_3, r_4)^T, \boldsymbol{\xi}_b = (\xi_3, \xi_4)^T$ and

$$\mathbf{B} = \begin{pmatrix} b_1 & b_2 \\ -b_2^* & b_1^* \end{pmatrix}, \qquad b_1 \in \mathcal{B}_1,\ b_2 \in \mathcal{B}_2.$$

By stacking the above four received signals (2.2b) and (2.2d), the relationship between the transmitted and received signals within the four time slots can be represented in a more compact matrix form as

$$\mathbf{r} = \mathbf{U}\mathbf{h} + \boldsymbol{\xi}, \tag{2.3a}$$

where $\mathbf{r} = (r_1, r_2, r_3, r_4)^T, \boldsymbol{\xi} = (\xi_1, \xi_2, \xi_3, \xi_4)^T$ and

$$\mathbf{U} = \frac{1}{\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}} \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix} = \frac{1}{\sqrt{|a|^2 + |b_1|^2 + |b_2|^2}} \begin{pmatrix} a & 0 \\ 0 & a^* \\ b_1 & b_2 \\ -b_2^* & b_1^* \end{pmatrix}, \quad (2.3b)$$

for $a \in \mathcal{A}, b_1 \in \mathcal{B}_1, b_2 \in \mathcal{B}_2$. We would like to make the following comments on the unitary space-time block coded channel model (2.3):

1. *Why do we need four time slots*? For a noncoherent MIMO system with M transmitter antennas, it has been proved [71] that a necessary condition for a space-time block code to enable full diversity for the noncoherent ML receiver is $T \geq 2M$. Particularly for $M = 2$, we should need at least 4 time slots. Actually, we consider the shortest coherent time slots enabling the unique identification and full diversity. See more details in Chapter 4.

2. *Why is the symbol rate of $\frac{3}{4}$ per channel use reasonable*? The answer to this question is mainly motivated from the following observation: For a noncoherent MIMO communication system with M transmitter antennas and N receiver antennas, [43] have proved that in a high SNR regime and for the Rayleigh-faded channel, the average channel capacity is given by

$$C = M^* \left(1 - \frac{M^*}{T}\right) \log \mathrm{SNR} + O(1), \quad (2.4)$$

where $M^* = \min\{M, N, \lfloor \frac{T}{2} \rfloor\}$. This benchmark result tells us that the original noncoherent MIMO system can be asymptotically regarded as $M^* \left(1 - \frac{M^*}{T}\right)$

parallel spatial channels and thus, the number $M^*\left(1-\frac{M^*}{T}\right)$ is the total number of degrees of freedom to communication. The result also suggests us that the symbol rate of a space-time block code for the noncoherent MIMO channel should be $M^*\left(1-\frac{M^*}{T}\right)$. Especially for the noncoherent system with $T=4, M=2$ and $N=1$, the symbol rate should be $\frac{3}{4}$.

To formally state our first design problem, we make the following assumptions:

1. The channel coefficients h_1 and h_2 are samples of independent circularly-symmetric white Gaussian random variables with zero mean and unit variances, and remain constant for the first 4 time slots, after which they change to new independent values that are fixed for the next 4 time slots, and so on.

2. The elements of $\boldsymbol{\xi}$ are circularly-symmetric zero-mean complex Gaussian samples with covariance matrix $\sigma^2\mathbf{I}_4$;

3. During 4 observable time slots, the space-time block coding matrix $\mathbf{U}$ is transmitted with a, b_1 and b_2 being independently and equally likely chosen from the respective constellations $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$.

4. Channel state information is not available at either the transmitter or the receiver.

Under the above assumptions, our first primary purpose in this thesis is to solve the following problem.

Problem 1 *Design the constellation triple $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ for the collaborative unitary space-time block coded channel* (2.3) *such that*

1. *in the noise-free case, for any given nonzero received signal vector* $\mathbf{r} \neq \mathbf{0}$*, the equation reduced from* (2.3a)

$$\mathbf{r} = \mathbf{U}\mathbf{h}, \tag{2.5}$$

with respect to the transmitted symbol variables a*,* b_1 *and* b_2*, and the channel vector* $\mathbf{h}$ *has a unique solution, and*

2. *in the noisy environment, full diversity and the optimal coding gain are enabled for the noncoherent ML receiver.*

2.3 Alamouti-based Toeplitz Code

Now, we consider the space-time block code design problem for a general communication system with arbitrary even number of transmitter antennas and the coherent time T is a multiple of 4. For this problem, we make use of the Alamouti codes and the Toeplitz codes to generate a novel signalling scheme. Let p and q denote a pair of coprime positive integers. If we let $\mathcal{S}_p$ and $\mathcal{S}_q$ denote the p-ary and the q-ary PSK constellations, respectively, then, two kinds of the Alamouti codes are defined as

$$\mathcal{A}_p = \left\{ \begin{pmatrix} a_{p1} & a_{p2} \\ -a_{p2}^* & a_{p1}^* \end{pmatrix} : a_{p1}, a_{p2} \in \mathcal{S}_p \right\}, \tag{2.6a}$$

$$\mathcal{A}_q = \left\{ \begin{pmatrix} a_{q1} & a_{q2} \\ -a_{q2}^* & a_{q1}^* \end{pmatrix} : a_{q1}, a_{q2} \in \mathcal{S}_q \right\}. \tag{2.6b}$$

Our new noncoherent space-time block code is basically taking advantage of the above two Alamouti codes and the Toeplitz code and now is described as follows: during the first transmission period with $\frac{T}{2}$ time slots, a $\frac{T}{2} \times M$ Alamouti code $\mathcal{A}_p$-based Toeplitz codeword matrix

$$\boldsymbol{\Theta} = \begin{pmatrix} \boldsymbol{\Theta}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \boldsymbol{\Theta}_2 & \boldsymbol{\Theta}_1 & \dots & \mathbf{0} \\ \vdots & \boldsymbol{\Theta}_2 & \ddots & \vdots \\ \boldsymbol{\Theta}_L & \ddots & \ddots & \boldsymbol{\Theta}_1 \\ \mathbf{0} & \ddots & \ddots & \boldsymbol{\Theta}_2 \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \dots & \mathbf{0} & \boldsymbol{\Theta}_L \end{pmatrix}, \qquad \boldsymbol{\Theta}_m \in \mathcal{A}_p, \tag{2.7}$$

is transmitted over the channel (2.1), i.e.,

$$\mathbf{r}_\Theta = \boldsymbol{\Theta}\mathbf{h} + \boldsymbol{\xi}_\Theta, \tag{2.8}$$

where $L = \frac{T-M}{2} + 1$. During the second $\frac{T}{2}$ time slots transmission period, another $\frac{T}{2} \times M$ Alamouti code $\mathcal{A}_q$-based Toeplitz codeword matrix

$$\mathbf{\Phi} = \begin{pmatrix} \mathbf{\Phi}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{\Phi}_2 & \mathbf{\Phi}_1 & \dots & \mathbf{0} \\ \vdots & \mathbf{\Phi}_2 & \ddots & \vdots \\ \mathbf{\Phi}_L & \ddots & \ddots & \mathbf{\Phi}_1 \\ \mathbf{0} & \ddots & \ddots & \mathbf{\Phi}_2 \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \dots & \mathbf{0} & \mathbf{\Phi}_L \end{pmatrix}, \qquad \mathbf{\Phi}_m \in \mathcal{A}_q, \tag{2.9}$$

is sent through the channel (2.1) for transmission, i.e.,

$$\mathbf{r}_\Phi = \mathbf{\Phi}\mathbf{h} + \boldsymbol{\xi}_\Phi. \tag{2.10}$$

Collecting (2.8) and (2.10) yields

$$\mathbf{r} = \begin{pmatrix} \mathbf{r}_\Theta \\ \mathbf{r}_\Phi \end{pmatrix} = \begin{pmatrix} \mathbf{\Theta} \\ \mathbf{\Phi} \end{pmatrix} \mathbf{h} + \boldsymbol{\xi} = \mathbf{S}\mathbf{h} + \boldsymbol{\xi}, \tag{2.11}$$

where $\mathbf{r} = (\mathbf{r}_\Theta^T, \mathbf{r}_\Phi^T)^T, \mathbf{S} = (\mathbf{\Theta}^T, \mathbf{\Phi}^T)^T$ and $\boldsymbol{\xi} = (\boldsymbol{\xi}_\Theta^T, \boldsymbol{\xi}_\Phi^T)^T$. All such codeword matrices $\mathbf{S}$ form a noncoherent space-time block code, which, in this thesis, is called an Alamouti-based Toeplitz space-time block code and denoted by $\mathcal{S}$. As mentioned in Chapter 1, the Cayley transform and the exponential transform are two well-established transforms that convert respective linear dispersion codes and linear space-time block codes into unitary codes. Here, we provide an alternative strategy for the design of a unitary space-time block code by simply applying the QR decomposition to the nonunitary

code $\mathcal{S}$ designed by (2.8) and (2.10), i.e.,

$$\mathcal{Q}_s = \{\mathbf{Q}_s : \mathbf{S} = \mathbf{Q}_s\mathbf{R}_s, \mathbf{S} \in \mathcal{S}\}, \tag{2.12}$$

where $\mathbf{Q}_s$ is a column-wise unitary matrix and $\mathbf{R}_s$ is a square upper triangular matrix with positive diagonal entries. Now, instead of transmitting the codeword matrix $\mathbf{S}$, we transmit its Q-factor, i.e., $\mathbf{Q}_s$, through the channel (2.1) and the resulting received signal vector, denoted by $\mathbf{r}_{\text{qr}}$, is represented by

$$\mathbf{r}_{\text{qr}} = \mathbf{Q}_s\mathbf{h} + \boldsymbol{\xi}_{\text{qr}}. \tag{2.13}$$

The advantages of the unitary code design using the QR decomposition will be seen in Theorem 5 and explained in more details in Section 7.2.

Our second main task in this thesis is to solve the following problem.

Problem 2 *Prove that the nonunitary and unitary Alamouti-based Toeplitz space-time block codes enable the unique identification of the channel coefficients and the transmitted signals in the noise-free case as well as full diversity in the noise case.*

Chapter 3

Uniquely Factorable Constellation Pair

To solve the Problem 1, we need to appropriately design the constellation triple, $\mathcal{A}, \mathcal{B}_1, \mathcal{B}_2$. To this end, in this chapter, we propose a novel concept called Uniquely Factorable Constellation Pair (UFCP). Then, for Problem 2, we generalize the concept of UFCP onto Alamouti code to support our proof. Therefore, UFCP is the key concept in this thesis.

3.1 UFCP

Definition 1 *A pair of constellations $\mathcal{X}$ and $\mathcal{Y}$ is said to be a UFCP, which is denoted by $\mathcal{Y} \sim \mathcal{X}$, if there exist $x, \tilde{x} \in \mathcal{X}$ and $y, \tilde{y} \in \mathcal{Y}$ such that $x\tilde{y} = \tilde{x}y$, then $x = \tilde{x}$, $y = \tilde{y}$.*

In Chapter 4, we will see that it is this kind of the unique factorization of constellations that enables the unique identification of the channel and transmitted signals as well

as full diversity for collaborative unitary code presented in Section 2.2. The following example provides us with a trivial UFCP.

Example 1 *For any set $\mathcal{Y}$, if we take $\mathcal{X} = \{1\}$, then, $\mathcal{X}$ and $\mathcal{Y}$ form a UFCP.*

Example 1 tells us the constellation pair based on the training transmission scheme naturally forms a UFCP. In this thesis, we are interested in the design of non-trival UFCPs each element of which is a complex integer. To do that, we need to develop a necessary condition which a UFCP must satisfy.

Proposition 1 *Let $\mathcal{X}$ and $\mathcal{Y}$ form a UFCP. If $|\mathcal{Y}| \geq 2$, then, $0 \notin \mathcal{X}$.*

PROOF: Since $|\mathcal{Y}| \geq 2$, there exist two elements $y_1, y_2 \in \mathcal{Y}$ such that $y_1 \neq y_2$. Now, suppose that $0 \in \mathcal{X}$. Then, we would have $0 \times y_1 = 0 \times y_2 = 0$, which contradicts with the assumption that $\mathcal{X}$ and $\mathcal{Y}$ constitute a UFCP. This completes the proof of Proposition 1 □

From Proposition 1 and Definition 1, we can immediately obtain the following proposition:

Proposition 2 *For a pair of given constellations $\mathcal{X}$ and $\mathcal{Y}$ with each having finite size and $0 \notin \mathcal{X}$, if a new constellation $\mathcal{Z}$ is defined as*

$$\mathcal{Z} = \left\{ z : z = \frac{y}{x}, x \in \mathcal{X}, y \in \mathcal{Y} \right\},$$

then, such a pair of $\mathcal{X}$ and $\mathcal{Y}$ constitutes a UFCP if and only if

$$|\mathcal{Z}| = |\mathcal{X}| \times |\mathcal{Y}|. \tag{3.1}$$

PROOF: Define a map τ from $\mathcal{X} \times \mathcal{Y}$ to $\mathcal{Z}$ as

$$\tau : (x, y) \in \mathcal{X} \times \mathcal{Y} \longrightarrow \frac{y}{x} = z \in \mathcal{Z}. \tag{3.2}$$

It can be verified that τ is one-to-one correspondence if and only if $\frac{y}{x} \neq \frac{\widetilde{y}}{\widetilde{x}}$, i.e., $\widetilde{x}y \neq x\widetilde{y}$ for $(x, y) \neq (\widetilde{x}, \widetilde{y})$, which is equivalent to saying that a pair of the constellations $\mathcal{X}$ and $\mathcal{Y}$ constitutes a UFCP. On the other hand, since both $\mathcal{X} \times \mathcal{Y}$ and $\mathcal{Z}$ have finite size, τ is one-to-one correspondence if and only if $|\mathcal{Z}| = |\mathcal{X} \times \mathcal{Y}| = |\mathcal{X}| \times |\mathcal{Y}|$. This completes the proof of Proposition 2. □

Proposition 2 tells us that a UFCP $\mathcal{Y} \sim \mathcal{X}$ can be constructed by factorizing a constellation $\mathcal{Z}$ in such a way that each fraction is unique. For notation simplicity, this kind of construction is specifically denoted by $\mathcal{Z} = \frac{\mathcal{Y}}{\mathcal{X}}$. First, we consider $\mathcal{Z}$ to be a PSK constellation. It has been proved [77] if $\mathcal{Z}$ is pq-PSK constellation, and p, q are coprime numbers, then $\mathcal{Z}$ can be factorized into a UFCP $\mathcal{Y} \sim \mathcal{X}$, where $\mathcal{X}$ is p-PSK and $\mathcal{Y}$ is q-PSK constellation.

Example 2 *If $p = 3$, $q = 4$, and*

$$\begin{aligned} \mathcal{X} &= \{1, e^{j2\pi/3}, e^{j4\pi/3}\}, \\ \mathcal{Y} &= \{1, e^{j\pi/2}, e^{j\pi}, e^{j3\pi/2}\}, \end{aligned}$$

then, they constitute a UFCP $\mathcal{Y} \sim \mathcal{X}$.

3.2 Unique Factorizations of The Modified Cross QAM Constellation

Now, we consider factorizing other constellations rather other PSK, since PSK is not energy efficient. In general, when $\mathcal{Z}$ is sizable, it is not easy to find a non-trival unique factorization. However, for some special constellations, we can utilize this factorization to systematically construct a UFCP.

Definition 2 *A constellation is said to be rotation-invariant with respect to $e^{j\theta}$ if every element in the constellation multipled by $e^{j\theta}$ still belongs to the constellation.*

Example 3 *The square QAM constellation is rotation-invariant with respect to $e^{j\theta}$ with the angle θ being equal to $\pi/2, \pi$ and $3\pi/2$.*

In general, we can always have the following property, which can be verified directly by the definition and thus, whose poof is omitted.

Proposition 3 *Let $\mathcal{Z}$ be rotation-invariant with respect to $e^{j\pi/2}$, $e^{j\pi}, e^{j3\pi/2}$ and $0, r, rj \notin \mathcal{Z}$, where r is real. Then, the following statements are true:*

1. *If we let*

$$\begin{aligned}\mathcal{X} &= \{1, j\},\\ \mathcal{Y} &= \{z : z = z_{\text{re}} + jz_{\text{im}} \in \mathcal{Z}, z_{\text{re}}, z_{\text{im}} > 0\} \cup \{z : z = z_{\text{re}} + jz_{\text{im}} \in \mathcal{Z}, z_{\text{re}}, z_{\text{im}} < 0\},\end{aligned}$$

then, such a pair of $\mathcal{X}$ and $\mathcal{Y}$ constitutes a UFCP and $\mathcal{Z} = \frac{\mathcal{Y}}{\mathcal{X}}$.

2. If we let

$$\begin{aligned}\mathcal{X} &= \{1, -1, j, -j\},\\ \mathcal{Y} &= \{z : z = z_{\text{re}} + jz_{\text{im}} \in \mathcal{Z}, z_{\text{re}}, z_{\text{im}} > 0\},\end{aligned}$$

then, such a pair of $\mathcal{X}$ and $\mathcal{Y}$ forms another UFCP and $\mathcal{Z} = \frac{\mathcal{Y}}{\mathcal{X}}$.

The following two examples show us how to obtain the UFCPs by factorizing the 16-QAM constellation by Proposition 3.

Example 4 *Let $\mathcal{Z}$ be the 16-QAM constellation. By Proposition 3, a UFCP $\mathcal{Y} \sim \mathcal{X}$ is obtained by factorizing $\mathcal{Z}$:*

$$\begin{aligned}\mathcal{X} &= \{1, j\},\\ \mathcal{Y} &= \{3+3j, 3+j, 1+3j, 1+j, -1-j, -3-3j, -3-j, -1-3j\}.\end{aligned}$$

Example 5 *Again, applying an idea similar to Proposition 3 to the 16-QAM constellation yields another UFCP:*

$$\begin{aligned}\mathcal{X} &= \{1, -1, j, -j\},\\ \mathcal{Y} &= \{3+3j, 3+j, 1+3j, 1+j\}.\end{aligned}$$

In addition, it is noticed that for a given UFCP $\mathcal{Y} \sim \mathcal{X}$, when the symbol x is fixed, all the fractions of the form $z = \frac{y}{x}, y \in \mathcal{Y}$ can be chosen only from a certain subset of $\mathcal{Z}$, which will be employed in the design of the constellation triple $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ in Chapter 4. Therefore, we particularly give a formal definition as follows:

Definition 3 *Given a UFCP $\mathcal{Y} \sim \mathcal{X}$ and a fixed $x \in \mathcal{X}$, a set generated from x, denoted by $\mathcal{Z}_x$,*

$$\mathcal{Z}_x = \{z : z = \frac{y}{x}, y \in \mathcal{Y}\}, \tag{3.3}$$

is called a Group-x.

The groups have some interesting properties:

Proposition 4 *Let $\mathcal{Z} = \frac{\mathcal{Y}}{\mathcal{X}}$. Then, the following three statements are true:*

1. *Non-intersection: For any $x_1, x_2 \in \mathcal{X}, x_1 \neq x_2$, there is no intersection between Group-x_1 and Group-x_2, i.e.,*

$$\mathcal{Z}_{x_1} \cap \mathcal{Z}_{x_2} = \Phi. \tag{3.4}$$

2. *Decomposition: The union of all the groups is equal to the original constellation $\mathcal{Z}$, i.e.,*

$$\cup_{x \in \mathcal{X}} \mathcal{Z}_x = \mathcal{Z}. \tag{3.5}$$

3. *The number of groups is equal to $|\mathcal{X}|$ and $|\mathcal{Z}_x| = |\mathcal{Y}|$ for any $x \in \mathcal{X}$.*

Proof: Statement 2) is derived directly from the definition of the Group. Here, we only examine Statements 1) and 3). For any $x_1, x_2 \in \mathcal{X}$ and $x_1 \neq x_2$, suppose that there exists some z belonging to $\mathcal{Z}_{x_1} \cap \mathcal{Z}_{x_2}$. Then, $z \in \mathcal{Z}_{x_1}$ and $z \in \mathcal{Z}_{x_2}$ and thus, there exist $y_1, y_2 \in \mathcal{Y}$ such that $\frac{y_1}{x_1} = \frac{y_2}{x_2}$, which implies that $x_1 y_2 = x_2 y_1$. Since $\mathcal{X}$ and $\mathcal{Y}$ form a UFCP, we have $x_1 = x_2$ and $y_1 = y_2$, which contradicts with the

assumption that $x_1 \neq x_2$. Hence, $\mathcal{Z}_{x_1} \cap \mathcal{Z}_{x_2} = \Phi$, i.e., Statement 1) is true. Using the Statements 1) and 2), we obtain

$$|\mathcal{Z}| = \sum_{x \in \mathcal{X}} |\mathcal{Z}_x|. \tag{3.6}$$

By the definition of the group, we have $|\mathcal{Z}_x| = |\mathcal{Y}|$. Substituting this into (3.6) yields $|\mathcal{X}| \times |\mathcal{Y}| = |\mathcal{Z}|$. This completes the proof of Statement 3) and thus, of Proposition 4.

In spite of the fact that Proposition 2 tells us that a UFCP $\mathcal{Y} \sim \mathcal{X}$ can be constructed by factorizing a constellation $\mathcal{Z}$, in general, the UFCP $\mathcal{Y} \sim \mathcal{X}$ so derived from the given $\mathcal{Z}$ is not unique. In other words, the same constellation $\mathcal{Z}$ can generate two different UFCPs. For instance, consider the following example:

Example 6 *Let $\mathcal{Z}$ be the 16-QAM constellation. If we let*

$$\begin{aligned} \mathcal{X} &= \{1, -1, j, -j\}, \\ \mathcal{Y} &= \{3+3j, 3-j, -1+3j, -1-j\}, \end{aligned}$$

then, it can be verified that such a pair of constellations $\mathcal{X}$ and $\mathcal{Y}$ also forms a UFCP, which is different from the one given in Example 5.

Now, a natural question is: *for a given constellation $\mathcal{Z}$, which pair of constellations $\mathcal{X}$ and $\mathcal{Y}$ generated by $\mathcal{Z}$ is better?* A general answer to this question is hard to be given. However, in this thesis, we are interested in the UFCPs which are derived from the cross 2^K-ary QAM constellation [78] and every element of which is still a complex integer. This implicitly requires that each element of $\mathcal{X}$ must be of the unit-norm, i.e., ± 1 or $\pm j$. Specifically, we focus on such a UFCP generated from the cross QAM constellation that the minimum distance of $\mathcal{Y}$ is as large as possible. Since the

conventional 8-QAM constellation does not satisfy the rotation-invariant property, we need to modify it into a new 8-QAM constellation so as to be rotation-invariant under $e^{j\pi/2}$, $e^{j\pi}$ and $e^{j3\pi/2}$. For discussion self-containment, a formal definition of a 2^K-ary modified cross QAM constellation is provided here.

Definition 4 *A modofied 2^K-ary QAM constellation $\mathcal{Q}$ is defined as follows:*

1. *If K is even, $\mathcal{Q}$ is the standard square 2^K-ary QAM constellation, i.e.,*

$$\mathcal{Z} = \Big\{(2m-1) + (2n-1)j : -2^{\frac{K-2}{2}} + 1 \leq m, n \leq 2^{\frac{K-2}{2}}\Big\}.$$

2. *If $K = 3$, $\mathcal{Q}$ is a new 8-QAM constellation modified from the conventional 8-ary QAM constellation, i.e.,*

$$\mathcal{Q} = \Big\{1+3j, 1+j, 3-j, 1-j, -1-3j, -1-j, -3+j, -1+j\Big\}.$$

3. *If K is an odd number exceeding 3, $\mathcal{Q}$ is the union of a horizontal rectangular QAM constellation and a vertical rectangular QAM constellation, i.e.,*

$$\begin{aligned}\mathcal{Z} = &\big\{(2m-1) + (2n-1)j : -3 \times 2^{\frac{K-5}{2}} + 1 \leq m \leq 3 \times 2^{\frac{K-5}{2}}, -2^{\frac{K-3}{2}} + 1 \leq n \leq 2^{\frac{K-3}{2}}\big\} \\ &\bigcup \big\{(2m-1) + (2n-1)j : -2^{\frac{K-3}{2}} + 1 \leq m \leq 2^{\frac{K-3}{2}}, -3 \times 2^{\frac{K-5}{2}} + 1 \leq n \leq 3 \times 2^{\frac{K-5}{2}}\big\}.\end{aligned}$$

Proposition 5 *Let $\mathcal{Z}$ be the given modified 2^K-cross QAM constellation. Then, subject to $\mathcal{X} \subseteq \{1, -1, j, -j\}$ with a fixed size greater than one, one solution to the*

following optimization problem:

$$\{\mathcal{X}_{\text{opt}}, \mathcal{Y}_{\text{opt}}\} = \arg\max_{\frac{\mathcal{Y}}{\mathcal{X}}=\mathcal{Z}} \min_{y_1 \neq y_2 \in \mathcal{Y}} |y_1 - y_2|, \tag{3.8}$$

is given as follows:

1. *If* $|\mathcal{X}| = 2$*, then,*

$$\mathcal{X}_{\text{opt}}^{(1)} = \{1, j\}.$$

   (a) $K = 3$.

$$\mathcal{Y}_{\text{opt}}^{(1)} = \{1+3j, -1-3j, -1-j, 1+j\}. \tag{3.9}$$

   (b) $K = 5$.

$$\begin{aligned}\mathcal{Y}_{\text{opt}}^{(1)} = \{&-1+5j, 3+5j, -3+3j, 1+3j, 5+3j, -5+j, -1+j, 3+j,\\ &-3-j, 1-j, 5-j, -5-3j, -1-3j, 3-3j, -3-5j, 1-5j\}.\end{aligned} \tag{3.10}$$

   (c) $K \geq 4$. *In this case, the optimal* $\mathcal{Y}_{\text{opt}}^{(1)}$ *is determined as follows:*

      i. K *is even,*

$$\begin{aligned}\mathcal{Y}_{\text{opt}}^{(1)} = &\left\{(2^{\frac{K}{2}} - 1 - 4m) + (2^{\frac{K}{2}} - 1 - 4n)j : \ 0 \leq m, n \leq 2^{\frac{K-2}{2}} - 1\right\}\\ &\bigcup \left\{(2^{\frac{K}{2}} - 3 - 4m) + (2^{\frac{K}{2}} - 3 - 4n)j : \ 0 \leq m, n \leq 2^{\frac{K-2}{2}} - 1\right\}.\end{aligned} \tag{3.11}$$

ii. K is an odd number exceeding 5,

$$\begin{aligned}\mathcal{Y}_{\text{opt}}^{(1)} = &\Big\{(3\times 2^{\frac{K-3}{2}} - 1 - 4m) + (2^{\frac{K-1}{2}} - 1 - 4n)j\Big\}_{m=0,n=0}^{m=2^{\frac{K-3}{2}}-1,\, n=3\times 2^{\frac{K-5}{2}}-1} \\ &\bigcup \Big\{(2^{\frac{K-1}{2}} - 1 - 4m) + (3\times 2^{\frac{K-3}{2}} - 1 - 4n)j\Big\}_{m=0,n=0}^{m=3\times 2^{\frac{K-5}{2}}-1,\, n=2^{\frac{K-3}{2}}-1} \\ &\bigcup \Big\{(3\times 2^{\frac{K-3}{2}} - 3 - 4m) + (2^{\frac{K-1}{2}} - 3 - 4n)j\Big\}_{m=0,n=0}^{m=2^{\frac{K-3}{2}}-1,\, n=3\times 2^{\frac{K-5}{2}}-1} \\ &\bigcup \Big\{(2^{\frac{K-1}{2}} - 3 - 4m) + (3\times 2^{\frac{K-3}{2}} - 3 - 4n)j\Big\}_{m=0,n=0}^{m=3\times 2^{\frac{K-5}{2}}-1,\, n=2^{\frac{K-3}{2}}-1}.\end{aligned} \tag{3.12}$$

2. If $|\mathcal{X}| = 4$ and $K \geq 3$, then,

$$\mathcal{X}_{\text{opt}}^{(2)} = \{1, -1, j, -j\}.$$

(a) $K = 3$.

$$\mathcal{Y}_{\text{opt}}^{(2)} = \{1 + 3j, -1 - j\}.$$

(b) $K = 5$.

$$\mathcal{Y}_{\text{opt}}^{(2)} = \{-1 + 5j, 3 + 5j, -5 + j, -1 + j, 3 + j, -5 - 3j, -1 - 3j, 3 - 3j\}.$$

(c) $K \geq 4$. In this situation, the optimal $\mathcal{Y}_{\text{opt}}^{(2)}$ can be determined as follows:

i. K is even,

$$\mathcal{Y}_{\text{opt}}^{(2)} = \Big\{(2^{\frac{K}{2}} - 1 - 4m) + (2^{\frac{K}{2}} - 1 - 4n)j : \ 0 \leq m, n \leq 2^{\frac{K-2}{2}} - 1\Big\}. \tag{3.13}$$

ii. K is an odd number exceeding 5,

$$\mathcal{Y}_{\text{opt}}^{(2)} = \left\{(3\times 2^{\frac{K-3}{2}} - 1 - 4m) + (2^{\frac{K-1}{2}} - 1 - 4n)j\right\}_{m=0,n=0}^{m=3\times 2^{\frac{K-5}{2}}-1,\, n=2^{\frac{K-3}{2}}-1} \bigcup \left\{(2^{\frac{K-1}{2}} - 1 - 4m) + (3\times 2^{\frac{K-3}{2}} - 1 - 4n)j\right\}_{m=0,n=0}^{m=2^{\frac{K-3}{2}}-1,\, n=3\times 2^{\frac{K-5}{2}}-1}. \tag{3.14}$$

The proof of Proposition 5 is given in Appendix A.1. In principle, the optimal constellations $\mathcal{Y}_{\text{opt}}^{(1)}$ and $\mathcal{Y}_{\text{opt}}^{(2)}$ in Proposition 5 can be attained by starting at any corner point in $\mathcal{Z}$ with the largest energy and then, for $|\mathcal{X}| = 2$, successively selecting all nearest neighbors of the previously already selected points along the diagonal lines and for $|\mathcal{X}| = 4$, successively selecting all every other points of the previously already selected points along the horizontal and vertical lines. Fig. 3.1 visually demonstrates how the optimal constellations $\mathcal{Y}_{\text{opt}}^{(1)}$ and $\mathcal{Y}_{\text{opt}}^{(2)}$ in Proposition 5 have been obtained by starting at the corner point in the first quadrant with the largest energy via the diagonal line or the horizontal and vertical lines search over the cross QAM constellations when K is either even or odd. As an application of Proposition 5, we give the following example.

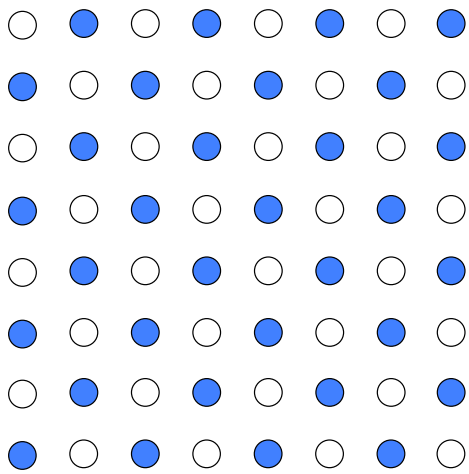
Example 7 *$K = 4$. By Proposition 5, we have that*

1. *if $|\mathcal{X}| = 2$, then,*

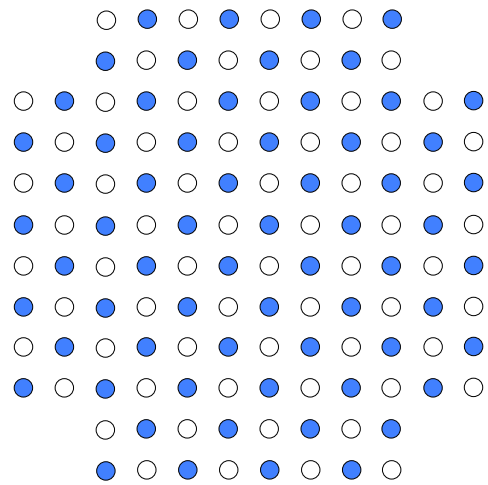
$$\begin{aligned}\mathcal{X}_{\text{opt}}^{(1)} &= \{1, j\},\\ \mathcal{Y}_{\text{opt}}^{(1)} &= \{3+3j, 1+j, -1+3j, 3-j, -3+j, -1-j, 1-3j, -3-3j\}.\end{aligned}$$

2. if $|\mathcal{X}| = 4$*, then,*

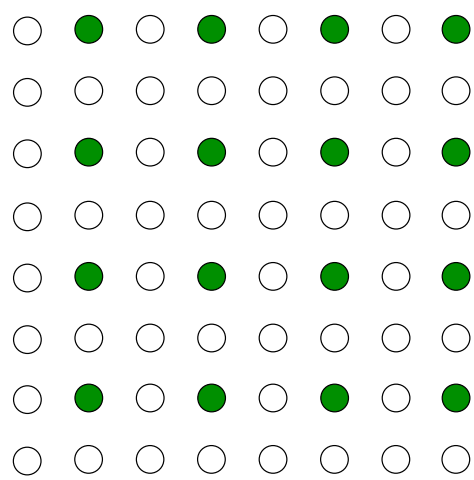
$$\begin{aligned}\mathcal{X}_{\text{opt}}^{(2)} &= \{1, -1, j, -j\},\\ \mathcal{Y}_{\text{opt}}^{(2)} &= \{3+3j, -1+3j, 3-j, -1-j\}.\end{aligned}$$



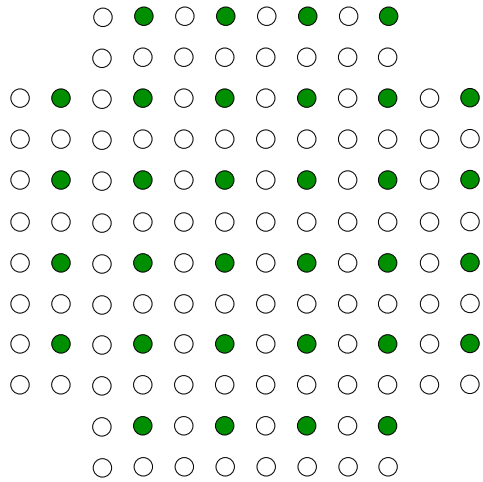
(a) Diagonal line search over the square QAM constellation for the optimal $\mathcal{Y}_{\text{opt}}^{(1)}$



(b) Diagonal search over the cross QAM constellation for the optimal $\mathcal{Y}_{\text{opt}}^{(1)}$



(c) Horizontal and vertical lines search over the square QAM constellation for the optimal $\mathcal{Y}_{\text{opt}}^{(2)}$



(d) Horizontal and vertical lines search over the cross QAM constellation for the optimal $\mathcal{Y}_{\text{opt}}^{(2)}$

Figure 3.1: The optimal UFCP selections from the square 64QAM and cross 128QAM constellations in Proposition 5

Chapter 4

Collaborative Unitary UFCP Space-Time Block Code

In this chapter, we take advantage of UFCPs established in Chapter 3 to carefully design the constellation triple $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ for collaborative unitary space-time block codes define in (2.3). We will show that it is the unique factorization of signals that results not only in the unique identification of the channel coefficients and the transmitted signals in the noise-free case, but in full diversity in the noise case as well.

