Blind Unique Channel Identification of Alamouti Space-Time Coded Channel via a Signalling Scheme

BLIND UNIQUE CHANNEL IDENTIFICATION OF ALAMOUTI SPACE-TIME CODED CHANNEL VIA A SIGNALLING SCHEME

By

LIN ZHOU, Bachelor of Eng. (Automatic Control)
Xidian University, Xi'an, China, 1999
Master of Eng. (Circuit and System)
Xidian University, Xi'an, China, 2002

A Thesis
Submitted to the School of Graduate Studies
in Partial Fulfilment of the Requirements
for the Degree
Master of Applied Science

McMaster University
December 2005

MASTER OF APPLIED SCIENCE (2006) MCMASTER UNIVERSITY

(Electrical and Computer Engineering) Hamilton, Ontario

TITLE: **Blind Unique Channel Identification of Alamouti Space-Time Coded Channel via a Signalling Scheme**

AUTHOR: Lin Zhou

Bachelor of Eng. (Automatic Control)

Xidian University, Xi'an, China, 1999

Master of Eng. (Circuit and System)

Xidian University, Xi'an, China, 2002

SUPERVISOR: Dr. Kon Max Wong

NUMBER OF PAGES: xii, 92

To my parents and Dong Xue

for their everlasting love and encouragement

Abstract

In this thesis, we present a novel signalling scheme for blind channel identification of Alamouti space-time coded (STBC) channel and a space-time coded multiple-input single-output (MISO) system under flat fading environment. By using p-ary and q-ary PSK signals (where p and q are co-prime integers), we prove that a) under a noise-free environment, only two distinct pairs of symbols are needed to uniquely decode the signal and identify the channel, and b) under complex Gaussian noise, if the pth and qth order statistics of the received signals are available, the channel coefficients can also be uniquely determined. In both cases, simple closed-form solutions are derived by exploiting specific properties of the Alamouti STBC code and linear Diophantine equation theory.

When only a limited number of received data are available, under Gaussian noise environment, we suggest the use of the semi-definite relaxation method and/or the sphere decoding method to implement blind ML detection so that the joint estimation of the channel and the transmitted symbols can be efficiently facilitated. Simulation results show that blind ML detection methods with our signalling scheme provide superior normalized mean square error in channel estimation compared to the method using only one constellation and that the average symbol error rate is close to that of the coherent detector (which necessitates perfect channel knowledge at the receiver), particularly when the SNR is high.

Acknowledgements

I would like to take this opportunity to thank my supervisor, Dr. Kon Max Wong, for his support, encouragement, and constructive guidance to my work.

I also thank Dr. Jian-Kang Zhang, for his inspiration, suggestion and patience to the completion of this project.

Thanks also to all members of the ASPC research group of McMaster University for their expertise and insightful discussions on this project, especially Dr. T. N. Davidson, for his organizing group study to provide me relative knowledge background of digital communication, and Dr. Zhi-Quan Luo, for helping me in some algorithm implementations.

I am grateful to the staff in our department, in particular Cheryl, Helen, Terry and Cosmin, whose efficient works help me out a lot of trouble.

Last but not least, I want to thank my parents (Wei Zhou and Zhen-Ning Ma) and Dong Xue for their endless love and support which played an instrumental role in my completing this project.

Abbreviations and Acronyms

MISO	Multiple-Input Single-Output
SISO	Single-Input Single-Output
STBC	Space-Time Block Code
Alamouti STBC	Alamouti Space-Time Block Coded
OSTBC	Orthogonal Space-Time Block Code
CSI	Channel State Information
DFT	Discrete Fourier Transform
IDFT	Inverse Discrete Fourier Transform
ML	Maximum Likelihood
PSK	Phase-Shift Keying
CM	Constant Modulus
p-PSK	p-ary PSK constellation
q-PSK	q-ary PSK constellation
QAM	Quadture Amplitude Modulation
M-QAM	M-ary QAM constellation
MSE	Mean Square Error
SER	Symbol Error Rate
SNR	Signal-to-Noise Ratio
PDF	Probability Distribution Function
PSD	Positive Semi-Definite

SDR	Semi-Definite Relaxation
BQP	Boolean Quadratic Programming
SE search	Schnorr-Euchner search
OFDM	Orthogonal Frequency Division Multiplexing

Notations

a	Scalar a, lowercase letter denotes scalar
$\mathbf{a}$	Vector $\mathbf{a}$, boldface lowercase letter denotes column vector
$\mathbf{A}$	Matrix $\mathbf{A}$, boldface uppercase letter denotes matrix
$(\cdot)^T$	the transpose of a vector or a matrix
$(\cdot)^*$	the conjugate of a scalar or a vector or a matrix
$(\cdot)^H$	the hermitian of a vector or a matrix
$(\cdot)^i$	the power i of a scalar or a matrix
$[\mathbf{a}]_i$ or a_i	the ith element of vector $\mathbf{a}$
$[\mathbf{A}]_{ij}$ or a_{ij}	the $(i,j)^{th}$ element of matrix $\mathbf{A}$
$\lvert\mathbf{A}\rvert$ or $\det(\mathbf{A})$	the determinant of matrix $\mathbf{A}$
$\text{vec}(\mathbf{A})$	the column vector obtained by stacking the columns of matrix $\mathbf{A}$
$\lvert a\rvert$	the absolute value of scalar a
$\lvert\lvert\mathbf{a}\rvert\rvert_2$	the Euclidean norm, defined as $\lvert\lvert\mathbf{a}\rvert\rvert_2^2 = \mathbf{a}^H\mathbf{a}$
$\lvert\lvert\mathbf{A}\rvert\rvert_F$	the Frobenius matrix norm, defined as $\lvert\lvert\mathbf{A}\rvert\rvert_F^2 = \text{tr}(\mathbf{A}\mathbf{A}^H)$
j	the imaginary unit, defined as $j^2 = -1$
$\mathbf{I}_m$	the $m \times m$ identity matrix
$\mathbf{A} \succeq 0$	$\mathbf{A}$ is a positive semi-definite matrix
$\mathbf{A} \succ 0$	$\mathbf{A}$ is a positive definite matrix
$\text{tr}(\mathbf{A})$	the sum of all diagonal elements of matrix $\mathbf{A}$

$\mathbb{C}$	the complex number set
$\mathbb{R}$	the real number set
$\mathbb{Z}^{\dagger}$	the positive integer set
$\mathcal{S}$	the constellation set
$\mathcal{A}$	the feasible set
$\exp(t)$	e^t
$\lceil x \rceil$	the greatest integer not exceeding x
$x \bmod N$	$x \bmod N$ denotes $x - N\lceil \frac{x}{N} \rceil$, $N \neq 0$
$\arg\min_x f(x)$	the minimizing argument of the function $f(x)$
$\arg(\cdot)$	the phase angle in an interval $0 \leq \arg(\cdot) < 2\pi$
$\mathrm{E}[\cdot]$	the statistical expectation operator
$s = \mathrm{Quant}(t)$	the quantization operator sets s to the element of $\mathcal{S}$
	that is closest (in terms of Euclidean distance) to t
$\mathrm{round}(x)$	the quantized integer closest to $x \in \mathbb{R}$
$\mathrm{sign}(x)$	1 if $x > 0$, and -1 if $x \leq 0$
M_{rand}	the number of randomization
$\gcd(m, n)$	the greatest common divisor of positive integers m and n
$\varphi(n)$	the Euler function; i.e., the number of all positive integers
	that do not exceed n and are prime to n
$\binom{m}{n}$	the binomial coefficient $\frac{m!}{n!(m-n)!}$
$m \vert n$	n is divisible by m
$n!$	$n(n-1)(n-2)\cdots 1$
$n!!$	$n(n-2)(n-4)\cdots 2$ (or 1), if n is even (or odd)

Contents

List of Figures

Chapter 1

Introduction

1.1 The Channel Estimation Problem

Wireless communication is a fast growing field in the communication industry because it has many applications, such as cellular mobile communication, multimedia transmission, wireless sensor networks, etc. With the explosive proliferation of personal computers, especially laptop and palmtop computers, many potential applications and services appear. As a result, reliable and high-speed information transmission through wireless communication systems is required.

In wireless communication, after the signals are transmitted from the source, a number of distinct path rays arise from the source to the receiver due to the scattering, reflection and diffraction from the objects surrounding the source. While these so-called "multipath propagation" phenomena may cause attenuation of the signal, they can also lead to spreading of the signal in time, frequency and space domains. Such multipath interference and distortion on the received signal significantly affects transmission accuracy and efficiency. To mitigate such distortion and improve the spectral efficiency, techniques employing multiple antennas and space-time block coding [1–4] which maintain satisfactory performance over fading channels have been

proposed recently. In the particular case of downlink (such as that of a mobile system receiving signals from a base station), the receiver is typically required to be small and hence may not be practical to deploy multiple antennas at the receiver. For this reason, the base station is usually equipped with multiple transmitter antennas, and a space-time coding technique is used to introduce correlation between the transmitted symbols from different antennas (in spatial domain) at different time slots (in temporal domain) and thus, achieves transmission diversity and power gain over the uncoded system.

In particular, since Alamouti [3] first established a very simple orthogonal space-time block code (OSTBC), the OSTBC [3,5] has attracted much attention because it can achieve maximum diversity and because its coherent maximum likelihood detection can be realized as a linear processor. However, in order to optimally decode an OSTBC, full channel state information (CSI) must be exactly known at the receiver. Unfortunately, wireless channels often change with time, and perfect knowledge of CSI is not easy to be tracked at the receiver. Although noncoherent detection schemes based on differential encoding techniques [8–11] can also be employed here with no requirement for channel estimation directly, nonetheless, these schemes often suffer from error propagation resulting in loss of performance [3]. Therefore, channel estimation becomes a key issue in space-time communication system design and influences the reconstruction of input signals at the receiver.

In the existing channel estimation methods, classical training-based schemes [6,7] transmit both training signals and information-carrying signals, and utilize the training signals and the observation at the receiver to estimate the channel. However, the resulting limitation of effective data throughput [6,7] represents a penalty in performance. To avoid having to transmit training signals, considerable research efforts have been directed to develop techniques of "blind channel estimation" [12, 13, 17] recently. These techniques identify and estimate the transmission channel using only

the received (perhaps noisy) signals at the receiver. The essence of these algorithms is to exploit the structure of the channel and/or the property of transmitted signals. The subspace method is one such method exploiting the channel structure and the second order statistics of input signals [18–20]. Another important example of such blind estimation methods is the ML method of detection [13] which is usually optimal for large samples but in general, does not have a closed-form solution. Also, its implementation may be too complicated due to the existence of local maxima.

In a special downlink case of the Alamouti STBC channel, the currently available blind channel estimation methods [32–38] all have the ambiguity issues, which need to be resolved by adding pilot symbols. Thus, these methods can only be called *semi-blind* and the need for the pilot symbols further renders the spectral efficiency not fully exploited. Also, some blind methods [21–25] handle the channel estimation problem with the exploitation of signal properties, e.g., finite alphabets, symmetry, constant modulus, etc. However, for the Alamouti STBC channel, these methods still have ambiguity issues and thus, cannot provide a precise channel estimate since the phase properties of communication signals have not been fully exploited. To resolve these ambiguities in estimation of Alamouti STBC channel, we propose a new signalling scheme for blind channel estimation in this thesis.

1.2 Contribution of this Thesis

The goal of this thesis is to develop a novel signalling scheme for blind channel estimation to resolve the ambiguity issues in estimation of Alamouti STBC channel and a space-time coded MISO channel [31].

For the Alamouti STBC channel, we observe that the essential reason for the existence of rotational ambiguity or sign ambiguity in the currently available channel estimation methods is that the objectives in their formulated optimization problems

are invariant under some rotation transformation for the commonly used QAM and PSK constellations. A proper signalling scheme is therefore needed to resolve the ambiguity. In this thesis, our important contribution is that the proposed blind channel estimation technique can eliminate the ambiguity by co-transmitting of a p-ary PSK and a q-ary PSK signal, with p and q being co-prime. Using this new strategy, we prove that a) in the noise-free case, only two distinct pairs of symbols are needed to *uniquely* determine the channel coefficients and decode the signal, and b) in the case for which complex Gaussian noise is present and for which the pth-order and qth-order statistics on the received signals are available, the channel coefficients can also be uniquely determined. In both cases, simple closed-form solutions are derived by exploiting specific property of the Alamouti code and linear Diophantine equation theory. When only limited received signals are available, we equip blind ML detection methods with our signalling scheme, and propose to use the semi-definite relaxation (SDR) algorithm [37, 41, 42] or the sphere decoding algorithm [?, 43] to approximate ML detection so that the joint estimation of the channel and symbols can be efficiently implemented.

As an extension of our technique to other channels, we apply a specific space-time coding technique [31] to multi-input single-output system with an even number of transmitter antennas. We demonstrate this system has an equivalent representation which consists of multiple Alamouti STBC subchannels. Hence, our blind channel estimation technique is also useful to the estimation of this particular space-time coded MISO communication system.

1.3 Structure of this Thesis

The thesis is structured as follows:

- In the introductory chapter, we present the channel estimation problem and

briefly introduce the existing channel estimation methods. We also outline the primary contributions of this thesis.

- In the second chapter, we first introduce the channel model of linear MISO communication system. Then, we discuss a simple case of Alamouti STBC channel and a space-time code for linear MISO system. Finally, we derive a equivalent representation for this space-time coded MISO system.

- In Chapter 3, we review the existing channel estimation algorithms in three main categories: training-based methods; (semi-) blind methods; and others. In particular, we discuss the currently available blind channel estimation methods for the Alamouti STBC channel and analyze the existence of ambiguities in these methods.

- In Chapter 4, we propose a simple signalling scheme for the estimation of Alamouti STBC channel. Simple closed-form solutions and simulation results are presented in both the noise-free and the complex Gaussian noise cases.

- In Chapter 5, we consider the application of our signalling scheme to blind ML detection methods for Alamouti STBC channel. We further employ the SDR-ML algorithm and the sphere decoding algorithm to efficiently solve this blind ML channel estimation and symbol detection problem.

- In Chapter 6, we discuss conclusion on this work and some suggestions for future work.