4.1 Signal Designs and Unique Identification

In order for the code (2.3b) to enable the unique identification of the channel and the transmitted signals as well as full diversity, the three constellations $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ must work cooperatively. There may exist many cooperative agreements to make these constellations work together. Different collaborative ways will produce different codes,

but in this thesis, we require that $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ cooperate in such a way that $\mathcal{A}$ and $\mathcal{B}_1$, $\mathcal{A}$ and $\mathcal{B}_2$ constitute two pairs of UFCPs. In other words, the same constellation $\mathcal{A}$ collaborates with both the constellations $\mathcal{B}_1$ and $\mathcal{B}_2$. More explanations of why such a collaborative scheme is adopted will be given after Theorem 1. To make the selection of these constellations more clear, we change notation $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ into the respective $\mathcal{X}, \mathcal{Y}_1$ and $\mathcal{Y}_2$. Correspondingly, the code now takes the following form:

$$\mathcal{U} = \left\{ \mathbf{U} = \frac{1}{\sqrt{|x|^2 + |y_1|^2 + |y_2|^2}} \begin{pmatrix} x & 0 \\ 0 & x^* \\ y_1 & y_2 \\ -y_2^* & y_1^* \end{pmatrix} : \quad x \in \mathcal{X}, y_1 \in \mathcal{Y}_1, y_2 \in \mathcal{Y}_2 \right\}, \quad (4.1)$$

where $\mathcal{Y}_1 \sim \mathcal{X}$ and $\mathcal{Y}_2 \sim \mathcal{X}$ constitute two UFCPs. Such a code $\mathcal{U}$ is called a collaborative unitary UFCP space-time block code.

Theorem 1 *Let $\mathcal{Y}_1 \sim \mathcal{X}$, and $\mathcal{Y}_2 \sim \mathcal{X}$ be two UFCPs. Then, for any given nonzero received signal vector without noise, i.e., $\mathbf{r} = \mathbf{U}\mathbf{h}$, the code $\mathcal{U}$ designed by* (4.1) *enables the unique identification of the channel coefficients and the transmitted signals.*

Proof: Using the code structure (4.1), we have

$$\mathbf{r}_x = \frac{1}{\sqrt{|x|^2 + |y_1|^2 + |y_2|^2}} \mathbf{X}\mathbf{h}, \quad (4.2a)$$

$$\mathbf{r}_y = \frac{1}{\sqrt{|x|^2 + |y_1|^2 + |y_2|^2}} \mathbf{Y}\mathbf{h}, \quad (4.2b)$$

where $\mathbf{X}$ and $\mathbf{Y}$ are defined by

$$\begin{aligned}\mathbf{X} &= \begin{pmatrix} x & 0 \\ 0 & x^* \end{pmatrix}, \\ \mathbf{Y} &= \begin{pmatrix} y_1 & y_2 \\ -y_2^* & y_1^* \end{pmatrix}.\end{aligned}$$

Since $|\mathcal{Y}_i| > 1$ for $i = 1, 2$, by Proposition 1 we have $x \neq 0$ and as a result, the matrix $\mathbf{X}$ is invertible. Eliminating $\mathbf{h}$ from (4.2) yields

$$\mathbf{r}_y = \mathbf{Y}\mathbf{X}^{-1}\mathbf{r}_x. \tag{4.3}$$

Notice that $\mathbf{Y}\mathbf{X}^{-1} = \begin{pmatrix} \frac{y_1}{x} & -(\frac{y_2}{x})^* \\ \frac{y_2}{x} & (\frac{y_1}{x})^* \end{pmatrix}$ is the Alamouti codeword matrix. Therefore, equation (4.3) can be rewritten as

$$\widetilde{\mathbf{r}}_y = \mathbf{R}_x\mathbf{u}, \tag{4.4}$$

where $\widetilde{\mathbf{r}}_y = (r_y(1), r_y^*(2))^T$, $\mathbf{u} = (y_1/x, y_2/x)^T$ and $\mathbf{R}_x$ is given by

$$\mathbf{R}_x = \begin{pmatrix} r_x(1) & -r_x(2) \\ r_x^*(2) & r_x^*(1) \end{pmatrix}.$$

It can be verified that $\mathbf{R}_x$ is unitary up to a scale. In addition, since $\mathbf{r} = (\mathbf{r}_x^T, \mathbf{r}_y^T)^T \neq \mathbf{0}$ and $\mathbf{X}$ is invertible, we have $\mathbf{h} \neq \mathbf{0}$ and thus, $\mathbf{r}_x \neq \mathbf{0}$, which is equivalent to the fact

that $\mathbf{R}_x$ is invertible. Therefore, from (4.4) we obtain

$$\mathbf{u} = \mathbf{R}_x^{-1}\widetilde{\mathbf{r}}_y. \tag{4.5}$$

That is

$$\frac{y_1}{x} = \frac{r_x^*(1)r_y(1) + r_x(2)r_y^*(2)}{|r_x(1)|^2 + |r_x(2)|^2}, \tag{4.6a}$$

$$\frac{y_2}{x} = \frac{-r_x^*(2)r_y(1) + r_x(1)r_y^*(2)}{|r_x(1)|^2 + |r_x(2)|^2}. \tag{4.6b}$$

Since $\mathcal{X}$ and $\mathcal{Y}_i$ form the two UFCPs and $x \in \mathcal{X}$ and $y_i \in \mathcal{Y}_i$ for $i = 1, 2$, once their quotients y_i/x have been determined, then, x and y_i themselves can be uniquely determined. In other words, there exists a unique triple x, y_1 and y_2 such that (4.6) is satisfied. Moreover, after we have determined x and y_i, then, the channel vector $\mathbf{h}$ can be uniquely determined by $\mathbf{h} = \sqrt{|x|^2 + |y_1|^2 + |y_2|^2}\,\mathbf{X}^{-1}\mathbf{r}_x = \sqrt{|x|^2 + |y_1|^2 + |y_2|^2}\,\mathbf{Y}^{-1}\mathbf{r}_y$. This completes the proof of Theorem 1. □

Some observations on Theorem 1 are made as follows:

1. Theorem 1 tells us that using the UFCP code (4.1), the channel coefficients and the transmitted signals can be uniquely identified by *only* processing the four received signals. Theorem 1 is very desirable in the design of noncoherent constellations, since if a signal design is not able to provide the unique identication of the channel and the transmitted signals in the noise-free case, then, the reliable estimation of the signal will not be guaranteed, even in high SNR.

2. From the proof of Theorem 1, i.e., (4.6), we can observe that if either $\mathcal{Y}_1 \sim \mathcal{X}$ or $\mathcal{Y}_2 \sim \mathcal{X}$, then, the channel coefficients and the transmitted signals can be

still uniquely identified. In addition, (4.6a) divided by (4.6b) gives us

$$\frac{y_1}{y_2} = \frac{r_x^*(1)r_y(1) + r_x(2)r_y^*(2)}{-r_x^*(2)r_y(1) + r_x(1)r_y^*(2)}.$$

Now, it can be seen clearly that if $\mathcal{Y}_1 \sim \mathcal{Y}_2$, then, y_1, y_2 and thus, x can be uniquely determined. As a result, the channel coefficients can also be uniquely determined. Therefore, it is worth emphasizing the fact that it is the unique factorization of constellations proposed in Chapter 3 that enables the channel coefficients and the transmitter signals to be uniquely identified. In a word, the unique identification of both the channel coefficients and the transmitted signals requires three constellations collaboration.

3. The aforementioned Observations 2) tells us that there are several ways in which the three constellations $\mathcal{A}, \mathcal{B}_1$ and $\mathcal{B}_2$ can collaborate so that both the channel coefficients and the transmitted signals are able to be uniquely identified. However, in this thesis we adopt $\mathcal{Y}_1 \sim \mathcal{X}$ and $\mathcal{Y}_2 \sim \mathcal{X}$, since the same constellation $\mathcal{X}$ collaborating with the other two constellations $\mathcal{Y}_1$ and $\mathcal{Y}_2$ not only enables the unique identification and thus, full diversity (see Theorem 2), but also provides an opportunity for the two transmitter antennas to accumulate their minimum Euclidean distances such that the coding gain is increased. See more details in Chapter 5.

4.2 Full Diversity

In order to analyze full diversity of the UFCP code (4.1), let us first consider a general space-time block coded noncoherent MIMO system with M transmitter antennas, N

receiver antennas and flat fading channels as follows:

$$\boldsymbol{\Upsilon} = \mathbf{SH} + \boldsymbol{\Xi}, \tag{4.7}$$

where $\boldsymbol{\Upsilon}$ denotes a $T \times N$ received signal matrix, $\mathbf{H}$ denotes an $M \times N$ channel matrix, $\mathbf{S}$ is a $T \times M$ codeword matrix and $\boldsymbol{\Xi}$ denotes a $T \times N$ noise matrix. We assume that the elements ξ_{tn} of $\boldsymbol{\Xi}$ are samples of independent circularly-symmetric zero-mean complex Gaussian random variables with variance σ^2. Under these assumptions, the probability density function of the received signal matrix $\boldsymbol{\Upsilon}$ conditioned on the transmitted signal matrix $\mathbf{S}$ is the Gaussian distribution, i.e., $\frac{1}{\pi^{TN}\det(\mathbf{SS}^H+\sigma^2\mathbf{I})} \times \exp\left(-\frac{\mathrm{Tr}\left(\boldsymbol{\Upsilon}^H(\mathbf{SS}^H+\sigma^2\mathbf{I})^{-1}\boldsymbol{\Upsilon}\right)}{\sigma^2}\right)$, and thus, its likelihood is given by $-\frac{\mathrm{Tr}\left(\boldsymbol{\Upsilon}^H(\mathbf{SS}^H+\sigma^2\mathbf{I})^{-1}\boldsymbol{\Upsilon}\right)}{\sigma^2} - \ln\det(\mathbf{SS}^H + \sigma^2\mathbf{I}) - TN\ln\pi$. Then, the maximum likelihood (ML) receiver for the noncoherent MIMO system is equivalent to solving the following optimization problem: $\hat{\mathbf{S}} = \arg\min_{\mathbf{S}}\{\Delta_s - \mathrm{Tr}\left(\boldsymbol{\Upsilon}^H\boldsymbol{\Theta}_s\boldsymbol{\Upsilon}\right)\}$, where $\boldsymbol{\Theta}_s = \frac{1}{\sigma^2}\mathbf{S}\left(\sigma^2\mathbf{I} + \mathbf{S}^H\mathbf{S}\right)^{-1}\mathbf{S}^H$ and $\Delta_s = \log\det\left(\sigma^2\mathbf{I} + \mathbf{S}^H\mathbf{S}\right)$. To avoid estimating the variance of noise, consider the conditional probability density function of the received signal matrix $\boldsymbol{\Upsilon}$ given the channel matrix $\mathbf{H}$ and the transmitted signal matrix $\mathbf{S}$, i.e., $\frac{1}{\pi^{TN}\sigma^{2TN}} \times \exp\left(-\frac{\|\boldsymbol{\Upsilon}-\mathbf{SH}\|_F^2}{\sigma^2}\right)$ and thus, its likelihood is given by $-\frac{\|\boldsymbol{\Upsilon}-\mathbf{SH}\|_F^2}{\sigma^2} - TN\ln\pi - 2TN\ln\sigma$. The *generalized likelihood ratio test* (GLRT) receiver for the joint estimation of $\mathbf{H}$ and $\mathbf{S}$ is to maximize the likelihood, which is essentially equivalent to solving the following nonlinear least square error optimization problem [71, 79, 80]:

$$\{\hat{\mathbf{H}}, \hat{\mathbf{S}}\} = \arg\min_{\mathbf{H},\mathbf{S}} \|\boldsymbol{\Upsilon} - \mathbf{SH}\|_F^2. \tag{4.8}$$

Its solution can be obtained by first estimating the transmitted signal matrix $\mathbf{S}$ as

$$\hat{\mathbf{S}} = \arg\max_{\mathbf{S}} \operatorname{Tr}\left(\boldsymbol{\Upsilon}^H \mathbf{S}\left(\mathbf{S}^H\mathbf{S}\right)^{-1}\mathbf{S}^H\boldsymbol{\Upsilon}\right), \tag{4.9}$$

and then, estimating the channel matrix $\mathbf{H}$ as $\hat{\mathbf{H}} = \left(\hat{\mathbf{S}}^H\hat{\mathbf{S}}\right)^{-1}\hat{\mathbf{S}}^H\boldsymbol{\Upsilon}$. Particularly for any unitary code, the ML receiver and the GLRT receiver for the optimal estimation of the transmitted signal matrix are equivalent, i.e., $\hat{\mathbf{S}} = \arg\max_{\mathbf{S}} \operatorname{Tr}\left(\boldsymbol{\Upsilon}^H\mathbf{S}\mathbf{S}^H\boldsymbol{\Upsilon}\right)$. In addition, [71] analyzed the asymptotic performance of the GLRT detector for the noncoherent MIMO system and proved the following lemma.

Lemma 1 *Let a $2M \times 2M$ matrix $\mathbf{R}_{s\hat{s}}$ be defined as $\mathbf{R}_{s\hat{s}} = \left(\mathbf{S}, \hat{\mathbf{S}}\right)^H\left(\mathbf{S}, \hat{\mathbf{S}}\right)$. If each matrix $\mathbf{R}_{s\hat{s}}$ has full rank for all pairs of distinct codewords $\mathbf{S}$ and $\hat{\mathbf{S}}$, then, the resulting space-time block code provides full diversity for the GLRT receiver, and moreover, the pair-wise error probability $\mathrm{P}_{\mathrm{GLRT}}(\mathbf{S} \to \hat{\mathbf{S}})$ of transmitting $\mathbf{S}$ and deciding in favor of $\hat{\mathbf{S}} \neq \mathbf{S}$ has the following asymptotic formula:*

$$\mathrm{P}_{\mathrm{GLRT}}(\mathbf{S} \to \hat{\mathbf{S}}) = \frac{\begin{pmatrix} 2MN-1 \\ MN \end{pmatrix} \det^N(\hat{\mathbf{S}}^H\hat{\mathbf{S}})}{\det^N(\mathbf{R}_{s\hat{s}})} \times \mathrm{SNR}^{-MN} + o\left(\mathrm{SNR}^{-MN}\right).$$

Lemma 12 tells us that the full rank of the matrices $\mathbf{R}_{s\hat{s}}$ for all the distinct codewords $\mathbf{S}$ and $\hat{\mathbf{S}}$ assures full diversity. It is not difficult to prove that a necessary condition for $\mathbf{R}_{s\hat{s}}$ to have full rank is $T \geq 2M$. Hence, in this thesis, we consider the case of the shortest coherent time slots when it is possible for the UFCP code design to enables unique identification of both the channel coefficients and the transmitted signals as well as full diversity.

Theorem 2 *Let $\mathcal{Y}_1 \sim \mathcal{X}$, and $\mathcal{Y}_2 \sim \mathcal{X}$ constitute two UFCPs. Then, the code $\mathcal{U}$ designed by* (4.1) *enables full diversity for the noncoherent ML receiver. Furthermore, the pair-wise error probability* $\mathrm{P}_{\mathrm{ML}}(\mathbf{U} \to \hat{\mathbf{U}})$ *of transmitting* $\mathbf{U}$ *and deciding in favor of* $\hat{\mathbf{U}} \neq \mathbf{U}$ *has the following asymptotic formula:*

$$\mathrm{P}_{\mathrm{ML}}(\mathbf{U} \to \hat{\mathbf{U}}) = \frac{3}{\det(\mathbf{R}_{u\hat{u}})} \times \mathrm{SNR}^{-2} + o\big(\mathrm{SNR}^{-2}\big),$$

where $\mathbf{R}_{u\hat{u}} = \big(\mathbf{U}, \hat{\mathbf{U}}\big)^H \big(\mathbf{U}, \hat{\mathbf{U}}\big)$.

Proof: We first note that since the UFCP code (4.1) is unitary, we have $\det(\mathbf{U}^H\mathbf{U}) = \det(\hat{\mathbf{U}}^H\hat{\mathbf{U}}) = 1$. By Lemma 12, we only need to prove that $\mathbf{R}_{u\hat{u}}$ is invertible for any pair of distinct $\mathbf{U}$ and $\hat{\mathbf{U}}$. Since $\big(\mathbf{U}, \hat{\mathbf{U}}\big)$ is a square matrix and $\mathbf{R}_{u\hat{u}} = \big(\mathbf{U}, \hat{\mathbf{U}}\big)^H \big(\mathbf{U}, \hat{\mathbf{U}}\big)$, proving that the matrix $\mathbf{R}_{u\hat{u}}$ is invertible is equivalent to proving that the matrix $\big(\mathbf{U}, \hat{\mathbf{U}}\big)$ is invertible. Notice that

$$\big(\mathbf{U}, \hat{\mathbf{U}}\big) = \frac{1}{\sqrt{|x|^2 + |y_1|^2 + |y_2|^2}} \begin{pmatrix} x & 0 & \hat{x} & 0 \\ 0 & x^* & 0 & \hat{x}^* \\ y_1 & y_2 & \hat{y}_1 & \hat{y}_2 \\ -y_2^* & y_1^* & -\hat{y}_2^* & \hat{y}_1^* \end{pmatrix}. \tag{4.10}$$

By some algebraic manipulations, we can obtain that the determinant of $\big(\mathbf{U}, \hat{\mathbf{U}}\big)$ is given by $\det\big(\mathbf{U}, \hat{\mathbf{U}}\big) = \big(\big|\frac{y_1}{x} - \frac{\hat{y}_1}{\hat{x}}\big|^2 + \big|\frac{y_2}{x} - \frac{\hat{y}_2}{\hat{x}}\big|^2\big)/\big(|x|^2 + |y_1|^2 + |y_2|^2\big)^2$. Since $\mathcal{X}$ and $\mathcal{Y}_i$ for $i = 1, 2$ forms two UFCPs for any $\mathbf{U} \neq \hat{\mathbf{U}}$, i.e., $(x, y_1, y_2) \neq (\hat{x}, \hat{y}_1, \hat{y}_2)$, we have $\det\big(\mathbf{U}, \hat{\mathbf{U}}\big) \neq 0$. In addition, the asymptotic formula can be immediately obtained by utilizing Lemma 12 again with $M = 2, N = 1$ and $\mathbf{S} = \mathbf{U}$. This completes the proof of Theorem 2. $\square$

From the proof of Theorem 2 we can observe that it is the unique factorization of our designed constellations that enables the matrix $\mathbf{R}_{y\hat{y}}$ to have full rank. In addition, we can also observe that Comment 2) on Theorem 1 is still a sufficient condition for the matrix $\mathbf{R}_{y\hat{y}}$ to have full rank. Therefore, noncoherent full diversity also requires the three constellations collaboration.

Chapter 5

Optimal Designs of Collaborative Unitary UFCP Space-Time Block Code

Our main task in this chapter is to efficiently and effectively optimize the coding gain for the collaborative unitary UFCP space-time block codes generated from the energy-efficient cross QAM constellations.

5.1 Problem Formulation

Theorems 1 and 2 tell us that the unitary code designed by (4.1) enables the unique identification of the channel coefficients and the transmitted signals as well as full diversity for the noncoherent ML receiver. Therefore, the code design partially gives a solution to Problem 1. In order to further optimize its error performance, we can see from the asymptotic formula of the pair wise error probability in Theorem 2 that when

SNR is large, the error performance is dominated by the term $\det\big((\mathbf{U},\hat{\mathbf{U}})^H(\mathbf{U},\hat{\mathbf{U}})\big)$. Hence, following the way similar to coherent MIMO communications [4], we define the coding gain for the unitary code as

$$G(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2)=\min_{\mathbf{U}\neq\hat{\mathbf{U}},\mathbf{U},\hat{\mathbf{U}}\in\mathcal{U}}\sqrt{\det\big((\mathbf{U},\hat{\mathbf{U}})^H(\mathbf{U},\hat{\mathbf{U}})\big)}. \tag{5.1}$$

Theoretically speaking, we should maximize the coding gain $G(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2)$ directly among all two UFCPs $\mathcal{Y}_1\sim\mathcal{X}$ and $\mathcal{Y}_2\sim\mathcal{X}$. However, this optimization problem, in general, is too difficult to be solved, since the optimal design of constellations is generally extremely difficult to be reformulated into a tractable optimization problem, even for an additive white Gaussian noise channel [78, 81–86]. To make the problem tractable, in this thesis, we restrict ourself to using the energy-efficient cross QAM constellations to generate the two UFCPs $\mathcal{Y}_1\sim\mathcal{X}$ and $\mathcal{Y}_2\sim\mathcal{X}$ with $\mathcal{X}\subseteq\{-1,-j,1,j\}$. Specifically, let $\mathcal{Z}_1$ and $\mathcal{Z}_2$ be two given 2^p-ary and 2^q-ary cross QAM constellations, respectively. Then, the three constellations $\mathcal{X},\mathcal{Y}_1$ and $\mathcal{Y}_2$ are selected in such a way that $\mathcal{Z}_1=\frac{\mathcal{Y}_1}{\mathcal{X}}$ and $\mathcal{Z}_2=\frac{\mathcal{Y}_2}{\mathcal{X}}$. In addition, it is not difficult to verify that if $\mathcal{Z}_1=\frac{\mathcal{Y}_1}{\mathcal{X}}$ and $\mathcal{Z}_2=\frac{\mathcal{Y}_2}{\mathcal{X}}$, then, $\alpha\mathcal{Z}_1=\frac{\alpha\mathcal{Y}_1}{\mathcal{X}}$ and $\alpha\mathcal{Z}_2=\frac{\alpha\mathcal{Y}_2}{\mathcal{X}}$ for any positive α. Therefore, a family of UFCP codes resulting from the cross QAM constellations and an energy scale α is characterized by

$$\mathcal{U}_\alpha(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2)=\left\{\mathbf{U}_\alpha=\frac{1}{\sqrt{|x|^2+\alpha^2|y_1|^2+\alpha^2|y_2|^2}}\begin{pmatrix}x & 0\\ 0 & x^*\\ \alpha y_1 & \alpha y_2\\ -\alpha y_2^* & \alpha y_1^*\end{pmatrix}:\ x\in\mathcal{X},y_1\in\mathcal{Y}_1,y_2\in\mathcal{Y}_2\right\} \tag{5.2}$$

By employing the code structure (5.2) and performing some algebraic manipulations, the expression (5.1) can be further simplified into

$$\begin{aligned} G_\alpha(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) &= \min_{(x,y_1,y_2)\neq(\hat{x},\hat{y}_1,\hat{y}_2),x,\hat{x}\in\mathcal{X},y_1,\hat{y}_1\in\mathcal{Y}_1,y_2,\hat{y}_2\in\mathcal{Y}_2} \frac{\alpha^2\left(|\frac{y_1}{x}-\frac{\hat{y}_1}{\hat{x}}|^2+|\frac{y_2}{x}-\frac{\hat{y}_2}{\hat{x}}|^2\right)}{(1+\alpha^2(|\frac{y_1}{x}|^2+|\frac{y_2}{x}|^2))(1+\alpha^2(|\frac{\hat{y}_1}{\hat{x}}|^2+|\frac{\hat{y}_2}{\hat{x}}|^2))} \\ &= \min_{(x,y_1,y_2)\neq(\hat{x},\hat{y}_1,\hat{y}_2),x,\hat{x}\in\mathcal{X},y_1,\hat{y}_1\in\mathcal{Y}_1,y_2,\hat{y}_2\in\mathcal{Y}_2} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2), \end{aligned} \tag{5.3}$$

where notation $G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2)$ is defined as

$$G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) = \frac{\alpha^2\left(|\frac{y_1}{x}-\frac{\hat{y}_1}{\hat{x}}|^2+|\frac{y_2}{x}-\frac{\hat{y}_2}{\hat{x}}|^2\right)}{(1+\alpha^2(|\frac{y_1}{x}|^2+|\frac{y_2}{x}|^2))(1+\alpha^2(|\frac{\hat{y}_1}{\hat{x}}|^2+|\frac{\hat{y}_2}{\hat{x}}|^2))}, \tag{5.4}$$

which is called a *coding gain function*. Our design problem is now formally stated as follows:

Problem 3 *Let $|\mathcal{U}_\alpha(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2)| = 2^r$ $(r \geq 4)$ be fixed. Find an energy scale α, three nonnegative integers δ, p and q satisfying a total transmission bits constraint: $p+q-\delta = r$, and the unique factorizations of a pair of the 2^p-ary and 2^q-ary cross QAM constellations $\mathcal{Z}_1$ and $\mathcal{Z}_2$, i.e., $\mathcal{Z}_1 = \mathcal{Y}_1/\mathcal{X}$ and $\mathcal{Z}_2 = \mathcal{Y}_2/\mathcal{X}$ with $\mathcal{X} \subseteq \{-1,-j,1,j\}$ and $|\mathcal{X}| = 2^\delta$, such that the coding gain $G_\alpha(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2)$ is maximized, i.e.,*

$$\{\widetilde{\alpha},\widetilde{\delta},\widetilde{p},\widetilde{q},\widetilde{\mathcal{X}},\widetilde{\mathcal{Y}}_1,\widetilde{\mathcal{Y}}_2\} = \arg\max_{p+q-\delta=r}\ \max_{\mathcal{Z}_1=\mathcal{Y}_1/\mathcal{X},\mathcal{Z}_2=\mathcal{Y}_2/\mathcal{X}}\ \max_{\alpha} G_\alpha(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2).$$

5.2 The Solution to Problem 3

In order to solve each individual optimization problem in Problem 3, we first introduce some notation for discussion simplicity. Recall that $\mathcal{Q}$ denotes the modified 2^K-ary

cross QAM defined in Definition 4. Let P denote one of its corner points with the largest energy E, and let P_1 and P_2 denote the two nearest neighbors of this corner point, with the respective energies $E_{\rm s}$ and $E_{\rm t}$, where $E_{\rm s} \geq E_{\rm t}$. For given positive integers u, v and w satisfying $u + v = w$ with $u \geq v$, let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ denote the respective modified 2^u-ary and 2^v-ary cross QAM constellations; Z_i denotes one of the corner point in $\mathcal{Q}_i$ with the largest energy E_i; Its two nearest neighbors are denoted by Z_{i1} and Z_{i2}, respectively, with energies being E_{i1} and E_{i2}, where $E_{i1} \geq E_{i2}$. Specifically, for a given positive integer $w \geq 4$, integers $\widetilde{u}$ and $\widetilde{v}$ are defined as follows:

$$\begin{cases} \widetilde{u} = \widetilde{v} = \frac{w}{2} & \text{if } w \text{ is even,} \\ \widetilde{u} = \frac{w+1}{2}, \widetilde{v} = \frac{w-1}{2} & \text{if } w \text{ is odd.} \end{cases} \tag{5.5}$$

Correspondingly, all notation $\widetilde{\mathcal{Q}}_i, \widetilde{E}_{i1}$ and $\widetilde{E}_{i2}$ are defined in the same way as $\mathcal{Q}_i, E_{i1}$ and E_{i2}. As will be seen shortly in the following discussions on the solution to Problem 3, the integers u, v and w are to be replaced by p, q and $r - \delta$, respectively, and thus, $\mathcal{Q}_i$ is to be regarded as $\mathcal{Z}_i$. Hence, the corresponding positive integers $\widetilde{p}$ and $\widetilde{q}$ and energy notation $\widetilde{E}_i^{(\delta)}, \widetilde{E}_{i1}^{(\delta)}$ and $\widetilde{E}_{i2}^{(\delta)}$ are used directly without the need of redefinitions. Some properties regrading these energies are collected as the following Lemma.

Lemma 2 *For the modified 2^K-ary cross QAM $\mathcal{Q}$, the following statements are true:*

1. *If $K = 3$, then, each corner point has only one nearest neighbor, $E = 10$ and $E_{\rm s} = 2$.*

2. *If K is even, then, $E = 2(2^{\frac{K}{2}} - 1)^2$ and $E_{\rm s} = E_{\rm t} = (2^{\frac{K}{2}} - 1)^2 + (2^{\frac{K}{2}} - 3)^2$.*

3. *If K is odd and greater than 3, then, $E = (2^{\frac{K-1}{2}} - 1)^2 + (3 \times 2^{\frac{K-3}{2}} - 1)^2$,*

$$E_{\mathrm{s}} = (2^{\frac{K-1}{2}} - 3)^2 + (3 \times 2^{\frac{K-3}{2}} - 1)^2 \textit{ and } E_{\mathrm{t}} = (2^{\frac{K-1}{2}} - 1)^2 + (3 \times 2^{\frac{K-3}{2}} - 3)^2.$$

Lemma 2 can be verified directly by the calculation and thus, its proof is omitted. Now, applying Lemma 2 to a pair of the QAM constellations $\mathcal{Q}_1$ and $\mathcal{Q}_2$ yields Lemma 3:

Lemma 3 *Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ denote the modified 2^u-ary and 2^v-ary QAM constellations, respectively, with $u \geq v \geq 2$. Then,*

$$E_2 + E_{11} \leq E_1 + E_{21}, \tag{5.6a}$$

$$E_2 + E_{12} \leq E_1 + E_{22}. \tag{5.6b}$$

The proof of Lemma 3 is provided in Appdendix A.2.

Lemma 4 *Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ denote the modified 2^u-ary and 2^v-ary QAM constellations, respectively, with $u \geq v \geq 2$. Then, the following four inequalities hold:*

$$E_1 + E_2 \geq \widetilde{E}_1 + \widetilde{E}_2, \tag{5.7a}$$

$$\sqrt{E_1 + E_{21}} + \sqrt{E_1 + E_{22}} \geq \sqrt{\widetilde{E}_1 + \widetilde{E}_{21}} + \sqrt{\widetilde{E}_1 + \widetilde{E}_{22}}, \tag{5.7b}$$

$$\sqrt{E_1 + E_2} + \sqrt{E_1 + E_{21}} \geq \sqrt{\widetilde{E}_1 + \widetilde{E}_2} + \sqrt{\widetilde{E}_1 + \widetilde{E}_{21}}, \tag{5.7c}$$

$$\sqrt{E_1 + E_{21}} + \sqrt{E_2 + E_{11}} \geq \sqrt{\widetilde{E}_1 + \widetilde{E}_{21}} + \sqrt{\widetilde{E}_2 + \widetilde{E}_{11}}. \tag{5.7d}$$

The proof of Lemma 4 is postponed to Appendix A.3. We also need the following lemma, whose proof is given in Appendix A.4.

Lemma 5 *Let $\widetilde{\mathcal{Q}}_1$ and $\widetilde{\mathcal{Q}}_2$ represent the modified $2^{\widetilde{u}}$-ary and $2^{\widetilde{v}}$-ary QAM constellations with $\widetilde{u}$ and $\widetilde{v}$ defined in* (5.5)*. Then,*

$$\widetilde{E}_1 + \widetilde{E}_{22} \leq \widetilde{E}_2 + \widetilde{E}_{11}, \quad \text{when } w \text{ is even,} \tag{5.8a}$$

$$\widetilde{E}_1 + \widetilde{E}_{22} \geq \widetilde{E}_2 + \widetilde{E}_{11}, \quad \text{when } w \text{ is odd.} \tag{5.8b}$$

Now, it is time to start solving Problem 3. Let us consider the following three cases where δ possibly occurs.

5.2.1 $\delta = 0$

In this case, the constellation $\mathcal{X}$ includes only one element, i.e., $\mathcal{X} = \{x\}$, where $x = \pm 1, \pm j$. Since $\mathbf{r} = \mathbf{U}\mathbf{h} + \boldsymbol{\xi}$ and matrix $\text{diag}(x^*\mathbf{I}_2, \mathbf{I}_2)$ is unitary, we have $\text{diag}(x^*\mathbf{I}_2, \mathbf{I}_2)\mathbf{r} = \text{diag}(x^*\mathbf{I}_2, \mathbf{I}_2)\mathbf{U}\mathbf{h} + \text{diag}(x^*\mathbf{I}_2, \mathbf{I}_2)\boldsymbol{\xi}$, with $\text{diag}(x^*\mathbf{I}_2, \mathbf{I}_2)\boldsymbol{\xi}$ having the same statistical property as $\boldsymbol{\xi}$ and

$$\text{diag}(x^*\mathbf{I}_2, \mathbf{I}_2)\mathbf{U}_\alpha = \frac{1}{\sqrt{1 + \alpha^2(|y_1|^2 + |y_2|^2)}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \alpha y_1 & \alpha y_2 \\ -\alpha y_2^* & \alpha y_1^* \end{pmatrix}. \tag{5.9}$$

Therefore, we only need to consider the case where $x = 1$. In this situation, $\mathcal{Z}_1 = \mathcal{Y}_1, \mathcal{Z}_2 = \mathcal{Y}_2$ and $G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2)$ is reduced to

$$G_\alpha(1, \mathbf{y}; 1, \hat{\mathbf{y}} | \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) = \frac{\alpha^2(|y_1 - \hat{y}_1|^2 + |y_2 - \hat{y}_2|^2)}{(1 + \alpha^2(|y_1|^2 + |y_2|^2))(1 + \alpha^2(|\hat{y}_1|^2 + |\hat{y}_2|^2))}. \tag{5.10}$$

Let us first consider a special case where $|\mathcal{Z}_2| = 4$. In this case, $|y_2| = |\hat{y}_2| = 2$ and hence,

$$G_\alpha(1, \mathbf{y}; 1, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) = \frac{\alpha^2(|y_1 - \hat{y}_1|^2 + |y_2 - \hat{y}_2|^2)}{(1 + \alpha^2(|y_1|^2 + 2))(1 + \alpha^2(|\hat{y}_1|^2 + 2))}. \tag{5.11}$$

It is very interesting to observe that for any fixed $\alpha, \mathcal{X}$ and $\mathcal{Y}_i$, the objection function $G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}})|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2)$ with respect to the variables $x, \hat{x}, \mathbf{y}$ and $\hat{\mathbf{y}}$ is minimized when its numerator achieves the minimum and simultaneously, its denominator achieves the maximum, both optimums being achieved when y_2 is the nearest neighbor of $\hat{y}_2$ and $y_1 = \hat{y}_1 = Z_1$ is the corner point with the largest energy E_1 in $\mathcal{Z}_1$. Therefore, the minimum in this case is given by

$$G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) = \min_{\mathbf{y} \neq \hat{\mathbf{y}}} G_\alpha(1, \mathbf{y}; 1, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) = 4\alpha/(1 + \alpha(2 + E_1))^2. \tag{5.12}$$

Now, we consider a general case where $|\mathcal{Z}_2| \geq 8$. In this case, notice that

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) = \min\{ & \min_{(|y_1|,|y_2|)=(|\hat{y}_1|,|\hat{y}_2|),\text{either } |y_1|=\sqrt{2} \text{ or } |y_2|=\sqrt{2}} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2), \\ & \min_{(|y_1|,|y_2|)=(|\hat{y}_1|,|\hat{y}_2|),|y_1|>\sqrt{2},|y_2|>\sqrt{2}} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2), \\ & \min_{(|y_1|,|y_2|)\neq(|\hat{y}_1|,|\hat{y}_2|)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2)\}. \end{aligned} \tag{5.13}$$

Realizing the following facts is key to obtaining the minimum of the objection function (5.10) with respect to variables $x, \hat{x}, \mathbf{y}$ and $\hat{\mathbf{y}}$:

(a) Under the conditions that $\mathbf{y} \neq \hat{\mathbf{y}}, (|y_1|, |y_2|) = (|\hat{y}_1|, |\hat{y}_2|)$ and either $|y_1| = \sqrt{2}$ or $|y_2| = \sqrt{2}$, the numerator of the objection function (5.10) is lower-bounded

by $4\alpha^2$, i.e.,

$$\alpha^2(|y_1 - \hat{y}_1|^2 + |y_2 - \hat{y}_2|^2) \geq 4\alpha^2, \tag{5.14a}$$

where the equality holds when either y_2 is the nearest neighbor of $\hat{y}_2$, i.e., $|y_2 - \hat{y}_2| = 2$, and $y_1 = \hat{y}_1$ or y_1 is the nearest neighbor of $\hat{y}_1$ and $y_2 = \hat{y}_2$. The denominator of the objection function (5.10) is upper-bounded by

$$(1 + \alpha^2(|y_1|^2 + |y_2|^2))(1 + \alpha^2(|\hat{y}_1|^2 + |\hat{y}_2|^2)) \leq (1 + \alpha^2(E_1 + 2))^2, \tag{5.14b}$$

where the equality holds when both y_1 and $\hat{y}_1$ are the corner points in $\mathcal{Z}_1$ with each having the largest energy E_1. Therefore, both equalities in (5.14a) and (5.14b) hold simultaneously when both y_1 and $\hat{y}_1$ are the corner points in $\mathcal{Z}_1$ with each having the largest energy E_1 and y_2 is the nearest neighbor of $\hat{y}_2$.

(b) Under the conditions that $(|y_1|, |y_2|) = (|\hat{y}_1|, |\hat{y}_2|), |y_1| > \sqrt{2}, |y_2| > \sqrt{2}$ and $\mathbf{y} \neq \hat{\mathbf{y}}$, the numerator of the objection function (5.10) is lower-bounded by

$$\alpha^2(|y_1 - \hat{y}_1|^2 + |y_2 - \hat{y}_2|^2) \geq \begin{cases} 8\alpha^2 & \text{if } |y_1| > E_{11} \text{ and } |y_2| > E_{21} \\ 4\alpha^2 & \text{if either } |y_1| \leq E_{11} \text{ or } |y_2| \leq E_{21} \end{cases} \tag{5.15a}$$

The denominator of the objection function (5.10) is upper-bounded by

$$\begin{aligned} &(1 + \alpha^2(|y_1|^2 + |y_2|^2))(1 + \alpha^2(|\hat{y}_1|^2 + |\hat{y}_2|^2)) \\ \leq &\begin{cases} (1 + \alpha^2(E_1 + E_2))^2 & \text{if } |y_1| > E_{11} \text{ and } |y_2| > E_{21} \\ (1 + \alpha^2(E_1 + E_{21}))^2 & \text{if either } |y_1| \leq E_{11} \text{ or } |y_2| \leq E_{21} \end{cases}. \end{aligned} \tag{5.15b}$$

(c) If $|\mathcal{Z}_1| \geq |\mathcal{Z}_2|$ and $(|y_1|, |y_2|) \neq (|\hat{y}_1|, |\hat{y}_2|)$, then, $E_1 \geq E_2$. Note that the numerator of the objection function (5.10) is lower-bounded by

$$\alpha^2(|y_1 - \hat{y}_1|^2 + |y_2 - \hat{y}_2|^2) \geq 4\alpha^2, \tag{5.16a}$$

where the equality holds when either y_2 is the nearest neighbor of $\hat{y}_2$ and $y_1 = \hat{y}_1$ or y_1 is the nearest neighbor of $\hat{y}_1$ and $y_2 = \hat{y}_2$. In addition, the denominator of the objection function (5.10) is upper-bounded by

$$(1 + \alpha^2(|y_1|^2 + |y_2|^2))(1 + \alpha^2(|\hat{y}_1|^2 + |\hat{y}_2|^2)) \leq (1 + \alpha^2(E_1 + E_2))(1 + \alpha^2(E_1 + E_{21})), \tag{5.16b}$$

where the equality holds when both y_1 and $\hat{y}_1$ are the corner points in $\mathcal{Z}_1$ with each having the largest energy E_1, while one of y_2 and $\hat{y}_2$ is the corner point in $\mathcal{Z}_2$ with the largest energy E_2, and the other is of the second largest energy E_{21}. In other words, the upper bound $(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_1+E_{21}))$ is the second largest maximum of the denominator of the objection function (5.10). Very interestingly, under this condition, both equalities in (5.16a) and (5.16b) are able to be achieved at the same time when $y_1 = \hat{y}_1$ is the corner point having the largest energy E_1 in $\mathcal{Z}_1$, y_2 is the nearest neighbor of $\hat{y}_2$ and of the largest energy E_2 and $\hat{y}_2$ has the second largest energy E_{21} in $\mathcal{Z}_2$.

The above three observations reveal that

$$\min_{(|y_1|,|y_2|)=(|\hat{y}_1|,|\hat{y}_2|),|y_1|=\sqrt{2}\,\text{or}\,|y_2|=\sqrt{2}} G_\alpha(1,\mathbf{y};1,\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) = \frac{4\alpha^2}{(1+\alpha^2(E_1+2))^2}, \tag{5.17a}$$

$$\min_{(|y_1|,|y_2|)=(|\hat{y}_1|,|\hat{y}_2|),|y_1|>\sqrt{2},|y_2|>\sqrt{2}} G_\alpha(1,\mathbf{y};1,\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) \geq \frac{4\alpha^2}{(1+\alpha^2(E_1+E_{21}))^2}, \tag{5.17b}$$

$$\min_{(|y_1|,|y_2|)\neq(|\hat{y}_1|,|\hat{y}_2|)} G_\alpha(1,\mathbf{y};1,\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) = \frac{4\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_1+E_{21}))}. \tag{5.17c}$$

When $|\mathcal{Z}_2| > 4$, $E_1 > E_{21} \geq 2$ and as a result, comparing (5.17a) with (5.17c) gives us

$$\frac{4\alpha^2}{(1+\alpha^2(E_1+2))^2} > \frac{4\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_1+E_{21}))}.$$

and thus, we have

$$\min_{(|y_1|,|y_2|)=(|\hat{y}_1|,|\hat{y}_2|),|y_1|=\sqrt{2}\,\text{or}\,|y_2|=\sqrt{2}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) > \min_{(|y_1|,|y_2|)\neq(|\hat{y}_1|,|\hat{y}_2|)} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2). \tag{5.18a}$$

In addition, since $E_2 > E_{21}$, we can obtain from (5.17b) and (5.17c) that

$$\begin{aligned} &\min_{(|y_1|,|y_2|)=(|\hat{y}_1|,|\hat{y}_2|),|y_1|>\sqrt{2},|y_2|>\sqrt{2}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) \\ &\quad > \min_{(|y_1|,|y_2|)\neq(|\hat{y}_1|,|\hat{y}_2|)} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2). \end{aligned} \tag{5.18b}$$

Combining (5.13) with (5.18) yields

$$G_\alpha(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) = \frac{4\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_1+E_{21}))}. \tag{5.19}$$

Since if $|\mathcal{Z}_2| = 4$, $E_2 = E_{21}$, the conclusion (5.19) includes (5.12) as a special case. Therefore, no matter whether or not $|\mathcal{Z}_2| > 4$, we always have (5.19). Notice that (5.19) can be rewritten as

$$\begin{aligned} G_\alpha(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) &= \frac{4}{(\alpha^{-1}+\alpha(E_1+E_2))(\alpha^{-1}+\alpha(E_1+E_{21}))} \\ &= \frac{4}{\alpha^{-2}+\alpha^2(E_1+E_2)(E_1+E_{21})+(2E_1+E_2+E_{21})} \quad (5.20a) \\ &\leq \frac{4}{2\sqrt{(E_1+E_2)(E_1+E_{21})}+(2E_1+E_2+E_{21})} \quad (5.20b) \\ &= \frac{4}{\left(\sqrt{E_1+E_2}+\sqrt{E_1+E_{21}}\right)^2}, \end{aligned}$$

where we have used the arithmetic mean and the geometric mean inequality from (5.20a) to (5.20b): $a+b \geq 2\sqrt{ab}$, and the equality holds when $\alpha = 1/\sqrt[4]{(E_1+E_2)(E_1+E_{21})}$.

Thus, we have

$$\begin{aligned}\max_{\alpha} G_{\alpha}(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) &= \frac{4}{\left(\sqrt{E_1+E_2}+\sqrt{E_1+E_{21}}\right)^2} \\ &\leq \frac{4}{\left(\sqrt{\widetilde{E}_1^{(0)}+\widetilde{E}_2^{(0)}}+\sqrt{\widetilde{E}_1^{(0)}+\widetilde{E}_{21}^{(0)}}\right)^2}, \end{aligned} \tag{5.21}$$

where we have used Lemma 4 with $w=r, u=p, v=q$ and $\mathcal{Q}_i=\mathcal{Z}_i$ and the inequality in (5.21) holds when $p=\widetilde{p}$ and $q=\widetilde{q}$. All the above discussions can be summarized as Property 1.

Property 1 *When $p \geq q$ and $\delta = 0$, the optimal solution to Problem 3 is given as follows:*

1. *If r is even, then, $\widetilde{p}=\widetilde{q}=r/2$.*

2. *If r is odd, then, $\widetilde{p}=(r+1)/2, \widetilde{q}=(r-1)/2$.*

Once the optimal $\widetilde{p}$ and $\widetilde{q}$ have been determined, then, $\widetilde{\mathcal{X}}^{(0)}=\{1\}$, $\widetilde{\mathcal{Y}}_1^{(0)}$ is the $2^{\widetilde{p}}$-ary QAM constellation $\widetilde{\mathcal{Z}}_1$, $\widetilde{\mathcal{Y}}_2^{(0)}$ is the $2^{\widetilde{q}}$-ary QAM constellation $\widetilde{\mathcal{Z}}_2$ and the optimal energy scale $\widetilde{\alpha}$ is determined by

$$\widetilde{\alpha}=\frac{1}{\sqrt[4]{(\widetilde{E}_1^{(0)}+\widetilde{E}_2^{(0)})(\widetilde{E}_1^{(0)}+\widetilde{E}_{21}^{(0)})}}. \tag{5.22}$$

Moreover, the optimal coding gain is given by

$$G(\widetilde{\mathcal{X}}^{(0)},\widetilde{\mathcal{Y}}_1^{(0)},\widetilde{\mathcal{Y}}_2^{(0)})=\frac{4}{\left(\sqrt{\widetilde{E}_1^{(0)}+\widetilde{E}_2^{(0)}}+\sqrt{\widetilde{E}_1^{(0)}+\widetilde{E}_{21}^{(0)}}\right)^2}. \tag{5.23}$$

In fact, Property 1 gives us an optimal design of the unitary training Alamouti code based on the cross QAM constellations.

5.2.2 $\delta = 1$

In this case, there are in total six possibilities in choosing the constellation $\mathcal{X}$, i.e., $\mathcal{X} = \{1, -1\}, \mathcal{X} = \{1, j\}, \mathcal{X} = \{1, -j\}, \mathcal{X} = \{-1, j\}, \mathcal{X} = \{-1, -j\}, \mathcal{X} = \{j, -j\}$. In order to attain the optimal solution, we take the following two steps.

Step 1: Determine $G_\alpha(\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) = \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)})$, where constellations $\mathcal{X}^{(1)}$ and $\mathcal{Y}_i^{(1)}$ are derived from Proposition 5 with $\mathcal{Z} = \mathcal{Z}_i$, i.e., $\mathcal{X}^{(1)} = \{1, j\}$ and $\mathcal{Y}_i^{(1)} = \mathcal{Y}_{i,\text{opt}}$. To do that, we first represent $G_\alpha(\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)})$ as

$$G_\alpha(\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) = \min\Big\{ \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T), x=\hat{x}} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}), \\ \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T), x\neq\hat{x}} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) \Big\}, \quad (5.24)$$

which leads us to individually considering the following two optimization problems.

(a) $x = \hat{x}$. In this case, the objection function in (5.3) is simplified into

$$G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) = \frac{\alpha^2(|y_1 - \hat{y}_1|^2 + |y_2 - \hat{y}_2|^2)}{(1 + \alpha^2(|y_1|^2 + |y_2|^2))(1 + \alpha^2(|\hat{y}_1|^2 + |\hat{y}_2|^2))}, \quad (5.25)$$

since $|x| = |\hat{x}| = 1$. Following the discussion very similar to the case when

$\delta = 0$, we can obtain

$$\min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T),x=\hat{x}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)})$$
$$= \begin{cases} \frac{8\alpha^2}{(1+\alpha^2(E_1+E_2))^2} & \text{if } q=5 \text{ or } q=2 \text{ or } q=4 \text{ and } p=5 \\ \frac{8\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_1+E_{21}))} & \text{if } q=3 \\ \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))^2} & \text{if } q \text{ is even and greater than 2 and } p\neq 5 \\ \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_{22}))} & \text{if } q \text{ is an odd integer exceeding 5} \end{cases}. \tag{5.26}$$

(b) $x \neq \hat{x}$. Under this condition, we further split the feasible domain of the optimization problem: $\min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T),x\neq\hat{x}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)})$, into four disjoint sub-domians as follows:

$$\mathcal{D}_{11} = \{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T) : x\neq\hat{x}, (|y_1|,|\hat{y}_1|) = (E_1,E_1), (|y_2|,|\hat{y}_2|) = (E_2,E_2)\},$$
$$\mathcal{D}_{12} = \{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T) : x\neq\hat{x}, (|y_1|,|\hat{y}_1|) = (E_1,E_1), (|y_2|,|\hat{y}_2|) \neq (E_2,E_2)\},$$
$$\mathcal{D}_{13} = \{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T) : x\neq\hat{x}, (|y_1|,|\hat{y}_1|) \neq (E_1,E_1), (|y_2|,|\hat{y}_2|) = (E_2,E_2)\},$$
$$\mathcal{D}_{14} = \{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T) : x\neq\hat{x}, (|y_1|,|\hat{y}_1|) \neq (E_1,E_1), (|y_2|,|\hat{y}_2|) \neq (E_2,E_2)\}.$$

Therefore, we have

$$\min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T),x\neq\hat{x}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)})$$
$$= \min_{1\leq k\leq 4} \min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{1k}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)}). \tag{5.27}$$

Now, let us first consider each inner minimization problem.

(a) When $(x, \mathbf{y}^T, \hat{x}, \hat{\mathbf{y}}^T) \in \mathcal{D}_{11} \cup \mathcal{D}_{12}$ and $|\mathcal{Z}_1| \geq 8$, $|\frac{y_1}{x} - \frac{\hat{y}_1}{\hat{x}}| > 4$ and as a result, the numerator of $G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)})$ is lower bounded by

$$\Big|\frac{y_1}{x} - \frac{\hat{y}_1}{\hat{x}}\Big|^2 + \Big|\frac{y_2}{x} - \frac{\hat{y}_2}{\hat{x}}\Big|^2 \geq 16\alpha^2. \tag{5.28}$$

Under the same condition, the denominator of $G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)})$ is upper bounded by

$$\Big(1 + |\frac{y_1}{x}|^2 + |\frac{y_2}{x}|^2\Big)\Big(1 + |\frac{\hat{y}_1}{\hat{x}}|^2 + |\frac{\hat{y}_2}{\hat{x}}|^2\Big) \leq (1 + \alpha^2(E_1 + E_2))^2. \tag{5.29}$$

Combining (5.28) with (5.29) results in

$$\min_{(x, \mathbf{y}^T, \hat{x}, \hat{\mathbf{y}}^T) \in \mathcal{D}_{11} \cup \mathcal{D}_{12}} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) \geq \frac{16\alpha^2}{(1 + \alpha^2(E_1 + E_2))^2}. \tag{5.30}$$

(b) When $(x, \mathbf{y}^T, \hat{x}, \hat{\mathbf{y}}^T) \in \mathcal{D}_{14}$, we first notice that the numerator of the objective is lower bounded by

$$\Big|\frac{y_1}{x} - \frac{\hat{y}_1}{\hat{x}}\Big|^2 + \Big|\frac{y_2}{x} - \frac{\hat{y}_2}{\hat{x}}\Big|^2 \geq 8\alpha^2, \tag{5.31}$$

since $\big|\frac{y_1}{x} - \frac{\hat{y}_1}{\hat{x}}\big|^2 \geq 4$ and $\big|\frac{y_2}{x} - \frac{\hat{y}_2}{\hat{x}}\big|^2 \geq 4$. In addition, the denominator of the objective is upper bounded by

$$\begin{aligned} &\Big(1 + |\frac{y_1}{x}|^2 + |\frac{y_2}{x}|^2\Big)\Big(1 + |\frac{\hat{y}_1}{\hat{x}}|^2 + |\frac{\hat{y}_2}{\hat{x}}|^2\Big) \\ &\leq (1 + \alpha^2(E_1 + E_{21}))(1 + \alpha^2(E_{11} + E_2)). \end{aligned} \tag{5.32}$$

Now, let us argue that both equalities can be achieved simultaneously. Since $x, \hat{x} \in \mathcal{X} = \{1, j\}$, without loss of generality, we can always assume that $x = 1$ and $\hat{x} = j$. Recall the definition and properties of the Group-x which we have discussed in Chapter 3. If we use $\mathcal{Z}_{i,1}$ and $\mathcal{Z}_{i,j}$ to denote two groups generated by $\mathcal{Y}_i \sim \mathcal{X}$ for $i = 1, 2$, then, we have $\mathcal{Z}_{i,1} \cup \mathcal{Z}_{i,j} = \mathcal{Z}_i$ and $\mathcal{Z}_{i,1} \cap \mathcal{Z}_{i,j} = \Phi$. Also, recall that notation Z_i denote one of corner points in $\mathcal{Z}_i$ with the largest energy E_i, and notation Z_{i1} and Z_{i2} denote its two nearest neighbors in $\mathcal{Z}_i$, i.e., $|Z_i - Z_{i1}| = |Z_i - Z_{i2}| = 2$, with the respective energies E_{i1} and E_{i2}. Then, $Z_{i1} \in \mathcal{Z}_{i,j}$ for $i = 1, 2$, since $\mathcal{Z}_{i,1} = \mathcal{Y}_i$ and $d_{\min}(\mathcal{Y}_i) > 2$. Hence, if we set $y_i = Z_i$ and $\hat{y}_i = jZ_{i1}$, then, both the equalities in (5.31) and (5.32) hold at the same time and thus,

$$\begin{aligned} &\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{14}} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_{11}+E_2))}. \end{aligned} \tag{5.33}$$

(c) When $(x, \mathbf{y}^T, \hat{x}, \hat{\mathbf{y}}^T) \in \mathcal{D}_{13}$, we need to consider two possibilities: $|\mathcal{Z}_2| = 4$ and $|\mathcal{Z}_2| \geq 8$. If $|\mathcal{Z}_2| \geq 8$, then, following the discussion similar to the Situation a), we can obtain

$$\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{13}} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) \geq \frac{16\alpha^2}{(1+\alpha^2(E_1+E_2))^2}. \tag{5.34}$$

If $|\mathcal{Z}_2| = 4$, then, $|y_2| = |\hat{y}_2| = 2$ and $|y_2/x - \hat{y}_2/\hat{x}| = 2$. Following the same discussion as the Situation b) and choosing $y_1 = Z_1, \hat{y}_1 = jZ_{11}$, we

can have

$$\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{13}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)}) = \frac{8\alpha^2}{(1+\alpha^2(E_1+2))(1+\alpha^2(E_{11}+2))}. \tag{5.35}$$

If we make the convention that $E_2 = E_{21} = 2$ when $\mathcal{Z}_2$ is the 4-QAM constellation, then, equation (5.33) includes (5.35) as a special case. To compare (5.30) with (5.33), we need to prove that the following inequality

$$3(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_{11}+E_2)) \geq (1+\alpha(E_1+E_2))^2, \tag{5.36}$$

is true for any positive α. To do that, we first establish an energy inequality:

$$3E_1E_{11} + 3E_1E_2 + 3E_{11}E_{21} + 3E_2E_{21} \geq (E_1+E_2)^2. \tag{5.37}$$

To show this, let us discuss the following four possibilities.

(a) $|\mathcal{Z}_1| = |\mathcal{Z}_2| = 8$. In this special case, it can be verified by calculation that $3E_1E_{11} + 3E_1E_2 + 3E_{11}E_{21} + 3E_2E_{21} = 432$ and $(E_1+E_2)^2 = 400$. Thus, the inequality (5.37) is true in this particular situation.

(b) $|\mathcal{Z}_2| = 4$. Since $3E_{11} + 4 \geq E_1$, we have

$$\begin{aligned} &3E_1E_{11} + 3E_1E_2 + 3E_{11}E_{21} + 3E_2E_{21} \\ &= E_1(3E_{11}+4) + 2(3E_{11}+4-E_1) + 4E_1 + 4 \\ &\geq E_1^2 + 2E_1E_2 + 4 = (E_1+E_2)^2. \end{aligned} \tag{5.38a}$$

(c) $|\mathcal{Z}_1| > |\mathcal{Z}_2| = 8$, In this case, note that $2E_{11} \geq E_1, E_1 > E_{11} \geq E_2$. Hence, we attain

$$\begin{aligned}
&3E_1E_{11} + 3E_1E_2 + 3E_{11}E_{21} + 3E_2E_{21} \\
&> 2E_1E_{11} + 2E_1E_2 + E_1E_{11} \\
&= E_1^2 + 2E_1E_2 + E_2^2 = (E_1 + E_2)^2. \qquad (5.38b)
\end{aligned}$$

(d) $|\mathcal{Z}_1| \geq |\mathcal{Z}_2| > 8$. Then, $2E_{11} \geq E_1$ and $2E_{21} > E_2$ and as a result,

$$\begin{aligned}
&3E_1E_{11} + 3E_1E_2 + 3E_{11}E_{21} + 3E_2E_{21} \\
&> 2E_1E_{11} + 2E_1E_2 + 2E_2E_{21} \\
&> E_1^2 + 2E_1E_2 + E_2^2 = (E_1 + E_2)^2. \qquad (5.38c)
\end{aligned}$$

Combining (5.38a), (5.38b) with (5.38c) gives us

$$\begin{aligned}
&3(1 + \alpha^2(E_1 + E_{21}))(1 + \alpha^2(E_{11} + E_2)) \\
&= 3 + 3(E_1 + E_2 + E_{11} + E_{21})\alpha^2 + (3E_1E_{11} + 3E_1E_2 + 3E_{11}E_{21} + 3E_2E_{21}))\alpha^4 \\
&\geq 1 + 2(E_1 + E_2)\alpha^2 + (E_1 + E_2)^2\alpha^4 \\
&= (1 + \alpha(E_1 + E_2))^2. \qquad (5.39)
\end{aligned}$$

Hence, the inequality (5.36) is true. Now, comparing (5.30) with (5.33) and

using (5.36) lead to

$$\frac{\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{11}\cup\mathcal{D}_{12}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)})}{\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{14}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)})} \geq \frac{2(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_{11}+E_2)}{(1+\alpha^2(E_1+E_2))^2} \geq 1, \tag{5.40}$$

if $|\mathcal{Z}_2| \geq 8$, which is equivalent to the fact that

$$\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{11}\cup\mathcal{D}_{12}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)}) \geq \min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{14}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)}). \tag{5.41}$$

Using the same argument, we can derive that

$$\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{14}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)}) \leq \min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T)\in\mathcal{D}_{13}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)}). \tag{5.42}$$

Combining (5.27) with (5.41) and (5.42) altogether tells us that

$$\min_{(x,\mathbf{y}^T,\hat{x},\hat{\mathbf{y}}^T),x\neq\hat{x}} G_\alpha(x,\mathbf{y};\hat{x},\hat{\mathbf{y}}|\mathcal{X}^{(1)},\mathcal{Y}_1^{(1)},\mathcal{Y}_2^{(1)}) = \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_{11}+E_2))}. \tag{5.43}$$

Substituting (5.26) and (5.43) into (5.24) yields

$$G_\alpha(\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}) = \begin{cases} \frac{8\alpha^2}{(1+\alpha^2(E_1+E_2))^2} & \text{if } p \geq q = 5 \text{ or } p = 5, q = 4, \\ \frac{8\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_1+E_{21}))} & \text{if } p \geq q = 3, \\ \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_{22}))} & \text{if } p > q, q \neq 3, 4, 5, \\ \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_{11}+E_2))} & \text{if } p = q \neq 3, 5 \end{cases}. \tag{5.44}$$

Step 2: Establish the achievable upper bound of the coding gain for any fixed UFCP, i.e.,

$$G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \leq G_\alpha(\mathcal{X}^{(1)}, \mathcal{Y}_1^{(1)}, \mathcal{Y}_2^{(1)}), \tag{5.45}$$

for any positive α. As we have mentioned before, when $\delta = 1$, there are totally six candidates regarding the constellation $\mathcal{X}$, i.e., $\mathcal{X} = \{1, -1\}, \mathcal{X} = \{1, j\}, \mathcal{X} = \{1, -j\}, \mathcal{X} = \{-1, j\}, \mathcal{X} = \{-1, -j\}, \mathcal{X} = \{j, -j\}$. Here we only consider the case where $\mathcal{X} = \{1, -1\}$, since the discussion for the other cases are very similar. Now, we examine the following possibilities:

Case 1: $q = 3$. In this case, since $\mathcal{Z}_2$ includes the 4-QAM constellation as a subset, there are two points y_{20} and $\hat{y}_{20}$ in $\mathcal{Y}_2$ such that $|y_{20} - \hat{y}_{20}| = 2$ and $|y_{20}| = |\hat{y}_{20}| = 2$ and thus,

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x, \mathbf{y}^T) \neq (\hat{x}, \hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha((1, Z_1, y_{20}; 1, Z_1, \hat{y}_{20}) | \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{4\alpha^2}{(1 + \alpha^2(E_1 + 2))(1 + \alpha^2(E_1 + 2))}. \end{aligned} \tag{5.46a}$$

Case 2: $q = 5$. There are totally 8 corner points in $\mathcal{Z}_2$ with the largest energy and $\mathcal{Y}_2$ includes four of them. If two of the four points, say y_{20} and $\hat{y}_{20}$, are in the same quadrant, i.e., $|y_{20} - \hat{y}_{20}| = 2\sqrt{2}$, then, we have

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha(1, Z_1, y_{20}; 1, Z_1, \hat{y}_{20}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_2))^2}. \end{aligned} \tag{5.46b}$$

Case 3: $p > q$ and $q \neq 3, 5$.

(a) $Z_{21} \in \mathcal{Y}_2$. Then, we have

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha((1, Z_1, Z_2; 1, Z_1, Z_{21})|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{4\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_2))}. \end{aligned} \tag{5.46c}$$

(b) $Z_{22} \in \mathcal{Y}_2$. Similarly, we can obtain

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha(1, Z_1, Z_2; 1, Z_1, Z_{22})|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{4\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_1+E_2))}. \end{aligned} \tag{5.46d}$$

(c) $Z_{21}, Z_{22} \notin \mathcal{Y}_2$. Then, $-Z_{21}, -Z_{22} \in \mathcal{Y}_2$ and as a consequence, we arrive at

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha((1, Z_1, -Z_{21}; 1, Z_1, -Z_{22})|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_{22}))}. \end{aligned} \tag{5.46e}$$

Case 4: $p = q$ and $q \neq 3, 5$. We consider the following possibilities:

(a) If either $Z_{11} \in \mathcal{Y}_1$ or $Z_{21} \in \mathcal{Y}_2$, then, following Case 3-(a), we can have

$$G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \leq \frac{4\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_2))}, \tag{5.46f}$$

where $E_1 = E_2$ and $E_{11} = E_{21}$.

(b) If either $Z_{12} \in \mathcal{Y}_1$ or $Z_{22} \in \mathcal{Y}_2$, then, similar to Case 3-(b), we can obtain

$$G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \leq \frac{4\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_1+E_2))}, \tag{5.46g}$$

where $E_1 = E_2$ and $E_{12} = E_{22}$.