- In appendix, we provide the proofs of two theorems given in Chapter 4 and also include a description of the Euclid Algorithm.

Chapter 2

MISO Communication System

In this chapter, we consider the application of space-time coding technique to linear MISO communication system equipped with an even number of transmitter antennas. We first discuss a simple case of Alamouti STBC channel. Then, utilizing a space-time coding scheme proposed by Shang-Ho Tsai [31], we establish the model of this space-time coded MISO system and derive its equivalent system representation.

2.1 MISO Channel Model

Here, we introduce the general complex baseband model of a linear MISO system which has N transmitter antennas and a single receiver antenna, as shown in Figure 2.1. Each of the transmitter antennas synchronously sends one symbol in one time slot, i.e., symbols $x_1, x_2, \cdots, x_N$ are simultaneously transmitted from Antenna 1 to Antenna N. Hence, the received signal z in the baseband is a linear superposition of these transmitted symbols perturbed by additive noise ξ,

$$z = \sum_{k=1}^{N} x_k h_k + \xi \tag{2.1}$$

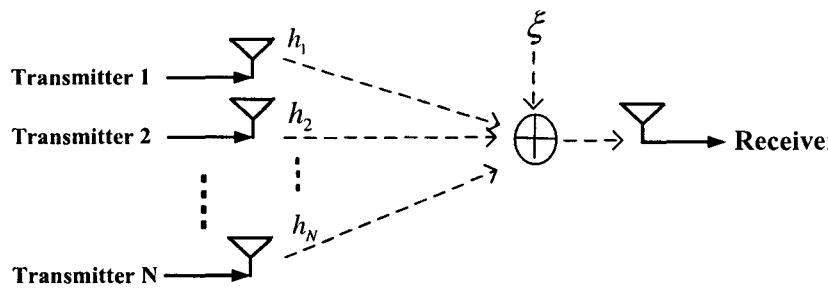

Figure 2.1: Diagram of MISO wireless communication system

where $x_k, k = 1, \cdots, N$ are independently selected from a signal set with unit average power, h_k denotes the channel coefficient from the k-th transmitter antenna to the receiver antenna, and ξ denotes the circularly-symmetric complex independent Gaussian noise with zero-mean and variance σ^2. Here, noise is said to be circularly-symmetric complex independent Gaussian if its real and image parts are both i.i.d. Gaussian random variables with $\mathcal{N}(0, \sigma^2/2)$.

Throughout this thesis, we only consider flat fading environments in which all fading coefficients $h_k, k = 1, \cdots, N$ are assumed to be independent and constant over one observable period and may randomly change in next observable period.

For a particular time slot, if we stack all transmitted symbols $x_k, k = 1, \cdots, N$ on different transmitter antennas into a vector $\mathbf{x}$ of dimension $N \times 1$ and stack all channel coefficients $h_k, k = 1, \cdots, N$ into a vector $\mathbf{h}$ of dimension $N \times 1$, then the received signal z in Eq. (2.1) can be rewritten in a compact matrix form as

$$z = \mathbf{x}\mathbf{h} + \xi \tag{2.2}$$

where $\mathbf{x} = [x_1, x_2, \cdots, x_N]$ and $\mathbf{h} = [h_1, h_2, \cdots, h_N]^T$.

2.2 Alamouti STBC Channel Model

To apply space-time coding technique to linear MISO system, we first introduce a simple case of the Alamouti STBC channel model in this section.

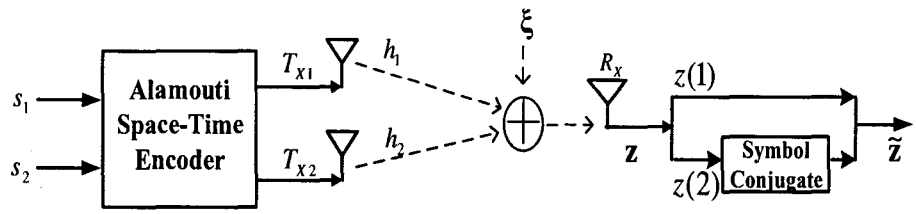

Figure 2.2: Diagram of the Alamouti STBC channel

The Alamouti STBC code was first established by Alamouti [3] for a flat fading wireless communication system with two transmitter antennas and a single receiver antenna as shown in Fig. 2.2. The transmitted symbols from the two transmitter antennas arrive at the receiver via two different channels. Thus, the discrete baseband received signal can be written as

$$z = h_1 s_1 + h_2 s_2 + \xi \tag{2.3}$$

where z is the received signal, h_1 and h_2 are the respective channel coefficients from the transmitter Antennas 1 and 2 to the receiver antenna, s_1 and s_2 are the two corresponding transmitted symbols from these two antennas, and ξ is a circularly symmetric complex Gaussian noise with zero-mean and variance σ^2. Throughout this thesis, we assume that $|h_1|^2 + |h_2|^2 \neq 0$ and h_1 and h_2 remain constant within T transmission time slots.

If this system employs the Alamouti space-time block coding scheme, each set of two transmitted symbols spans over two consecutive time slots which is designated a *frame*. For example, during the first time slot of the ith frame, s_{i1} and s_{i2} are simultaneously transmitted from Antennas 1 and 2, respectively; during the second

time slot of the ith frame, $-s_{i2}^*$ and s_{i1}^* are transmitted simultaneously from Antennas 1 and 2, respectively. Thus, the Alamouti code of the ith frame has the following structure

$$\mathbf{S}_i = \begin{bmatrix} s_{i1} & s_{i2} \\ -s_{i2}^* & s_{i1}^* \end{bmatrix} \tag{2.4}$$

and we can further get $\mathbf{S}_i\mathbf{S}_i^H = \left(|s_{i1}|^2 + |s_{i2}|^2\right)\mathbf{I}_2$, i.e., column or row vectors of $\mathbf{S}_i$ are orthogonal to each other and both have equal norm. Thus, the Alamouti code actually is a two-dimensional OSTBC [5]. Furthermore, at the receiver antenna, the received signals in the two consecutive time slots of the ith frame can be written in a matrix form

$$\begin{bmatrix} z_i(1) \\ z_i(2) \end{bmatrix} = \begin{bmatrix} s_{i1} & s_{i2} \\ -s_{i2}^* & s_{i1}^* \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} \xi_i(1) \\ \xi_i(2) \end{bmatrix} \tag{2.5}$$

where $[\xi_i(1), \xi_i(2)]^T$ denotes the circularly-symmetric complex Gaussian noise vector with zero-mean and variance $\sigma^2\mathbf{I}_2$ in the two time slots.

As we can observe in Eq. (2.5), each one of the channel coefficients $h_k, k = 1, 2$ has been used twice to transmit signals. After using the "symbol conjugate" operator, the conjugated received signals of the ith frame can be expressed by

$$\begin{bmatrix} \tilde{z}_i(1) \\ \tilde{z}_i(2) \end{bmatrix} = \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix} \begin{bmatrix} s_{i1} \\ s_{i2} \end{bmatrix} + \begin{bmatrix} \xi_i(1) \\ \xi_i^*(2) \end{bmatrix} \tag{2.6}$$

where $\tilde{z}_i(1) = z_i(1)$ and $\tilde{z}_i(2) = z_i^*(2)$. The two column vectors of the equivalent channel matrix, say, $[h_1, h_2^*]^T$ and $[h_2, -h_1^*]^T$, are orthogonal and thus, no interference exists between the transmission of s_{i1} and s_{i2}. If the channel matrix $\mathbf{H} = \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}$

is exactly known at the receiver, left-multiplying both sides of Eq. (2.6) by $\mathbf{H}^H$, we have

$$\begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}^H \begin{bmatrix} \tilde{z}_i(1) \\ \tilde{z}_i(2) \end{bmatrix} = \begin{bmatrix} |h_1|^2 + |h_2|^2 & 0 \\ 0 & |h_1|^2 + |h_2|^2 \end{bmatrix} \begin{bmatrix} s_{i1} \\ s_{i2} \end{bmatrix} + \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}^H \begin{bmatrix} \xi_i(1) \\ \xi_i^*(2) \end{bmatrix} \quad (2.7)$$

which can be further rewritten as

$$\begin{bmatrix} \bar{z}_i(1) \\ \bar{z}_i(2) \end{bmatrix} = \begin{bmatrix} s_{i1} \\ s_{i2} \end{bmatrix} + \begin{bmatrix} \bar{\xi}_i(1) \\ \bar{\xi}_i(2) \end{bmatrix} \quad (2.8)$$

with

$$\begin{bmatrix} \bar{z}_i(1) \\ \bar{z}_i(2) \end{bmatrix} = \frac{1}{|h_1|^2 + |h_2|^2} \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}^H \begin{bmatrix} \tilde{z}_i(1) \\ \tilde{z}_i(2) \end{bmatrix}$$

$$\begin{bmatrix} \bar{\xi}_i(1) \\ \bar{\xi}_i(2) \end{bmatrix} = \frac{1}{|h_1|^2 + |h_2|^2} \begin{bmatrix} h_1 & h_2 \\ h_2^* & -h_1^* \end{bmatrix}^H \begin{bmatrix} \xi_i(1) \\ \xi_i^*(2) \end{bmatrix}$$

Now, from Eq. (2.8), we can simply quantize $\bar{z}_i(1)$ and $\bar{z}_i(2)$ respectively to get the estimation of the signals s_{i1} and s_{i2}, i.e.,

$$\hat{s}_{in} = \arg \min_{s_{in} \in \mathcal{S}} \left|\left| \bar{z}_i(n) - s_{in} \right|\right|^2 \quad (2.9)$$

where $n = 1, 2$ and $\mathcal{S}$ denotes the constellation set. Therefore, it shows that the orthogonal structure of the channel matrix can greatly simplify the complexity of decoding method.

2.3 A Space-Time Coded MISO System

In this section, we introduce a space-time code design and apply it to linear MISO communication system with an even number of transmitter antennas, as shown in Figure 2.3. When a permutation matrix and a discrete Fourier transform (DFT) matrix are employed at both ends, we can derive an alternative representation for this space-time coded MISO system.

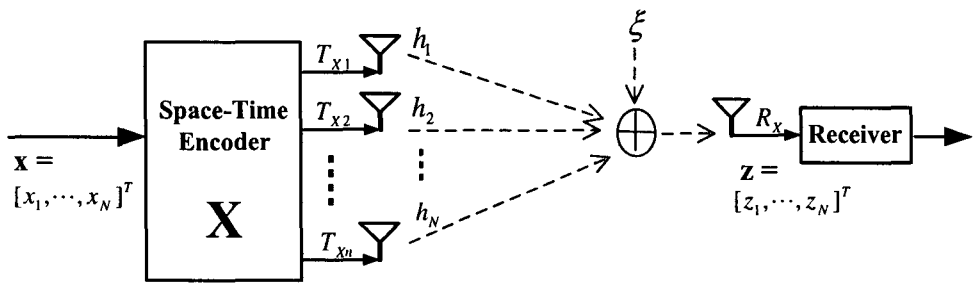

Figure 2.3: Diagram of space-time coded MISO system

2.3.1 A Space-Time Code Design

In [31], Shang-Ho Tsai et al. proposed a rate-one space-time block code to a multiple-antenna system. To describe this space-time coding scheme, we define a vector $\bar{\mathbf{x}}$ of dimension $N \times 1$, with its kth element given by

$$[\bar{\mathbf{x}}]_k = \begin{cases} [\mathbf{x}^*]_k, & k = 1,3,\cdots,N-1 \\ [-\mathbf{x}^*]_k, & k = 2,4,\cdots,N \end{cases} \tag{2.10}$$

During N time slots, say, $t = 1,2,\cdots,N$, vector $\mathbf{x} = [x_1, x_2, \cdots, x_N]^T$ is space-time coded by the following procedure,

- When t is odd, we transmit x_k by the antenna indexed $\big[((k-t) \bmod N) + 1\big]$.
- When t is even, we transmit $[\bar{\mathbf{x}}]_k$ by the antenna indexed $\big[((t-k) \bmod N) + 1\big]$.

Therefore, we obtain the $N \times N$ space-time block code $\mathbf{X}$ with its (u, v)-th element expressed as

$$[\mathbf{X}]_{uv} = \begin{cases} x_{[((u+v-2) \bmod N)+1]}, & u = 1, 3, \ldots, N-1 \\ (-1)^v x^*_{[((u-v) \bmod N)+1]}, & u = 2, 4, \ldots, N \end{cases} \tag{2.11}$$

for $v = 1, 2, \cdots, N$.

For example: a 6×6 dimension space-time block code $\mathbf{X}$ is

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ -x_2^* & x_1^* & -x_6^* & x_5^* & -x_4^* & x_3^* \\ x_3 & x_4 & x_5 & x_6 & x_1 & x_2 \\ -x_5^* & x_3^* & -x_2^* & x_1^* & -x_6^* & x_5^* \\ x_5 & x_6 & x_1 & x_2 & x_3 & x_4 \\ -x_6^* & x_5^* & -x_4^* & x_3^* & -x_2^* & x_1^* \end{bmatrix} \tag{2.12}$$

where the row denotes the time dimension, (i.e., the uth row denotes the symbols transmitted by the N antennas at the uth time slot), and the column denotes the space dimension, (i.e., the vth column denotes the symbols transmitted by the vth antenna during the N time slots). In other words, the symbol $[\mathbf{X}]_{uv}$ is transmitted from the v-th antenna at the u-th time slot.

During N transmission time slots, by assuming that the channel is invariant, we can stack the N received signals $z_k, k = 1, 2, \cdots, N$ into a vector $\mathbf{z}$ and express the block transmission model in a matrix form as

$$\mathbf{z} = \mathbf{X}\mathbf{h} + \boldsymbol{\xi} \tag{2.13}$$

where $\mathbf{z} = [z_1, z_2, \cdots, z_N]^T$, $\mathbf{X}$ is the $N \times N$ space-time block code matrix, $\mathbf{h} = [h_1, h_2, \cdots, h_N]^T$, and $\boldsymbol{\xi} = [\xi_1, \xi_2, \cdots, \xi_N]^T$ is the Gaussian noise vector.