(c) $Z_{11}, Z_{12} \notin \mathcal{Y}_1$ and $Z_{21}, Z_{22} \notin \mathcal{Y}_2$. Then, $-Z_{11}, -Z_{12} \in \mathcal{Y}_1, -Z_{21}, -Z_{22} \in \mathcal{Y}_2$ and as a result, we attain

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha((1, Z_1, -Z_{21}; -1, -Z_{11}, Z_2)|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_{11}))}. \end{aligned} \tag{5.46h}$$

Comparing (5.46) with (5.24) gives (5.45) as required. Now, using the geometrical and arithmetical mean inequality and then, applying Lemma 4 to (5.45) and (5.44) result in

$$G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \leq G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}), \tag{5.47}$$

where

$$G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) = \begin{cases} \frac{2}{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}} & \text{if } p \geq q = 5 \text{ or } p = 5, q = 4, \\ \frac{8}{\left(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}}+\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}}\right)^2} & \text{if } p \geq q = 3, \\ \frac{8}{\left(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}}+\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{22}^{(1)}}\right)^2} & \text{if } p > q, q \neq 3, 4, 5, \\ \frac{8}{\left(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}}+\sqrt{\widetilde{E}_{11}^{(1)}+\widetilde{E}_2^{(1)}}\right)^2} & \text{if } p = q \neq 3, 5 \end{cases} \tag{5.48}$$

All the above discussions can be concluded as Property 2:

Property 2 *When $\delta = 1$, one of the optimal solution to Problem 3 is that $\widetilde{\mathcal{X}}^{(1)} = \{1, j\}$ and that $\widetilde{p}, \widetilde{q}$ and $\widetilde{\mathcal{Y}}_i^{(1)}$ are determined as follows:*

1. *If r is even, then, $\widetilde{p} = (r+2)/2, \widetilde{q} = r/2$, $\widetilde{\mathcal{Y}}_i^{(1)} = \widetilde{\mathcal{Y}}_{i,\text{opt}}$ and*

$$\widetilde{\alpha} = \begin{cases} \frac{1}{\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}}} & \text{if } r = 10 \text{ or } r = 8, \\ \frac{1}{\sqrt[4]{(\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}))(\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)})}} & \text{if } r = 6, \\ \frac{1}{\sqrt[4]{(\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}))(\widetilde{E}_1^{(1)}+\widetilde{E}_{22}^{(1)})}} & \text{if } r \neq 6, 8, 10. \end{cases} \tag{5.49}$$

Furthermore, the optimal coding gain is given by

$$G_{\widetilde{\alpha}}(\widetilde{\mathcal{X}},\widetilde{\mathcal{Y}}_1,\widetilde{\mathcal{Y}}_2)=\begin{cases}\frac{2}{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}} & \text{if } r=10 \text{ or } r=8,\\ \frac{8}{(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}}+\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}})^2} & \text{if } r=6,\\ \frac{8}{(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}}+\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{22}^{(1)}})^2} & \text{if } r\neq 6,8,10.\end{cases} \tag{5.50}$$

2. *If r is odd, then, $\widetilde{p}=\widetilde{q}=(r+1)/2$, $\widetilde{\mathcal{Y}}_i^{(1)}=\widetilde{\mathcal{Y}}_{i,\text{opt}}$ and*

$$\widetilde{\alpha}=\begin{cases}\frac{1}{\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}}} & \text{if } r=9,\\ \frac{1}{\sqrt[4]{(\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}))(\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)})}} & \text{if } r=5,\\ \frac{1}{\sqrt[4]{(\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}))(\widetilde{E}_{11}^{(1)}+\widetilde{E}_2^{(1)})}} & \text{if } r\neq 5,9.\end{cases} \tag{5.51}$$

Furthermore, the optimal coding gain is given by

$$G_{\widetilde{\alpha}}(\widetilde{\mathcal{X}},\widetilde{\mathcal{Y}}_1,\widetilde{\mathcal{Y}}_2)=\begin{cases}\frac{2}{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}} & \text{if } r=9,\\ \frac{8}{(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}}+\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}})^2} & \text{if } r=5,\\ \frac{8}{(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}}+\sqrt{\widetilde{E}_{11}^{(1)}+\widetilde{E}_2^{(1)}})^2} & \text{if } r\neq 5,9.\end{cases} \tag{5.52}$$

Actually, Property 2 also suggests us that for $\delta=1$, the optimal UFCP designed by Proposition 5 is still optimal in the sense of maximizing the coding gain.

5.2.3 $\delta = 2$

In this case, $\mathcal{X}=\{1,-1,j,-j\}$. We examine the following possibilities:

(a) If either $Z_{11} \in \mathcal{Y}_1$ or $Z_{21} \in \mathcal{Y}_2$, then, we can have either

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T) \neq (\hat{x}, \hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}} | \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha(1, Z_1, Z_2; 1, Z_{11}, Z_2 | \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2), \\ &= \frac{4\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_{11}+E_2))}, \end{aligned} \tag{5.53a}$$

or

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &\leq G_\alpha(1, Z_1, Z_{21}; 1, Z_1, Z_2 | \mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2), \\ &= \frac{4\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_2))}. \end{aligned} \tag{5.53b}$$

(b) If either $Z_{12} \in \mathcal{Y}_1$ or $Z_{22} \in \mathcal{Y}_2$, then, similar to situation (a), we can obtain

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \leq \max\{ &\frac{4\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_{12}+E_2))}, \\ &\frac{4\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_1+E_2))}\} \\ = &\frac{4\alpha^2}{(1+\alpha^2(E_1+E_2))(1+\alpha^2(E_{12}+E_2))}, \end{aligned} \tag{5.53c}$$

since $E_{12} + E_2 \leq E_1 + E_{22}$ according to Lemma 3.

(c) If $Z_{11}, Z_{12} \notin \mathcal{Y}_1$ and $Z_{21}, Z_{22} \notin \mathcal{Y}_2$, then, $Z_{11}, Z_{12} \in \mathcal{Z}_{1,-1} \cup \mathcal{Z}_{1,j} \cup \mathcal{Z}_{1,-j}$ and $Z_{21}, Z_{22} \in \mathcal{Z}_{2,-1} \cup \mathcal{Z}_{2,j} \cup \mathcal{Z}_{2,-j}$. In this case, one of the following two possibilities must occur:

(a) If either $Z_{11}, Z_{12} \in \mathcal{Z}_{1,x_1}$ or $Z_{21}, Z_{22} \in \mathcal{Z}_{2,x_2}$, then, we have either

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha(1, Z_{11}, Z_2; 1, Z_{12}, Z_2|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2), \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_{11}+E_2))(1+\alpha^2(E_{12}+E_2))}, \end{aligned} \tag{5.53d}$$

or

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &\leq G_\alpha(1, Z_1, Z_{21}; 1, Z_1, Z_{22}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2), \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_{22}))}. \end{aligned} \tag{5.53e}$$

(b) If neither Z_{11}, Z_{12} nor Z_{21}, Z_{22} belong to the same group, then, by the pigeonhole principle, there exists an $x_0 \in \mathcal{X}$ such that one of the following four statements must be true:

i. $Z_{11} \in \mathcal{Z}_{1,x_0}$ and $Z_{21} \in \mathcal{Z}_{2,x_0}$. As a result, we attain

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &= \min_{(x,\mathbf{y}^T)\neq(\hat{x},\hat{\mathbf{y}}^T)} G_\alpha(x, \mathbf{y}; \hat{x}, \hat{\mathbf{y}}|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &\leq G_\alpha((1, Z_1, Z_{21}; x_0, Z_{11}, Z_2)|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_2+E_{11}))}. \end{aligned} \tag{5.53f}$$

ii. $Z_{12} \in \mathcal{Z}_{1,x_0}$ and $Z_{21} \in \mathcal{Z}_{2,x_0}$. Similarly, we can arrive at

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &\leq G_\alpha((1, Z_1, Z_{21}; x_0, Z_{12}, Z_2)|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_2+E_{12}))}. \end{aligned} \tag{5.53g}$$

iii. $Z_{11} \in \mathcal{Z}_{1,x_0}$ and $Z_{22} \in \mathcal{Z}_{2,x_0}$. Then,

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &\leq G_\alpha((1, Z_1, Z_{22}; x_0, Z_{11}, Z_2)|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_2+E_{11}))}. \end{aligned} \tag{5.53h}$$

iv. $Z_{12} \in \mathcal{Z}_{1,x_0}$ and $Z_{22} \in \mathcal{Z}_{2,x_0}$. Also, we can have

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) &\leq G_\alpha((1, Z_1, Z_{22}; x_0, Z_{12}, Z_2)|\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \\ &= \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_2+E_{12}))}. \end{aligned} \tag{5.53i}$$

Now, comparing (5.53) results in a common upper bound on $G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2)$ in Case 2 as follows:

$$\begin{aligned} G_\alpha(\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2) \leq \max \Big\{ & \frac{8\alpha^2}{(1+\alpha^2(E_{11}+E_2))(1+\alpha^2(E_{12}+E_2))}, \\ & \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{21}))(1+\alpha^2(E_1+E_{22}))}, \\ & \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_2+E_{12}))} \Big\} \\ = \max \Big\{ & \frac{8\alpha^2}{(1+\alpha^2(E_{11}+E_2))(1+\alpha^2(E_{12}+E_2))}, \\ & \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_2+E_{12}))} \Big\}, \end{aligned} \tag{5.54}$$

since $E_2 + E_{12} \leq E_1 + E_{21}$, $E_{12} + E_2 \leq E_1 + E_{22}$ and $E_2 + E_{11} \leq E_1 + E_{21}$ by Lemma 3. Following the same trick as the case when $\delta = 1$, using the geometrical and arithmetical mean inequality first and then, Lemma 4 arrive at the fact that

$$\begin{aligned} \frac{8\alpha^2}{(1+\alpha^2(E_{11}+E_2))(1+\alpha^2(E_{12}+E_2))} &\leq \frac{8}{\left(\sqrt{\widetilde{E}_1^{(2)}+\widetilde{E}_{22}^{(2)}}+\sqrt{\widetilde{E}_2^{(2)}+\widetilde{E}_{12}^{(2)}}\right)^2}, \\ \frac{8\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_2+E_{12}))} &\leq \frac{8}{\left(\sqrt{\widetilde{E}_{11}^{(2)}+\widetilde{E}_2^{(2)}}+\sqrt{\widetilde{E}_{12}^{(2)}+\widetilde{E}_2^{(2)}}\right)^2}. \end{aligned}$$

Therefore, it follows from this that

$$
\begin{aligned}
G(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) &= \max_{\alpha} G_{\alpha}(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) \\
\leq \max_{\alpha}\max &\left\{\frac{8\alpha^2}{(1+\alpha^2(E_{11}+E_2))(1+\alpha^2(E_{12}+E_2))}\right. \\
&\left.\frac{8\alpha^2}{(1+\alpha^2(E_1+E_{22}))(1+\alpha^2(E_2+E_{12}))}\right\} \\
&\leq \left\{\frac{8}{\left(\sqrt{\widetilde{E}_1^{(2)}+\widetilde{E}_{22}^{(2)}}+\sqrt{\widetilde{E}_2^{(2)}+\widetilde{E}_{12}^{(2)}}\right)^2},\right. \\
&\left.\frac{8}{\left(\sqrt{\widetilde{E}_{11}^{(2)}+\widetilde{E}_2^{(2)}}+\sqrt{\widetilde{E}_{12}^{(2)}+\widetilde{E}_2^{(2)}}\right)^2}\right\} \\
&= \begin{cases} \frac{8}{\left(\sqrt{\widetilde{E}_1^{(2)}+\widetilde{E}_{22}^{(2)}}+\sqrt{\widetilde{E}_2^{(2)}+\widetilde{E}_{12}^{(2)}}\right)^2}, & \text{if } r \text{ is even,} \\ \frac{8}{\left(\sqrt{\widetilde{E}_{11}^{(2)}+\widetilde{E}_2^{(2)}}+\sqrt{\widetilde{E}_{12}^{(2)}+\widetilde{E}_2^{(2)}}\right)^2}, & \text{if } r \text{ is odd,} \end{cases}
\end{aligned}
$$

where we have used Lemma 5 in the last step. All the above discussions can be conclude as the following property:

Property 3 *For given r and $\mathcal{X} = \{1, -1, j, -j\}$, we have*

$$
G(\mathcal{X},\mathcal{Y}_1,\mathcal{Y}_2) \leq \begin{cases} \frac{8}{\left(\sqrt{\widetilde{E}_1^{(2)}+\widetilde{E}_{22}^{(2)}}+\sqrt{\widetilde{E}_2^{(2)}+\widetilde{E}_{12}^{(2)}}\right)^2}, & \text{if } r \text{ is even,} \\ \frac{8}{\left(\sqrt{\widetilde{E}_{11}^{(2)}+\widetilde{E}_2^{(2)}}+\sqrt{\widetilde{E}_{12}^{(2)}+\widetilde{E}_2^{(2)}}\right)^2}, & \text{if } r \text{ is odd.} \end{cases} \tag{5.55}
$$

Properties 1, 2 and 3 lead us to giving the following theorem as one of the optimal solutions to Problem 3.

Bit Rate	$G_{\widetilde{\alpha}}(\widetilde{\mathcal{X}}, \widetilde{\mathcal{Y}}_1, \widetilde{\mathcal{Y}}_2)$	$\lvert\widetilde{\mathcal{X}}\rvert$	$\widetilde{\mathcal{Z}}_1, \widetilde{\mathcal{Z}}_2$	$\widetilde{\alpha}$
1	0.250	1	4-QAM, 4-QAM	0.5
1.25	0.127	2	8-QAM, 8-QAM	0.254
1.5	0.0839	2	8-QAM, 16-QAM	0.206
1.75	0.0614	2	16-QAM, 16-QAM	0.189
2	0.0385	2	16-QAM, 32-QAM	0.137
2.25	0.0294	2	32-QAM, 32-QAM	0.121
2.5	0.0156	1	32-QAM, 32-QAM	0.125
2.75	0.0116	2	64-QAM, 64-QAM	0.0762
3	0.00820	2	64-QAM, 128-QAM	0.0640
3.25	0.00633	2	128-QAM, 128-QAM	0.0563

Table 5.1: Maximum coding gains for different transmission bit rates using optimal designs

5.2.4 One Optimal Solution to Problem 3

Theorem 3 *One of the optimal solutions to Problem 3 is given as follows:*

1. *If $r = 4$, then, $\widetilde{\delta} = 0, \widetilde{p} = \widetilde{q} = 2, \widetilde{\mathcal{X}} = \{1\}, \widetilde{\mathcal{Y}}_1 = \widetilde{\mathcal{Y}}_2 = \mathcal{Z}_1 = \mathcal{Z}_2$ is the 4-QAM constellation and $\widetilde{\alpha} = 1/\sqrt{2}$. Moreover, the optimal coding gain is $G_{\widetilde{\alpha}}(\widetilde{\mathcal{X}}, \widetilde{\mathcal{Y}}_1, \widetilde{\mathcal{Y}}_2) = 1/4$.*

2. *If $r = 10$, then, $\widetilde{\delta} = 0, \widetilde{p} = \widetilde{q} = 5, \widetilde{\mathcal{X}} = \{1\}, \widetilde{\mathcal{Y}}_1 = \widetilde{\mathcal{Y}}_2 = \mathcal{Z}_1 = \mathcal{Z}_2$ is the 32-QAM constellation and $\widetilde{\alpha} = \frac{1}{2\sqrt[4]{255}}$. Moreover, the optimal coding gain is $G_{\widetilde{\alpha}}(\widetilde{\mathcal{X}}, \widetilde{\mathcal{Y}}_1, \widetilde{\mathcal{Y}}_2) = \frac{1}{(\sqrt{15}+\sqrt{17})^2}$.*

3. *If r is even, then, $\widetilde{p} = (r+2)/2, \widetilde{q} = r/2$, $\widetilde{\mathcal{Y}}_i = \widetilde{\mathcal{Y}}_{i,\text{opt}}$ and*

$$\widetilde{\alpha} = \begin{cases} \frac{1}{\sqrt[4]{(\widetilde{E}_1+\widetilde{E}_2))(\widetilde{E}_1+\widetilde{E}_{21})}} & \text{if } r = 6, \\ \frac{1}{\sqrt[4]{(\widetilde{E}_1+\widetilde{E}_{21}))(\widetilde{E}_1+\widetilde{E}_{22})}} & \text{if } r \neq 6, 10. \end{cases} \tag{5.56}$$

Furthermore, the optimal coding gain is given by

$$G_{\widetilde{\alpha}}(\widetilde{\mathcal{X}},\widetilde{\mathcal{Y}}_1,\widetilde{\mathcal{Y}}_2)=\begin{cases}\frac{8}{(\sqrt{\widetilde{E}_1+\widetilde{E}_2}+\sqrt{\widetilde{E}_1+\widetilde{E}_{21}})^2} & \text{if } r=6,\\ \frac{8}{(\sqrt{\widetilde{E}_1+\widetilde{E}_{21}}+\sqrt{\widetilde{E}_1+\widetilde{E}_{22}})^2} & \text{if } r\neq 6,10.\end{cases} \tag{5.57}$$

4. *If r is an odd integer exceeding 4, then, $\delta=1,\widetilde{p}=\widetilde{q}=(r+1)/2$, $\widetilde{\mathcal{Y}}_i=\widetilde{\mathcal{Y}}_{i,\text{opt}}$ and*

$$\widetilde{\alpha}=\begin{cases}\frac{1}{\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}}} & \text{if } r=9,\\ \frac{1}{\sqrt[4]{(\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}))(\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)})}} & \text{if } r=5,\\ \frac{1}{\sqrt[4]{(\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)})(\widetilde{E}_{11}^{(1)}+\widetilde{E}_2^{(1)})}} & \text{if } r\neq 5,9.\end{cases} \tag{5.58}$$

Furthermore, the optimal coding gain is given by

$$G_{\widetilde{\alpha}}(\widetilde{\mathcal{X}},\widetilde{\mathcal{Y}}_1,\widetilde{\mathcal{Y}}_2)=\begin{cases}\frac{2}{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}} & \text{if } r=9,\\ \frac{8}{\left(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_2^{(1)}}+\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}}\right)^2} & \text{if } r=5,\\ \frac{8}{\left(\sqrt{\widetilde{E}_1^{(1)}+\widetilde{E}_{21}^{(1)}}+\sqrt{\widetilde{E}_{11}^{(1)}+\widetilde{E}_2^{(1)}}\right)^2} & \text{if } r\neq 5,9.\end{cases} \tag{5.59}$$

The proof of Theorem 3 is given in Appendix A.5. The maximum coding gains using the optimal UFCPs determined by Theorem 3 are listed in Table 5.1 for various transmission bit rates, which is also shown in Fig. 5.1. Some observations on Theorem 3 are made as follows:

1. Theorem 3 tells us that the training scheme based on the Alamouti code using the 4-QAM and 32-QAM constellations is optimal when either one bit or 2.5

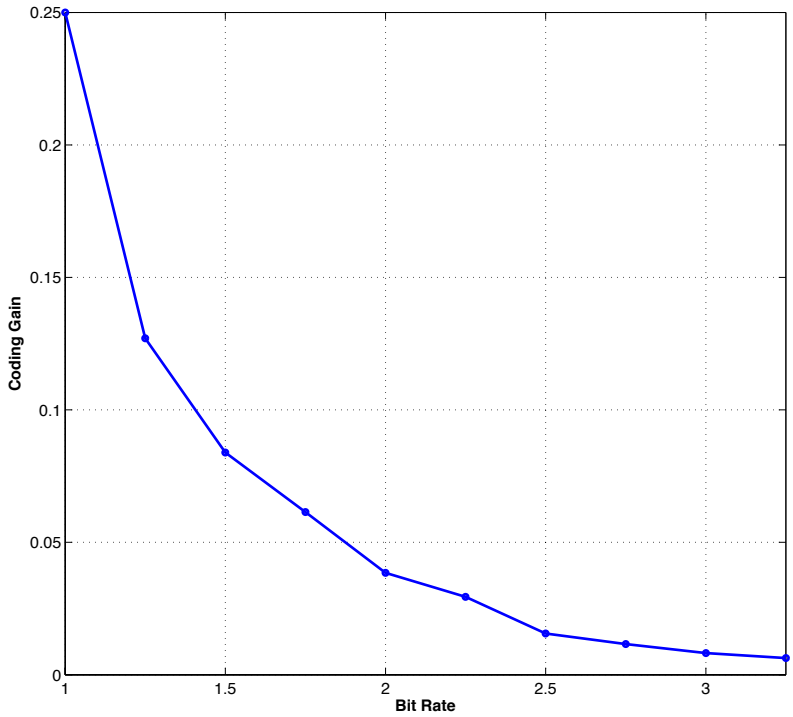


Figure 5.1: The optimal coding gains versus transmission bit rates

bits per channel use is transmitted.

2. In spite of the fact that from Proposition 5 we know that increasing the number of the groups is increasing the minimum Euclidian distance of the constellation $\mathcal{Y}$, the accumulated minimum Euclidian distance along the two transmitter antennas between two distinct groups is always equal to 8. In addition, increasing the number of groups is also increasing the size of the constellations and thus, increasing the energies of the three corner points. As a result, the UFCP code using four groups cannot enable the optimal coding gain.

Chapter 6

Unique Identification and Full Diversity for Alamouti-based Toeplitz Code

The main purpose of this chapter is to reveal and prove two important unique factorization propositions on the Alamouti codes. With these, we further show that the nonunitary and unitary Alamouti-based Toeplitz codes designed in Section 2.3 enable the unique identification of the channel and the transmitted signals in the noise-free case as well as full diversity for the GLRT receiver in the noisy case. To fulfill this goal, we make use of some fundamentals of Galois Theory and algebraic number theory.

6.1 Some Basic Definitions and Properties in Algebraic Theory

For completeness of the exposition, we start by briefly introducing some definitions and properties extracted from [87–90].

6.1.1 The Greatest Common Factor, The Least Common Multiple and Euler's Totient Function

Let us first introduce the following concept.

Definition 5 *Let m and n be two given rational integers. If there is a positive rational integer d such that d is a common factor of m and n, and any other common factor of m and n is a factor of d, then, such d is called the greatest common factor of m and n, denoted by* $\gcd(m, n)$.

Property 4 *Let m and n be two given rational integers. Then, there are two rational integers m_1 and n_1 such that*

$$\gcd(m, n) = m_1 m + n_1 n. \tag{6.1}$$

Definition 6 *Let m and n be two given rational integers. If there is a positive rational integer l such that l is a common multiple of m and n, and any other common multiple of m and n is a multiple of l, then, such l is called the least common multiple of m and n, denoted by* $\mathrm{lcm}(m, n)$.

Property 5 *Let m and n be two given rational integers. Then,*

$$\gcd(m,n)\mathrm{lcm}(m,n) = mn. \tag{6.2}$$

Definition 7 *The totient function $\phi(n)$, also called Euler's totient function, is defined as the number of positive rational integers less than or equal to n that are relatively prime to (i.e., do not contain any factor in common with) n, where 1 is counted as being relatively prime to all numbers.*

Since a number less than or equal to and relatively prime to a given number is called a totative, the totient function $\phi(n)$ can be simply defined as the number of totatives of n. For instance, there are eight totatives of 24 (1, 5, 7, 11, 13, 17, 19, and 23) and thus, $\phi(24) = 8$. The Euler's totient function has the following property.

Property 6 *Let m and n be two positive rational integers. Then, $\phi(m)\phi(n) = \phi(l)\phi(d)$, where l is the least common multiple and d is the greatest common divisor of m and n.*

6.1.2 Galois Theory

The main idea of Galois theory is to associate any polynomial $f(x)$ with a group of permutations of the roots of $f(x)$.

Definition 8 *$\mathbb{F}$ is a field if $\mathbb{F}$ is an Abelian group under addition, $\mathbb{F} - \{0\}$ is an Abelian group under multiplication and multiplication distributes over addition.*

If $\mathbb{F} \subseteq \mathbb{K}$ are fields, then, $\mathbb{K}$ is called a field extension of $\mathbb{F}$, which is denoted by $\mathbb{K}/\mathbb{F}$. Given a field extension $\mathbb{K}/\mathbb{F}$, then $\mathbb{K}$ can be considered as a vector space over $\mathbb{F}$. The dimension of this vector space is called the degree of the extension, and is denoted by $[\mathbb{K} : \mathbb{F}]$. If $[\mathbb{K} : \mathbb{F}] = \infty$, $\mathbb{K}$ is an infinite extension of $\mathbb{F}$. Otherwise, $\mathbb{K}$ is a finite extension.

Property 7 *Let $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ be fields. Then*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}]. \tag{6.3}$$

Let $\mathbb{K}$ be a field. A ring isomorphism from $\mathbb{K}$ to $\mathbb{K}$ itself is usually called an automorphism of $\mathbb{K}$.

Definition 9 *If $\mathbb{K}$ is a field extension of $\mathbb{K}$. An automorphism σ of $\mathbb{K}$ is called a $\mathbb{F}$-automorphism if $\sigma(x) = x$ for every x in $\mathbb{F}$. The Galois group Gal($\mathbb{K}/\mathbb{F}$) is the set of all $\mathbb{F}$-automorphisms of $\mathbb{K}$. If $|$Gal($\mathbb{K}/\mathbb{F}$)$| = [\mathbb{K} : \mathbb{F}] < \infty$, then $\mathbb{K}/\mathbb{F}$ is called Galois extension.*

Property 8 *Let $\mathbb{K}$ be a finite Galois extension of $\mathbb{F}$, and let $\mathbb{L}$ be an arbitrary extension of $\mathbb{F}$. Then, $[\mathbb{K}\mathbb{L} : \mathbb{L}] = [\mathbb{K} : \mathbb{K} \cap \mathbb{L}]$.*

To prove our results, we also need to define the norm of Galois extension.

Definition 10 *If $\mathbb{K}/\mathbb{F}$ is Galois with Galois group G, then for all $\kappa \in \mathbb{K}$, the norm of κ is defined as*

$$N_{\mathbb{K}/\mathbb{F}}(\kappa) = \prod_{\sigma \in G} \sigma(\kappa).$$

We can see that the norm of a Galois extension is nothing but the product of all $\mathbb{F}$-automorphisms in the Galois group of κ.

6.1.3 Cyclotomic Polynomials and Cyclotomic Extension

Consider a minimal field extension of $\mathbb{F}$ that contains all the roots of the polynomial. Given a field extension $\mathbb{L}/\mathbb{K}$ and a subset Ω of $\mathbb{L}$, $\mathbb{K}(\Omega)$ denotes the smallest subfield of $\mathbb{L}$ which contains $\mathbb{K}$ and Ω. If Ω consists of only one element ω, $\mathbb{K}(\omega)$ is a shorthand for $\mathbb{K}(\Omega)$. A field extension of the form $\mathbb{L} = \mathbb{K}(\omega)$ is called a simple extension and ω is called a primitive element of the extension.

Definition 11 *An n-th root of unity is a complex number z satisfying the equation $z^n - 1 = 0$, $n \in \mathbb{N}$, i.e. is a root of the polynomial $z^n - 1$.*

By the fundamental theorem of algebra, we know that the equation $z^n - 1 = 0$ has exactly n roots of unity all of which are located on the unit circle of the complex plane. In this way, they form vertices of an n sided regular polygon and thus are related to the theory of circle cutting or division, i.e. cyclotomy. An algebraic integer ζ is called an algebraic unit if it is a divisor of 1, i.e., if ζ^{-1} is an algebraic integer. All the nth roots of unity are algebraic units. The set of all n^{th} roots of unity forms a multiplicative cyclic group. The order or exponent of an nth root of unity z in $\mathbb{C}$ is the smallest positive integer m such that $z^m = 1$.

Definition 12 *An nth root of the unity is said to be a primitive n^{th} root of the unity if its order is n, i.e. z is a primitive n^{th} root of unity if $z^k \neq 1$ for $k = 1, 2, \cdots, n$.*

Let us now consider the field extension $\mathbb{F}(\omega)/\mathbb{F}$, where ω is an nth root of the unity.

Definition 13 *If $\omega \in \mathbb{C}$ with $\omega^n = 1$, then ω is an nth root of unity in $\mathbb{C}$, then the field extension $\mathbb{F}(\omega)/\mathbb{F}$ is called a cyclotomic extension.*

Particularly, if ω is a primitive nth root of unity in $\mathbb{C}$, then, $\mathbb{Q}(\omega)/\mathbb{Q}$ is called cyclotomic field, denoted by $\mathbb{Q}_n$.

Definition 14 *The nth cyclotomic polynomial $\Phi_n(x)$ is an integer-valued monic polynomial whose roots are the simple primitive n^{th} roots of the unity, i.e.,*

$$\Phi_n(x) = \prod_{k=1}^{\phi(n)} (x - x_k), \tag{6.4}$$

where x_k's are the primitive n^{th} roots of the unity.

Property 9 *Let n be any positive integer. Then, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

Property 9 tells us that $\Phi_n(x)$ is the minimal polynomial of ω over $\mathbb{Q}$. Hence, the degree of $\mathbb{Q}_n$ is $\phi(n)$, where $\phi(n)$ is the Euler's totient function. Particularly, the Galois group for the cyclotomic extension $\mathbb{Q}_n$ can be described by $\text{Gal}(\mathbb{Q}_n) = \{\sigma_i : \gcd(i, n) = 1\}$, where σ_i is determined by $\sigma_i(\omega) = \omega^i$.

Definition 15 *An algebraic integer is a complex number that is a root of some monic polynomial (leading coefficient 1) with coefficients in $\mathbb{Z}$.*

Specially for a primitive n-th root of unity ζ_n, we have the following property:

Property 10 *$\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of the cyclotomic field $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$.*

If κ is an algebraic integer of $\mathbb{Q}(\zeta_n)$, the norm of κ has the following property.

Property 11 *If $\kappa \in \mathbb{Z}[\zeta_n]$, then, $N_{\mathbb{Q}_n/\mathbb{Q}}(\kappa)$ is a rational integer.*

6.2 Two Kinds of Unique Factorizations for Alamouti Codes

First, we establish the following Lemma, a particular statement of which appears in [**?**]. For discussion self-containment, a proof for a more general case is provided in Appendix A.6.

Lemma 6 *Let two cyclotomic rings $\mathbb{Z}[\zeta_m]$ and $\mathbb{Z}[\zeta_n]$ be generated by the respective ζ_m and ζ_n. Then,*

$$\mathbb{Z}[\zeta_m] \cap \mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_d], \tag{6.5}$$

where $d = \gcd(m, n)$.

Now, it is time for us to develop two kinds of unique factorizations on the two Alamouti codes using Lemma 6. The proofs of these two propositions are postponed to Appendix A.7 and Appendix A.8.

Proposition 6 *For a pair of given coprime positive integers p and q, let the two Alamouti codes $\mathcal{A}_p$ and $\mathcal{A}_q$ be defined in* (2.6)*. If there exist four codeword matrices $\mathbf{A}_p, \hat{\mathbf{A}}_p \in \mathcal{A}_p$ and $\mathbf{A}_q, \hat{\mathbf{A}}_q \in \mathcal{A}_q$ such that $\mathbf{A}_p^{-1}\hat{\mathbf{A}}_p = \mathbf{A}_q^{-1}\hat{\mathbf{A}}_q$, then, $\mathbf{A}_p = \hat{\mathbf{A}}_p$ and $\mathbf{A}_q = \hat{\mathbf{A}}_q$.*

Proposition 6 tells us that the factorization of the two Alamouti codes $\mathcal{A}_p$ and $\mathcal{A}_q$ is unique in the sense of multiplication. Furthermore, the following proposition also tells us that such factorization is still unique for any shift within these two codes. In other words, the unique factorization of the two Alamouti codes $\mathcal{A}_p$ and $\mathcal{A}_q$ is shift-invariant.

Proposition 7 *For a pair of given coprime positive integers p and q, let the two Alamouti codes $\mathcal{A}_p$ and $\mathcal{A}_q$ be defined in* (2.6)*. If there exist six codeword matrices $\mathbf{A}_p, \widetilde{\mathbf{A}}_p, \bar{\mathbf{A}}_p \in \mathcal{A}_p$ and $\mathbf{A}_q, \widetilde{\mathbf{A}}_q, \bar{\mathbf{A}}_q \in \mathcal{A}_q$ such that $\mathbf{A}_p^{-1}(\bar{\mathbf{A}}_p - \widetilde{\mathbf{A}}_p) = \mathbf{A}_q^{-1}(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q)$, then, $\bar{\mathbf{A}}_p = \widetilde{\mathbf{A}}_p$ and $\bar{\mathbf{A}}_q = \widetilde{\mathbf{A}}_q$.*

Propositions 6 and 7 together play a key role in the unique identification of the channel and the transmitted signals as well as in the analysis of full diversity in this chapter.

6.3 Unique Identification

Our purpose in this section is to prove that the nonunitary and unitary Alamouti-based Toeplitz space-time block codes designed in Section 2.3 are capable of providing the unique identification of the channel coefficients and the transmitted symbols. To this end, let $\mathbf{u} = (\mathbf{u}_1^T, \mathbf{u}_2^T, \cdots, \mathbf{u}_{T/2}^T)^T$ and $\mathbf{v} = (\mathbf{v}_1^T, \mathbf{v}_2^T, \cdots, \mathbf{v}_{T/2}^T)^T$ be two corresponding block received signal vectors from (2.8) and (2.10) in the noise-free environment, i.e.,

$$\mathbf{u} = \mathbf{\Theta}\mathbf{h}, \tag{6.6a}$$

$$\mathbf{v} = \mathbf{\Phi}\mathbf{h}, \tag{6.6b}$$

where each of $\mathbf{u}_t = (u_{2t-1}, u_{2t})^T$ and $\mathbf{v}_t = (v_{2t-1}, v_{2t})^T$ for $t = 1, 2, \cdots, T/2$ is a 2×1 vector. Similarly, let $\mathbf{w}_{\mathrm{qr}}$ be the received signal vector from (2.13) in the noise-free case, i.e.,

$$\mathbf{w}_{\mathrm{qr}} = \mathbf{Q}_s\mathbf{h}. \tag{6.7}$$

Also, for discussion convenience, let $\mathbf{h} = (\mathbf{h}_1^T, \mathbf{h}_2^T, \cdots, \mathbf{h}_{M/2}^T)^T$ with $\mathbf{h}_n = (h_{2n-1}, h_{2n})^T$ for $n = 1, 2, \cdots, M/2$. Now, we are in a position to formally state the second main result of this thesis.

Theorem 4 *(Unique Identification) Given the two co-prime positive integers p and q, let $\mathbf{u}, \mathbf{v}$ and $\mathbf{w}_{\text{qr}}$ be given by the respective (6.6) and* (6.7)*. Then, the following two statements are true.*

1. *For any nonzero received signal vector $\mathbf{w} = (\mathbf{u}^T, \mathbf{v}^T)^T$, if we let r denote the maximum integer such that $\|\mathbf{u}_1\|\|\mathbf{v}_1\| = \|\mathbf{u}_2\|\|\mathbf{v}_2\| = \|\mathbf{u}_{r-1}\|\|\mathbf{v}_{r-1}\| = 0$, then, $\mathbf{h}_1 = \mathbf{h}_2 = ... = \mathbf{h}_{r-1} = 0$, and the other remaining channel coefficients $\mathbf{h}_r, \mathbf{h}_{r+1}, ..., \mathbf{h}_{M/2}$ and all the transmitted symbols in $\mathbf{\Theta}$ and $\mathbf{\Phi}$ can be uniquely determined.*

2. *For any nonzero received signal vector $\mathbf{w}_{\text{qr}}$, the channel vector $\mathbf{h}$ and the transmitted unitary codeword matrix $\mathbf{Q}_s$ can be uniquely determined.*

Proof: First, we prove Statement 1 of Theorem 4. The proof captures the following four steps.