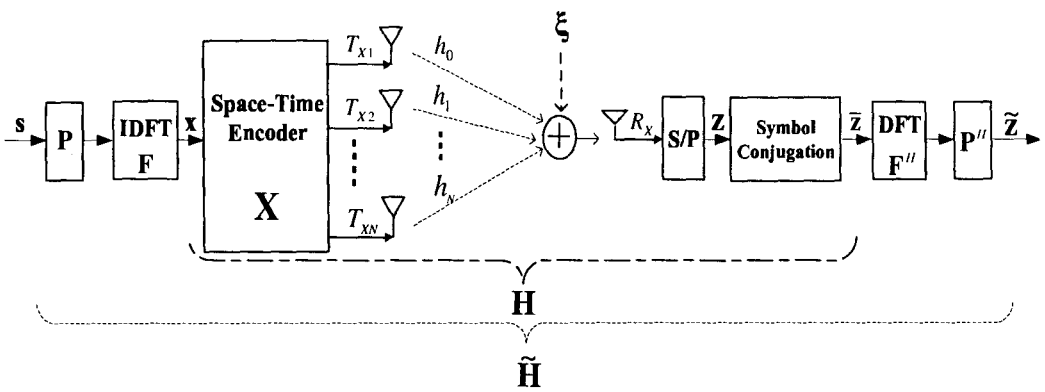

Figure 2.4: Diagram of space-time coded MISO system with precoders

2.3.2 Equivalent Representation of the Space-Time MISO System

As shown in Figure 2.4, if a permutation operator and DFT operator are used at both ends, we will obtain an equivalent system representation for the above space-time coded MISO system. In the following, we will give its derivation in details.

At the transmitter part, the input signal vector $\mathbf{s} = [s_1, s_2, \cdots, s_N]^T$ is sequentially passed through a permutation matrix $\mathbf{P}$, a inverse discrete Fourier transform (IDFT) matrix $\mathbf{F}$, and the space-time encoder discussed in previous subsection. The (u, v)-th element of this permutation matrix $\mathbf{P}$ is given by

$$[\mathbf{P}]_{uv} = \begin{cases} 1, & u = 1, 2, \cdots, \frac{N}{2},\ v = 2u - 1 \\ 1, & u = \frac{N}{2} + 1, \frac{N}{2} + 2, \cdots, N,\ v = 2u - N \\ 0, & \text{otherwise} \end{cases} \tag{2.14}$$

For example: if $N = 6$, matrix $\mathbf{P}$ has the following structure,

$$\mathbf{P} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{2.15}$$

Further, the (u, v)-th element of the IDFT matrix $\mathbf{F}$ is given by

$$[\mathbf{F}]_{uv} = \frac{1}{\sqrt{N}} e^{j\frac{2\pi}{N}(u-1)(v-1)} \tag{2.16}$$

for $u = 1, 2, \cdots, N$ and $v = 1, 2, \cdots, N$. Therefore, the symbol vector to be space-time encoded, denoted by $\mathbf{x}$, is

$$\mathbf{x} = \mathbf{FPs} \tag{2.17}$$

where $\mathbf{x} = [x_1, x_2, \cdots, x_N]^T$ and $\mathbf{s} = [s_1, s_2, \cdots, s_N]^T$. Next, vector $\mathbf{x}$ is space-time coded by the coding technique in Eq. (2.11).

When the encoded matrix $\mathbf{X}$ is transmitted from N antennas over N time slots, we obtain N received signals $z_k, k = 1, 2, \cdots, N$ from Eq. (2.13) at the receiver. As observed in Figure 2.4, the received signals are then through "symbol conjugate" operator, i.e.,

$$[\bar{\mathbf{z}}]_k = \begin{cases} [\mathbf{z}]_k, & k = 1, 3, \cdots, N-1 \\ [\mathbf{z}^*]_k, & k = 2, 4, \cdots, N \end{cases} \tag{2.18}$$

After some mathematical manipulations, the vector $\bar{\mathbf{z}}$ can be expressed as

$$\bar{\mathbf{z}} = \mathbf{Hx} + \bar{\boldsymbol{\xi}} = \mathbf{HFPs} + \bar{\boldsymbol{\xi}} \tag{2.19}$$

where the noise vector $\bar{\boldsymbol{\xi}}$ is

$$[\bar{\boldsymbol{\xi}}]_k = \begin{cases} [\boldsymbol{\xi}]_k, & k = 1, 3, \cdots, N-1 \\ [\boldsymbol{\xi}^*]_k, & k = 2, 4, \cdots, N \end{cases} \tag{2.20}$$

and the (u, v)-th element of channel matrix $\mathbf{H}$ is determined by

$$[\mathbf{H}]_{u\,v} = \begin{cases} h_{[((v-u) \bmod N)+1]}, & u = 1, 3, \cdots, N-1 \\ (-1)^{v-1} h^*_{[((u-v) \bmod N)+1]}, & u = 2, 4, \cdots, N \end{cases} \tag{2.21}$$

for $v = 1, 2, \cdots, N$. For example: the 6×6 space-time coded channel matrix $\mathbf{H}$ has the following form

$$\mathbf{H} = \begin{bmatrix} h_1 & h_2 & h_3 & h_4 & h_5 & h_6 \\ h_2^* & -h_1^* & h_6^* & -h_5^* & h_4^* & -h_3^* \\ h_5 & h_6 & h_1 & h_2 & h_3 & h_4 \\ h_4^* & -h_3^* & h_2^* & -h_1^* & h_6^* & -h_5^* \\ h_3 & h_4 & h_5 & h_6 & h_1 & h_2 \\ h_6^* & -h_5^* & h_4^* & -h_3^* & h_2^* & -h_1^* \end{bmatrix} \tag{2.22}$$

Subsequently, vector $\bar{\mathbf{z}}$ is sent through the DFT operator $\mathbf{F}^H$ and the permutation operator $\mathbf{P}^H$, namely, left-multiplying both sides of Eq. (2.19) by matrices $\mathbf{F}^H$ and $\mathbf{P}^H$, we have

$$\mathbf{P}^H\mathbf{F}^H\bar{\mathbf{z}} = \mathbf{P}^H\mathbf{F}^H\mathbf{H}\mathbf{F}\mathbf{P}\mathbf{s} + \mathbf{P}^H\mathbf{F}^H\bar{\boldsymbol{\xi}} \tag{2.23}$$

To simplify the notation of the above equation, we define $N \times 1$ vector $\tilde{\mathbf{z}} \triangleq \mathbf{P}^H\mathbf{F}^H\bar{\mathbf{z}}$, $N \times N$ matrix $\tilde{\mathbf{H}} \triangleq \mathbf{P}^H\mathbf{F}^H\mathbf{H}\mathbf{F}\mathbf{P}$, and $N \times 1$ vector $\tilde{\boldsymbol{\xi}} \triangleq \mathbf{P}^H\mathbf{F}^H\bar{\boldsymbol{\xi}}$. Then, an equivalent

system model is thus established as

$$\tilde{\mathbf{z}} = \tilde{\mathbf{H}}\mathbf{s} + \tilde{\boldsymbol{\xi}} \tag{2.24}$$

Notice that matrix $\tilde{\mathbf{H}}$ has the following structure,

$$\tilde{\mathbf{H}} = \begin{bmatrix} \tilde{h}_{11} & \tilde{h}_{12} & 0 & 0 & \cdots & \cdots & 0 & 0 \\ \tilde{h}_{12}^* & -\tilde{h}_{11}^* & 0 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \tilde{h}_{21} & \tilde{h}_{22} & & & \vdots & \vdots \\ 0 & 0 & \tilde{h}_{22}^* & -\tilde{h}_{21}^* & & & \vdots & \vdots \\ \vdots & \vdots & & & \ddots & \ddots & 0 & 0 \\ \vdots & \vdots & & & \ddots & \ddots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 0 & \tilde{h}_{\frac{N}{2},1} & \tilde{h}_{\frac{N}{2},2} \\ 0 & 0 & \cdots & \cdots & 0 & 0 & \tilde{h}_{\frac{N}{2},2}^* & -\tilde{h}_{\frac{N}{2},1}^* \end{bmatrix} \tag{2.25}$$

where

$$\begin{aligned} \tilde{h}_{i1} &= \frac{1}{N}\sum_{v=1}^{N}\left[\sum_{u=1,\text{odd}}^{N-1}\exp\left(j\frac{2\pi}{N}\Big(v-u\Big)i\right)h_{[((v-u) \bmod N)+1]}\right. \\ &\quad \left. + \sum_{u=2,\text{even}}^{N}\exp\left(j\frac{2\pi}{N}\Big(v-u\Big)i\right)(-1)^{v-1}h^*_{[((u-v) \bmod N)+1]}\right] \\ \tilde{h}_{i2} &= \frac{1}{N}\sum_{v=1}^{N}\left[\sum_{u=1,\text{odd}}^{N-1}\exp\left(j\frac{2\pi}{N}\left(v\frac{i-2}{2}-u\frac{i+N-2}{2}\right)\right)h_{[((v-u) \bmod N)+1]}\right. \\ &\quad \left. + \sum_{u=2,\text{even}}^{N}\exp\left(j\frac{2\pi}{N}\left(v\frac{i-2}{2}-u\frac{i+N-2}{2}\right)(-1)^{v-1}h^*_{[((u-v) \bmod N)+1]}\right] \end{aligned}$$

for $i = 1, 2, \cdots, \frac{N}{2}$. As we can observe Eq. (2.25), matrix $\tilde{\mathbf{H}}$ has a block-diagonal structure with all off-block-diagonal elements being zero. Therefore, the channel

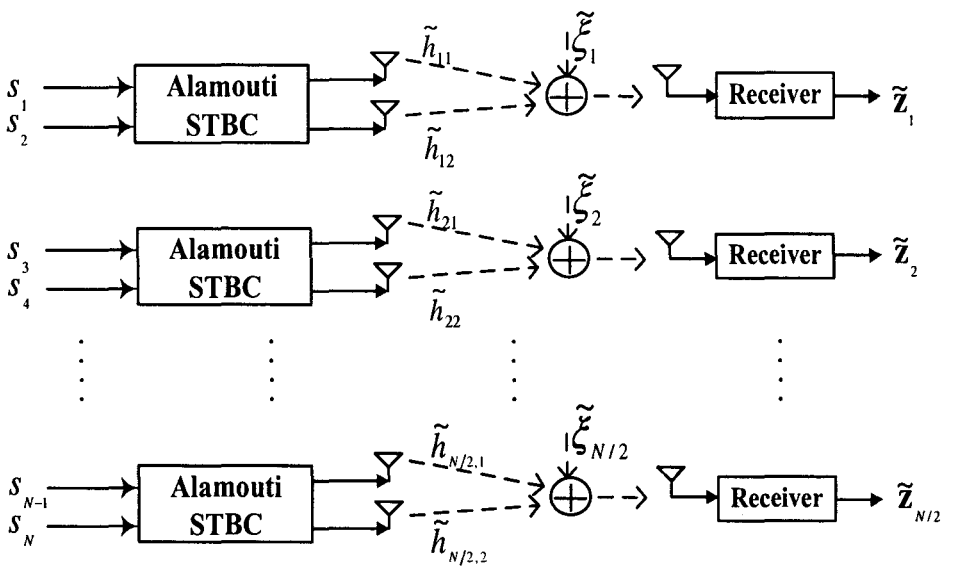

Figure 2.5: Equivalent Representation of the system in Figure 2.4.

model in Eq. (2.24) can be further represented by

$$\begin{bmatrix} \tilde{\mathbf{z}}_1 \\ \vdots \\ \tilde{\mathbf{z}}_{\frac{N}{2}} \end{bmatrix} = \begin{bmatrix} \tilde{\mathbf{H}}_1 & & \\ & \ddots & \\ & & \tilde{\mathbf{H}}_{\frac{N}{2}} \end{bmatrix} \begin{bmatrix} \mathbf{s}_1 \\ \vdots \\ \mathbf{s}_{\frac{N}{2}} \end{bmatrix} + \begin{bmatrix} \tilde{\boldsymbol{\xi}}_1 \\ \vdots \\ \tilde{\boldsymbol{\xi}}_{\frac{N}{2}} \end{bmatrix} \tag{2.27}$$

where $\tilde{\mathbf{z}}_i = [\tilde{z}_{2i-1}, \tilde{z}_{2i}]^T$, $\tilde{\mathbf{H}}_i = \begin{bmatrix} \tilde{h}_{i1} & \tilde{h}_{i2} \\ \tilde{h}_{i2}^* & -\tilde{h}_{i1}^* \end{bmatrix}$, $\mathbf{s}_i = [s_{2i-1}, s_{2i}]^T$, and $\tilde{\boldsymbol{\xi}}_i = [\tilde{\xi}_{2i-1}, \tilde{\xi}_{2i}]^T$ for $i = 1, 2, \cdots, \frac{N}{2}$. Here, each subchannel has exactly the same structure as the Alamouti space-time coded channel in Eq. (2.6), i.e.,

$$\begin{aligned} \tilde{\mathbf{z}}_i &= \tilde{\mathbf{H}}_i \mathbf{s}_i + \tilde{\boldsymbol{\xi}}_i \\ &= \begin{bmatrix} \tilde{h}_{i1} & \tilde{h}_{i2} \\ \tilde{h}_{i2}^* & -\tilde{h}_{i1}^* \end{bmatrix} \begin{bmatrix} s_{2i-1} \\ s_{2i} \end{bmatrix} + \begin{bmatrix} \tilde{\xi}_{2i-1} \\ \tilde{\xi}_{2i} \end{bmatrix} \end{aligned} \tag{2.28}$$

Remark:

a) Eq. (2.24) to Eq. (2.28) tell us that the space-time coded MISO communication system given by Eq. (2.13) can be equivalently represented by multiple Alamouti STBC subchannels if a particular permutation matrix and a DFT matrix are properly utilized at both ends. In Figure 2.5, we depict this alternative system representation.

b) As a result, the channel estimation problem for this space-time coded MISO system is similar to that problem for the Alamouti STBC channel.

Therefore, in the following chapters of this thesis, we will concentrate on the channel estimation problem for the Alamouti STBC channel.