Step 1. First, we consider the first two received signals in each of $\mathbf{u}$ and $\mathbf{v}$. In this case, we have

$$\begin{cases} \mathbf{u}_1 = \mathbf{\Theta}_1 \mathbf{h}_1, \\ \mathbf{v}_1 = \mathbf{\Phi}_1 \mathbf{h}_1. \end{cases} \tag{6.8}$$

Therefore, if $\|\mathbf{u}_1\|\|\mathbf{v}_1\| = 0$, then, either $\mathbf{u}_1$ or $\mathbf{v}_1$ is zero, and thus, we know from (6.8) that $\mathbf{h}_1$ is zero, since both $\mathbf{\Theta}$ and $\mathbf{\Phi}$ are invertible. Similarly, we can obtain $\mathbf{h}_2 = \cdots = \mathbf{h}_{r-1} = 0$.

Step 2. We continue to proceed the r-th two received signals in each of $\mathbf{u}$ and $\mathbf{v}$. In this case, we have received

$$\begin{cases} \mathbf{u}_r = \mathbf{\Theta}_1 \mathbf{h}_r, \\ \mathbf{v}_r = \mathbf{\Phi}_1 \mathbf{h}_r. \end{cases} \tag{6.9}$$

Since $\|\mathbf{u}_r\|\|\mathbf{v}_r\| \neq 0$, $\mathbf{u}_r = (u_{2r-1}, u_{2r})^T \neq \mathbf{0}$ and $\mathbf{v}_r = (v_{2r-1}, v_{2r})^T \neq \mathbf{0}$. Eliminating $\mathbf{h}_r$ from (6.9) gives us

$$\mathbf{\Theta}_1 \mathbf{\Phi}_1^{-1} \mathbf{v}_r = \mathbf{u}_r. \tag{6.10}$$

By taking advantage of the Alamouti code structure, (6.10) can be equivalently rewritten as

$$\mathbf{\Theta}_1 \mathbf{\Phi}_1^{-1} = \mathbf{W}_0 = \begin{pmatrix} w_{01} & w_{02} \\ -w_{02}^* & w_{01}^* \end{pmatrix},$$

where $w_{01} = \frac{u_{2r-1}v_{2r-1}^* + u_{2r}^* v_{2r}}{|v_{2r-1}|^2 + |v_{2r}|^2}$ and $w_{02} = \frac{u_{2r-1}v_{2r}^* - u_{2r}^* v_{2r-1}}{|v_{2r-1}|^2 + |v_{2r}|^2}$. Now, by Proposition 6, $\mathbf{\Theta}_1, \mathbf{\Phi}_1$ and thus, $\mathbf{h}_r$ can be uniquely determined.

Step 3. Now, we consider the next received signals for both blocks:

$$\begin{cases} \mathbf{u}_{r+1} = \mathbf{\Theta}_2 \mathbf{h}_r + \mathbf{\Theta}_1 \mathbf{h}_{r+1}, \\ \mathbf{v}_{r+1} = \mathbf{\Phi}_2 \mathbf{h}_r + \mathbf{\Phi}_1 \mathbf{h}_{r+1}. \end{cases} \tag{6.11}$$

Eliminating $\mathbf{h}_{r+1}$ from (6.11) results in

$$\mathbf{\Theta}_1^{-1}(\mathbf{u}_{r+1} - \mathbf{\Theta}_2 \mathbf{h}_r) = \mathbf{\Phi}_1^{-1}(\mathbf{v}_{r+1} - \mathbf{\Phi}_2 \mathbf{h}_r), \tag{6.12}$$

where $\mathbf{\Theta}_1, \mathbf{\Phi}_1$ and $\mathbf{h}_r$ are already known from Step 2. After some algebraic manipulations, (6.12) can be simplified into

$$(\mathbf{\Theta}_1^{-1}\mathbf{\Theta}_2 - \mathbf{\Phi}_1^{-1}\mathbf{\Phi}_2)\mathbf{h}_r = \mathbf{c}_1, \tag{6.13}$$

where $\mathbf{c}_1 = (c_{11}, c_{12})^T = \mathbf{\Theta}_1^{-1}\mathbf{u}_{r+1} - \mathbf{\Phi}_1^{-1}\mathbf{v}_{r+1}$. Again, by making use of the Alamouti code structure, (6.13) can be equivalently re-expressed by

$$\mathbf{\Theta}_1^{-1}\mathbf{\Theta}_2 - \mathbf{\Phi}_1^{-1}\mathbf{\Phi}_2 = \mathbf{W}_1, \tag{6.14}$$

where $\mathbf{W}_1$ is the Alamouti codeword matrix,

$$\mathbf{W}_1 = \begin{pmatrix} w_{11} & w_{12} \\ -w_{12}^* & w_{11}^* \end{pmatrix},$$

with $w_{11} = \frac{c_{11}h_{r1}^* + c_{12}^* h_{r2}}{|h_{r1}|^2 + |h_{r2}|^2}$ and $w_{12} = \frac{c_{11}^* h_{r2} + c_{12} h_{r1}^*}{|h_{r1}|^2 + |h_{r2}|^2}$. By Proposition 7, for the given $\mathbf{\Theta}_1, \mathbf{\Phi}_1$ and $\mathbf{W}_1$, the solution to (6.14) with respect to the variables $\mathbf{\Theta}_2$ and $\mathbf{\Phi}_2$ is unique.

In general, we proceed to consider determining the $(r+m-1)$-th channel coefficient for $1 < m \leq M/2 - r + 1$. In this case, we have received

$$\begin{cases} \mathbf{u}_{r+m-1} = \mathbf{\Theta}_1\mathbf{h}_{r+m-1} + \mathbf{\Theta}_2\mathbf{h}_{r+m-2} + ... + \mathbf{\Theta}_m\mathbf{h}_r, \\ \mathbf{v}_{r+m-1} = \mathbf{\Phi}_1\mathbf{h}_{r+m-1} + \mathbf{\Phi}_2\mathbf{h}_{r+m-2} + ... + \mathbf{\Phi}_m\mathbf{h}_r. \end{cases} \tag{6.15}$$

This is equivalent to

$$\begin{cases} \mathbf{u}_{r+m-1} - \sum_{i=1}^{m-2} \mathbf{h}_{r+i}\mathbf{\Theta}_{m-i} = \mathbf{\Theta}_1\mathbf{h}_{r+m-1} + \mathbf{\Theta}_m\mathbf{h}_r, \\ \mathbf{v}_{r+m-1} - \sum_{i=1}^{m-2} \mathbf{h}_{r+i}\mathbf{\Phi}_{m-i} = \mathbf{\Phi}_1\mathbf{h}_{r+m-1} + \mathbf{\Phi}_m\mathbf{h}_r. \end{cases} \tag{6.16}$$

Eliminating $\mathbf{h}_{r+m-1}$ yields

$$\begin{aligned}(\mathbf{\Theta}_1^{-1}\mathbf{\Theta}_m - \mathbf{\Phi}_1^{-1}\mathbf{\Phi}_m)\mathbf{h}_r &= \mathbf{\Theta}_1^{-1}(\mathbf{u}_{r+m-1} - \sum_{i=1}^{m-2}\mathbf{h}_{r+i}\mathbf{\Theta}_{m-i}) - \mathbf{\Phi}_1^{-1}(\mathbf{v}_{r+m-1} - \sum_{i=1}^{m-2}\mathbf{h}_{r+i}\mathbf{\Phi}_{m-i}) \\ &= \mathbf{c}_m = (c_{m1}, c_{m2})^T. \end{aligned} \tag{6.17}$$

Once more, by utilizing the Alamouti code structure, (6.17) can be rewritten as

$$\mathbf{\Theta}_1^{-1}\mathbf{\Theta}_m - \mathbf{\Phi}_1^{-1}\mathbf{\Phi}_m = \mathbf{W}_m, \tag{6.18}$$

$\mathbf{W}_m$ is also the Alamouti codeword matrix, i.e.,

$$\mathbf{W}_m = \begin{pmatrix} w_{m1} & w_{m2} \\ -w_{m2}^* & w_{m1}^* \end{pmatrix}$$

with $w_{m1} = \frac{c_{m1}h_{r1}^* + c_{m2}^* h_{r2}}{|h_{r1}|^2 + |h_{r2}|^2}$ and $w_{m2} = \frac{c_{m1}^* h_{r2} + c_{m2} h_{r1}^*}{|h_{r1}|^2 + |h_{r2}|^2}$. Again, by Proposition 7, $\mathbf{\Theta}_m$ and $\mathbf{\Phi}_m$, and thus $\mathbf{h}_{r+m-1}$ can be uniquely determined.

Step 4. $M/2 - r + 1 < m \leq L$. At this moment, notice that

$$\mathbf{\Theta}_{m-M/2+r}\mathbf{h}_{M/2} + \mathbf{\Theta}_{m-M/2+r+1}\mathbf{h}_{M/2-1} + \cdots + \mathbf{\Theta}_m\mathbf{h}_r = \mathbf{u}_{r+m-1}, \tag{6.19a}$$

$$\mathbf{\Phi}_{m-M/2+r}\mathbf{h}_{M/2} + \mathbf{\Phi}_{m-M/2+r+1}\mathbf{h}_{M/2-1} + \cdots + \mathbf{\Phi}_m\mathbf{h}_r = \mathbf{v}_{r+m-1}. \tag{6.19b}$$

Since the channel coefficients $\mathbf{h}_{r+\ell}$ and the transmitted codeword matrices $\mathbf{\Theta}_{m-\ell}, \mathbf{\Phi}_{m-\ell}$ for $\ell = 0, 1, 2, \cdots, M/2 - r$ have been all determined by the previous three steps, from (6.19), solving for $\mathbf{\Theta}_m$ and $\mathbf{\Phi}_m$, we can determine the other remaining transmitted signals from the remaining received signals uniquely due to the fact that $\mathbf{h}_r \neq \mathbf{0}$. This completes the proof of Statement 1 in Theorem 4.

Now, let us consider proving the Statement 2 of Theorem 4. Since $\mathbf{S}$ has full column rank, if we let its QR decomposition be $\mathbf{S} = \mathbf{Q}_s\mathbf{R}_s$ with $\mathbf{R}_s$ being an square upper triangular matrix and having the nongegative diagonal entries, then, $\mathbf{R}_s$ is invertible. Hence, $\mathbf{Q}_s = \mathbf{S}\mathbf{R}_s^{-1}$. Substituting this into (6.7) yields

$$\mathbf{w}_{\mathrm{qr}} = \mathbf{Q}_s\mathbf{h} = \mathbf{S}\mathbf{R}_s^{-1}\mathbf{h} = \mathbf{S}\widetilde{\mathbf{h}}, \tag{6.20}$$

where $\widetilde{\mathbf{h}} = \mathbf{R}_s^{-1}\mathbf{h}$. Using the Statement 1 that we have just proved, we know that for the given nonzero received vector $\mathbf{w}_{\mathrm{qr}}$, the solution to (6.20) with respect to variables $\mathbf{S}$ and $\widetilde{\mathbf{h}}$ is unique. Since the QR decomposition with the R-factor having positive diagonal entries is unique [91], for the given $\mathbf{S}$, there exists a unique pair of $\mathbf{Q}_s$ and $\mathbf{R}_s$ such that $\mathbf{S} = \mathbf{Q}_s\mathbf{R}_s$ and thus, $\mathbf{h}$ is uniquely determined by $\mathbf{h} = \mathbf{R}_s\widetilde{\mathbf{h}}$. This completes the proof of the Statement 2 and thus, Theorem 4. □

Some observations on Theorem 4 are made as follows:

1. Theorem 4 tells us that the channel coefficients can be uniquely identified by *only* transmitting two block signals with each symbol selected from two co-prime PSK constellations.

2. If we set $p = 2^m$ and $q = 2^m+1$ with m being a positive integer, then, p and q are coprime. Therefore, Theorems 4 holds for such a pair of p and q. In addition, if we want the original symbol sets $\mathcal{S}_p$ and $\mathcal{S}_q$ to contain the same integer bits, we can delete any one element, say $b_0 = \exp\left(\frac{2\pi j n_0}{q}\right)$ for some integer n_0 with $0 \leq n_0 \leq q-1$, from $\mathcal{S}_q$, i.e., $\overline{\mathcal{S}}_q = \mathcal{S}_q - \{b_0\}$. Thus, there are totally 2^m elements in the remaining set $\overline{\mathcal{S}}_q$ and Theorems 4 still holds for such a pair of constellations $\mathcal{S}_p$ and $\overline{\mathcal{S}}_q$.

3. It can be seen from the proof of Theorem 4 that it is the unique factorization Propositions 6 and 7 that assure that the nonunitary and unitary codes are able to allow the channel and the transmitted signal being identified uniquely.

6.4 Full Diversity

When the channel statistics of the fading and the noise is known at the receiver, the maximum likelihood criterion can be employed for noncoherent detection [92]. Under the assumptions made in Section 2.1, the noncoherent ML detector for our channel models (2.11) and (2.13) is to solve an optimization problem: $\hat{\mathbf{Z}} = \arg\min_{\mathbf{Z}}\{\Delta_z - \boldsymbol{\gamma}^H \boldsymbol{\Theta}_z \boldsymbol{\gamma}\}$, where $\boldsymbol{\Theta}_z = \frac{1}{\sigma^2}\mathbf{Z}\left(\sigma^2\mathbf{I} + \mathbf{Z}^H\mathbf{Z}\right)^{-1}\mathbf{Z}^H$ and $\Delta_z = \log\det\left(\sigma^2\mathbf{I} + \mathbf{Z}^H\mathbf{Z}\right)$ with $\boldsymbol{\gamma}$ and $\mathbf{Z}$ being equal to either $\boldsymbol{\gamma} = \mathbf{r}$ and $\mathbf{Z} = \mathbf{S}$ or $\boldsymbol{\gamma} = \mathbf{r}_{\mathrm{qr}}$ and $\mathbf{Z} = \mathbf{Q}_s$. The GLRT receiver requires neither the knowledge of the fading and noise statistics, nor the knowledge of their realizations [67, 71, 80]. The criterion can be simply stated as $\hat{\mathbf{Z}} = \arg\max_{\mathbf{Z}}\{\boldsymbol{\gamma}^H\mathbf{Z}\left(\mathbf{Z}^H\mathbf{Z}\right)^{-1}\mathbf{Z}^H\boldsymbol{\gamma}\}$. In general, the GLRT receiver provides a suboptimal solution. Now, suppose we use the GLRT receiver. In order to examine full diversity, for any pair of distinct codewords $\mathbf{Z}$ and $\widetilde{\mathbf{Z}}$, let

$$\begin{pmatrix} \mathbf{Z}^H \\ \widetilde{\mathbf{Z}}^H \end{pmatrix}\left(\mathbf{Z}, \widetilde{\mathbf{Z}}\right) = \mathbf{P}_{zz}. \tag{6.21}$$

Brehler and Varanasi [71] proved the following property.

Property 12 *If matrices $\mathbf{P}_{zz}$ have full rank for all pair of distinct codewords $\mathbf{Z}$ and $\widetilde{\mathbf{Z}}$, then, the code-book provides full diversity for the GLRT receiver.*

Now, it is time for us to formally state the second result in this thesis.

Theorem 5 *(Noncoherent full diversity) Let p and q be given the two co-prime positive integers. Then, both the nonunitary and unitary Alamouti-based Toeplitz space-time block codes $\mathcal{S}$ and $\mathcal{Q}_s$ enable full diversity for the GLRT receiver.*

PROOF: By Property 12, it suffices to prove that all the matrices $\mathbf{P}_{zz}$ have full rank for all pair of distinct codewords $\mathbf{Z}$ and $\widetilde{\mathbf{Z}}$. Notice that the fact that $\mathbf{P}_{zz}$ has full rank is equivalent the fact that $(\mathbf{Z}, \widetilde{\mathbf{Z}})$ has full column rank. Let us first consider the nonunitary code. In this case, $\mathbf{Z} = \mathbf{S}$. If there existed a pair of distinct codeword matrices $\mathbf{S}$ and $\widetilde{\mathbf{S}}$ such that the matrix $(\mathbf{S}, \widetilde{\mathbf{S}})$ does not have full column rank, the linear equations $\begin{pmatrix} \mathbf{S} & \widetilde{\mathbf{S}} \end{pmatrix} \begin{pmatrix} \mathbf{h} \\ -\widetilde{\mathbf{h}} \end{pmatrix} = \mathbf{0}$ with respect to variable vectors $\mathbf{h}$ and $-\widetilde{\mathbf{h}}$ would have a nonzero solution $\mathbf{h}_0$ and $\widetilde{\mathbf{h}}_0$. Then, we have $\mathbf{S}\mathbf{h}_0 = \widetilde{\mathbf{S}}\widetilde{\mathbf{h}}_0 = \mathbf{z}_0$. In other words, for a given nonzero received signal $\mathbf{z}_0$, equation $\mathbf{z}_0 = \mathbf{S}\mathbf{h}$ has two distinct pair of solutions. This contradicts with the result given by Theorem 4. Therefore, $(\mathbf{S}, \widetilde{\mathbf{S}})$ must have full column rank for any pair of distinct codeword matrices $\mathbf{S}$ and $\widetilde{\mathbf{S}}$. It can be verified that $\mathbf{A}$ has full rank is equivalent to the fact that matrix $(\mathbf{S}, \widetilde{\mathbf{S}})$ has full column rank. By Property 12, our nonunitary Alamouti-based Toeplitz space-time block code provides full diversity for the GLRT receiver.

Now, we consider the unitary case. Note that if we let $\mathbf{S} = \mathbf{Q}_s\mathbf{R}_s$ and $\widetilde{\mathbf{S}} = \mathbf{Q}_{\widetilde{s}}\mathbf{R}_{\widetilde{s}}$, then, we have

$$(\mathbf{S}, \widetilde{\mathbf{S}}) = (\mathbf{Q}_s, \mathbf{Q}_{\widetilde{s}}) \begin{pmatrix} \mathbf{R}_s & 0 \\ 0 & \mathbf{R}_{\widetilde{s}} \end{pmatrix}. \tag{6.22}$$

Using the statement which has been just proved in Theorem 5 for the nonunitary code, i.e., the matrix $(\mathbf{S}, \widetilde{\mathbf{S}})$ for any pair of distinct codewords $\mathbf{S}$ and $\widetilde{\mathbf{S}}$ has full column rank, $\mathrm{diag}(\mathbf{R}_s, \mathbf{R}_{\widetilde{s}})$ must be invertible and thus, $(\mathbf{Q}_s, \mathbf{Q}_{\widetilde{s}})$ has full column rank. Hence, our

unitary code also enables full diversity for the GLRT receiver. This completes the proof of Theorem 5. □

Here, we would like to emphasize an important fact observed from the proof of Theorem 5. By Property 12, we know that the key to assuring full diversity is to design the code $\mathcal{S}$ such that for all pair of distinct matrices $\mathbf{S}$ and $\widetilde{\mathbf{S}}$, $\mathbf{P}_{ss}$ always have full rank, whereas the examination of full rank is reduced to examine whether or not the solution to the equation, $\mathbf{r} = \mathbf{Sh}$, with respect to the variables $\mathbf{S}$ and $\mathbf{h}$ is unique for any given nozero $\mathbf{r}$. Therefore, combining this with Comments 3) of Theorem 4 tells us that the essential reason for the unique identification and full diversity roots from the unique factorization Propositions 6 and 7. In other words, it is Propositions 6 and 7 that enable $\mathbf{P}_{ss}$ to have full rank and thus, full diversity.

Chapter 7

Detection and Simulations

7.1 Detection and Simulations for Collaborative Unitary UFCP Code

In this section, we carry out computer simulations and compare the error performance of the collaborative unitary UFCP code design proposed in the thesis with those of other schemes in the literatures which can be used in a small noncoherent MISO system having two transmitter antennas and a single receiver antenna, where channel state information is completely unknown at both the transmitter and the receiver and the coherence time is $T = 2M = 4$. All the schemes that we would like to compare here are described as follows:

(a) *Differential unitary code based on Alamouti coding scheme and PSK constellations.* This design with the fast closed-form ML decoder was proposed in [57, 59]

and two unitary codeword matrices are $\mathbf{U}_1 = \mathbf{I}_2$ and

$$\mathbf{U}_2 = \frac{1}{\sqrt{2}} \times \begin{pmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix}, \tag{7.1}$$

where s_1 and s_2 are randomly, independently and equally likely chosen from the 2^{r_1}-ary and 2^{r_2}-ary phase shift keying (PSK) constellations, respectively, with the two integers a and b determined as follows:

$$\begin{cases} r_1 = r_2 = \frac{r}{2} & \text{if } r \text{ is even,} \\ r_1 = \frac{r+1}{2}, r_2 = \frac{r-1}{2} & \text{if } r \text{ is odd.} \end{cases} \tag{7.2}$$

For the necessity of performance comparison and decoding with the GLRT receiver, these two unitary matrices are normalized and then, stacked into one codeword matrix, which is denoted by $\mathbf{S}_a$,

$$\mathbf{S}_a = \frac{1}{\sqrt{2}} \times \begin{pmatrix} \mathbf{U}_1 \\ \mathbf{U}_2 \end{pmatrix}, \tag{7.3}$$

where the normalization constant assures $\mathrm{E}\big[\mathrm{tr}\big(\mathbf{S}_a^H \mathbf{S}_a\big)\big] = 2$.

(b) *SNR-efficient training Alamouti code.* This SNR-efficient training scheme using the Alamouti code was presented in [93]. The codeword matrices are characterized

by

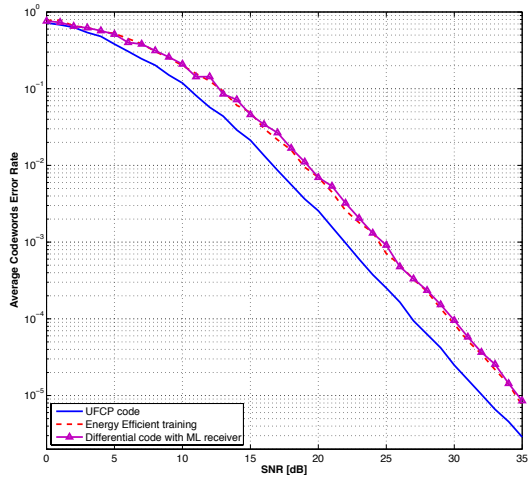
$$\mathbf{S}_b = \frac{1}{\sqrt{E_b}} \times \begin{pmatrix} \sqrt{E_b/2} & 0 \\ 0 & \sqrt{E_b/2} \\ s_1 & s_2 \\ -s_2^* & s_1^* \end{pmatrix}, \tag{7.4}$$

where s_1 and s_2 are randomly and equally likely chosen from either the 2^{r_1}-ary and 2^{r_2}-ary cross QAM constellations, respectively, with the determination of the two integers r_1 and r_2 being the same as (7.2). The energy constant E_b is normalized in such a way that $\mathrm{E}\big[\mathrm{tr}\big(\mathbf{S}_b^H \mathbf{S}_b\big)\big] = 2$. Here, the optimal average energy distribution over the training phase and communication phase is attained by maximizing the training efficiency [5, 43, 93].

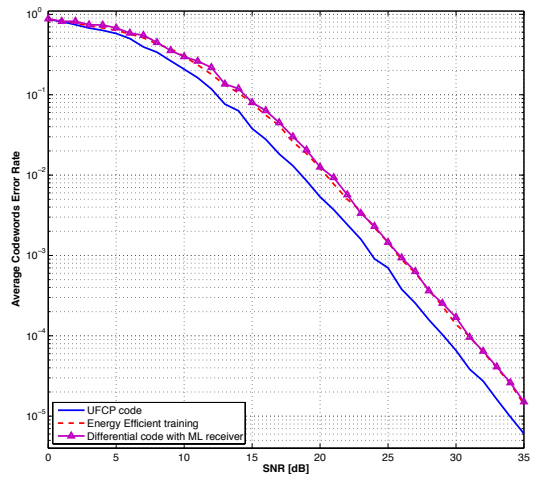
(c) *Optimal unitary UFCP code.* The code design is proposed in this thesis and the codeword matrix is of the form:

$$\mathbf{S}_b = \frac{1}{\sqrt{1 + \widetilde{\alpha}^2 |y_1|^2 + \widetilde{\alpha}^2 |y_2|^2}} \times \begin{pmatrix} x & 0 \\ 0 & x \\ \widetilde{\alpha} y_1 & \widetilde{\alpha} y_2 \\ -\widetilde{\alpha} y_2^* & \widetilde{\alpha} y_1^* \end{pmatrix}, \qquad x \in \widetilde{\mathcal{X}}, y_1 \in \widetilde{\mathcal{Y}}_1, y_2 \in \widetilde{\mathcal{Y}}_2, \tag{7.5}$$

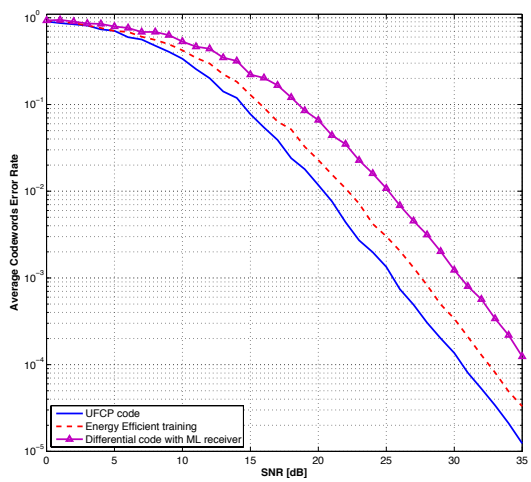
where the optimal energy scale $\widetilde{\alpha}$ and three constellations $\widetilde{\mathcal{X}}, \widetilde{\mathcal{Y}}_1$ and $\widetilde{\mathcal{Y}}_2$ are determined according to Theorem 3. It can be seen that the above three transmission schemes have the same spectrum efficiency, i.e., each transmission rate is $R_b = r/4$ bits per channel use. To make all error performance comparisons fair, we decode all the codes



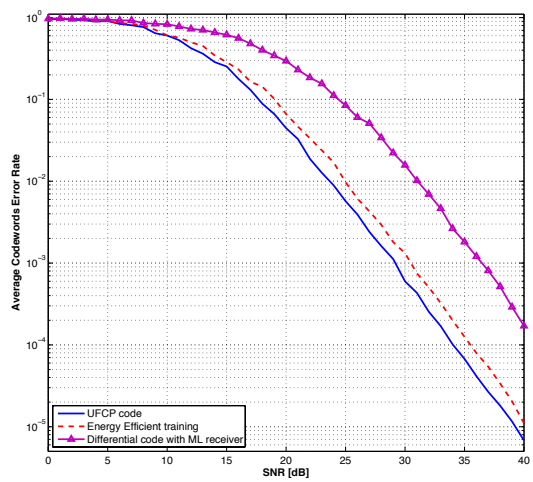
(a) $R_b = 1.25$ bits per channel use



(b) $R_b = 1.5$ bits per channel use



(c) $R_b = 1.75$ bits per channel use



(d) $R_b = 2.25$ bits per channel use

Figure 7.1: Performance comparison of unitary UFCP codes with currently available noncoherent codes

using the GLRT detector, i.e.,

$$\hat{\mathbf{S}} = \arg\max_{\mathbf{S}\in\mathcal{S}} \mathrm{Tr}\left(\boldsymbol{\Upsilon}^H \mathbf{S}\left(\mathbf{S}^H\mathbf{S}\right)^{-1}\mathbf{S}^H\boldsymbol{\Upsilon}\right).$$

All the average codeword error rates against SNR are shown Fig. 7.1. It is observed that the optimal collaborative unitary UFCP code designed in this thesis performs the best error performance among all the three coding schemes.

7.2 Detection and Simulations for Alamouti-based Toeplitz Code

In this section, we compare the nonunitary and unitary Alamouti-based Toeplitz space-time block code presented in this thesis with training scheme and differential codes by carrying out computer simulations.

Let us rewrite the channel model with the respective non-unitary and unitary codes as

$$\begin{aligned} \mathbf{r} &= \mathbf{S}\mathbf{h} + \boldsymbol{\xi}, \\ \mathbf{r}_{\mathrm{qr}} &= \mathbf{Q}_s\mathbf{h} + \boldsymbol{\xi}_{\mathrm{qr}}. \end{aligned}$$

As we have discussed in Section 6.4, the GLRT receiver for decoding codeword $\mathbf{S}$ given the received signal matrix $\mathbf{r}$ is essentially to solve the following optimization problem:

$$\hat{\mathbf{S}} = \arg\max_{\mathbf{S}\in\mathcal{S}} \mathrm{Tr}(\mathbf{r}^H\mathbf{S}(\mathbf{S}^H\mathbf{S})^{-1}\mathbf{S}^H\mathbf{r}). \tag{7.6}$$

In spite of the fact that the GLRT receiver, in general, is a suboptimal receiver, for decoding the unitary codeword $\mathbf{Q}_s$ given the received signal matrix $\mathbf{r}_{\mathrm{rq}}$, it is equivalent

to the noncoherent ML receiver, i.e.,

$$\mathbf{Q}_{\hat{s}} = \arg\max_{\mathbf{S}\in\mathcal{S}} \mathrm{Tr}(\mathbf{r}_{\mathrm{rq}}^H \mathbf{Q}_s \mathbf{Q}_s^H \mathbf{r}_{\mathrm{rq}}). \tag{7.7}$$

Since $\mathbf{S}(\mathbf{S}^H\mathbf{S})^{-1}\mathbf{S}^H = \mathbf{Q}_s\mathbf{R}_s((\mathbf{Q}_s\mathbf{R}_s)^H\mathbf{Q}_s\mathbf{R}_s)^{-1}(\mathbf{Q}_s\mathbf{R}_s)^H = \mathbf{Q}_s\mathbf{Q}_s^H$, the optimization problem (7.7) is equivalent to

$$\hat{\mathbf{S}} = \arg\max_{\mathbf{S}\in\mathcal{S}} \mathrm{Tr}(\mathbf{r}_{\mathrm{rq}}^H \mathbf{S}(\mathbf{S}^H\mathbf{S})^{-1}\mathbf{S}^H \mathbf{r}_{\mathrm{rq}}). \tag{7.8}$$

In other words, decoding the unitary codeword $\mathbf{Q}_s$ is equivalent to decoding the original non-unitary codeword $\mathbf{S}$. The only major difference between (7.6) and (7.8) is that in (7.6), the received signal matrix is $\mathbf{r}$, whereas in (7.8), the received signal matrix is $\mathbf{r}_{\mathrm{rq}}$. In addition, the decoding algorithm (7.8) is optimal for the ML receiver, whereas the algorithm (7.6) is suboptimal. Unfortunately, until now we have not found any decoding algorithm to efficiently implement (7.8).

We perform computer simulations to examine the error performance of the nonunitary and unitary Alamouti-based Toeplitz space-time block codes and compare them with the training scheme and the differential codes. In the simulation, we choose $T = 12$ and $M = 4$. In this case, the codeword matrix of the nonunitary code (2.7) and (2.9) takes the form of $\mathbf{S} = (\mathbf{X}^T, \mathbf{Y}^T)^T$, where

$$\mathbf{X} = \begin{pmatrix} \mathbf{X}_1 & 0 \\ \mathbf{X}_2 & \mathbf{X}_1 \\ 0 & \mathbf{X}_2 \end{pmatrix}, \quad \mathbf{Y} = \begin{pmatrix} \mathbf{Y}_1 & 0 \\ \mathbf{Y}_2 & \mathbf{Y}_1 \\ 0 & \mathbf{Y}_2 \end{pmatrix},$$

with each of $\mathbf{X}_i$ and $\mathbf{Y}_i$ for $i = 1, 2$ is the Alamouti codeword matrix, i.e.,

$$\mathbf{X}_1 = \begin{pmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{pmatrix}, \quad \mathbf{X}_2 = \begin{pmatrix} x_3 & x_4 \\ -x_4^* & x_3^* \end{pmatrix}, \tag{7.9}$$

$$\mathbf{Y}_1 = \begin{pmatrix} y_1 & y_2 \\ -y_2^* & y_1^* \end{pmatrix}, \quad \mathbf{Y}_2 = \begin{pmatrix} y_3 & y_4 \\ -y_4^* & y_3^* \end{pmatrix}. \tag{7.10}$$

Hence, the unitary codeword matrix is the Q-factor of the QR decomposition of $\mathbf{S}$ with positive diagonal entries. We select that x_ℓ and y_ℓ for $\ell = 1, 2, 3, 4$ are randomly, independently and equally likely from the respective 3-PSK and 4-PSK constellation so that the GLRT detector is possible to be implemented using an exhaust search. Therefore, the hybrid symbol rate of both the nonunitary and unitary codes is 2/3 symbols per channel use. The other two systems that we would like to compare are as follows:

(a) *SNR-efficient training scheme based on the orthogonal space-time block codes.* This SNR-efficient training scheme was reported in [93]. The codeword matrices are characterized by

$$\mathbf{Z}_a = \frac{1}{\sqrt{2+\sqrt{2}}} \times \begin{pmatrix} 2^{-\frac{3}{4}} \times \mathbf{I}_4 \\ \mathbf{Z}_{a1} \\ \mathbf{Z}_{a2} \end{pmatrix},$$

where

$$\mathbf{Z}_{a1} = \frac{1}{\sqrt{24}} \times \begin{pmatrix} z_{a1} & z_{a2} & z_{a3} & 0 \\ -z_{a2}^* & z_{a1}^* & 0 & -z_{a3} \\ -z_{a3}^* & 0 & z_{a1}^* & z_{a2} \\ 0 & z_{a3}^* & -z_{a2}^* & z_{a1} \end{pmatrix}, \quad \mathbf{Z}_{a2} = \frac{1}{\sqrt{88}} \times \begin{pmatrix} z_{a4} & z_{a5} & z_{a6} & 0 \\ -z_{a5}^* & z_{a4}^* & 0 & -z_{a6} \\ -z_{a6}^* & 0 & z_{a4}^* & z_{a5} \\ 0 & z_{a6}^* & -z_{a5}^* & z_{a4} \end{pmatrix}.$$

To make the same bit rate as our systems, we first form a 3-QAM constellation by deleting any one point from the standard 4-QAM and then, randomly, independently and equally likely choose $z_{a\ell}$ for $\ell = 1, 2, 3, 4$ from this 3-QAM constellation and $z_{a\ell}$ for $\ell = 5, 6$ from the 16-QAM constellation. Here, all the energy constants are normalized in such a way that the training efficiency of the average energy distribution over the training phase and communication phase is optimized [42, 43, 93]. The detector for the training system is the GLRT receiver.