Chapter 3

Review of Channel Estimation Methods

In the introductory chapter, we stated that multiple antennas and STBC [1–4] have been deployed in recent wireless communication system design to improve the spectral efficiency and mitigate multipath interference distortion. In particular, the OSTBC [3,5] has attracted much attention because it enables full diversity with a linear processing ML detector. However, all these advantages are based on the exact knowledge of the channel coefficients being available at the receiver. Since most wireless channels change with time, perfect knowledge of CSI is not easy to be tracked at the receiver. Channel estimation is thus required.

Up till now, various channel estimation methods including training-based techniques and blind (semi-blind) estimation methods, have been proposed for space-time communication systems. In this chapter, we briefly describe these estimation methods in categories. Then we turn our attention to blind channel estimation methods for the Alamouti STBC channel, and further analyze the reason of existing the ambiguities in these methods.

3.1 Training-based Channel Estimation

The basic idea of training-based estimation methods is to estimate the channels either from the observations of only training signals or from the observations of the superposition of training and information signals. The former methods transmit the training symbols, which are known at both the transmitter and the receiver, and estimate the channels using these symbols and their resulting observations. The latter methods transmit the training symbols multiplexed with information bearing symbols and then, estimate the channels by exploiting all the observations of these symbols and the statistics of information symbols.

Training-based estimation methods simplify the challenging task of the receiver design. However, a substantial penalty in performance comes from the limitation of effective data throughput [6, 7]. The reason is that training signals do not carry any information, i.e., the more training signals are imbedded in a data packet, the less information signals can be transmitted. Thus, it turns out to be a tradeoff between the bandwidth efficiency and estimation accuracy. That is, more training symbols will provide better channel estimation and less decoding error; otherwise, fewer training symbols will result in worse channel estimation and more decoding error. In addition, the training-based schemes are not effective and practical in fast fading channels whose fading coefficients are only invariant over small data packet.

3.2 Blind (Semi-Blind) Channel Estimation

In recent years, "blind channel estimation" [12, 13, 17] has received considerable research interests. These techniques use only the received (perhaps noisy) signals at the receiver to identify and estimate the transmission channel. The essence of these

methods is to exploit the structure of the channel and/or the property of transmitted signals. In the following section, we will describe two important blind channel estimation methods, i.e., the statistic-based methods (second-order and higher-order statistic) and the ML-based method.

3.2.1 Second-Order Statistical Method

Second-order statistical methods [18–20] exploit the signal or noise subspace from the second-order statistics on the received signals. Input signals are randomly produced with a known second-order statistics (distribution), and the additive noises are uncorrelated with input signals. These statistical methods are often able to give an estimate of the channels in closed-form structure.

In blind channel estimation, the subspace method is one such method commonly used because of the simplicity and computation efficiency. The subspace-based methods require either the channel has a specific structure like block-Hankel matrix or the transmitted space-time code matrix has a block-Toeplitz structure.

In addition, the second-order statistical methods usually need a large amount of samples to achieve near maximum likelihood performance. In other words, the channel is commonly required to remain constant in a long observation period.

3.2.2 Higher-Order Statistical Method

In the scenarios where second-order statistics are not sufficient to assure the identification or estimation of channels, higher-order statistics in both time and frequency domains may be exploited for estimating the channels [26,28–30]. For example, single-input single-output (SISO) communication system cannot employ the multichannel diversity. Higher-order statistics on the observations is thus needed in channel estimation.

Higher-order statistical methods, compared to second-order statistical methods, usually require many more samples to precisely estimate the channel. As a result, these higher-order statistical methods always need expensive computation complexity.

3.2.3 Maximum Likelihood (ML) Method

Another important parameter estimation algorithm is the Maximum Likelihood (ML) estimation method, which is theoretically optimal for large samples so as to carry out the linear minimum variance unbiased estimators [13].

In the following, we describe the theory of ML estimation method. Let $p(z|x)$ denote the conditional probability density function (PDF) with z being the observation and x being the deterministic parameter. Given only the observation z, the task is to estimate the parameter x by its most likely value such that the associated conditional PDF $p(z|x)$ can achieve the maximum value. Thus, we write $p(z|x)$ as a function of x, which is referred as the likelihood function. The ML estimation method is employed in signal detection at the receiver based on a simple idea that different transmitted signals produce distinct received signals, and any given received signal is more probable to come from the transmitted signal than other signals.

When the ML method is applied to blind channel estimation problem, input signal vector $\mathbf{x} = [x_1, x_2, \cdots, x_N]^T$ and channel vector $\mathbf{h} = [h_1, h_2, \cdots, h_N]^T$ in Eq. (2.2) become both unknown deterministic parameters to be estimated. In other words, the goal of blind ML channel estimation method is to find the most reasonable values for both input signals and channel coefficients to achieve the maximum value of the conditional PDF, i.e.,

$$\{\hat{\mathbf{x}}, \hat{\mathbf{h}}\} = \arg\max_{\mathbf{x},\mathbf{h}} \log p\left(z|\mathbf{x}, \mathbf{h}\right), \tag{3.29}$$

where $p\left(z|\mathbf{x}, \mathbf{h}\right)$ is the conditional PDF of the received signal z conditioned on both

the input signal vector $\mathbf{x}$ and the channel vector $\mathbf{h}$.

In general, the blind ML channel estimation method does not yield a closed-form solution to the channel, but generally derive an optimization problem instead, e.g. the problem (3.29). Such problem is often solved by numerical algorithms which recursively converge to the minimum value of cost function. Despite of the possibility of achieving the minimum value, there still exist several important issues, e.g. the number of samples, convergence speed, the existence of local minima and initialization. All these greatly affect the performance and computational expense.

In particular, if input signals come from a finite alphabet set, the joint estimation of the channel and input signals usually involves an exhaustive search, whose computational complexity may make it infeasible for large number of input signals.

3.3 Signal Property Exploitation Technique

There are several other blind equalizer design and channel estimation methods which exploit the properties of input signals instead of the specific structures of channels. Digital communication signals possess many properties, such as source independence, constant modulus, finite alphabet, symmetry and so on [12]. These properties can be utilized to blindly identify or estimate channels, for example,

1. Constant Modulus property: Some communication signals possess constant modulus (CM) property, i.e., the envelope of the signal is constant. FM signal and phase modulated signal are examples of such CM signals. This property is widely used in recent blind equalizer design and source separation problem, such as constant modulus algorithm (CMA) [14–16,21]. In some subspace-based channel estimation methods, the CM property and the second order statistics of the Pulse Shift Keying (PSK) constellation signals are exploited to arrive at the solution of the channel estimate being the eigenvectors of a simultaneous

diagonalization problem [12].

2. Symmetry property: In [24,25], the symmetry property of the quadrature amplitude modulation (QAM) signals is employed, instead of the second order statistics, to blindly equalize the fractional channels [22], [23] by solving convex optimization problems.

Despite of the exploitation of these signal properties, there still exist phase rotational ambiguity and sign ambiguity issues in blind equalization and channel estimation methods. The reason for this is that these methods did not fully employ the phase properties of digital communication signals. Although these methods can easily identify the amplitude information of channels, but the phase information still cannot be identified.

3.4 Differential Encoding Technique

Recently, some noncoherent detection schemes have been proposed. Contrary to coherent detection which fully necessitates the channel state information at the receiver, noncoherent detection schemes explore differential encoding and decoding technique [8–11] to directly detect the input signals with no requirement for channel estimation. However, compared to coherent detection [3], these methods often suffer from error propagation resulting in loss of performance at high SNR.

3.5 Ambiguity Analysis for the Estimation of Alamouti STBC Channel

In previous sections, we reviewed a number of classical channel estimation and symbol detection methods applicable for the OSTBC system [32–38]. In this section, we will

consider the special case of the Alamouti STBC channel and discuss the blind channel estimation methods in such case.

By exploiting the orthogonality of the Alamouti code, the subspace method was applied to such a system so as to obtain an exact value of the channel matrix up to an unknown unitary matrix factor [32]. This rotational ambiguity results in the channel not being able to be identified uniquely even in the noise-free case. Although such ambiguity can be partially resolved by using different linear precoders for odd and even symbols to warrant channel identifiability [33], it still suffers from scale ambiguity which essentially cannot be handled by the subspace method based on solving a quadratic optimization problem. An improved transmission scheme using a linear precoder with different powers at the different transmitted symbols was proposed in [34, 35], and a closed-form solution to the channel estimation was derived. Unfortunately, this scheme requires an assumption that the noise power is known in advance, and there is still the sign ambiguity.

In addition, to address the rotational ambiguity in the blind ML channel estimation and symbol detection problem, several schemes have also been proposed in [36, 37]. The essence of these methods is to derive the objective function for ML detection as a homogenous quadratic function and therefore, the resulting optimization problem can be efficiently solved using the SDR-ML detector [36, 37] or sphere decoder [37, 43]. Unfortunately, a rotational ambiguity of the detected signal still exists. Since pilot symbols have to be added, these schemes can only be called *semi-blind* and the need of the pilot symbols in these methods to resolve the rotational ambiguity further renders the spectral efficiency not fully exploited.

From the results in [32, 36, 38], we observe that the essential reason for the existence of rotational ambiguity or sign ambiguity in the currently available blind channel estimation methods for the Alamouti STBC channel is that the objectives

in their formulated optimization problems are invariant under some rotation transformation for the commonly used QAM and PSK constellations. This can be clearly demonstrated as follows: Let $\{s_{i1}, s_{i2}\}$ and $\{s_{(i+1)1}, s_{(i+1)2}\}$ be the two selected pair of symbols to be transmitted in the consecutive ith and $(i+1)$th frame and let the transmitted signal matrix and the channel coefficient vector be respectively given by

$$\mathbf{S} \triangleq \begin{bmatrix} s_{i1} & s_{i2} \\ -s_{i2}^* & s_{i1}^* \\ s_{(i+1)1} & s_{(i+1)2} \\ -s_{(i+1)2}^* & s_{(i+1)1}^* \end{bmatrix} \quad \text{and} \quad \mathbf{h} \triangleq \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} \tag{3.30}$$

1. For a square QAM constellation $\mathcal{S}_Q$, then both $\{s_{i1}, s_{i2}\}, \{s_{(i+1)1}, s_{(i+1)2}\} \in \mathcal{S}_Q$. At the receiver, the received signals in the four time slots $\mathbf{z} = [z_i(1) \;\; z_i(2) \;\; z_{i+1}(1) \;\; z_{i+1}(2)]^T$ can be written in two different ways

$$\mathbf{z} = \mathbf{S}\,\mathbf{h} = \mathbf{S}'\,\mathbf{h}' \tag{3.31}$$

where

$$\mathbf{S}' = \mathbf{S}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{h}' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^H \mathbf{h} \tag{3.32}$$

Thus, using the received vector $\mathbf{z}$ to detect the symbols and to estimate the channel coefficients may result in two possible sets of solutions: $\{\mathbf{S}, \mathbf{h}\}$ or, $\{\mathbf{S}', \mathbf{h}'\}$.

2. Similarly, rotational ambiguity exists if only one M-PSK constellation $\mathcal{S}_M$ is used. In this case, for the two consecutive frames, $\{s_{i1}, s_{i2}\}, \{s_{(i+1)1}, s_{(i+1)2}\} \in \mathcal{S}_M$. Thus, from the transmitted symbols in two consecutive frames of the

Alamouti STBC channel, the received signals can be written as

$$\mathbf{z} = \mathbf{S}\,\mathbf{h} = \mathbf{S}_m\,\mathbf{h}_m \tag{3.33}$$

where $\mathbf{S}$ is given by Eq. (3.30), $\mathbf{S}_m = \mathbf{S}\,\mathrm{diag}(e^{j\frac{2m\pi}{M}},\ e^{-j\frac{2m\pi}{M}})$, $\mathbf{h}_m = \mathrm{diag}(e^{-j\frac{2m\pi}{M}},\ e^{j\frac{2m\pi}{M}})\,\mathbf{h}$, $m = 0, \cdots, M-1$.

From the two cases above, it can be seen that if the symbols are chosen from the same constellation for transmission through the Alamouti STBC channel, then neither the symbols nor the channel coefficients can be uniquely determined. No matter how many frames of symbols are transmitted by increasing the number of rows in $\mathbf{S}$ of Eq. (3.30), as long as the symbols are selected from only one constellation, rotational ambiguity will exist. In order to eliminate the ambiguity, the *careful designed* signalling scheme should be sought. This is the main idea of this thesis.

Chapter 4

Blind Channel Identification with a New Signalling Scheme

In this chapter, we propose a novel signalling scheme for unique blind identification of the Alamouti STBC channel. Using this new strategy, we will prove that a) in the noise-free case, only two distinct pairs of symbols are needed to *uniquely* determine the channel coefficients and decode the symbols, and b) in the case for which complex Gaussian noise are added and for which the pth-order and qth-order statistics on the received signals are available, the channel coefficients can also be uniquely determined. In both cases, simple closed-form solutions are derived.

4.1 The Proposed Signalling Scheme

Now, we present the simple signalling scheme as follows:

Let $\mathcal{S}_p$ and $\mathcal{S}_q$ represent the p-PSK and q-PSK constellation sets respectively, where p and q are predetermined positive co-prime integers. Suppose in the first time slot of the ith frame, we transmit from Antenna 1 a symbol $s_{pi} \in \mathcal{S}_p$, i.e., selected from the p-PSK constellation, and from Antenna 2 a symbol $s_{qi} \in \mathcal{S}_q$, i.e., selected

from the q-PSK constellation. Then, according to the Alamouti scheme, the received signal vector for the ith frame is

$$\begin{bmatrix} z_i(1) \\ z_i(2) \end{bmatrix} = \begin{bmatrix} s_{pi} & s_{qi} \\ -s_{qi}^* & s_{pi}^* \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} \xi_i(1) \\ \xi_i(2) \end{bmatrix}, \qquad i = 1, 2, \cdots \tag{4.34a}$$

Or, in more compact matrix form,

$$\mathbf{z}_i = \mathbf{S}_i \mathbf{h} + \boldsymbol{\xi}_i, \qquad i = 1, 2, \cdots \tag{4.34b}$$

where $\mathbf{z}_i = [z_i(1) \;\; z_i(2)]^T$, $\mathbf{h} = [h_1 \;\; h_2]^T$, $\boldsymbol{\xi}_i = [\xi_i(1) \;\; \xi_i(2)]^T$, and $\mathbf{S}_i = \begin{bmatrix} s_{pi} & s_{qi} \\ -s_{qi}^* & s_{pi}^* \end{bmatrix}$. Eqs. (4.34) represent the new designed signalling scheme proposed in this thesis for the ith frame of the Alamouti coding scheme. In the following sections, we will show that this proposed strategy can facilitate the *blind unique* detection of the transmitted signals in the noise-free case and identification of the channel coefficients in the noisy case.

4.2 Blind Unique Channel and Signal Identification in Noise-Free Case

In this section, we will examine the proposed signalling scheme above under the noise-free environment. In two consecutive frames i and $i+1$, we send out the symbol pairs $\{s_{pi}, s_{qi}\}, \{-s_{qi}^*, s_{pi}^*\}$ and $\{s_{p(i+1)}, s_{q(i+1)}\}, \{-s_{q(i+1)}^*, s_{p(i+1)}^*\}$ for the four consecutive time slots, where $s_{pi}, s_{p(i+1)} \in \mathcal{S}_p$, and $s_{qi}, s_{q(i+1)} \in \mathcal{S}_q$. Thus, if there is no noise, from

Eqs. (4.34), we have the received signals for the two consecutive frames given by,

$$\mathbf{z}_i = \mathbf{S}_i\mathbf{h} \tag{4.35a}$$

$$\mathbf{z}_{i+1} = \mathbf{S}_{i+1}\mathbf{h} \tag{4.35b}$$

Solving Eqs. (4.35) for $\mathbf{h}$ yields

$$\mathbf{h} = \frac{1}{2}{\mathbf{S}_i}^H\mathbf{z}_i = \frac{1}{2}{\mathbf{S}_{i+1}}^H\mathbf{z}_{i+1} \tag{4.36}$$

Eliminating $\mathbf{h}$ in the above equation yields

$$\mathbf{z}_{i+1} = \frac{1}{2}\mathbf{S}_{i+1}\mathbf{S}_i^H\mathbf{z}_i = \mathbf{A}_i\,\mathbf{z}_i \tag{4.37}$$

where $\mathbf{A}_i = \begin{bmatrix} a_{i1} & a_{i2} \\ -a_{i2}^* & a_{i1}^* \end{bmatrix}$ with a_{i1} and a_{i2} denoted by

$$a_{i1} \triangleq \frac{1}{2}\left(s_{p(i+1)}s_{pi}^* + s_{q(i+1)}s_{qi}^*\right) \tag{4.38a}$$

$$a_{i2} \triangleq \frac{1}{2}\left(s_{pi}s_{q(i+1)} - s_{qi}s_{p(i+1)}\right) \tag{4.38b}$$

Now, taking conjugate of $z_{i+1}(2)$, Eq. (4.37) can be rewritten as

$$\tilde{\mathbf{z}}_{i+1} = \tilde{\mathbf{Z}}_i\,\mathbf{a}_i \tag{4.39}$$

where $\tilde{\mathbf{z}}_{i+1} = [z_{i+1}(1) \quad z_{i+1}^*(2)]^T$, $\tilde{\mathbf{Z}}_i = \begin{bmatrix} z_i(1) & z_i(2) \\ z_i^*(2) & -z_i^*(1) \end{bmatrix}$ and $\mathbf{a}_i = [a_{i1} \quad a_{i2}]^T$, from which we obtain

$$a_{i1} = \big(z_i^*(1)z_{i+1}(1) + z_i(2)z_{i+1}^*(2)\big)/\big(|z_i(1)|^2 + |z_i(2)|^2\big) \tag{4.40a}$$

$$a_{i2} = \big(z_i^*(2)z_{i+1}(1) - z_i(1)z_{i+1}^*(2)\big)/\big(|z_i(1)|^2 + |z_i(2)|^2\big) \tag{4.40b}$$

i.e., the values of a_{i1} and a_{i2} can be obtained from the received signals. We left-multiply the definition of a_{i1} in Eq. (4.38a) by $s_{pi}s_{qi}$, i.e.,

$$\begin{aligned} s_{pi}s_{qi}a_{i1} &= \frac{1}{2}\, s_{pi}s_{qi}\big(s_{p(i+1)}s_{pi}^* + s_{q(i+1)}s_{qi}^*\big) \\ &= \frac{1}{2}\big(s_{qi}s_{p(i+1)}s_{pi}^*s_{pi} + s_{pi}s_{q(i+1)}s_{qi}^*s_{qi}\big) \\ &= \frac{1}{2}\big(s_{qi}s_{p(i+1)}|s_{pi}|^2 + s_{pi}s_{q(i+1)}|s_{qi}|^2\big) \\ &= \frac{1}{2}\big(s_{qi}s_{p(i+1)} + s_{pi}s_{q(i+1)}\big) \end{aligned} \tag{4.41}$$

where $|s_{pi}|^2 = 1$ and $|s_{qi}|^2 = 1$ come from the property of PSK symbol. Combining Eq. (4.41) and Eq. (4.38b), we have

$$s_{pi}s_{qi}a_{i1} = \frac{1}{2}\big(s_{qi}s_{p(i+1)} + s_{pi}s_{q(i+1)}\big) \tag{4.42a}$$

$$a_{i2} = \frac{1}{2}\big(s_{pi}s_{q(i+1)} - s_{qi}s_{p(i+1)}\big) \tag{4.42b}$$

After some mathematical manipulation, the above equations become

$$s_{pi}s_{qi}a_{i1} + a_{i2} = s_{pi}s_{q(i+1)} \tag{4.43a}$$

$$s_{pi}s_{qi}a_{i1} - a_{i2} = s_{qi}s_{p(i+1)} \tag{4.43b}$$

Now, the key question here is: For the given values of a_{i1} and a_{i2} in Eqs. (4.40), do the quadratic equations (4.43) have a unique set of solutions for the transmitted symbol variables s_{pn} and s_{qn}, $n = i,\ i+1$? The following theorem provides us with the answer.

4.2.1 Closed-Form Solution

Theorem 1 [57, 58] *Let $s_{pn} \in \mathcal{S}_p$ and $s_{qn} \in \mathcal{S}_q$ for $n = i,\ i+1$ be symbols to be transmitted in the time frames i and $i+1$ respectively, p and q being co-prime positive integers. Let $\mathbf{z}_i = [z_i(1), z_i(2)]^T$ and $\mathbf{z}_{i+1} = [z_{i+1}(1), z_{i+1}(2)]^T$ be two distinct received signal vectors from the Alamouti STBC channel within the two consecutive time frames (four time slots). a_{i1} and a_{i2} are determined by Eqs. (4.40). The four transmitted symbols are uniquely determined as follows:*

1. *$a_{i1} = 0$. We have*

$$s_{pi} = \exp\left(j\frac{2\pi}{p}\left(\frac{k_1}{q}\left(1 - p^{\varphi(q)}\right) + p\left\lceil\frac{k_1 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{4.44a}$$

$$s_{qi} = \exp\left(j\frac{2\pi}{q}\left(k_2 p^{\varphi(q)-1} - q\left\lceil\frac{k_2 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{4.44b}$$

$$s_{p(i+1)} = \exp\left(j\frac{2\pi}{p}\left(\frac{k_2}{q}\left(1 - p^{\varphi(q)}\right) + p\left\lceil\frac{k_2 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{4.44c}$$

$$s_{q(i+1)} = \exp\left(j\frac{2\pi}{q}\left(k_1 p^{\varphi(q)-1} - q\left\lceil\frac{k_1 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{4.44d}$$

where $\varphi(\cdot)$ denotes the Euler function [39], and integers k_1, k_2 are

$$k_1 = \frac{\arg(a_{i2})pq}{2\pi}, \quad k_1 \in [0, pq)$$

$$k_2 = \frac{\arg(-a_{i2})pq}{2\pi}, \quad k_2 \in [0, pq)$$

2. $a_{i1} \neq 0$. *Let* $a_{i1} \triangleq |a_{i1}|e^{j\theta_{i1}}, \theta_{i1} \in [-\pi, \pi)$, $a_{i2} \triangleq |a_{i2}|e^{j\theta_{i2}}, \theta_{i2} \in [-\pi, \pi)$ *and* $\alpha \triangleq \arccos|a_{i1}|$. *Then, we have*

$$s_{pi} = \exp\left(j\frac{2\pi}{p}\left(\frac{k}{q}\left(1-p^{\varphi(q)}\right)+p\left\lceil\frac{kp^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{4.45a}$$

$$s_{qi} = \exp\left(j\frac{2\pi}{q}\left(kp^{\varphi(q)-1}-q\left\lceil\frac{kp^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{4.45b}$$

$$s_{p(i+1)} = \exp\left(j\,2\pi\ell_p/p\right)s_{pi} \tag{4.45c}$$

$$s_{q(i+1)} = \exp\left(j\,2\pi\ell_q/q\right)s_{qi} \tag{4.45d}$$

Here, integers ℓ_p *and* ℓ_q *are uniquely determined as follows:*

(a) For $\alpha \leq \theta_{i1} < 2\pi - \alpha$, *we have*

$$\begin{cases} \ell_p = \frac{(\theta_{i1}+\alpha)p}{2\pi}, \quad \ell_q = \frac{(\theta_{i1}-\alpha)q}{2\pi}, & \text{if } e^{j\,p(\theta_{i1}+\alpha)} = 1 \text{ and } e^{j\,q(\theta_{i1}-\alpha)} = 1 \\ \ell_p = \frac{(\theta_{i1}-\alpha)p}{2\pi}, \quad \ell_q = \frac{(\theta_{i1}+\alpha)q}{2\pi}, & \text{if } e^{j\,p(\theta_{i1}-\alpha)} = 1 \text{ and } e^{j\,q(\theta_{i1}+\alpha)} = 1 \end{cases}$$

(b) For $-\alpha \leq \theta_{i1} < \alpha$, *we have*

$$\begin{cases} \ell_p = \frac{(\theta_{i1}+\alpha)p}{2\pi}, \quad \ell_q = \frac{(\theta_{i1}-\alpha+2\pi)q}{2\pi}, & \text{if } e^{j\,p(\theta_{i1}+\alpha)} = 1 \text{ and } e^{j\,q(\theta_{i1}-\alpha)} = 1 \\ \ell_p = \frac{(\theta_{i1}-\alpha+2\pi)p}{2\pi}, \quad \ell_q = \frac{(\theta_{i1}+\alpha)q}{2\pi}, & \text{if } e^{j\,p(\theta_{i1}-\alpha)} = 1 \text{ and } e^{j\,q(\theta_{i1}+\alpha)} = 1 \end{cases}$$

(c) For $-2\pi + \alpha \leq \theta_{i1} < -\alpha$, *we have*

$$\begin{cases} \ell_p = \frac{(\theta_{i1}+\alpha+2\pi)p}{2\pi}, \quad \ell_q = \frac{(\theta_{i1}-\alpha+2\pi)q}{2\pi}, & \text{if } e^{j\,p(\theta_{i1}+\alpha)} = 1 \text{ and } e^{j\,q(\theta_{i1}-\alpha)} = 1 \\ \ell_p = \frac{(\theta_{i1}-\alpha+2\pi)p}{2\pi}, \quad \ell_q = \frac{(\theta_{i1}+\alpha+2\pi)q}{2\pi}, & \text{if } e^{j\,p(\theta_{i1}-\alpha)} = 1 \text{ and } e^{j\,q(\theta_{i1}+\alpha)} = 1 \end{cases}$$

In addition, integer k is uniquely determined by

$$k = \begin{cases} \frac{\left(\theta_{i2}-\theta_{i1}+\frac{\pi}{2}\right)pq}{2\pi} \mod pq, & \text{if } \ell_p = \frac{(\theta_{i1}+\alpha-2l\pi)p}{2\pi} \\ \frac{\left(\theta_{i2}-\theta_{i1}-\frac{\pi}{2}\right)pq}{2\pi} \mod pq, & \text{if } \ell_p = \frac{(\theta_{i1}-\alpha-2l\pi)p}{2\pi} \end{cases}$$

with $l = 0, -1$.

Furthermore, the channel coefficients h_1 and h_2 in $\mathbf{h}$ can be uniquely determined by

$$\mathbf{h} = \frac{1}{2}\,\mathbf{S}_i^H \mathbf{z}_i \tag{4.46}$$

■

The proof of Theorem 1 is given in Appendix A. We like to make the following remarks on this theorem:

1. Theorem 1 not only tells us that the channel coefficients can be uniquely identified by transmitting two distinct symbol pairs selected from two co-prime PSK constellations in four time slots, but also provides simple and closed-form solutions to both the channel coefficients and the transmitted symbols.

2. In the noise-free case, two different received signal vectors are the smallest number of data required to uniquely identify the Alamouti STBC channel and transmitted symbols. In other words, if only one received signal vector is given, then, from Eq. (4.35a) we cannot uniquely determine the transmitted symbols $\{s_{pi}, s_{qi}\}$ or the channel coefficients h_1 and h_2.

3. To carry out our new signalling scheme as described in Section 4.1, p and q must be co-prime integer. Otherwise, ambiguity will occur. This can be demonstrated by considering a 4-PSK constellation $\mathcal{S}_4$ and a 6-PSK constellation $\mathcal{S}_6$ for which $\gcd(4,6) = 2$. For the two consecutive frames, let the matrix of the selected

symbols to be transmitted be $\mathbf{S}$ as given in Eq. (3.30) where $\{s_{i1}, s_{(i+1)1} \in \mathcal{S}_4\}$ and $\{s_{i2}, s_{(i+1)2} \in \mathcal{S}_6\}$. We can easily see that the received signal vector in the four time slots $\mathbf{z} = [z_i(1) \;\; z_i(2) \;\; z_{i+1}(1) \;\; z_{i+1}(2)]^T$ can be written as

$$\mathbf{z} = \mathbf{S}\,\mathbf{h} = \tilde{\mathbf{S}}\,\tilde{\mathbf{h}} \tag{4.47}$$

where $\tilde{\mathbf{S}} = \mathbf{S}\,\mathrm{diag}(-1, \; -1)$ and $\tilde{\mathbf{h}} = \mathrm{diag}(-1, \; -1)\,\mathbf{h}$. Thus, using the received vector $\mathbf{z}$ to detect the symbols and estimate the channel coefficients results in two possible sets of solutions: $\{\mathbf{S}, \; \mathbf{h}\}$ or, $\{\tilde{\mathbf{S}}, \; \tilde{\mathbf{h}}\}$, i.e., there is *sign* ambiguity in this case.