(b) *Differential codes based on the orthogonal space-time block codes.* This design with the fast closed-form ML decoder was presented in [57, 59]. To make a fair comparison, three unitary codeword matrices are $\mathbf{Z}_{b1} = \mathbf{I}_4$,

$$\mathbf{Z}_{b2} = \frac{1}{\sqrt{3}} \times \begin{pmatrix} z_{b1} & z_{b2} & z_{b3} & 0 \\ -z_{b2}^* & z_{b1}^* & 0 & -z_{b3} \\ -z_{b3}^* & 0 & z_{b1}^* & z_{b2} \\ 0 & z_{b3}^* & -z_{b2}^* & z_{b1} \end{pmatrix}, \quad \mathbf{Z}_{b3} = \frac{1}{\sqrt{3}} \times \begin{pmatrix} z_{b4} & z_{b5} & z_{b6} & 0 \\ -z_{b5}^* & z_{b4}^* & 0 & -z_{b6} \\ -z_{b6}^* & 0 & z_{b4}^* & z_{b5} \\ 0 & z_{b6}^* & -z_{b5}^* & z_{b4} \end{pmatrix},$$

where $z_{b\ell}$ for $\ell = 1, 2, 3, 4$ and $z_{b\ell}$ for $\ell = 5, 6$ are randomly, independently and equally likely chosen from the 3-PSK and 16-PSK constellations, respectively. The detector for the system is the differential receiver [57, 59]. Despite the fact that the above four

systems have different symbol rates, the transmission bit rate is same, i.e., 1.195 bits per channel use. All simulation results are shown in Fig. 7.2. It can be observed

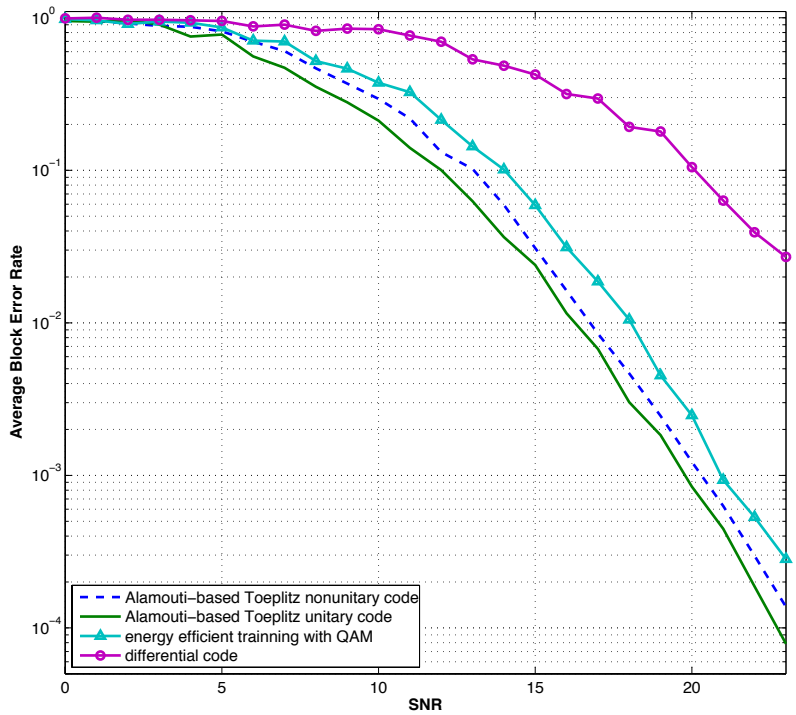


Figure 7.2: Error performance comparison of Alamouti-based Toeplitz codes with differential codes and training scheme

from Fig. 7.2 that both nonunitary and the unitary designs proposed in this thesis outperform the differential code and the training scheme. Specifically at an average codeword error rate of 10^{-3}, our new designs obtain a 2dB gain over the training schem and more than 10dB gain over the differential code. However, it should be pointed that the differential receiver is much simpler than the GLRT receiver.

Chapter 8

Conclusion and Discussions

In this thesis, we have considered a wireless communication system having even number of transmitter antennas and a single receiver antenna, in which the channel coefficients are assumed to be unknown at either the transmitter or the receiver, but remain constant for the first T time slots, after which they change to new independent values that are fixed for the next T time slots, and so on.

Particularly if the number of transmitter antennas is two, we have developed a novel concept called the uniquely factorable constellation pair for the systematic design of full diversity unitary space-time block code. By simply normalizing the two Alamouti codes and carefully selecting three constellations, a full diversity unitary code design with a symbol rate 3/4 has been attained. It has been shown that it is the unique factorization of constellation pairs that guarantees that the unique identification of both the channel coefficients and the transmitted signals in the noise-free case as well as full diversity in the noise case. In addition, to further enhance error performance, the optimal unitary UFCP code enabling the maximum coding gain has been designed from a pair of energy-efficient cross QAM constellations subject to a

bit rate constraint. After a careful examination of the fractional coding gain function, in this thesis we have taken two major steps maximizing the coding gain:

1. The energy scale has been carefully designed to compress the first three largest energy points of the QAM constellations in the denominator of the objective;

2. The two UFCPs have been designed so carefully that the one constellation collaborates with the other two constellations through the two transmitter antennas maximizing the minimum of the numerator and at the same time, avoiding the corner points with the largest energy as many as possible achieving the minimum.

In other words, the optimal coding gain has been obtained by constellations collaboration and energy compression. It is for this reason that we have also called the optimal UFCP code designed in this thesis as the *energy-efficient collaborative UFCP code*. Computer simulations have demonstrated that error performance of the optimal unitary UFCP code presented in this thesis outperforms those of the differential code and the SNR-efficient training code, which, to the best knowledge of the authors, is the best code in current literatures for the system.

For arbitrary even number of transmitter antennas system, we have considered the systematic design of noncoherent nonunitary space-time block codes by taking advantage of the Alamouti code and Toeplitz matrix structure. After that, the unitary Alamouti-based Toeplitz space-time block code has been immediately obtained by just applying the QR decomposition to the nonunitary code. Using the fundamentals of Galois theory and algebraic number theory, we have revealed and rigorously proved two important unique factorization properties on the two Alamouti codes: (a)

The multiplication of any two codeword matrices from the one code is uniquely distinguishable from the other (the uniqueness of factorization itself); (b) *The multiplication of any codeword matrix and the difference between any two codeword matrices from the one code is uniquely distinguishable from the other (the shift-invariant uniqueness of factorization).* In addition, we have further shown that it is these two kinds of the unique factorizations that allow both the channel coefficients and the transmitted signals being able to be identified uniquely by only processing two block received signals as well as noncoherent full diversity achieved with the GLRT receiver. Simulations have demonstrated that the error performance of the nonunitary and unitary codes with the GLRT decoder in this thesis are substantially superior to those of the differential codes and the signal-to-noise-ratio (SNR)-efficient training scheme based on the coherent orthogonal space-time block codes in literature.

As we have seen, the concept of the UFCP plays an important role in the systematic design of nonunitary and unitary space-time block codes for the MIMO system having even transmitter antennas and a single receiver antenna. However, some constructions and properties on the UFCP and the related transmission scheme which have been reported in this thesis are just initiative. Some significant issues still remain unsolved:

1. The construction of the optimal UFCPs for the design of the unitary space-time block code has been derived from the cross QAM constellations. How about the hexagonal constellations? since the hexagonal constellations carved from the Eisenstein integer ring are supposed to be more energy-efficient than the QAM constellations carved from the Gaussian integer ring [84]. Generally, which constellation is optimal to generate a unitary UFCP space-time block

code with the optimal coding gain?

2. So far we have not found any efficient decoding algorithm for the nonunitary and unitary Alamouti-based Toeplitz codes with the GLRT receiver. How to utilize the Toeplitz structure of the non-unitary code design and the simple structure of the unitary code design based on the QR decomposition for decoding is still under our investigation. In addition, it is known that the PSK constellation is not as energy-efficient as the QAM constellation. Hence, a natural question is: how to construct a pair of constellations from the QAM constellation instead of a pair of coprime PSK constellations such that the resulting two Alamouti codes still possess the two unique factorizations.

3. If an answer to the previous question is positive, then, a further question arises from the following observation: as we have known, the coding scheme for the basic 2-by-2 block which has been adopted in this thesis is the Alamouti scheme. In spite of the fact that the Alamouti code is optimal in many senses for such coherent system, it is not optimal anymore for such noncoherent system, since it was proved that unitary codes are optimal for general noncoherent MIMO communications, whereas the Alamouti code resulting from the QAM constellation is not unitary in general. Only when the constellation is the PSK, the resulting Alamouti code is unitary. However, the PSK constellation is not as energy-efficient as the QAM constellation. In addition, although this thesis has proposed a simple method for the design of the unitary code jusy by normalizing the two Alamouti codes, a deep insight into the fractional coding gain function exposures the drawback of the Alamouti scheme in the nocoherent case, i.e., too large energies are contributed to the denominator. Hence, a question is: is

it possible to find another coding scheme that has the same minimum of the numerator but a smaller maximum of the denominator as the Alamouti scheme?

Appendix A

Appendix

A.1 Proof of Proposition 5

We consider the following two cases: **Case 1**: $|\mathcal{X}| = 2$, i.e., there are only two elements in $\mathcal{X}$. Let $\mathcal{X} = \{x_1, x_2\}$, where $x_1, x_2 \in \{1, -1, -j, j\}$. By Proposition 5, we have $\mathcal{Z} = \mathcal{Z}_{x_1} \cup \mathcal{Z}_{x_2}$ with $\mathcal{Z}_{x_1} \cap \mathcal{Z}_{x_2} = \Phi$. In fact, $\mathcal{Z}_{x_1} = x_1^*\mathcal{Y} = x_2^*\mathcal{Y}$ and thus, $d_{\min}(\mathcal{Z}_{x_1}) = d_{\min}(\mathcal{Z}_{x_2}) = d_{\min}(\mathcal{Y})$. Let P be one of the corner point in $\mathcal{Z}$ with the largest energy. Without loss of generality, we can always assume $P \in \mathcal{Z}_{x_1}$. The following three possibilities need to be considered seperately.

1. $K = 3$. In this case, let P_1 is the first nearest neighbor of P, i.e., $|P - P_1| = 2$, and P_2 is the second nearest neighbor of P, i.e, $|P - P_2| = 2\sqrt{2}$. If $P_1 \in \mathcal{Z}_{x_1}$, then, $d_{\min}(\mathcal{Y}) = d_{\min}(\mathcal{Z}_{x_1}) \leq |P - P_1| \leq 2$; If $P_2 \in \mathcal{Z}_{x_1}$, then, $d_{\min}(\mathcal{Y}) = d_{\min}(\mathcal{Z}_{x_1}) \leq |P - P_2| \leq 2\sqrt{2}$; Otherwise, both P_1 and P_2 must lie in $\mathcal{Z}_{x_2}$ and as a result, $d_{\min}(\mathcal{Y}) = d_{\min}(\mathcal{Z}_{x_2}) \leq |P_1 - P_2| = 2\sqrt{2}$. At any rate, the minimum

distance of $\mathcal{Y}$ is upper-bounded by

$$d_{\min}(\mathcal{Y}) \leq 2\sqrt{2}. \tag{A.1}$$

On the other hand, it can be verified directly by calculation that the constellation given by (3.9) satisfies three conditions: (a) $|\mathcal{Y}_{\text{opt}}^{(1)}| = 4$; (b) $d_{\min}(\mathcal{Y}_{\text{opt}}^{(1)}) = 2\sqrt{2}$; (c) $\mathcal{Y}_{\text{opt}}^{(1)}$ and $\mathcal{X}_{\text{opt}}^{(1)}$ indeed form a UFCP. Therefore, $\mathcal{Y}_{\text{opt}}^{(1)}$ is optimal.

2. $K = 5$. In this case, P has the two nearest neighbors, which are denoted by P_1 and P_2, i.e., $|P - P_1| = |P - P_2| = 2$. If one of P_1 and P_2, say, P_1, belongs to the Group-x_1, $\mathcal{Z}_{x_1}$, then, $d_{\min}(\mathcal{Y}) = d_{\min}(\mathcal{Z}_{x_1}) \leq |P - P_1| = 2$. Otherwise, both P_1 and P_2 must lie in $\mathcal{Z}_{x_2}$ and as a result, $d_{\min}(\mathcal{Y}) = d_{\min}(\mathcal{Z}_{x_2}) \leq |P_1 - P_2| = 2\sqrt{2}$. Hence, the minimum distance of $\mathcal{Y}$ is always upper-bounded by

$$d_{\min}(\mathcal{Y}) \leq 2\sqrt{2}. \tag{A.2}$$

Now, following the argument similar to the Possibility 1) of $K = 3$, we can say that the constellation $\mathcal{Y}_{\text{opt}}^{(1)}$ given by (3.10) is indeed optimal.

3. $K \geq 4$ is even. Similar to the possibility of $K = 5$, we can prove $d_{\min}(\mathcal{Y}) \leq 2\sqrt{2}$. In addition, notice that the constellation determined by (3.11) has two properties: (a) $|\mathcal{Y}_{\text{opt}}^{(1)}| = 2^K$; (b) $y_1 - y_2 = 2(1-j)z$ for any two distinct points y_1 and y_2 in $\mathcal{Y}_{\text{opt}}^{(1)}$, where z is some complex integer. As a consequence, $d_{\min}(\mathcal{Y}) = 2\sqrt{2}$. Let us now check whether or not such a pair of $\mathcal{X}_{\text{opt}}^{(1)}$ and $\mathcal{Y}_{\text{opt}}^{(1)}$ constitutes a UFCP. Suppose that there exist $x, \widetilde{x} \in \mathcal{X}$ and $y, \widetilde{y} \in \mathcal{Y}$ such that $x\widetilde{y} = \widetilde{x}y$, then, $(\widetilde{y} - y)x = (\widetilde{x} - x)y$. If $x = \widetilde{x}$, then, $y = \widetilde{y}$, since $x \neq 0$. If $x \neq \widetilde{x}$, then,

$x - \widetilde{x} = \pm(1-j)$. Combining this with the fact $(\widetilde{y} - y) = 2(1-j)z$, we have $2z = \pm y$, which is impossible. Thus, $x = \widetilde{x}$ and $y = \widetilde{y}$. In other words, a pair of the constellations $\mathcal{X}_{\text{opt}}^{(1)}$ and $\mathcal{Y}_{\text{opt}}^{(1)}$ constitutes a UFCP. Therefore, in this case, $\mathcal{Y}_{\text{opt}}^{(1)}$ is optimal.

4. $K > 5$ is odd. Following almost the same discussion as the possibility of the even K exceeding 2, we can also arrive at the fact that the constellation given by (3.12) is still optimal.

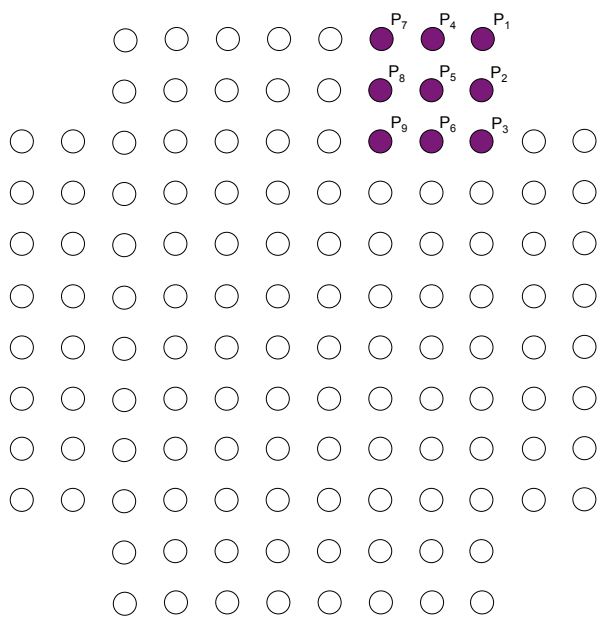


Figure A.1: Nine corner points in the cross QAM constellation

Case 2: $|\mathcal{X}| = 4$. In this case, possibilities for $K = 3$ and 5 can be verified directly by calculation. In addition, since the possibility for even K greater than 2 is similar to that for odd K exceeding 5, here we only provide a proof for the situation when K is an odd number greater than 5. By Proposition 4, $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_{-1} \cup \mathcal{Z}_j \cup \mathcal{Z}_{-j}$ with $\mathcal{Z}_{x_k} \cap \mathcal{Z}_{x_\ell} = \Phi$ for $k \neq \ell = 1, 2, 3, 4$. Actually, $\mathcal{Z}_{x_k} = x_k^* \mathcal{Y}$, since $x_k \in \mathcal{X} = \{\pm 1, \pm j\}$.

Thus, we have $d_{\min}(\mathcal{Z}_{x_\ell}) = d_{\min}(\mathcal{Y})$. Let P_i for $i = 1, \cdots, 9$ be nine points in the first quadrant around the corner of $\mathcal{Z}$ shown in Fig. A.1. Using the pigeon principal, there exists one Goup, say, $\mathcal{Z}_{x_{k_0}}$, including at least three of these nine points, say, P_{i_1}, P_{i_2} and P_{i_3}. Among these three points, if there exist two of them lying either in the same row or in the same column, then, $d_{\min}(\mathcal{Y}) = d_{\min}(\mathcal{Z}_{x_{k_0}}) \leq 4$. Otherwise, these three points locate in different rows and different columns and thus, $d_{\min}(\mathcal{Y}) = d_{\min}(\mathcal{Z}_{x_{k_0}}) \leq 2\sqrt{2}$. Therefore, in any case, we can always have $d_{\min}(\mathcal{Y}) \leq 4$. On the other hand, notice that the constellation determined by (3.14) possesses two features: (a) $|\mathcal{Y}^{(2)}_{\text{opt}}| = 2^K$; (b) $y_1 - y_2 = 4z$ for any two distinct points y_1 and y_2 in $\mathcal{Y}^{(1)}_{\text{opt}}$, where z is some complex integer. Hence, we have $d_{\min}(\mathcal{Y}) = 4$. Let us now examine whether such a pair of the constellations $\mathcal{X}^{(2)}_{\text{opt}}$ and $\mathcal{Y}^{(2)}_{\text{opt}}$ forms a UFCP. Suppose that there exist $x, \widetilde{x} \in \mathcal{X}$ and $y, \widetilde{y} \in \mathcal{Y}$ such that $x\widetilde{y} = \widetilde{x}y$, then, we have

$$(\widetilde{y} - y)x = (\widetilde{x} - x)y. \tag{A.3}$$

If $x = \widetilde{x}$, then, $y = \widetilde{y}$, since $x \neq 0$. If $x \neq \widetilde{x}$, then, $x - \widetilde{x} = \pm 2, \pm 2j, \pm 1 \pm j$. No matter whatever situation occurs, once we have substituted $(\widetilde{y} - y) = 4z$ into (A.3), we can always obtain $y = 2z_0$ for some complex integer z_0, where we have used the fact that $2 = (1 + j)(1 - j)$. This implies that y is an even number, which is impossible. Thus, $x = \widetilde{x}$ and $y = \widetilde{y}$ and $\mathcal{X}^{(1)}_{\text{opt}}$ and $\mathcal{Y}^{(1)}_{\text{opt}}$ indeed constitute a UFCP. Therefore, in this case, $\mathcal{Y}^{(1)}_{\text{opt}}$ is optimal. This completes the proof of Proposition 5. $\square$

A.2 Proof of Lemma 3

Since the proof of (5.6b) is much similar to that of (5.6a), we only provide a proof for (5.6a), which can be fulfilled by considering the following possibilities:

1. $v = 3$. In this case, Lemma 2 tells us that $E_2 = 10$ and $E_{21} = 2$. Hence, the inequality (5.6a) is reduced to

$$8 + E_{11} \leq E_1. \tag{A.4}$$

   If $u = 3$, $E_1 = 10$, $E_{11} = 2$, so $E_1 - E_{11} = 8$, inequality (A.4) is hold. If u is an odd number exceeding 3, then, by Lemma 2, we have $E_1 = (2^{\frac{u-1}{2}} - 1)^2 + (3 \times 2^{\frac{u-3}{2}} - 1)^2$ and $E_{11} = (2^{\frac{u-1}{2}} - 3)^2 + (3 \times 2^{\frac{u-3}{2}} - 1)^2$. Thus, we obtain $E_1 - E_{11} = (2^{\frac{u-1}{2}} - 1)^2 - (2^{\frac{u-1}{2}} - 3)^2 = 4 \times 2^{\frac{u-1}{2}} - 8 \geq 8$, since $2^{\frac{u-1}{2}} \geq 4$. Hence, in this case, the inequality (A.4) is also true. If u is an even integer, then, by Lemma 2 again, we have $E_1 = 2(2^{\frac{u}{2}} - 1)^2$ and $E_{11} = (2^{\frac{u}{2}} - 1)^2 + (2^{\frac{u}{2}} - 3)^2$ so that $E_1 - E_{11} = (2^{\frac{u}{2}} - 1)^2 - (2^{\frac{u}{2}} - 3)^2 = 4 \times 2^{\frac{u}{2}} - 8 \geq 8$, since $u \geq 4$. Hence, the inequality (A.4) is still true.

2. v is an odd number exceeding 3. In this case, Lemma 2 gives us that $E_2 = (2^{\frac{v-1}{2}} - 1)^2 + (3 \times 2^{\frac{v-3}{2}} - 1)^2$ and $E_{21} = (2^{\frac{v-1}{2}} - 3)^2 + (3 \times 2^{\frac{v-3}{2}} - 1)^2$ so that $E_2 - E_{21} = (2^{\frac{v-1}{2}} - 1)^2 - (2^{\frac{v-1}{2}} - 3)^2 = 4 \times (2^{\frac{v-1}{2}} - 2)$. On the other hand, if u is an odd number not less than v, then, Lemma 2 gives us that $E_1 = (2^{\frac{p-1}{2}} - 1)^2 + (3 \times 2^{\frac{u-3}{2}} - 1)^2$ and $E_{11} = (2^{\frac{u-1}{2}} - 3)^2 + (3 \times 2^{\frac{u-3}{2}} - 1)^2$ so that $E_1 - E_{11} = (2^{\frac{u-1}{2}} - 1)^2 - (2^{\frac{u-1}{2}} - 3)^2 = 4 \times (2^{\frac{u-1}{2}} - 2) \geq 4 \times (2^{\frac{v-1}{2}} - 2)$, since the exponential function 2^t is increasing and $u \geq v$. Therefore, in this case, we have $E_1 - E_{11} \geq E_2 - E_{21}$, which is equivalent to the fact that $E_2 + E_{11} \leq$

$E_1 + E_{21}$. If u is an even number not less than v, then, using Lemma 2 again yields $E_1 = 2(2^{\frac{u}{2}} - 1)^2$ and $E_{11} = (2^{\frac{u}{2}} - 1)^2 + (2^{\frac{u}{2}} - 3)^2$. Hence, we have $E_1 - E_{11} = (2^{\frac{u}{2}} - 1)^2 - (2^{\frac{u}{2}} - 3)^2 = 4 \times (2^{\frac{u}{2}} - 2) \geq 4 \times (2^{\frac{v-1}{2}} - 2) = E_2 - E_{21}$. Hence, in this case, the inequality (5.6a) holds.

3. v is an even number greater than or equal to 2. Similarly, by Lemma 2, we can have $E_2 - E_{21} = 4 \times (2^{\frac{v}{2}} - 2)$ and

$$E_1 - E_{11} = \begin{cases} 4 \times (2^{\frac{u}{2}} - 2) \geq E_2 - E_{21} & \text{if } u \text{ is even and not less than 2} \\ 8 & \text{if } u = 3 \\ 4 \times (2^{\frac{u-1}{2}} - 2) \geq E_2 - E_{21} & \text{if } u \text{ is an odd number exceeding 3} \end{cases}.$$

Notice that when $u = 3$, v must be 2, since $u \geq v \geq 2$. Then, in this case, $E_2 - E_{21} = 2 - 2 = 0$. Therefore, we can always obtain $E_1 - E_{11} \geq E_2 - E_{21}$.

This completes the proof of Lemma 3. □

A.3 Proof of Lemma 4

Here, we only give the proof of (5.7b), since the proofs of the other inequalities are much similar. To do that, let us consider the following situations.

1. w is an even number not less than 4. In this case, since $u + v = w$, both u and v are either even or odd. If both u and v are even, then, Lemma 2 provides us with $E_1 = 2(2^{\frac{u}{2}} - 1)^2$ and $E_{21} = E_{22} = (2^{\frac{v}{2}} - 1)^2 + (2^{\frac{v}{2}} - 3)^2$. Then, we have $E_1 + E_{21} = 2(2^{\frac{u}{2}} - 1)^2 + (2^{\frac{v}{2}} - 1)^2 + (2^{\frac{v}{2}} - 3)^2 = 2(2^{\frac{u}{2}} - 1)^2 + (2^{\frac{w-u}{2}} - 1)^2 + (2^{\frac{w-u}{2}} - 3)^2$. Since $u \geq v$, $w > u \geq w/2$. Now, consider the following function in terms of

variable t:

$$f(t) = 2(2^{\frac{t}{2}} - 1)^2 + (2^{\frac{w-t}{2}} - 1)^2 + (2^{\frac{w-t}{2}} - 3)^2 \qquad \text{for } t \geq w/2.$$

Then, the first order derivative of $f(t)$ with respect to t is given by

$$f'(t) = 2(2^{\frac{t}{2}} - 1)2^{\frac{t}{2}} \ln 2 - (2^{\frac{w-t}{2}} - 1)2^{\frac{w-t}{2}} \ln 2 - (2^{\frac{w-t}{2}} - 3)2^{\frac{w-t}{2}} \ln 2,$$

for $w > t \geq w/2$. Since the exponential function $2^{\frac{t}{2}}$ is increasing and $t \geq w - t$, $(2^{\frac{t}{2}} - 1)2^{\frac{t}{2}} \geq (2^{\frac{w-t}{2}} - 3)2^{\frac{w-t}{2}}$ and thus, $f'(t) \geq 0$, showing that $f(t)$ is an increasing function. Therefore, we have $f(p) \geq f(r/2)$, i.e., $E_1 + E_{21} \geq \widetilde{E}_1 + \widetilde{E}_{21}$. Consequently, the inequality (5.7b) holds in this case. Similarly, if both p and q are odd, we can also prove that (5.7b) still holds.

2. w is an odd number exceeding 4. Since $u + v = w$, either u is even and v is odd or u is odd and v is even. If u is even and v is odd, by Lemma 2, we obtain $E_1 = 2(2^{\frac{u}{2}} - 1)^2$ $E_{21} = (2^{\frac{v-1}{2}} - 3)^2 + (3 \times 2^{\frac{v-3}{2}} - 1)^2$ and hence, $E_1 + E_{21} = 2(2^{\frac{u}{2}} - 1)^2 + (2^{\frac{v-1}{2}} - 3)^2 + (3 \times 2^{\frac{v-3}{2}} - 1)^2 = 2(2^{\frac{u}{2}} - 1)^2 + (2^{\frac{w-u-1}{2}} - 3)^2 + (3 \times 2^{\frac{w-u-3}{2}} - 1)^2$, where $w > u \geq (w+1)/2$. This leads us to considering a function:

$$g(t) = 2(2^{\frac{t}{2}} - 1)^2 + (2^{\frac{w-t-1}{2}} - 3)^2 + (3 \times 2^{\frac{w-t-3}{2}} - 1)^2,$$

for $w > t \geq (w+1)/2$. The first order derivative of $g(t)$ is

$$g'(t) = 2(2^{\frac{t}{2}} - 1)2^{\frac{t}{2}} \ln 2 - (2^{\frac{w-t-1}{2}} - 3)2^{\frac{w-t-1}{2}} \ln 2 - 3 \times (3 \times 2^{\frac{w-t-3}{2}} - 1)2^{\frac{w-t-3}{2}} \ln 2,$$

for $w > t \geq (w+1)/2$. Since $2^{\frac{t}{2}}$ is increasing and $t \geq w - t$, we arrive at the fact that $\frac{1}{2} \times (2^{\frac{t}{2}} - 1)2^{\frac{t}{2}} \geq \frac{1}{2} \times (2^{\frac{w-t}{2}} - 1)2^{\frac{w-t}{2}} \geq (2^{\frac{w-t-1}{2}} - 3)2^{\frac{w-t-1}{2}}$. In addition, notice that $(2 - \frac{1}{2}) \times (2^{\frac{t}{2}} - 1)2^{\frac{t}{2}} > (2 - \frac{1}{2}) \times (2^{\frac{w-t}{2}} - 1)2^{\frac{w-t}{2}} = 3\sqrt{2} \times (2\sqrt{2} \times 2^{\frac{w-t-3}{2}} - 1)2^{\frac{w-t-3}{2}} > 3 \times (3 \times 2^{\frac{w-t-3}{2}} - 1)2^{\frac{w-t-3}{2}}$ because of the fact that $2^{\frac{w-t-3}{2}} \geq 1$. As a result, $g'(t) \geq 0$ and $g(t)$ is increasing. Hence, $g(u) \geq g((w+1)/2)$, i.e., $E_1 + E_{21} \geq \widetilde{E}_1 + \widetilde{E}_{21}$. This can be also proved to be true if u is odd and v is even. Analogously, we can prove that $E_1 + E_{22} \geq \widetilde{E}_1 + \widetilde{E}_{22}$. Therefore, the inequality (5.7b) holds.

This completes the proof of Lemma 4. □

A.4 Proof of Lemma 5

We prove Lemma 5 by considering the following four different cases for w.

1. $w = 4\ell$, where ℓ is a positive integer not less than 1. In this case, by the definition of $\widetilde{u}$ and $\widetilde{v}$ in (5.5), we have $\widetilde{u} = \widetilde{v} = w/2 = 2\ell$ and thus, $\widetilde{E}_1 = \widetilde{E}_2$, $\widetilde{E}_{11} = \widetilde{E}_{22}$, which implies that $\widetilde{E}_1 - \widetilde{E}_{11} = \widetilde{E}_2 - \widetilde{E}_{22}$.

2. $w = 4\ell + 1$. Then, (5.5) tells us that $\widetilde{u} = (w+1)/2 = 2\ell + 1$ is odd, whereas $\widetilde{v} = (w-1)/2 = 2\ell$ is even. Particularly when $\ell = 1$, $\widetilde{u} = 3$ and $\widetilde{v} = 2$. In this specular case, $\widetilde{E}_1 - \widetilde{E}_{11} = 10 - 2 = 6$ and $\widetilde{E}_2 - \widetilde{E}_{22} = 2 - 2 = 0$, resulting in $\widetilde{E}_1 - \widetilde{E}_{11} > \widetilde{E}_2 - \widetilde{E}_{22}$. If $\ell > 1$, then, by Lemma 2, we have $\widetilde{E}_1 - \widetilde{E}_{11} = 4 \times 2^{\frac{\widetilde{u}-1}{2}} - 8$ and $\widetilde{E}_2 - \widetilde{E}_{22} = (2^{\frac{\widetilde{v}}{2}} - 1)^2 - (2^{\frac{\widetilde{v}}{2}} - 3)^2 = 4 \times 2^{\frac{\widetilde{v}}{2}} - 8$. Since $\frac{\widetilde{u}-1}{2} = \frac{\widetilde{v}}{2} = \ell$, in this case we obtain $\widetilde{E}_1 - \widetilde{E}_{11} = \widetilde{E}_2 - \widetilde{E}_{22}$.

3. $w = 4\ell + 2$. From the definition of $\widetilde{u}$ and $\widetilde{v}$ given in (5.5) we know that $\widetilde{u} = \widetilde{v} = w/2 = 2\ell + 1$. This means that both $\widetilde{u}$ and $\widetilde{v}$ are odd. Then,

Lemma 2 gives us $\widetilde{E}_1 - \widetilde{E}_{11} = (2^{\frac{\widetilde{u}-1}{2}} - 1)^2 - (2^{\frac{\widetilde{u}-1}{2}} - 3)^2 = 4 \times 2^{\frac{\widetilde{u}-1}{2}} - 8$ and $\widetilde{E}_2 - \widetilde{E}_{22} = (3 \times 2^{\frac{\widetilde{v}-3}{2}} - 1)^2 - (3 \times 2^{\frac{\widetilde{v}-3}{2}} - 3)^2 = 12 \times 2^{\frac{\widetilde{v}-3}{2}} - 8$. Since $12 \times 2^{\frac{\widetilde{v}-3}{2}} = 6 \times 2^{\frac{\widetilde{u}-1}{2}} > 4 \times 2^{\frac{\widetilde{u}-1}{2}}$, implying $\widetilde{E}_1 - \widetilde{E}_{11} < \widetilde{E}_2 - \widetilde{E}_{22}$.