4.2.2 Simulation Results

To verify the validity of Theorem 1, we consider using the Q-PSK ($p = 4$) and T-PSK ($q = 3$) constellations in construction of the Alamouti code and transmit two time frames according to our scheme, i.e., we form the matrix $\mathbf{S}$ of the symbols to be transmitted as given in Eq. (3.30) where $\{s_{i1}, s_{(i+1)1} \in \mathcal{S}_4\}$ and $\{s_{i2}, s_{(i+1)2} \in \mathcal{S}_3\}$ where $\mathcal{S}_4$ and $\mathcal{S}_3$ are respectively the set of symbols in a Q-PSK and a T-PSK constellation and tried to detect these four transmitted symbols according to the formulas given in Theorem 1. We tested the following cases:

a) The four transmitted symbols are all different.

b) We fix the two constellations such that they have one common symbol, i.e., in our transmission $s_{i1} = s_{(i+1)2} = 1$, and two other different symbols for each constellation are also transmitted.

c) The two transmitted Q-PSK symbols are different, but the same T-PSK symbols are transmitted over the two consecutive frames.

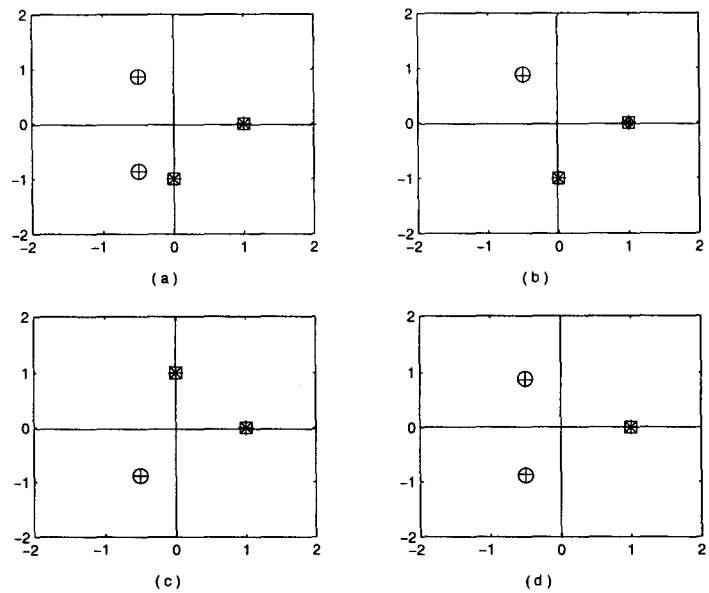

Figure 4.6: Identification of the transmitted symbols in noise-free case
□ Transmitted QPSK symbol, * Identified QPSK symbol,
○ Transmitted TPSK symbol, + Identified TPSK symbol.

d) The two transmitted TPSK symbols are different, but the two same Q-PSK symbols are transmitted over the two consecutive frames.

Each of the above tests was repeated 1000 times with different symbols selected within the freedom of each case. Without exception, the symbols were correctly identified in every test. Fig. 4.6 shows a typical result of each of the cases tested.

4.3 Blind Unique Channel Identification in Complex Gaussian Noise Case

Let us now consider the use of our signalling scheme in the Alamouti STBC channel contaminated with white complex Gaussian noise. We assume that the two symbols s_p and s_q sent over the two transmitter antennas are independent and equally likely

chosen from the respective p-PSK and q-PSK constellations, p and q being co-prime positive integers. In this case, for each frame, the received signal vector in the two time slots can be expressed as

$$\begin{bmatrix} z(1) \\ z(2) \end{bmatrix} = \begin{bmatrix} s_p & s_q \\ -s_q^* & s_p^* \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} \xi(1) \\ \xi(2) \end{bmatrix} \tag{4.48}$$

where $[\xi(1), \xi(2)]^T$ is circularly-symmetric complex Gaussian noise vector with zero-mean and variance $\sigma^2\mathbf{I}_2$. The following theorem states that, for this case, the channel coefficients can be uniquely identified.

4.3.1 Closed-Form Solution

Theorem 2 [57,58] *Let two positive integers p and q be co-prime and $\mathrm{E}[z^p(l)]$ and $\mathrm{E}[z^q(l)]$ for $l = 1, 2$ be available at the receiver. Then, we have*

$$\begin{cases} h_1^p = \mathrm{E}[z^p(1)] \\ h_1^q = (-1)^q \mathrm{E}[z^q(2)] \end{cases} \quad \begin{cases} h_2^p = \mathrm{E}[z^p(2)] \\ h_2^q = \mathrm{E}[z^q(1)] \end{cases} \tag{4.49}$$

From this, the channel coefficients h_1 and h_2 can be uniquely determined by

$$h_1 = \left|\mathrm{E}[z^p(1)]\right|^{1/p} e^{j\theta_1},\ h_2 = \left|\mathrm{E}[z^p(2)]\right|^{1/p} e^{j\theta_2} \tag{4.50}$$

where

$$\begin{aligned} \theta_1 &= \frac{\arg\left(\mathrm{E}[z^p(1)]\right) + 2n_1\pi}{p} = \frac{\arg\left((-1)^q \mathrm{E}[z^q(2)]\right) + 2m_1\pi}{q} \\ \theta_2 &= \frac{\arg\left(\mathrm{E}[z^p(2)]\right) + 2n_2\pi}{p} = \frac{\arg\left(\mathrm{E}[z^q(1)]\right) + 2m_2\pi}{q} \end{aligned}$$

with integers m_ℓ, n_ℓ, k_ℓ *for* $\ell = 1, 2$ *given by*

$$m_l = (-k_\ell)p^{\varphi(q)-1} - q\left\lceil \frac{(-k_\ell)p^{\varphi(q)-1}}{q} \right\rceil \tag{4.51a}$$

$$n_l = \frac{k_\ell}{q}\left(1 - p^{\varphi(q)}\right) - p\left\lceil \frac{(-k_\ell)p^{\varphi(q)-1}}{q} \right\rceil \tag{4.51b}$$

$$k_1 = \frac{\arg\left((-1)^q \mathrm{E}[z^q(2)]\right)p - \arg\left(\mathrm{E}[z^p(1)]\right)q}{2\pi} \tag{4.51c}$$

$$k_2 = \frac{\arg\left(\mathrm{E}[z^q(1)]\right)p - \arg\left(\mathrm{E}[z^p(2)]\right)q}{2\pi} \tag{4.51d}$$

■

The proof of Theorem 2 is given in Appendix B. Thus, even in complex Gaussian noise, provided that the pth- and qth-order statistics on the received signals are available, our signalling scheme can yield a unique closed-form solution to the channel coefficients.

4.3.2 Simulation Results

To test the validity of Theorem 2, computer simulations have been carried out in which the channel coefficients are estimated using Eq. (4.50) of Theorem 2. In order to obtain the pth- and qth- order statistics on the received signals, we transmit N frames of symbols during one observation block while the channel coefficients are invariant. The signal-to-noise ratio (SNR) here is defined as the average transmitted symbol energy to noise ratio, i.e., E_s/N_0. At each SNR, the normalized mean square error (MSE) of the channel estimate averaged over $K = 200$ trials $\left(\bar{\epsilon}_h^2 = \frac{1}{K}\sum_{k=1}^{K} \|\mathbf{h}_k - \hat{\mathbf{h}}_k\|^2/\|\mathbf{h}_k\|^2\right)$ is evaluated. At each trial the channel is randomly generated following an i.i.d. circular Gaussian distribution.

Example 1: The purpose of this example is to show the average normalized MSE of the channel versus the frame number in one observation block. We consider using the

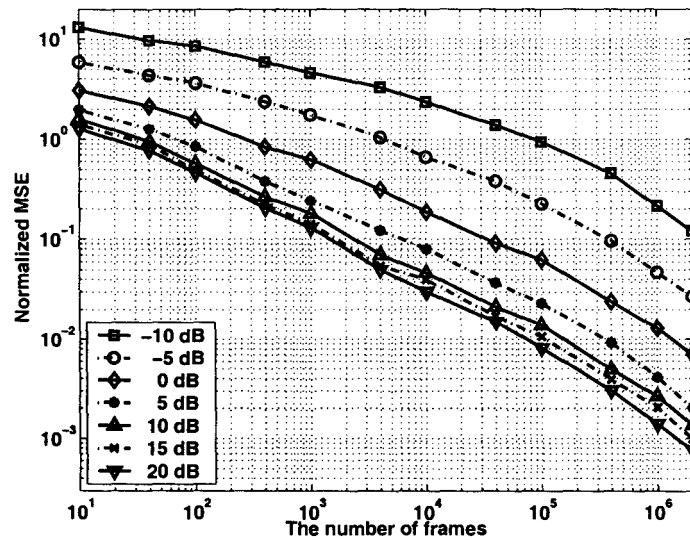

Figure 4.7: Channel normalized MSE vs. frame number in complex Gaussian noise.

Q-PSK ($p = 4$) and T-PSK ($q = 3$) constellations in construction of the Alamouti code and thus, Q-PSK and T-PSK symbols are independently and equally likely selected, i.e., $s_{pi} \in \mathcal{S}_4$ and $s_{qi} \in \mathcal{S}_3$ for the ith transmission frame. The results are shown in Figure 4.7. It can be observed that the average normalized MSE monotonically decreases as the frame number increases at different SNR values.

Example 2: here, we are interested in the average normalized MSE of the channel versus the value of SNR. We depict three average normalized MSE curves in Figure 4.8, each of which is obtained by transmitting a different frame number in one block, i.e., $N = 10^4, 10^5$ or 10^6. This figure tells us that the average normalized MSE monotonically decreases as the SNR increases in all three cases. The more frames are used for the estimation, the greater is the accuracy. The difference in SNR requirement for the same estimation accuracy can be quite considerable for the cases of $N = 10^5$ and $N = 10^6$.

The simulations above verify our theoretical results in Theorem 2. When the channel is sufficiently stationary to allow the pth- and qth-order statistics on the

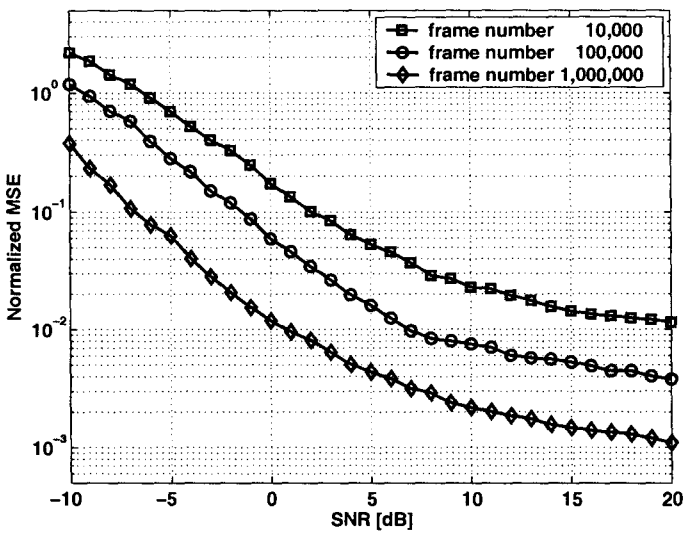

Figure 4.8: Channel normalized MSE vs. SNR in complex Gaussian noise.

received signals to be obtained accurately at the receiver, the proposed technique will provide us with unique estimates of the channel coefficients. However, a large number of data frames has to be transmitted to achieve a reasonable accuracy in the estimation of the Alamouti STBC channel using Theorem 2. In practice, the channel coefficients of a wireless communication system often change randomly from one observation block to the next. Thus, only a limited number of samples may be available during one observation block and may not be sufficient for estimating accurately the higher order statistics on the received signal. In this case, it is well known [27] that the optimal solution is the joint estimation of the channel coefficients and the signals based on maximum likelihood (ML) criterion. In next chapter, we will discuss blind ML channel estimation and symbol detection method in details.

Chapter 5

Blind ML Channel Estimation and Symbol Detection

When only finite samples are available at the receiver, the channel coefficients and input signals are both unknown parameters to be estimated. By taking advantage of the orthogonality of the Alamouti code, we will formulate the process of ML detection for the transmitted symbols using the signalling scheme proposed in Section 4.1. We also propose to use either the semi-definite relaxation method or the sphere decoding method to efficiently implement blind ML channel estimation and symbol detection for our designed constellation.

5.1 Formulation of Blind ML Detection

The following formulation of blind ML detection is similar to that given in [36]. However, it is developed independently here.

Now, suppose we have received L frames, i.e., $2L$ observable time slots, of signal vectors $\{\mathbf{z}_i\}$, $i = 1, 2, \cdots, L$, where $\mathbf{z}_i = [z_i(1) \;\; z_i(2)]^T$. We make the following two assumptions:

1. The channel coefficients h_1 and h_2 are invariant during L time frames.

2. During $2L$ observable time slots, L consecutive Alamouti coding matrices,

$$\mathbf{S}_i = \begin{bmatrix} s_{pi} & s_{qi} \\ -s_{qi}^* & s_{pi}^* \end{bmatrix}, \quad i = 1, \cdots, L \tag{5.52}$$

   are transmitted, where s_{pi} and s_{qi} are independent and equally likely chosen from the respective p-PSK and q-PSK constellations with p and q being co-prime positive integers.