4. $w = 4\ell+3$. In this case, $\widetilde{u} = (w+1)/2 = 2\ell+2$ is even and $\widetilde{v} = (w-1)/2 = 2\ell+1$ is odd. Specially for $\ell = 1$, we have $\widetilde{u} = 4, \widetilde{v} = 3$ and thus, $\widetilde{E}_1 - \widetilde{E}_{11} = 18 - 10 = 8$ and $\widetilde{E}_2 - \widetilde{E}_{22} = 10 - 2 = 8$. Hence, we have $\widetilde{E}_1 - \widetilde{E}_{11} = \widetilde{E}_2 - \widetilde{E}_{22}$ in this particular case. If $\ell > 1$, then, by Lemma 2 again, we can attain that $\widetilde{E}_1 - \widetilde{E}_{11} = (2^{\frac{\widetilde{u}}{2}} - 1)^2 - (2^{\frac{\widetilde{u}}{2}} - 3)^2 = 4 \times 2^{\frac{\widetilde{u}}{2}} - 8$ and $\widetilde{E}_2 - \widetilde{E}_{22} = 12 \times 2^{\frac{\widetilde{v}-3}{2}} - 8$. Because of the fact that $4 \times 2^{\frac{\widetilde{u}}{2}} = 4 \times 2^{\frac{\widetilde{v}+1}{2}} = 16 \times 2^{\frac{\widetilde{v}-3}{2}} > 12 \times 2^{\frac{\widetilde{v}-3}{2}}$, we have $\widetilde{E}_1 - \widetilde{E}_{11} > \widetilde{E}_2 - \widetilde{E}_{22}$.

Now, summing up all the above results ends the proof of Lemma 5. □

A.5 Proof of Theorem 3

We prove Theorem 3 by considering the following situations:

1. $r = 4$. In this case, we know from Properties 1, 2 and 3 that

$$\begin{aligned} G(\widetilde{\mathcal{X}}^{(0)}, \widetilde{\mathcal{Y}}_1^{(0)}, \widetilde{\mathcal{Y}}_2^{(0)}) &= \frac{1}{4}, \\ G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) &= \frac{1}{6}, \\ G(\widetilde{\mathcal{X}}^{(2)}, \widetilde{\mathcal{Y}}_1^{(2)}, \widetilde{\mathcal{Y}}_2^{(2)}) &\leq \frac{2}{(\sqrt{5}+\sqrt{3})^2} < \frac{1}{4}. \end{aligned}$$

Therefore, the optimal coding gain is $1/4, \widetilde{\delta} = 0, \widetilde{p} = \widetilde{q} = 2$, and $\widetilde{\mathcal{X}}$ and $\widetilde{\mathcal{Y}}$ are the 4-QAM constellation.

2. $r = 10$. Similarly, Properties 1, 2 and 3 tell us that

$$\begin{aligned} G(\widetilde{\mathcal{X}}^{(0)}, \widetilde{\mathcal{Y}}_1^{(0)}, \widetilde{\mathcal{Y}}_2^{(0)}) &= \frac{1}{(\sqrt{15}+\sqrt{17})^2}, \\ G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) &= \frac{1}{66}, \\ G(\widetilde{\mathcal{X}}^{(2)}, \widetilde{\mathcal{Y}}_1^{(2)}, \widetilde{\mathcal{Y}}_2^{(2)}) &\leq \frac{1}{86}. \end{aligned}$$

Hence, the optimal coding gain is $\frac{1}{(\sqrt{15}+\sqrt{17})^2}, \widetilde{\delta} = 0, \widetilde{p} = \widetilde{q} = 5$, and $\widetilde{\mathcal{X}}$ and $\widetilde{\mathcal{Y}}$ are the cross 32-QAM constellation.

3. r is an even integer exceeding 4 and not equal to 10. In this case, we consider the following two possibilities:

   (a) If $r = 6$, then, Properties 1, 2 and 3 give us

$$\begin{aligned} G(\widetilde{\mathcal{X}}^{(0)}, \widetilde{\mathcal{Y}}_1^{(0)}, \widetilde{\mathcal{Y}}_2^{(0)}) &= \frac{1}{\left(\sqrt{3}+\sqrt{5}\right)^2}, \\ G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) &= \frac{2}{\left(\sqrt{5}+\sqrt{7}\right)^2}, \\ G(\widetilde{\mathcal{X}}^{(2)}, \widetilde{\mathcal{Y}}_1^{(2)}, \widetilde{\mathcal{Y}}_2^{(2)}) &\leq \frac{1}{14}. \end{aligned}$$

   Thus, in this case, we have $\widetilde{\delta} = 1, \widetilde{p} = 4, \widetilde{q} = 3$.

(b) If $r \neq 6$, then, we have from Properties 1, 2 and 3 that

$$\begin{aligned}
G(\widetilde{\mathcal{X}}^{(0)}, \widetilde{\mathcal{Y}}_1^{(0)}, \widetilde{\mathcal{Y}}_2^{(0)}) &= \frac{4}{\left(\sqrt{\widetilde{E}_1^{(0)} + \widetilde{E}_2^{(0)}} + \sqrt{\widetilde{E}_1^{(0)} + \widetilde{E}_{21}^{(0)}}\right)^2}, \\
G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) &= \frac{8}{\left(\sqrt{\widetilde{E}_1^{(1)} + \widetilde{E}_{21}^{(1)}} + \sqrt{\widetilde{E}_1^{(1)} + \widetilde{E}_{22}^{(1)}}\right)^2}, \\
G(\widetilde{\mathcal{X}}^{(2)}, \widetilde{\mathcal{Y}}_1^{(2)}, \widetilde{\mathcal{Y}}_2^{(2)}) &\leq \frac{8}{\left(\sqrt{\widetilde{E}_1^{(2)} + \widetilde{E}_{22}^{(2)}} + \sqrt{\widetilde{E}_2^{(2)} + \widetilde{E}_{12}^{(2)}}\right)^2}.
\end{aligned}$$

Recall the following facts:

i. $\widetilde{E}_1^{(2)} = \widetilde{E}_2^{(2)}, \widetilde{E}_{12}^{(2)} = \widetilde{E}_{22}^{(2)}$, $\widetilde{E}_1^{(2)}$ is the largest energy among all the points in the $2^{r/2+1}$-ary cross QAM constellation and $\widetilde{E}_{12}^{(2)}$ is the energy of the second neighbor of the point with the largest energy in the constellation.

ii. $\widetilde{E}_1^{(1)}$ is the largest energy among all the points in the $2^{r/2+1}$-ary cross QAM constellation, while $\widetilde{E}_{21}^{(1)}$ and $\widetilde{E}_{22}^{(1)}$ are the respective energies of the first and second neighbors of the point with the largest energy in the $2^{r/2}$-ary cross QAM constellation.

iii. $\widetilde{E}_1^{(0)} = \widetilde{E}_2^{(0)}$, $\widetilde{E}_1^{(0)}$ is the largest energy among all the points in the $2^{r/2}$-ary cross QAM constellation and $\widetilde{E}_{21}^{(0)}$ is the energy of the first neighbor of the point with the largest energy in the constellation.

Hence, we obtain $\widetilde{E}_{12}^{(2)} > \widetilde{E}_{21}^{(1)} > \widetilde{E}_{22}^{(1)}$ and as a result, $G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) > G(\widetilde{\mathcal{X}}^{(2)}, \widetilde{\mathcal{Y}}_1^{(2)}, \widetilde{\mathcal{Y}}_2^{(2)})$. In addition, since

$$\frac{G(\widetilde{\mathcal{X}}^{(0)}, \widetilde{\mathcal{Y}}_1^{(0)}, \widetilde{\mathcal{Y}}_2^{(0)})}{G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)})} = \left(\frac{\sqrt{\widetilde{E}_1^{(1)} + \widetilde{E}_{21}^{(1)}} + \sqrt{\widetilde{E}_1^{(1)} + \widetilde{E}_{22}^{(1)}}}{\sqrt{2\widetilde{E}_1^{(0)} + 2\widetilde{E}_2^{(0)}} + \sqrt{2\widetilde{E}_1^{(0)} + 2\widetilde{E}_{21}^{(0)}}}\right)^2 \leq 1, \quad \text{(A.5)}$$

where we have used the facts that $\widetilde{E}_{21}^{(0)} = \widetilde{E}_{21}^{(1)} \geq \widetilde{E}_{22}^{(1)}$ and that $2\widetilde{E}_{1}^{(0)} \geq \widetilde{E}_{1}^{(1)}$ if $r \geq 6$, we attain $G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) > G(\widetilde{\mathcal{X}}^{(0)}, \widetilde{\mathcal{Y}}_1^{(0)}, \widetilde{\mathcal{Y}}_2^{(0)})$. Therefore, in this case, the optimal coding gain is $G(\widetilde{\mathcal{X}}, \widetilde{\mathcal{Y}}_1, \widetilde{\mathcal{Y}}_2)$ is $G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)})$.

4. r is an odd integer exceeding 4. There are three cases which need to be considered: a) $r = 5$, b) $r = 9$ and c) $r \neq 5, 9$. However, since the discussions on Cases a) and b) are much similar to the previous cases $r = 6$ and $r = 10$, we only consider Case c). In this situation, Properties 1, 2 and 3 provide us with

$$\begin{aligned}
G(\widetilde{\mathcal{X}}^{(0)}, \widetilde{\mathcal{Y}}_1^{(0)}, \widetilde{\mathcal{Y}}_2^{(0)}) &= \frac{4}{\left(\sqrt{\widetilde{E}_1^{(0)} + \widetilde{E}_2^{(0)}} + \sqrt{\widetilde{E}_1^{(0)} + \widetilde{E}_{21}^{(0)}}\right)^2}, \\
G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)}) &= \frac{8}{\left(\sqrt{\widetilde{E}_1^{(1)} + \widetilde{E}_{21}^{(1)}} + \sqrt{\widetilde{E}_{11}^{(1)} + \widetilde{E}_2^{(1)}}\right)^2}, \\
G(\widetilde{\mathcal{X}}^{(2)}, \widetilde{\mathcal{Y}}_1^{(2)}, \widetilde{\mathcal{Y}}_2^{(2)}) &\leq \frac{8}{\left(\sqrt{\widetilde{E}_{11}^{(2)} + \widetilde{E}_2^{(2)}} + \sqrt{\widetilde{E}_{12}^{(2)} + \widetilde{E}_2^{(2)}}\right)^2}.
\end{aligned}$$

Notice the following facts:

(a) $\widetilde{E}_2^{(2)}$ is the largest energy among all the points in the $2^{(r+1)/2}$-ary cross QAM constellation, $\widetilde{E}_{11}^{(2)}$ and $\widetilde{E}_{12}^{(2)}$ are the energies of the first and second neighbors of the points with the largest energies in the $2^{(r+3)/2}$-ary cross QAM constellations.

(b) $\widetilde{E}_1^{(1)} = \widetilde{E}_1^{(2)}, \widetilde{E}_{11}^{(1)} = \widetilde{E}_{21}^{(1)}$, $\widetilde{E}_1^{(1)}$ is the largest energy among all the points in the $2^{(r+1)/2}$-ary cross QAM constellation and $\widetilde{E}_{11}^{(1)}$ is the energy of the first neighbor of the point with the largest energy in the constellation.

(c) $\widetilde{E}_1^{(0)}$ is the largest energy among all the points in the $2^{(r+1)/2}$-ary cross QAM constellation, $\widetilde{E}_2^{(0)}$ is the largest energy among all the points in the

$2^{(r-1)/2}$-ary cross QAM constellation and $\widetilde{E}_{21}^{(0)}$ is the energy of the first neighbor of the point with the largest energy in the $2^{(r-1)/2}$-ary cross QAM constellation.

Now, following the way similar to the previous case where $r \geq 8$ is even but not equal to 10, we can prove that $G(\widetilde{\mathcal{X}}^{(1)}, \widetilde{\mathcal{Y}}_1^{(1)}, \widetilde{\mathcal{Y}}_2^{(1)})$ is still the optimal coding gain.

This completes the proof of Theorem 3. □

A.6 Proof of Lemma 6

In order to prove this lemma, we first prove the following two statements, i.e.,

$$\mathbb{Q}_m \mathbb{Q}_n = \mathbb{Q}_l, \tag{A.6a}$$

$$\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}_d, \tag{A.6b}$$

where $l = \mathrm{lcm}(m, n)$ and $d = \gcd(m, n)$. These two statements are one of excises in [87] without proof. For completeness of the exposition, we give a proof here. On one hand, consider any element $\zeta_m^{i_m} \cdot \zeta_n^{i_n}$ in $\mathbb{Q}_m \mathbb{Q}_n$:

$$\zeta_m^{i_m} \cdot \zeta_n^{i_n} = \exp\left(\frac{j2i_m\pi}{m}\right) \exp\left(\frac{j2i_n\pi}{n}\right) = \exp\left(\frac{j2(i_m n + i_n m)\pi}{mn}\right), \tag{A.7}$$

where i_m, i_n are integers. By Property 5, we know that $ld = mn$. Substituting this into (A.7) results in

$$\zeta_m^{i_m} \cdot \zeta_n^{i_n} = \exp\left(\frac{j2(i_m n + i_n m)\pi}{dl}\right) = \exp\left(\frac{j2(i_m n/d + i_n m/d)\pi}{l}\right) = \exp\left(\frac{j2i_l\pi}{l}\right),$$

where i_l is the integer with $0 \leq i_l < l-1$ such that $i_l = i_m n/d + i_n m/d \mod l$. This means that $\zeta_m^{i_m} \cdot \zeta_n^{i_n} \in \mathbb{Q}_l$ thus, $\mathbb{Q}_m\mathbb{Q}_n \subseteq \mathbb{Q}_l$. On the other hand, consider any element $\zeta_l^{\ell_l}$ in $\mathbb{Q}_l$. By Property 4, for any given integer d, there are a pair of integers ℓ_m and ℓ_n such that $d = m\ell_n + n\ell_m$. Hence, $\ell_l = \ell_l\ell_n m/d + \ell_l\ell_m n/d$ and as a result, $\zeta_l^{\ell_l} = \exp\left(\frac{j2\ell_l\pi}{l}\right) = \exp\left(\frac{j2(\ell_l\ell_n m+\ell_l\ell_m n)\pi}{dl}\right)$. This, by Property 5, can be further simplified into $\zeta_l^{\ell_l} = \exp\left(\frac{j2\ell_l\ell_m\pi}{m}\right)\exp\left(\frac{j2\ell_l\ell_n\pi}{n}\right) \in \mathbb{Q}_m\mathbb{Q}_n$, implying $\mathbb{Q}_l \subseteq \mathbb{Q}_m\mathbb{Q}_n$. Therefore, we have $\mathbb{Q}_l = \mathbb{Q}_m\mathbb{Q}_n$. This means that Statement (A.6a) is true. Now, let us consider Statement (A.6b). Since d is a common divisor of m and n, $\mathbb{Q}_d \subseteq \mathbb{Q}_n, \mathbb{Q}_d \subseteq \mathbb{Q}_m$ and thus, $\mathbb{Q}_d \subseteq \mathbb{Q}_m \cap \mathbb{Q}_n$. On the other hand, by Property 7 we have

$$[\mathbb{Q}_m : \mathbb{Q}] = [\mathbb{Q}_m : \mathbb{Q}_m \cap \mathbb{Q}_n] \cdot [\mathbb{Q}_m \cap \mathbb{Q}_n : \mathbb{Q}], \tag{A.8}$$

$$[\mathbb{Q}_l : \mathbb{Q}] = [\mathbb{Q}_l : \mathbb{Q}_n] \cdot [\mathbb{Q}_n : \mathbb{Q}]. \tag{A.9}$$

Using (A.6a) and then, Property 8 with $K = \mathbb{Q}_m$ and $L = \mathbb{Q}_n$ give us

$$[\mathbb{Q}_l : \mathbb{Q}_n] = [\mathbb{Q}_m\mathbb{Q}_n : \mathbb{Q}_n] = [\mathbb{Q}_m : \mathbb{Q}_m \cap \mathbb{Q}_n]. \tag{A.10}$$

Substituting (A.10) into (A.9) yields

$$[\mathbb{Q}_l : \mathbb{Q}] = [\mathbb{Q}_m : \mathbb{Q}_m \cap \mathbb{Q}_n] \cdot [\mathbb{Q}_n : \mathbb{Q}]. \tag{A.11}$$

From (A.9) and (A.11) we eliminate $[\mathbb{Q}_m : \mathbb{Q}_m \cap \mathbb{Q}_n]$ so that

$$[\mathbb{Q}_m \cap \mathbb{Q}_n : \mathbb{Q}] = \frac{[\mathbb{Q}_m : \mathbb{Q}] \cdot [\mathbb{Q}_n : \mathbb{Q}]}{[\mathbb{Q}_l : \mathbb{Q}]} = \frac{\phi(m) \cdot \phi(n)}{\phi(l)} = \phi(d),$$

where we have used Properties 9 and 6. Since the degree of $\mathbb{Q}_d$ over $\mathbb{Q}$ is also equal to $\phi(d)$, we have $\mathbb{Q}_n \cap \mathbb{Q}_m = \mathbb{Q}_d$. Hence, Statement (A.6b) is also true. Now, using Property 10 and (A.6), we can complete the proof of Lemma 6. $\square$

A.7 Proof of Proposition 6

PROOF: Suppose that there are four matrices $\mathbf{A}_p \neq \hat{\mathbf{A}}_p \in \mathcal{A}_p$ and $\mathbf{A}_q \neq \hat{\mathbf{A}}_q \in \mathcal{A}_q$ such that

$$\hat{\mathbf{A}}_p^{-1}\mathbf{A}_p = \hat{\mathbf{A}}_q^{-1}\mathbf{A}_q. \tag{A.12}$$

Let

$$\hat{\mathbf{A}}_p^H = \begin{pmatrix} \hat{a}_{p1}^* & -\hat{a}_{p2} \\ \hat{a}_{p2}^* & \hat{a}_{p1} \end{pmatrix}, \quad \mathbf{A}_p = \begin{pmatrix} a_{p1} & a_{p2} \\ -a_{p2}^* & a_{p1}^* \end{pmatrix},$$
$$\hat{\mathbf{A}}_q^H = \begin{pmatrix} \hat{a}_{q1}^* & -\hat{a}_{q2} \\ \hat{a}_{q2}^* & \hat{a}_{q1} \end{pmatrix}, \quad \mathbf{A}_q = \begin{pmatrix} a_{q1} & a_{q2} \\ -a_{q2}^* & a_{q1}^* \end{pmatrix},$$

where

$$a_{pi} = \exp\big(\frac{j2\ell_i\pi}{p}\big), \qquad \hat{a}_{pi} = \exp\big(\frac{j2\hat{\ell}_i\pi}{p}\big) \in \mathcal{S}_p, \tag{A.13a}$$
$$a_{qi} = \exp\big(\frac{j2k_i\pi}{q}\big), \qquad \hat{a}_{qi} = \exp\big(\frac{j2\hat{k}_i\pi}{p}\big) \in \mathcal{S}_q, \tag{A.13b}$$

for $i = 1, 2$. Then, by using the Alamouti code and the PSK constellation properties, condition (A.12) is equivalent to

$$\hat{a}_{p1}^* a_{p1} + \hat{a}_{p2} a_{p2}^* = \hat{a}_{q1}^* a_{q1} + \hat{a}_{q2} a_{q2}^*, \tag{A.14a}$$

$$\hat{a}_{p1}^* a_{p2} - \hat{a}_{p2} a_{p1}^* = \hat{a}_{q1}^* a_{q2} - \hat{a}_{q2} a_{q1}^*. \tag{A.14b}$$

Since $\hat{a}_{p1}^* a_{p1} + \hat{a}_{p2} a_{p2}^*, \hat{a}_{p1}^* a_{p2} - \hat{a}_{p2} a_{p1}^* \in \mathbb{Z}[\zeta_p]$ and $\hat{a}_{q1}^* a_{q1} + \hat{a}_{q2} a_{q2}^*, \hat{a}_{q1}^* a_{q2} - \hat{a}_{q2} a_{q1}^* \in \mathbb{Z}[\zeta_q]$, we have from (A.14) that these four complex numbers $\hat{a}_{p1}^* a_{p1} + \hat{a}_{p2} a_{p2}^*, \hat{a}_{p1}^* a_{p2} - \hat{a}_{p2} a_{p1}^*, \hat{a}_{q1}^* a_{q1} + \hat{a}_{q2} a_{q2}^*, \hat{a}_{q1}^* a_{q2} - \hat{a}_{q2} a_{q1}^* \in \mathbb{Z}[\zeta_p] \cap \mathbb{Z}[\zeta_q] = \mathbb{Z}$, where we have used Lemma 6. This means that each of them must be a rational integer. Notice that

$$\begin{aligned} \hat{a}_{p1}^* a_{p1} + \hat{a}_{p2} a_{p2}^* &= \exp\Big(\frac{j2\pi(\ell_1 - \hat{\ell}_1)}{p}\Big) + \exp\Big(\frac{j2\pi(\hat{\ell}_2 - \ell_2)}{p}\Big) \\ &= 2\cos\frac{(\ell_1 + \ell_2 - \hat{\ell}_1 - \hat{\ell}_2)\pi}{p} \exp\Big(\frac{j\pi(\ell_1 + \hat{\ell}_2 - \hat{\ell}_1 - \ell_2)}{p}\Big). \end{aligned}$$

Hence, a necessary condition for $\hat{a}_{p1}^* a_{p1} + \hat{a}_{p2} a_{p2}^*$ to be a rational integer is that there exist two rational integers $f_1, g_1 \in \mathbb{Z}$ such that

$$\frac{(\ell_1 + \ell_2 - \hat{\ell}_1 - \hat{\ell}_2)\pi}{p} = \frac{\pi}{2} + f_1\pi \quad \text{or} \quad \frac{\pi(\ell_1 + \hat{\ell}_2 - \hat{\ell}_1 - \ell_2)}{p} = g_1\pi. \tag{A.15}$$

In the same token, since

$$\begin{aligned} \hat{a}_{p1}^* a_{p2} - \hat{a}_{p2} a_{p1}^* &= \exp\Big(\frac{j2\pi(\ell_2 - \hat{\ell}_1)}{p}\Big) - \exp\Big(\frac{j2\pi(\hat{\ell}_2 - \ell_1)}{p}\Big) \\ &= -2j\sin\frac{(\hat{\ell}_1 + \hat{\ell}_2 - \ell_1 - \ell_2)\pi}{p} \exp\Big(\frac{j\pi(\ell_2 + \hat{\ell}_2 - \ell_1 - \hat{\ell}_1)}{p}\Big), \end{aligned}$$

a necessary condition for $\hat{a}_{p1}^* a_{p2} - \hat{a}_{p2} a_{p1}^*$ to be a rational integer is that there are two rational integers $f_2, g_2 \in \mathbb{Z}$ such that

$$\frac{(\hat{\ell}_1 + \hat{\ell}_2 - \ell_1 - \ell_2)\pi}{p} = f_2\pi \quad \text{or} \quad \frac{\pi(\ell_2 + \hat{\ell}_2 - \ell_1 - \hat{\ell}_1)}{p} = \frac{\pi}{2} + g_2\pi. \tag{A.16}$$

From (A.15) and (A.16), we can conclude that if either $\frac{(\ell_1+\ell_2-\hat{\ell}_1-\hat{\ell}_2)\pi}{p} = \frac{\pi}{2} + f_1\pi$ or $\frac{\pi(\ell_2+\hat{\ell}_2-\ell_1-\hat{\ell}_1)}{p} = \frac{\pi}{2} + g_2\pi$, then, p must be even, and otherwise, we must have

$$\begin{aligned} \frac{\pi(\ell_1 + \hat{\ell}_2 - \hat{\ell}_1 - \ell_2)}{p} &= g_1\pi, \\ \frac{(\hat{\ell}_1 + \hat{\ell}_2 - \ell_1 - \ell_2)\pi}{p} &= f_2\pi, \end{aligned}$$

which is equivalent the fact that $2(\ell_1 - \hat{\ell}_1) = (g_1 - f_2)p$ and $2(\hat{\ell}_2 - \ell_2) = (g_1 + f_2)p$. This results in $a_{p1} = \hat{a}_{p1}$ and $a_{p2} = \hat{a}_{p2}$, which contradicts with the assumption. Therefore, a necessary condition for both $\hat{a}_{p1}^* a_{p1} + \hat{a}_{p2} a_{p2}^*$ and $\hat{a}_{p1}^* a_{p2} - \hat{a}_{p2} a_{p1}^*$ to be rational integers is that p must be even. On the other hand, using the same argument on the entries a_{qi} and $\hat{a}_{qi}$ from the cyclotomic ring $\mathbb{Z}[\zeta_q]$, we can arrive at the fact that a necessary condition for both $\hat{a}_{q1}^* a_{q1} + \hat{a}_{q2} a_{q2}^*$ and $\hat{a}_{q1}^* a_{q2} - \hat{a}_{q2} a_{q1}^*$ to be rational integers is that q must be even. This implies that 2 is one of common factor of p and q, which makes the contradiction that p and q are assumed to be coprime. Therefore, the assumption at the beginning of the proof that $\mathbf{A}_p \neq \hat{\mathbf{A}}_p$ and $\mathbf{A}_q \neq \hat{\mathbf{A}}_q$ is not true. This completes the proof of Proposition 6. $\square$

A.8 Proof of Proposition 7

PROOF: Suppose that there are six matrices $\mathbf{A}_p, \bar{\mathbf{A}}_p, \widetilde{\mathbf{A}}_p \in \mathcal{A}_p$ and $\mathbf{A}_q, \bar{\mathbf{A}}_q, \widetilde{\mathbf{A}}_q \in \mathcal{A}_q$ such that $\mathbf{A}_p^{-1}(\bar{\mathbf{A}}_p - \widetilde{\mathbf{A}}_p) = \mathbf{A}_q^{-1}(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q)$, which is equivalent to

$$\mathbf{A}_p^H(\bar{\mathbf{A}}_p - \widetilde{\mathbf{A}}_p) = \mathbf{A}_q^H(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q), \tag{A.17}$$

since $\mathbf{A}_p^{-1} = \mathbf{A}_p^H/4$ and $\mathbf{A}_q^{-1} = \mathbf{A}_q^H/4$. Let

$$\bar{\mathbf{A}}_p = \begin{pmatrix} \bar{a}_{p1} & \bar{a}_{p2} \\ -\bar{a}_{p2}^* & \bar{a}_{p1}^* \end{pmatrix}, \quad \widetilde{\mathbf{A}}_p = \begin{pmatrix} \tilde{a}_{p1} & \tilde{a}_{p2} \\ -\tilde{a}_{p2}^* & \tilde{a}_{p1}^* \end{pmatrix}, \quad \mathbf{A}_p = \begin{pmatrix} a_{p1} & a_{p2} \\ -a_{p2}^* & a_{p1}^* \end{pmatrix},$$
$$\bar{\mathbf{A}}_q = \begin{pmatrix} \bar{a}_{q1} & \bar{a}_{q2} \\ -\bar{a}_{q2}^* & \bar{a}_{q1}^* \end{pmatrix}, \quad \widetilde{\mathbf{A}}_q = \begin{pmatrix} \tilde{a}_{q1} & \tilde{a}_{q2} \\ -\tilde{a}_{q2}^* & \tilde{a}_{q1}^* \end{pmatrix}, \quad \mathbf{A}_q = \begin{pmatrix} a_{q1} & a_{q2} \\ -a_{q2}^* & a_{q1}^* \end{pmatrix},$$

where $a_{pi}, \bar{a}_{pi}, \widetilde{a}_{pi} \in \mathcal{S}_p \subseteq \mathbb{Z}[\zeta_p]$ and $a_{qi}, \bar{a}_{qi}, \widetilde{a}_{qi} \in \mathcal{S}_q \subseteq \mathbb{Z}[\zeta_q]$. Then, after some algebraic manipulations, we find that

$$\begin{aligned}
\mathbf{A}_p^H(\bar{\mathbf{A}}_p - \widetilde{\mathbf{A}}_p) &= \begin{pmatrix} a_{p1}^*(\bar{a}_{p1} - \tilde{a}_{p1}) + a_{p2}(\bar{a}_{p2}^* - \tilde{a}_{p2}^*) & a_{p1}^*(\bar{a}_{p2} - \tilde{a}_{p2}) - a_{p2}(\bar{a}_{p1}^* - \tilde{a}_{p1}^*) \\ a_{p2}^*(\bar{a}_{p1} - \tilde{a}_{p1}) - a_{p1}(\bar{a}_{p2}^* - \tilde{a}_{p2}^*) & a_{p1}(\bar{a}_{p1}^* - \tilde{a}_{p1}^*) + a_{p2}^*(\bar{a}_{p2} - \tilde{a}_{p2}) \end{pmatrix}, \\
\mathbf{A}_q^H(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q) &= \begin{pmatrix} a_{q1}^*(\bar{a}_{q1} - \tilde{a}_{q1}) + a_{q2}(\bar{a}_{q2}^* - \tilde{a}_{q2}^*) & a_{q1}^*(\bar{a}_{q2} - \tilde{a}_{q2}) - a_{q2}(\bar{a}_{q1}^* - \tilde{a}_{q1}^*) \\ a_{q2}^*(\bar{a}_{q1} - \tilde{a}_{q1}) - a_{q1}(\bar{a}_{q2}^* - \tilde{a}_{q2}^*) & a_{q1}(\bar{a}_{q1}^* - \tilde{a}_{q1}^*) + a_{q2}^*(\bar{a}_{q2} - \tilde{a}_{q2}) \end{pmatrix}.
\end{aligned}$$

Since the entries of $\mathbf{A}_p^H(\bar{\mathbf{A}}_p - \widetilde{\mathbf{A}}_p)$ belong to $\mathbb{Z}[\zeta_p]$ and the entries of $\mathbf{A}_q^H(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q)$ belong to $\mathbb{Z}[\zeta_q]$, a necessary condition for (A.17) to hold is that the entries of both $\mathbf{A}_p^H(\bar{\mathbf{A}}_p - \widetilde{\mathbf{A}}_p)$ and $\mathbf{A}_q^H(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q)$ must belong to the intersection between $\mathbb{Z}[\zeta_p]$ and $\mathbb{Z}[\zeta_q]$. However, Lemma 6 tells us that $\mathbb{Z}[\zeta_p] \cap \mathbb{Z}[\zeta_q] = \mathbb{Z}$. Hence, the entries of both

$\mathbf{A}_q^H(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q)$ and $\mathbf{A}_q^H(\bar{\mathbf{A}}_q - \widetilde{\mathbf{A}}_q)$ must be integers. Let

$$\begin{cases} a_{p1}^*(\bar{a}_{p1} - \tilde{a}_{p1}) + a_{p2}(\bar{a}_{p2}^* - \tilde{a}_{p2}^*) = k_1, \\ a_{p1}^*(\bar{a}_{p2} - \tilde{a}_{p2}) - a_{p2}(\bar{a}_{p1}^* - \tilde{a}_{p1}^*) = k_2, \end{cases} \tag{A.18a}$$

and

$$\begin{cases} a_{q1}^*(\bar{a}_{q1} - \tilde{a}_{q1}) + a_{q2}(\bar{a}_{q2}^* - \tilde{a}_{q2}^*) = k_1, \\ a_{q1}^*(\bar{a}_{q2} - \tilde{a}_{q2}) - a_{q2}(\bar{a}_{q1}^* - \tilde{a}_{q1}^*) = k_2, \end{cases} \tag{A.18b}$$

where both k_1 and k_2 are rational integers. For discussion clarity, let $\bar{x}_1 = a_{p1}^*\bar{a}_{p1} = \exp\left(\frac{j2\bar{\ell}_{p1}\pi}{p}\right), \tilde{x}_1 = a_{p1}^*\tilde{a}_{p1} = \exp\left(\frac{j2\tilde{\ell}_{p1}\pi}{p}\right), \bar{x}_2 = a_{p2}\bar{a}_{p2}^* = \exp\left(\frac{j2\bar{\ell}_{p2}\pi}{p}\right)$, $\tilde{x}_2 = a_{p2}\tilde{a}_{p2}^* = \exp\left(\frac{j2\tilde{\ell}_{p2}\pi}{p}\right), a_{p1}^*a_{p2} = \exp\left(\frac{j2\ell_p\pi}{p}\right)$ and $\bar{y}_1 = a_{q1}^*\bar{a}_{q1} = \exp\left(\frac{j2\bar{\ell}_{q1}\pi}{q}\right), \tilde{y}_1 = a_{q1}^*\tilde{a}_{q1} = \exp\left(\frac{j2\tilde{\ell}_{q1}\pi}{q}\right), \bar{y}_2 = a_{q2}\bar{a}_{q2}^* = \exp\left(\frac{j2\bar{\ell}_{q2}\pi}{q}\right), \tilde{y}_2 = a_{q2}\tilde{a}_{q2}^* = \exp\left(\frac{j2\tilde{\ell}_{q2}\pi}{q}\right), a_{q1}^*a_{q2} = \exp\left(\frac{j2\ell_q\pi}{q}\right)$. Then, (A.18a) and (A.18b) are reduced, respectively, into

$$\begin{cases} (\bar{x}_1 - \tilde{x}_1) + (\bar{x}_2 - \tilde{x}_2) = k_1, \\ (\bar{x}_1 - \tilde{x}_1) - (\bar{x}_2 - \tilde{x}_2) = -k_2 \exp\left(\frac{j2\ell_p\pi}{p}\right), \end{cases}$$

and

$$\begin{cases} (\bar{y}_1 - \tilde{y}_1) + (\bar{y}_2 - \tilde{y}_2) = k_1, \\ (\bar{y}_1 - \tilde{y}_1) - (\bar{y}_2 - \tilde{y}_2) = -k_2 \exp\left(\frac{j2\ell_q\pi}{q}\right). \end{cases}$$