Therefore, the received signals during L time frames can be stacked in a compact matrix form as

$$\mathbf{z} = \mathbf{S}\,\mathbf{h} + \boldsymbol{\xi} \tag{5.53}$$

where $\mathbf{z} = [\mathbf{z}_1^T \ \mathbf{z}_2^T \ \ldots \ \mathbf{z}_L^T]^T$ with $\mathbf{z}_i = [z_i(1) \ \ z_i(2)]^T$, $\mathbf{S} = [\mathbf{S}_1^T \ \ \mathbf{S}_2^T \ \ \cdots \ \ \mathbf{S}_L^T]^T$, $\mathbf{h} = [h_1 \ \ h_2]^T$ and $\boldsymbol{\xi} = [\boldsymbol{\xi}_1^T \ \boldsymbol{\xi}_2^T \ \cdots \ \boldsymbol{\xi}_L^T]^T$ with $\boldsymbol{\xi}_i = [\xi_i(1) \ \ \xi_i(2)]^T$. Given the received signal vector $\mathbf{z}$, the blind ML detection is to maximize the log-likelihood function with respect to the transmitted coding matrices and the channel vector, i.e.,

$$\{\hat{\mathbf{S}}, \hat{\mathbf{h}}\} = \arg\max_{\mathbf{S},\mathbf{h}} \ln p(\mathbf{z}|\mathbf{S}, \mathbf{h}) \tag{5.54}$$

where $p(\mathbf{z}|\mathbf{S}, \mathbf{h})$ is the density function of the received signal vector conditioned on both the transmitted coding matrix $\mathbf{S}$ and the channel vector $\mathbf{h}$. Since the noise vector $\boldsymbol{\xi}$ is zero-mean complex white Gaussian, Problem (5.54) can be reformulated to a nonlinear least squares (LS) optimization [13], i.e.,

$$\{\hat{\mathbf{S}}, \hat{\mathbf{h}}\} = \arg\min_{\mathbf{S},\mathbf{h}} \|\mathbf{z} - \mathbf{S}\mathbf{h}\|_2^2 \tag{5.55}$$

Since the received signal vector $\mathbf{z}$ is respectively linear in $\mathbf{S}$ and $\mathbf{h}$ from Eq. (5.53), we can write the joint optimization problem (5.55) as a sequential optimization,

$$\{\hat{\mathbf{S}}, \hat{\mathbf{h}}\} = \arg\min_{\mathbf{S}} \left\{ \min_{\mathbf{h}} \ \|\mathbf{z} - \mathbf{S}\mathbf{h}\|_2^2 \right\} \tag{5.56}$$

For the inner minimization, we differentiate the objective with respect to $\mathbf{h}$ and using the orthogonality of the Alamouti code, i.e., $\mathbf{S}_i^H \mathbf{S}_i = 2\,\mathbf{I}_2 \ \forall\ i$, we obtain

$$\mathbf{h} = (\mathbf{S}^H\mathbf{S})^{-1}\mathbf{S}^H\mathbf{z} \ = \frac{1}{2L}\mathbf{S}^H\mathbf{z} \tag{5.57}$$

which, when substituted into Eq. (5.56), yields

$$\hat{\mathbf{S}} = \arg\min_{\mathbf{S}} \left\{ \mathbf{z}^H\mathbf{z} - \frac{1}{2L}\mathbf{z}^H\mathbf{S}\mathbf{S}^H\mathbf{z} \right\} \tag{5.58}$$

Since the term $\mathbf{z}^H\mathbf{z}$ is fixed, the above optimization problem is equivalent to

$$\hat{\mathbf{S}} = \arg\max_{\mathbf{S}} \ (\mathbf{S}^H\mathbf{z})^H(\mathbf{S}^H\mathbf{z}) \tag{5.59}$$

We note that $\mathbf{S}^H\mathbf{z} = \sum_{i=1}^{L} \mathbf{S}_i^H\mathbf{z}_i$ with

$$\mathbf{S}_i^H\mathbf{z}_i = \begin{bmatrix} 0 & -z_i(2) \\ z_i(2) & 0 \end{bmatrix} \begin{bmatrix} s_{pi} \\ s_{qi} \end{bmatrix} + \begin{bmatrix} z_i(1) & 0 \\ 0 & z_i(1) \end{bmatrix} \begin{bmatrix} s_{pi}^* \\ s_{qi}^* \end{bmatrix} \tag{5.60}$$

Hence, $\mathbf{S}^H\mathbf{z}$ can be represented by

$$\mathbf{S}^H\mathbf{z} \ = \ \begin{bmatrix} -\sum_{i=1}^{L} z_i(2)s_{qi} + \sum_{i=1}^{L} z_i(1)s_{pi}^* \\ \sum_{i=1}^{L} z_i(2)s_{pi} + \sum_{i=1}^{L} z_i(1)s_{qi}^* \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \tag{5.61}$$

where

$$\begin{aligned} u_1 &= -\sum_{i=1}^{L} z_i(2)s_{qi} + \sum_{i=1}^{L} z_i(1)s_{pi}^* \\ &= [z_1(1), \cdots, z_L(1), -z_1(2), \cdots, -z_L(2)]\,\mathbf{s} \qquad (5.62a) \\ u_2 &= \sum_{i=1}^{L} z_i(2)s_{pi} + \sum_{i=1}^{L} z_i(1)s_{qi}^* \\ &= [z_1(2), \cdots, z_L(2), z_1(1), \cdots, z_L(1)]\,\mathbf{s}^* \qquad (5.62b) \end{aligned}$$

with $\mathbf{s} = \left[s_{p1}^*, \cdots, s_{pL}^*, s_{q1}, \cdots, s_{qL}\right]^T$. Substituting Eq. (5.61) and Eqs. (5.62) into Eq. (5.59), the objective function can be further reduced to

$$\begin{aligned} (\mathbf{S}^H\mathbf{z})^H(\mathbf{S}^H\mathbf{z}) &= \begin{bmatrix} u_1^*, & u_2^* \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = |u_1|^2 + |u_2^*|^2 \\ &= \mathbf{s}^H\bar{\mathbf{Z}}\bar{\mathbf{Z}}^H\mathbf{s} \qquad (5.63) \end{aligned}$$

where

$$\bar{\mathbf{Z}} = \begin{bmatrix} z_1^*(1), & \cdots & z_L^*(1), & -z_1^*(2), & \cdots & -z_L^*(2) \\ z_1(2), & \cdots & z_L(2), & z_1(1), & \cdots & z_L(1) \end{bmatrix}^T$$

Therefore, Eq. (5.59) can be rewritten as a homogenous quadratic optimization problem such that

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{s}\in\mathcal{A}} \{\mathbf{s}^H\bar{\mathbf{Z}}\bar{\mathbf{Z}}^H\mathbf{s}\} \qquad (5.64)$$

where the feasible set $\mathcal{A} = \underbrace{\mathcal{S}_p \times \mathcal{S}_p \times \cdots \times \mathcal{S}_p}_{L} \times \underbrace{\mathcal{S}_q \times \mathcal{S}_q \times \cdots \times \mathcal{S}_q}_{L} = \mathcal{S}_p^L \times \mathcal{S}_q^L$ is a $2L$ dimensional alphabet set. Once we obtain the solution $\hat{\mathbf{s}}$, the estimate of code matrix $\hat{\mathbf{S}}$ follows. By substituting $\hat{\mathbf{S}}$ and $\mathbf{z}$ into Eq. (5.57), we thus have the estimated value of the channel, i.e., $\hat{\mathbf{h}} = \frac{1}{2L}\hat{\mathbf{S}}^H\mathbf{z}$.

5.2 Algorithms to Solve this Problem

Due to the finite alphabet property of PSK symbol, in a general case, directly solving optimization problem (5.64) is a *nondeterministic polynomial-time* (NP) hard problem [40], i.e., the optimal solution must be found by a global search method requiring $\mathcal{O}(p^L q^L)$ multiplications. In this section, we employ the semi-definite relaxation (SDR) randomization method [37,41,42] and sphere decoding method [?,43] to efficiently solve the blind ML channel estimation and symbol detection problem.

5.2.1 Quasi ML Detection by Semi-Definite Relaxation [41]

The SDR-ML approach is an efficient algorithm closely approximating the blind ML detection with moderate worst-case computational cost. Generally, the SDR method consists of three steps:

1. Relax the feasible set of the original problem in a way such that the relaxed problem can be more efficiently solved;
2. Solve the relaxed problem;
3. Convert the solution of the relaxed problem to an approximate solution of the original problem.

Now, the maximization problem in Eq. (5.64) can be rewritten as

$$\hat{\mathbf{s}} = \arg\max_{\mathbf{s}\in\mathcal{A}} \left\{ \mathbf{s}^H \mathbf{A} \mathbf{s} \right\} \tag{5.65}$$

where $\mathbf{A} = \bar{\mathbf{Z}}\bar{\mathbf{Z}}^H \in \mathbb{C}^{2L\times 2L}$. Since $\mathbf{s}^H\mathbf{A}\mathbf{s} = \text{tr}(\mathbf{s}\mathbf{s}^H\mathbf{A}) = \text{tr}(\boldsymbol{\Sigma}\mathbf{A})$ with $\boldsymbol{\Sigma} = \mathbf{s}\mathbf{s}^H$, the problem (5.65) can be further rewritten as

$$\begin{aligned} \max \quad & \text{tr}(\boldsymbol{\Sigma}\mathbf{A}) && \text{(5.66a)} \\ \text{s.t.} \quad & \boldsymbol{\Sigma} = \mathbf{s}\mathbf{s}^H, \qquad \mathbf{s} \in \mathcal{A} && \text{(5.66b)} \\ & [\boldsymbol{\Sigma}]_{ii} = 1, \quad i = 1, \cdots, 2L && \text{(5.66c)} \end{aligned}$$

where Eq. (5.66c) comes from the property of PSK symbol, i.e., $s_i s_i^* = 1$ for all i and is a linear constraint. However, the constraint of Eq. (5.66b) implies that $\boldsymbol{\Sigma}$ is a positive semi-definite (PSD) matrix of rank one. If we omit this rank-one constraint and relax Eq. (5.66b) to merely a PSD constraint, then we have

$$\begin{aligned} \max \quad & \text{tr}(\boldsymbol{\Sigma}\mathbf{A}) && \text{(5.67a)} \\ \text{s.t.} \quad & \boldsymbol{\Sigma} \succeq \mathbf{0}, \quad \boldsymbol{\Sigma} \in \mathbb{C}^{2L\times 2L} && \text{(5.67b)} \\ & [\boldsymbol{\Sigma}]_{ii} = 1, \quad i = 1, \cdots, 2L && \text{(5.67c)} \end{aligned}$$

which is a *convex SDP* problem and its globally optimal solution can be efficiently found using the interior-point method [46]. To solve this complex-valued SDP problem, we need to convert it to an equivalent real-valued problem which can be verified to have the following expression,

$$\begin{aligned} \max \quad & \text{tr}(\overline{\boldsymbol{\Sigma}}\,\overline{\mathbf{A}}) && \text{(5.68a)} \\ \text{s.t.} \quad & \overline{\boldsymbol{\Sigma}} = \frac{1}{2}\begin{bmatrix} \boldsymbol{\Sigma}_R & -\boldsymbol{\Sigma}_I \\ \boldsymbol{\Sigma}_I & \boldsymbol{\Sigma}_R \end{bmatrix} && \text{(5.68b)} \\ & \boldsymbol{\Sigma}_R = \boldsymbol{\Sigma}_R^T \in \mathbb{R}^{2L\times 2L}, \ \boldsymbol{\Sigma}_I = -\boldsymbol{\Sigma}_I^T \in \mathbb{R}^{2L\times 2L} && \text{(5.68c)} \\ & \overline{\boldsymbol{\Sigma}} \succeq \mathbf{0}, \quad \overline{\boldsymbol{\Sigma}} \in \mathbb{R}^{4L\times 4L} && \text{(5.68d)} \\ & [\boldsymbol{\Sigma}_R]_{ii} = 1, \quad i = 1, \cdots, 2L && \text{(5.68e)} \end{aligned}$$

with

$$\overline{\mathbf{A}} = \begin{bmatrix} \mathbf{A}_R & -\mathbf{A}_I \\ \mathbf{A}_I & \mathbf{A}_R \end{bmatrix}$$

where $\mathbf{\Sigma}_R$ and $\mathbf{\Sigma}_I$ are the respective real and imaginary parts of $\mathbf{\Sigma}$, $\mathbf{A}_R$ and $\mathbf{A}_I$ are the respective real and imaginary parts of $\mathbf{A}$. Following Theorem 2 in [42], the problem (5.68) has a simpler formulation to be solved without considering the structural constraints (5.68b) and (5.68c), i.e.,

$$\begin{aligned} \max \quad & \mathrm{tr}(\overline{\mathbf{\Sigma}}\,\overline{\mathbf{A}}) && \text{(5.69a)} \\ \text{s.t.} \quad & \overline{\mathbf{\Sigma}} \succeq \mathbf{0}, \quad \overline{\mathbf{\Sigma}} \in \mathbb{R}^{4L\times 4L} && \text{(5.69b)} \\ & [\overline{\mathbf{\Sigma}}]_{ii} + [\overline{\mathbf{\Sigma}}]_{i+2L,i+2L} = 1, \quad i = 1, \cdots, 2L && \text{(5.69c)} \end{aligned}$$

which is again a convex optimization efficiently solvable by interior point methods. Once we obtain the solution, denoted by $\hat{\overline{\mathbf{\Sigma}}}$, then partition $\hat{\overline{\mathbf{\Sigma}}}$ into

$$\hat{\overline{\mathbf{\Sigma}}} = \begin{bmatrix} \hat{\mathbf{\Sigma}}_{11} & \hat{\mathbf{\Sigma}}_{12} \\ \hat{\mathbf{\Sigma}}_{21} & \hat{\mathbf{\Sigma}}_{22} \end{bmatrix}$$

where $\hat{\mathbf{\Sigma}}_{il} \in \mathbb{R}^{2L\times 2L}$ for all i, l. Therefore, the complex-valued SDR solution of Problem (5.67) is represented by

$$\hat{\mathbf{\Sigma}} = \left(\hat{\mathbf{\Sigma}}_{11} + \hat{\mathbf{\Sigma}}_{22}\right) + j\left(\hat{\mathbf{\Sigma}}_{21} - \hat{\mathbf{\Sigma}}_{12}\right) \tag{5.70}$$

Table 5.1: SDR-ML Randomization Estimator

Give the number of randomizations, denoted by M_{rand}, and

$$\mathbf{A} = \bar{\mathbf{Z}}\bar{\mathbf{Z}}^H, \qquad \overline{\mathbf{A}} = \begin{bmatrix} \mathbf{A}_R & -\mathbf{A}_I \\ \mathbf{A}_I & \mathbf{A}_R \end{bmatrix}$$

Step1. Solve the real-valued semidefinite program

$$\hat{\overline{\mathbf{\Sigma}}} = \arg\max_{\overline{\mathbf{\Sigma}} \in \mathbb{R}^{4L \times 4L}} \mathrm{tr}(\overline{\mathbf{\Sigma}}\,\overline{\mathbf{A}})$$

Step2. Partition the solution $\hat{\overline{\mathbf{\Sigma}}} = \begin{bmatrix} \hat{\mathbf{\Sigma}}_{11} & \hat{\mathbf{\Sigma}}_{12} \\ \hat{\mathbf{\Sigma}}_{21} & \hat{\mathbf{\Sigma}}_{22} \end{bmatrix}$, and let

$$\hat{\mathbf{\Sigma}} = (\hat{\mathbf{\Sigma}}_{11} + \hat{\mathbf{\Sigma}}_{22}) + j(\hat{\mathbf{\Sigma}}_{21} - \hat{\mathbf{\Sigma}}_{12})$$

Step3. (Randomization) Factorize $\hat{\mathbf{\Sigma}} = \hat{\mathbf{V}}^H\hat{\mathbf{V}}$.

for $k = 1, 2, \cdots, M_{rand}$

Randomly generate a complex vector $\mathbf{u}_k \in \mathbb{C}^{2L}$ which is uniformly distributed on an $2L$-dimensional unit sphere.