Therefore, $\bar{x}_1-\tilde{x}_1, \bar{x}_2-\tilde{x}_2$ and $\bar{y}_1-\tilde{y}_1, \bar{y}_2-\tilde{y}_2$ can be expressed in terms of $k_1, k_2, e^{j\theta}, \exp\left(\frac{j2\ell_p\pi}{p}\right)$ and $\exp\left(\frac{j2\ell_q\pi}{q}\right)$, respectively, as

$$\begin{cases} \bar{x}_1 - \tilde{x}_1 = \frac{k_1 - k_2 \exp\left(\frac{j2\ell_p\pi}{p}\right)}{2}, \\ \bar{x}_2 - \tilde{x}_2 = \frac{k_1 + k_2 \exp\left(\frac{j2\ell_p\pi}{p}\right)}{2}, \end{cases} \tag{A.19}$$

and

$$\begin{cases} \bar{y}_1 - \tilde{y}_1 = \frac{k_1 - k_2 \exp\left(\frac{j2\ell_q\pi}{q}\right)}{2}, \\ \bar{y}_2 - \tilde{y}_2 = \frac{k_1 + k_2 \exp\left(\frac{j2\ell_q\pi}{q}\right)}{2}. \end{cases} \tag{A.20}$$

As a result, we can have

$$\begin{aligned} |\bar{x}_1 - \tilde{x}_1|^2 + |\bar{x}_2 - \tilde{x}_2|^2 &= \frac{k_1^2 + k_2^2}{2}, \\ |\bar{y}_1 - \tilde{y}_1|^2 + |\bar{y}_2 - \tilde{y}_2|^2 &= \frac{k_1^2 + k_2^2}{2}. \end{aligned}$$

These, after using the properties of the PSK signals, can be equivalently rewritten as

$$\begin{aligned} &2\cos\left(\frac{2(\bar{\ell}_{p1} - \tilde{\ell}_{p1})\pi}{p}\right) + 2\cos\left(\frac{2(\bar{\ell}_{p2} - \tilde{\ell}_{p2})\pi}{p}\right) \\ &= 2\cos\left(\frac{2(\bar{\ell}_{q1} - \tilde{\ell}_{q1})\pi}{q}\right) + 2\cos\left(\frac{2(\bar{\ell}_{q2} - \tilde{\ell}_{q2})\pi}{q}\right) = \Delta, \end{aligned} \tag{A.21}$$

where $\Delta = \frac{8-(k_1^2+k_2^2)}{2}$. Notice the fact that if $e^{j\theta}$ is a r-PSK signal, then, $e^{-j\theta}$ is also a r-PSK signal and thus, $2\cos\theta = e^{j\theta} + e^{-j\theta}$ belongs to the ring $\mathbb{Z}[\zeta_r]$. Combining this fact with (A.21) and Property 6 gives us that $\Delta \in \mathbb{Z}[\zeta_p] \cap \mathbb{Z}[\zeta_q] = \mathbb{Z}$, which means that Δ is a rational integer. Hence, $k_1^2 + k_2^2$ must be even, implying that k_1 and k_2 are both odd or both even. In addition, since $|2\cos(\bar{\alpha} - \widetilde{\alpha}) + 2\cos(\bar{\beta} - \widetilde{\beta}))| \leq 4$, we

have $-4 \leq \Delta \leq 4$, which is equivalent to $k_1^2 + k_2^2 \leq 16$. Therefore, we need to only consider the following possibilities of k_1 and k_2:

1. Both k_1 and k_2 are even. In this case, we examine fours sub-situations below:

   (a) $k_1 = \pm 4, k_2 = 0$ or $k_1 = 0, k_2 = \pm 4$. Then, from (A.21) we know that

   $$\begin{aligned} &2\cos\left(\frac{2(\bar{\ell}_{p1} - \tilde{\ell}_{p1})\pi}{p}\right) + 2\cos\left(\frac{2(\bar{\ell}_{p2} - \tilde{\ell}_{p2})\pi}{p}\right) \\ &= 2\cos\left(\frac{2(\bar{\ell}_{q1} - \tilde{\ell}_{q1})\pi}{q}\right) + 2\cos\left(\frac{2(\bar{\ell}_{q2} - \tilde{\ell}_{q2})\pi}{q}\right) = -4. \quad \text{(A.22)} \end{aligned}$$

   Since $\cos x \geq -1$, where the equality holds if and only if $x = (2k + 1)\pi$ for $k \in \mathbb{Z}$, combining this with (A.22) results in $\cos\left(\frac{2(\bar{\ell}_{pi} - \tilde{\ell}_{pi})\pi}{p}\right) = \cos\left(\frac{2(\bar{\ell}_{qi} - \tilde{\ell}_{qi})\pi}{q}\right) = -1$ for $i = 1, 2$. Thus, there are four rational integers k_{pi} and k_{qi} for $i = 1, 2$ such that $2(\bar{\ell}_{pi} - \tilde{\ell}_{pi}) = (2k_{pi} + 1)p$ and $2(\bar{\ell}_{pi} - \tilde{\ell}_{pi}) = (2k_{qi} + 1)q$. As a consequence, 2 must be a common factor of p and q, which is impossible, since it is already assumed that $\gcd(p, q) = 1$.

   (b) $k_1 = k_2 = 0$. Then, from (A.19) and (A.20) we have $\bar{x}_1 = \tilde{x}_1, \bar{x}_2 = \tilde{x}_2$ and $\bar{y}_1 = \tilde{y}_1, \bar{y}_2 = \tilde{y}_2$, which means $\bar{a}_{p1} = \tilde{a}_{p1}, \bar{a}_{p2} = \tilde{a}_{p2}$ and $\bar{a}_{q1} = \tilde{a}_{q1}, \bar{a}_{q2} = \tilde{a}_{q2}$.

   (c) $k_1 = \pm 2$ and $k_2 = \pm 2$. In this case, $\Delta = 0$ and thus, (A.21) is reduced into $\cos\left(\frac{2(\bar{\ell}_{p1} - \tilde{\ell}_{p1})\pi}{p}\right) + \cos\left(\frac{2(\bar{\ell}_{p2} - \tilde{\ell}_{p2})\pi}{p}\right) = \cos\left(\frac{2(\bar{\ell}_{q1} - \tilde{\ell}_{q1})\pi}{q}\right) + \cos\left(\frac{2(\bar{\ell}_{q2} - \tilde{\ell}_{q2})\pi}{q}\right) = 0$, which is equivalent to the fact that there are two integers $k_p, k_q \in \mathbb{Z}$ such that $\frac{2(\bar{\ell}_{p1} - \tilde{\ell}_{p1})\pi}{p} = (2k_p + 1)\pi \pm \frac{2(\bar{\ell}_{p2} - \tilde{\ell}_{p2})\pi}{p}$ and $\frac{2(\bar{\ell}_{q1} - \tilde{\ell}_{q1})\pi}{q} = (2k_q + 1)\pi \pm \frac{2(\bar{\ell}_{q2} - \tilde{\ell}_{q2})\pi}{q}$. This infers that 2 must be a common factor of p and q, which cannot happen either.

   (d) $k_1 = 0, k_2 = \pm 2$ or $k_1 = \pm 2, k_2 = 0$. In this case, substituting k_1 and k_2

into (A.19) and (A.20) yields either

$$\begin{cases} \bar{x}_1 - \tilde{x}_1 = \mp \exp\left(\frac{j2\ell_p\pi}{p}\right), \\ \bar{x}_2 - \tilde{x}_2 = \pm \exp\left(\frac{j2\ell_p\pi}{p}\right), \end{cases} \tag{A.23}$$

$$\begin{cases} \bar{y}_1 - \tilde{y}_1 = \mp \exp\left(\frac{j2\ell_q\pi}{q}\right), \\ \bar{y}_2 - \tilde{y}_2 = \pm \exp\left(\frac{j2\ell_q\pi}{q}\right), \end{cases} \tag{A.24}$$

or

$$\begin{cases} \bar{x}_1 - \tilde{x}_1 = \pm 1, \\ \bar{x}_2 - \tilde{x}_2 = \pm 1, \end{cases} \tag{A.25}$$

$$\begin{cases} \bar{y}_1 - \tilde{y}_1 = \pm 1, \\ \bar{y}_2 - \tilde{y}_2 = \pm 1. \end{cases} \tag{A.26}$$

No mater whatever cases arise, we can always obtain that $|\bar{x}_i - \tilde{x}_i| = |\bar{y}_i - \tilde{y}_i| = 1$ for $i = 1, 2$, which is equivalent to the fact that $\left|2\sin\frac{(\bar{\ell}_{pi}-\tilde{\ell}_{pi})\pi}{p}\right| = \left|2\sin\frac{(\bar{\ell}_{qi}-\tilde{\ell}_{qi})\pi}{p}\right| = 1$. In other words, there are four integers $\check{k}_{pi}, \check{k}_{qi} \in \mathbb{Z}$ such that $\frac{(\bar{\ell}_{pi}-\tilde{\ell}_{pi})\pi}{p} = \check{k}_{pi}\pi \pm \pi/6$ and $\frac{(\bar{\ell}_{qi}-\tilde{\ell}_{qi})\pi}{q} = \check{k}_{qi}\pi \pm \pi/6$. Hence, 6 must be a common factor of p and q, which is impossible due to the fact that $\gcd(p, q) = 1$.

2. Both k_1 and k_2 are odd. In this case, extracting the real parts from (A.19)

and (A.20) gives us, respectively,

$$\cos\frac{2\bar{\ell}_{p1}\pi}{p} - \cos\frac{2\tilde{\ell}_{p1}\pi}{p} = \frac{k_1 + k_2\cos\frac{2\ell_p\pi}{p}}{2}, \tag{A.27a}$$

$$\cos\frac{2\bar{\ell}_{q1}\pi}{q} - \cos\frac{2\tilde{\ell}_{q1}\pi}{q} = \frac{k_1 + k_2\cos\frac{2\ell_q\pi}{q}}{2}. \tag{A.27b}$$

Notice that (A.27) can be represented by

$$\cos\frac{2\ell_p\pi}{p} = 2\cos\frac{2\bar{\ell}_{p1}\pi}{p} - 2\cos\frac{2\tilde{\ell}_{p1}\pi}{p} - k_1 - (k_2-1)\cos\frac{2\ell_p\pi}{p}, \tag{A.28a}$$

$$\cos\frac{2\ell_q\pi}{q} = 2\cos\frac{2\bar{\ell}_{q1}\pi}{q} - 2\cos\frac{2\tilde{\ell}_{q1}\pi}{q} - k_1 - (k_2-1)\cos\frac{2\ell_q\pi}{q}. \tag{A.28b}$$

Since k_2 is odd, $k_2 - 1$ is an even number. In addition, as we have mentioned above, if $e^{j\theta}$ is a r-PSK signal, then, $e^{-j\theta}$ is also a r-PSK signal and thus, $2\cos\theta = e^{j\theta} + e^{-j\theta}$ belongs to the ring $\mathbb{Z}[\zeta_r]$. Combing this fact with (A.28), we can conclude $\cos\frac{2\ell_p\pi}{p} \in \mathbb{Z}[\zeta_p]$ and $\cos\frac{2\ell_q\pi}{q} \in \mathbb{Z}[\zeta_q]$. Let σ_{p,m_p} and σ_{q,m_q} be the respective $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_q)$, where $\gcd(p, m_p) = \gcd(q, m_q) = 1$ for $1 \le m_p \le p$ and $1 \le m_q \le q$. From Section 6.1, we know that $\sigma_{p,m_p}(\zeta_p) = \zeta_p^{m_p}$ and $\sigma_{q,m_q}(\zeta_p) = \zeta_q^{m_q}$. Then,

$$\begin{aligned}
\sigma_{p,m_p}\Big(\cos\frac{2\ell_p\pi}{p}\Big) &= \frac{\sigma_{p,m_p}\big(e^{j\frac{2\ell_p\pi}{p}}\big) + \sigma_{p,m_p}\big(e^{-j\frac{2\ell_p\pi}{p}}\big)}{2} \\
&= \frac{e^{j\frac{2\ell_p m_p\pi}{p}} + e^{-j\frac{2\ell_p m_p\pi}{p}}}{2} = \cos\frac{2\ell_p m_p\pi}{p}, \\
\sigma_{q,m_q}\Big(\cos\frac{2\ell_q\pi}{q}\Big) &= \frac{\sigma_{q,m_q}\big(e^{j\frac{2\ell_q\pi}{q}}\big) + \sigma_{q,m_q}\big(e^{-j\frac{2\ell_q\pi}{q}}\big)}{2} \\
&= \frac{e^{j\frac{2\ell_q m_q\pi}{q}} + e^{-j\frac{2\ell_q m_q\pi}{q}}}{2} = \cos\frac{2\ell_q m_q\pi}{q}.
\end{aligned}$$

By Property 11, the norms of both $\cos\frac{2\ell_p\pi}{p}$ and $\cos\frac{2\ell_q\pi}{q}$ must be rational integers, i.e.,

$$N_{\mathbb{Z}[\zeta_p]/\mathbb{Z}}\Big(\cos\frac{2\ell_p\pi}{p}\Big) = \prod_{\sigma_{p,m_p}\in\mathrm{Gal}(\mathbb{Q}_p)} \sigma_{p,m_p}\Big(\cos\frac{2\ell_p\pi}{p}\Big) = \prod_{k=1,\gcd(p,m_p)=1}^{p} \cos\frac{2\ell_p m_p\pi}{p} \in \mathbb{Z},$$

$$N_{\mathbb{Z}[\zeta_q]/\mathbb{Z}}\Big(\cos\frac{2\ell_q\pi}{q}\Big) = \prod_{\sigma_{q,m_q}\in\mathrm{Gal}(\mathbb{Q}_q)} \sigma_{q,m_q}\Big(\cos\frac{2\ell_q\pi}{q}\Big) = \prod_{k=1,\gcd(q,m_q)=1}^{q} \cos\frac{2\ell_q m_q\pi}{q} \in \mathbb{Z}.$$

As a result, either $\cos\frac{2\ell_p m_p\pi}{p} = \pm 1$ for all m_p or there exists at least one m_p, say m_{p0}, such that $\cos\frac{2\ell_p m_{p0}\pi}{p} = 0$, and either $\cos\frac{2\ell_q m_q\pi}{q} = \pm 1$ for all m_q or there exists at least one m_q, say m_{q0}, such that $\cos\frac{2\ell_q m_{q0}\pi}{q} = 0$. Therefore, we need to examine the following four cases.

(a) $\cos\frac{2\ell_p m_{p0}\pi}{p} = \cos\frac{2\ell_q m_{q0}\pi}{q} = 0$. In this case, we can arrive at the fact that both p and q are even.

(b) $\cos\frac{2\ell_p m_{p0}\pi}{p} = 0$ and $\cos\frac{2\ell_q m_q\pi}{q} = \pm 1$. We already know that $\cos\frac{2\ell_p m_{p0}\pi}{p} = 0$ gives us that p must be even. In addition, if $\cos\frac{2\ell_q m_q\pi}{q} = -1$, we can also derive that q must be even too. If $\cos\frac{2\ell_q m_q\pi}{q} = 1$, then, ℓ_q must be a multiple of q, since each m_q is coprime to q. Thus, $\exp\big(\frac{j2\ell_q\pi}{q}\big) = 1$. Applying this to (A.20) yields $\bar{y}_1 - \tilde{y}_1 = \frac{k_1-k_2}{2}$, from which we can derive that the imaginary part of $\bar{y}_1 - \tilde{y}_1$, $-2\sin\frac{(\tilde{\ell}_{q1}-\bar{\ell}_{q1})\pi}{q}\cos\frac{(\bar{\ell}_{q1}+\tilde{\ell}_{q1})\pi}{q}$, must be equal to zero, i.e., $\sin\frac{\bar{\ell}_{q1}\pi}{q}\cos\frac{(\bar{\ell}_{q1}+\tilde{\ell}_{q1})\pi}{q} = 0$. This results in the fact that either $\sin\frac{\bar{\ell}_{q1}\pi}{q} = 0$ or $\cos\frac{(\bar{\ell}_{q1}+\tilde{\ell}_{q1})\pi}{q} = 0$. No matter which case occurs, q must be even.

(c) $\cos\frac{2\ell_p m_p\pi}{p} = \pm 1$ and $\cos\frac{2\ell_q m_{q0}\pi}{q} = 0$. Similar to the discussion on the above Case b), we can arrive at the same result that both p and q must be even.

(d) $\cos\frac{2\ell_p m_p \pi}{p} = \pm 1$ and $\cos\frac{2\ell_q m_q \pi}{q} = \pm 1$. Following the discussion much similar to the Case b) when $\cos\frac{2\ell_q m_q \pi}{q} = \pm 1$, we can attain that both p and q must be even.

Al the above four situations eventually leads us to making the same conclusion that both p and q are even, which is impossible due to the assumption of $\gcd(p, q) = 1$.

Until here, we have proved that only one possible case for k_1 and k_2 to make (A.17) hold is the case when $k_1 = k_2 = 0$, which is equivalent to $\bar{a}_{p1} = \tilde{a}_{p1}, \bar{a}_{p2} = \tilde{a}_{p2}$ and $\bar{a}_{q1} = \tilde{a}_{q1}, \bar{a}_{q2} = \tilde{a}_{q2}$, i.e., $\bar{\mathbf{A}}_p = \widetilde{\mathbf{A}}_p$ and $\bar{\mathbf{A}}_q = \widetilde{\mathbf{A}}_q$. This completes the proof of Proposition 7. $\square$

Bibliography

[1] I. Teletar, "Capacity of multi-antenna Gaussian channels," *AT & T Bell Labs, Tech. Rep.*, June. 1995.

[2] G. J. Foschini and M. J. Gans, "On limits of wireless communications in fading environments when using multiple antennae," *Wireless Personal Communications*, vol. 6, pp. 311–335, March 1998.

[3] A. L. Moustakas, "Communication through a diffusive medium: Coherence and capacity," *Science*, vol. 287, pp. 287–290, Jan. 2000.

[4] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high date rate wireless communication: performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[5] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1804–1824, Jul. 2002.

[6] R. W. Heath and A. J. Paulraj, "Linear dispersion codes for MIMO systems based on frame theory," *IEEE Trans Signal Processing*, vol. 50, pp. 2429–2441, Oct. 2002.

[7] H. E. Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Inform. Theory*, vol. 49, pp. 1097–1119, May. 2003.

[8] X. Ma and G. B. Giannakis, "Full-diversity full rate complex-field space-time coding," *IEEE Trans. Signal Processing*, vol. 51, pp. 2917–2930, Nov. 2003.

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

[10] J.-K. Zhang, J. Liu, and K. M. Wong, "Trace-orthonormal full diversity cyclotomic space-time codes," *IEEE Trans. Signal Processing*, vol. 55, pp. 618–630, Feb. 2007.

[11] H. Yao and G. W. Wornell, "Achieving the full MIMO diversity-vs-multiplexing frontier with rotation-based space-time codes," in *41th Annual Allerton Conf. on Comm. Control, and Comput.*, Monticello, IL, Oct. 2003.

[12] P. Dayal and M. K. Varanasi, "An optimal two transmit antenna space-time code and its stacked extensions," *IEEE Trans. Inform. Theory*, vol. 51, pp. 4348–4355, Dec 2005.

[13] J. C. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proceedings IEEE of ITW2003*, Paris, France, March 2003.

[14] J. C. Belfiore, G. R. Rekaya, and E. Viterbo, "The Golden code: A 2×2 full rate space-time code with non-vanishing determinants," *IEEE Trans. Inform. Theory*, vol. 51, pp. 1432–1436, Apr. 2005.

[15] G. Rekaya, J. C. Belfiore, and E. Viterbo, "Algebraic 3×3, 4×4 and 6×6 space-time codes with non-vanishing determiants," in *ISITA*, Parma, Italy, Oct. 2004.

[16] G. Wang and X.-G. Xia, "On optimal multi-layer cyclotomic space-time code designs," *IEEE Trans. Inform. Theory*, vol. 51, pp. 1102–1135, Mar. 2005.

[17] G.-Y. Wang, J.-K. Zhang, M. Amin, and K. M. Wong, "Space-time code design with non-vanishing determinants based on cyclic field extension families," *IEEE Trans. Inform. Theory, submitted for publication*, Aug. 2004.

[18] J.-K. Zhang, G.-Y. Wang, and K. M. Wong, "Optimal norm form integer space-time codes for two antenna MIMO systems," in *Int. Conf. Acoust., Speech, Signal Process.*, Philadelphia, USA, March 2005.

[19] G.-Y. Wang, J.-K. Zhang, Y. Zhang, and K. M. Wong, "Space-time code designs with non-vanishing determinants based on cyclic field extension families," in *Int. Conf. Acoust., Speech, Signal Process.*, Philadelphia, USA, March 2005.

[20] T. Kiran and B. S. Rajan, "STBC-schemes with nonvanishing determinant for certain number of transmit antennas," *IEEE Trans. Inform. Theory*, vol. 51, pp. 2984–2992, Aug. 2005.

[21] F. E. Oggier, G. Rekaya, J.-C. Belfiore, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inform. Theory*, vol. 52, pp. 3885–3902, Sep. 2006.

[22] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inform. Theory*, vol. 52, pp. 3869–3884, Sep. 2006.

[23] H. Liao and X.-G. Xia, "Some designs of full rate space time codes with nonvanishing determinant," *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2898–2908, Aug 2007.

[24] J. Liu, J.-K. Zhang, and K. M. Wong, "Full diversity codes for MISO systems equipped with linear or ML detectors," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4511–4527, Oct. 2008.

[25] Y. Shang and X.-G. Xia, "Space-time block codes achieving full diversity with linear receivers," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4528–4547, Oct. 2008.

[26] S. M. Alamouti, "A simple transmit diversity scheme for wireless commincations," *IEEE J. Select. Areas Commun*, vol. 16, pp. 1451–1458, Oct. 1998.

[27] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1456–1467, July. 1999.

[28] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space-time codes for complex signal constellations," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1122–1126, Feb. 2002.

[29] X.-B. Liang, "Orthogonal designs with maximal rates," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2468–2503, Oct. 2003.

[30] C. Yuen, Y. L. Guan, and T. T. Tjhuang, "Quasi-orthogonal STBC with minimum decoding complexity," *IEEE Trans. Wireless Commun.*, vol. 4, pp. 2089–2094, Sept. 2005.

[31] S. Karmakar and B. S. Rajan, "Multi-group quasi-orthogonal STBCs from clifford algebras," *IEEE Trans. Inform. Theory*, vol. 55, p. 223 231, Jan. 2009.

[32] D. N. Dao, C. Yuen, C. Tellambura, Y. L. Guan, and T. T. Tjhung, "Four-group decodable space-time block codes," *IEEE Trans. Signal Processing*, vol. 56, pp. 424–430, Jan. 2008.

[33] G. S. Rajan and B. S. Rajan, "Multigroup ML decodable collocated and distributed space-time block codes," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3221–3247, July 2010.

[34] S. Sezginer and H. Sari, "A full-rate full-diversity 2×2 space-time code for mobil WiMAX systems," in *Proc. IEEE 6th Int. Conf. Signal Processing and Communications*, Dubai, Nov. 2007.

[35] J. Paredes, A. B. Gershman, and M. G. Alkhansari, "A new full-rate full-diversity space-time block code with non-vanishing determinants and simplified maximum liklihood decoding," *IEEE Trans. Signal Processing*, vol. 56, pp. 2461–2469, June 2008.

[36] E. Biglieri, Y. Yong, and E. Viterbo, "On fast-decodable space-time block codes," *IEEE Trans. Inform. Theory*, vol. 55, pp. 524–530, Feb. 2009.

[37] S. Sirinaunpiboon, R. A. Clderbank, and S. D. Howard, "Fast essentially maximum likelihood decoding of the Golden code," *IEEE Trans. Inform. Theory*, vol. 57, pp. 3537–3541, June 2011.

[38] X. Guo and X.-G. Xia, "On full diversity space-time block codes with partial interference cancellation group decoding," *IEEE Trans. Inform. Theory*, vol. 55, pp. 4366–4385, Oct. 2009.

[39] T. Xu and X.-G. Xia, "On space-time code design with a conditional pic group decoding," *IEEE Trans. Inform. Theory*, vol. 57, pp. 3582–3593, June 2011.

[40] S. Sandhu and A. J. Paulraj, "Space-time block coding: A capacity perspective," *IEEE Commun. Letters*, vol. 4, pp. 384–386, Dec. 2000.

[41] T. L. Marzetta, "BLAST training: estimation channel characteristics for high-capacity space-time wireless," in *Proc. 37th Annu. Allerton Conf. Communications, Control, and Computing*, Sept. 22-24 1999.

[42] B. Hassibi and B. M. Hochwald, "How much training is needed in multiple-antenna wireless links?" *IEEE Trans. Inform. Theory*, vol. 49, pp. 951–963, Apr. 2003.

[43] L. Zheng and D. N. C. Tse, "Communication on the Grassmann manifold: a geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inform. Theory*, vol. 48, pp. 359–383, Feb. 2002.

[44] J. S. Richters, *"Communication over fading dispersive channels"*. MIT Res. Lab. Electronics, Cambridge, MA, Tech. Rep. 464, Nov. 30, 1967.

[45] I. Abou-Faycal, M. D. Trott, and S. Shamai, "The capacity of discrete-time memoryless Rayleigh-fading channels," *IEEE Trans. Inform. Theory*, vol. 47, pp. 1290–1301, May 2001.

[46] M. C. Gursoy, H. V. Poor, and S. Verdu, "The noncoherent Rician fading channelPart I: structure of the capacity-achieving input," *IEEE Trans. Wireless Commun.*, vol. 4, pp. 2193–2206, Sept. 2005.

[47] ——, "Noncoherent Rician fading channelPart II: spectral efficiency in the low-power regime," *IEEE Trans. Wireless Commun.*, vol. 4, pp. 2207–2221, Sept. 2005.

[48] J. Huang and S. P. Meyn, "Characterization and computation of optimal distribution for channel coding," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.

[49] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Trans. Inform. Theory*, vol. 46, pp. 543–564, Mar. 2000.

[50] B. Hughes, "Differential space-time modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2567–2578, Nov. 2000.

[51] B. M. Hochwald and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Commun.*, vol. 48, pp. 2041–2052, Dec. 2000.

[52] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE Journal on Select. Areas Commun.*, vol. 18, pp. 1169–1174, Jul. 2000.

[53] A. Shokrollahi, B. Hassibi, B. M. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2335–2367, Sept. 2001.

[54] B. Hassibi and B. M. Hochwald, "Cayley differential unitary space-time codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1485–1503, June 2002.

[55] B. M. Hochwald, T. L. Marzetta, T. J. Richardson, W. Sweldens, and R. Urbanke, "Systematic design of unitary space-time constellations," *IEEE Trans. Inform. Theory*, vol. 46, pp. 1962–1973, June 2000.

[56] T. L. Marzetta, B. Hassibi, and B. M. Hochwald, "Structured unitary space-time autocoding constellations," *IEEE Trans. Inform. Theory*, vol. 48, pp. 942–950, Apr. 2002.

[57] G. Ganesan and P. Stoica, "Differential modulation using space-time block codes," *IEEE Signal Processing Letters*, vol. 9, no. 2, pp. 57–59, Feb. 2002.

[58] Y. Jing and B. Hassibi, "Unitary space-time modulation via Cayley transformation," *IEEE Trans. Signal Processing*, vol. 51, pp. 2891–2904, Nov. 2003.

[59] X.-B. Liang and X.-G. Xia, "Fast differential unitary space-time demodulation via square orthogonal designs," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1331–1336, July 2005.

[60] A. L. Swindlehurst and G. Leus, "Blind and semi-blind equalization for generalized space-time block codes," *IEEE Trans. Signal Processing*, vol. 50, pp. 2489–2498, Oct. 2002.

[61] P. Stoica and G. Ganesan, "Space-time block codes: trained, blind and semi-blind detection," *Digital Signal Processing*, vol. 13, pp. 93–105, Jan. 2003.

[62] E. G. Larsson, P. Stoica, and J. Li, "Space-time block codes: maximum likelihood detection for unknown channels and unstructured interference," *IEEE Trans. Signal Processing*, vol. 51, pp. 362–372, Feb. 2003.

[63] S. Shahbazpanahi, A. B. Gershman, and J. H. Manton, "Closed-form blind MIMO channel estimation for orthogonal space-time block codes," *IEEE Trans. Signal Processing*, vol. 53, pp. 4506–4517, Dec. 2005.

[64] W.-K. Ma, B.-N. Vo, T. N. Davidson, and P. C. Ching, "Blind ML detection of orthogonal space-time block codes: efficient, high-performance implementations," *IEEE Trans. Signal Processing*, vol. 54, pp. 738–751, Feb. 2006.

[65] V. Tarokh and I.-M. Kim, "Existence and construction of noncoherent unitary space-time codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 3112–3117, Dec. 2002.

[66] M. M. McCloud, M. Brehler, and M. K. Varanasi, "Signal design and convolutional coding for noncoherent space-time communication on the block-Rayleigh-fading channel," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1186–1194, May 2002.

[67] D. Warrier and U. Madhow, "Spectrally efficient noncoherent communication," *IEEE Trans. Inform. Theory*, vol. 48, pp. 651–668, March 2002.

[68] W. Zhao, G. Leus, and G. Giannakis, "Orthogonal design of unitary constellations for uncoded and trellis coded non-coherent space-time systems," *IEEE Trans. Inform. Theory*, vol. 50, pp. 1319–1327, June 2004.

[69] I. Kammoun and J. C. Belfiore, "A new family of Grassmann space-time codes for non-coherent MIMO systems," *IEEE Commun. Letters*, vol. 7, pp. 528–530, Nov. 2003.

[70] T. Marzetta and B. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat-fading," *IEEE Trans. Inform. Theory*, vol. 45, pp. 139–157, Jan. 1999.

[71] M. Brehler and M. K. Varanasi, "Asymptotic error probability analysis of quadratic receiver in Rayleigh-fading channels with applications to a unified analysis of coherent and noncoherent space-time receivers," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2383–2399, Sept. 2001.

[72] R. H. Gohary and T. N. Davidson, "Non-coherent MIMO communication: Grassmannian constellation and efficient detection," in *IEEE Trans. Inform. Theory*, vol. 55, pp. 1176–1205, March 2009.

[73] F. Oggier and B. Hassibi, "Algebraic differential Cayley space-time codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1911–1919, May 2007.

[74] T. Cai and C. Tellambura, "Efficient blind receiver design for orthogonal space-time block codes," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1890–1899, May 2007.

[75] J.-K. Zhang and W.-K. Ma, "Full diversity blind Alamouti space-time block codes for unique identification of flat fading channels," *IEEE Trans. Signal Processing*, vol. 57, pp. 635–644, Feb. 2009.

[76] L. Zhou, J.-K. Zhang, and K. M. Wong, "A novel signaling scheme for blind unique identification of Alamouti space-time block coded channel," *IEEE Trans. Signal Processing*, vol. 55, pp. 2570–2582, June 2007.

[77] J.-K. Zhang and C. Yuen, "Full diversity blind signal designs for unique identification of frequency selective channels," *CoRR*, vol. abs/0805.3118, 2008.

[78] G. D. Forney and L.-F. Wei, "Multidimensional constellations–Part I: Introduction, figures of merit, and generalized cross constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, pp. 877–892, Aug. 1989.

[79] G. H. Golub and V. Pereyra, "The differentiation of pseudo-inverses and nonlinear least squares problems whose variables separate," *SIAM J. Num. Anal.*, vol. 10, pp. 413–432, 1973.

[80] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2148–2177, Oct. 1998.

[81] G. D. Forney, "Coset codes–Part I: Introduction and geometrical classification," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1123–1151, Sept. 1988.

[82] ——, "Coset codes–Part II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152–1187, Sept. 1988.

[83] ——, "Multidimensional constellations–Part II: Voronoi constellations," *IEEE Journal on Selected Areas in Communications*, vol. 7, pp. 941–958, Aug. 1989.

[84] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*. New York: Springer-Verlag, 1998.

[85] G. D. Forney and G. U. Ungerboeck, "Modulation and coding for linear Gaussian channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2384–2415, May 1998.

[86] R. G. Gallager, *Principles of Digital Communications.* Cambridge: Cambridge University Press, 2008.

[87] P. Morandi, *Field and Galois Theory.* New York: Springer, 1996.

[88] X. Giraud and J. C. Belfiore, "Constellations matched to the Rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol. 42, pp. 106–115, Jan. 1996.

[89] ——, "Algebraic tools build modulation schemes for fading channels," *IEEE Trans. Inform. Theory*, vol. 43, pp. 938–952, May 1997.

[90] L.-K. Hua, *Introduction to Number Theory.* Berlin ; New York: Springer-Verlag, 1982.

[91] G. Golub and C. F. V. Loan, *Matrix Computations (The third edition).* 2715 North Charles street, Baltimore Maryland: The John Hopkins University Press, 1996.

[92] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.

[93] P. Dayal, M. Brehler, and M. K. Varanasi, "Leveraging coherent space-time codes for noncoherent communication via training," *IEEE Trans. Inform. Theory*, vol. 50, no. 9, pp. 2058–2080, Sept 2004.