Compute $\hat{\mathbf{s}}(\mathbf{u}_k) = \mathrm{Quant}(\hat{\mathbf{V}}^H\mathbf{u}_k)$.

end;

Choose the approximate solution $\hat{\mathbf{s}} = \hat{\mathbf{s}}(\mathbf{u}_l)$, where $l = \arg\max_{k=1,\cdots,M_{rand}} \hat{\mathbf{s}}^H(\mathbf{u}_k)\mathbf{A}\hat{\mathbf{s}}(\mathbf{u}_k)$.

Step4. Thus, $\hat{\mathbf{s}}$ is treated as a solution to symbol detection.

From this optimum solution, an approximate solution to the original problem of Eq. (5.65) can be obtained using the Goemans-Williamson randomization technique [47, 48]. This randomization method has been found to achieve good approximation accuracy with a modest number of random search [41]. To apply this randomization process to our designed constellations, we perform Cholesky decomposition of $\hat{\mathbf{\Sigma}}$ resulting in $\hat{\mathbf{\Sigma}} = \hat{\mathbf{V}}^H\hat{\mathbf{V}}$ with $\hat{\mathbf{V}} = [\hat{\mathbf{v}}_1, \cdots, \hat{\mathbf{v}}_{2L}]$ being an upper triangular matrix. Then, we proceed the following steps:

1. Randomly generate a complex vector $\mathbf{u}_k \in \mathbb{C}^{2L}$ which is uniformly distributed on an $2L$-dimensional unit sphere.

2. For $k = 1, \cdots, M_{rand}$, where M_{rand} denotes the number of random search,

compute $\hat{\mathbf{s}}(\mathbf{u}_k) = \text{Quant}(\hat{\mathbf{V}}^H\mathbf{u}_k)$, where Quant$(t)$: the function $q = \text{Quant}(t)$ sets q to the element of $\mathcal{A}$ that is closest (in terms of Euclidean distance) to t. In other words, the entries in first half part of vector $\hat{\mathbf{V}}^H\mathbf{u}_k$ are quantized to symbols in p-PSK constellation, and the entries in second half part of vector $\hat{\mathbf{V}}^H\mathbf{u}_k$ are quantized to symbols in q-PSK constellation.

3. Choose the SDR approximate solution to be $\hat{\mathbf{s}} = \hat{\mathbf{s}}(\mathbf{u}_l)$, where $l = \arg\max_{k=1,\cdots,M_{rand}} \hat{\mathbf{s}}^H(\mathbf{u}_k)\mathbf{A}\hat{\mathbf{s}}(\mathbf{u}_k)$.

Finally, vector $\hat{\mathbf{s}}$ is treated as an approximate solution to the original optimization problem in Eq. (5.65). The pseudocode of this modified SDR-ML detector for our designed constellations is described in Table 5.1.

5.2.2 Blind ML Detection by Sphere Decoding

In this section, we consider the application of sphere decoding algorithm to our blind ML channel estimation and detection problem (5.64).

The sphere decoding algorithm [49, 54], which can optimally solve Boolean quadratic-programming (BQP) problem, has been recently used for coherent MIMO ML detection [43,50,51]. The basic idea of sphere decoding is a point search method, i.e., find the optimal lattice point that lies inside a sphere of given radius R centered at the received point, as shown in Fig. 5.9. In other words, only the lattice points within the square distance R^2 from the received point are considered in the metric minimization [49]. Among the several sphere decoder implementations [43,44,49–51], we choose a fast closest point search algorithm proposed in [43–45] based on the Schnorr-Euchner (SE) search strategy [52].

First, we notice that matrix $\bar{\mathbf{Z}}\bar{\mathbf{Z}}^H$ in Eq. (5.64) is not full rank. In fact, its rank is only two. Hence, we cannot directly use sphere decoding algorithm but have to reformulate the problem of Eq. (5.64). To do that, let matrix $\tilde{\mathbf{Z}}$ be an orthogonal

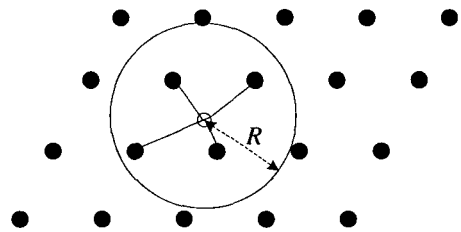

Figure 5.9: Geometrical representation of sphere decoding.

complementary matrix for the column-orthogonal matrix $\bar{\mathbf{Z}}$, and we have

$$\bar{\mathbf{Z}}\bar{\mathbf{Z}}^H + \tilde{\mathbf{Z}}\tilde{\mathbf{Z}}^H = ||\,\bar{\mathbf{Z}}\,||_2^2\,\mathbf{I}_{2L} \tag{5.71}$$

where $||\,\bar{\mathbf{Z}}\,||_2$ denotes the norm of matrix $\bar{\mathbf{Z}}$. With the unit-norm property of PSK symbol, the problem (5.64) has the following reformulation

$$\hat{\mathbf{s}} = \arg\min_{\mathbf{s}\in\mathcal{A}} \left\{\mathbf{s}^H\tilde{\mathbf{Z}}\tilde{\mathbf{Z}}^H\mathbf{s}\right\} \tag{5.72}$$

which can be further expressed as

$$\hat{\mathbf{s}} = \arg\min_{\mathbf{s}\in\mathcal{A}} \left\{\mathbf{s}^H\mathbf{P}\,\mathbf{s}\right\} \tag{5.73}$$

where $\mathbf{P} = \tilde{\mathbf{Z}}\tilde{\mathbf{Z}}^H + \mathbf{I}_{2L} \succ 0$ and full rank. Thus, the Cholesky factorization can be applied to this positive definite matrix $\mathbf{P}$, where $\mathbf{P} = \mathbf{G}^H\mathbf{G}$ with $\mathbf{G}$ being an upper triangular matrix. Furthermore, the problem above becomes

$$\hat{\mathbf{s}} = \arg\min_{\mathbf{s}\in\mathcal{A}} \left\{||\mathbf{G}\mathbf{s}||_2^2\right\} \tag{5.74}$$

Now, we are able to employ sphere decoding algorithm to this minimization problem. Sphere decoding only examines those candidate vectors $\mathbf{s}$ that all elements of $\mathbf{s}$ lie

inside a sphere of radius R [43], i.e.,

$$||\mathbf{Gs}||_2^2 \leq R^2 \tag{5.75}$$

Since matrix $\mathbf{G}$ has upper triangular matrix structure, the condition (5.75) can be checked element-wise. That being said, after we have found preliminary decisions $\hat{s}_l$ for the last $2L - i$ components $s_l, i + 1 \leq l \leq 2L$, we obtain a condition for the ith component $s_i, 1 \leq i < 2L$. To make this more clear, let g_{ik} denote the (i, k)-th entry of $\mathbf{G}$ with $1 \leq i, k \leq 2L$ and dist_{i+1}^2 denote the squared distance for the last $2L - i$ components, i.e.,

$$\text{dist}_{i+1}^2 = \sum_{l=i+1}^{2L} \left| \sum_{k=l}^{2L} g_{lk} \hat{s}_k \right|^2 \tag{5.76}$$

Then, the squared distance, dist_i^2, corresponding to the last $2L - i + 1$ components for the candidate symbols s_i, must satisfy the following distance constraint,

$$\text{dist}_i^2 = \left| g_{ii} s_i + \text{sum}(i) \right|^2 + \text{dist}_{i+1}^2 \leq R^2 \tag{5.77}$$

where $\text{sum}(i)$ denotes the linear combination of last $2L - i$ components for i-th search layer, i.e.,

$$\text{sum}(i) = \sum_{k=i+1}^{2L} g_{ik} \hat{s}_k \tag{5.78}$$

If some s_i is found to satisfy Eq. (5.77), the search will move up to the $(i-1)$th layer. Keep doing this search process until $i = 1$ is reached and thus, a valid vector $\hat{\mathbf{s}}$ is found in the sphere. Then, the search radius R is updated by

$$R = \left|\left|\mathbf{G}\hat{\mathbf{s}}\right|\right|_2 \tag{5.79}$$

and the search is repeated with this updated search radius R. Otherwise, if Eq. (5.77) cannot be satisfied for some index i, then, i is incremented and another candidate s_{i+1} is tested. If no possible $\mathbf{s}$ in this search process for some updated radius R can be found, the search is terminated.

In order to clearly understand the principle of sphere decoding originally for PAM constellation and properly modify to our designed PSK constellation, we like to recall the following key points in this algorithm [37, 43, 49, 52].

1. Initial search radius. Since the SE search strategy [43,52] is usually employed in fast sphere decoding algorithms, initial radius R is always unbounded and set at a reasonably large value so that at least one lattice point lies in the sphere. In practice, the choice of initial radius can be adjusted, i.e., if no point is found inside the sphere of radius R, the operation can be repeated with a greater radius.

2. The Viterbo-Boutros (VB) radius contraction [49]. This strategy attempts to accelerate the closest point search in lattice by iteratively contracting the search radius, which consists of three steps:

   (a) Given $\mathbf{G}$ and initial radius R_0, set the search radius $R = R_0$;

   (b) Find a lattice point $\mathbf{s} \in \mathcal{A}$ inside the sphere to satisfy $||\mathbf{Gs}||_2 < R$, then, save $\hat{\mathbf{s}} = \mathbf{s}$ and update $R = ||\mathbf{Gs}||_2$;

   (c) Repeat Step (b), otherwise, stop searching.

3. The Schnorr-Euchner (SE) search strategy [43, 52]. This strategy takes advantages of the Babai nearest plane algorithm [53] and the Pohst strategy [54–56] to improve the previous closest point algorithms by ordering the candidate symbols for a lattice point search in terms of nondecreasing distance from the transmitted symbol vector.

Table 5.2: Best Symbol Search that Minimizes Eq. (5.77)

f1. $[m_i, \text{step}_i, n_i] = \text{Bestsymbol}(\text{sum}(i), g_{ii}, M)$ // M is chosen to be p or q	
1. $\angle c = \text{angle}\,(-\text{sum}(i)/g_{ii})$	// phase $(-\pi < \angle c \leq \pi)$
2. $x = \frac{M}{2\pi}(\angle c)$	// phase index $(-\frac{M}{2} < x \leq \frac{M}{2},\ x \in \mathbb{R})$
3. $m_i = \text{round}(x)$	// integer phase index $(m_i \in \mathbb{Z})$
4. $n_i = 1$	// initialize the number of examined candidates
5. $\text{step}_i = \text{sign}(x - m_i)$	// initialize the step size for s_i

angle(x) denotes the phase angle of x, where angle($\cdot$) $\in (-\pi, \pi]$.
round(x) denotes the quantized integer closest to $x \in \mathbb{R}$.
sign(x) is 1 if $x > 0$, and -1 if $x \leq 0$.

Table 5.3: Next Symbol Selection using SE Search

f2. $[m_i, \text{step}_i, n_i] = \text{Nextsymbol}(m_i, \text{step}_i, n_i)$	
1. $m_i = m_i + \text{step}_i$	//zig-zag through the remaining symbols
2. $\text{step}_i = -\text{step}_i - \text{sign}(\text{step}_i)$	//update step size
3. $n_i = n_i + 1$	//update the number of examined candidates for s_i

Therefore, the key issue in the application of the sphere decoding principle to our blind ML channel estimation and detection problem is how to generalize the SE search strategy originally for PAM constellation to our designed PSK constellations. This generalization can be done by two stages: (a) Select the best candidate PSK symbol for s_i in the ith layer such that the distance dist_i starts with the smallest value, i.e., find the phase index m_i that minimizes dist_i in Eq. (5.77). (b) Otherwise, the search moves down to the $(i+1)$th layer and then, zigzag through the remaining phase indices such that dist_{i+1} increases monotonically. Owing to this nondecreasing property, the closest point search in lattice can be safely terminated as long as the distance exceeds the current sphere radius R.

Table 5.4: Pseudocode for Blind ML Sphere Decoder

SphereDecoder $(\mathbf{G}, p, q, 2L, R_0)$
Input: symbol size $2L$, $2L \times 2L$ upper triangular matrix $\mathbf{G}$, p-PSK constellation, q-PSK constellation
initial radius R_0
Output: the estimated symbol vector $\widehat{\mathbf{s}}$

$R = R_0$, $\text{dist}_{2L} = \lvert g_{2L,2L} \rvert$	// initialize sphere radius and distance
$s_{2L} = 1$, $m_{2L} = 0$	// initialize s_{2L} and phase index
$\text{step}_{2L} = -1$	// initialize step size of phase index
$n_{2L} = 1$	// initialize counter for examined candidates for s_{2L}
$i = 2L - 1$	// start with $(2L-1)$th layer
$\text{sum}(i) = g_{(2L-1)2L}$	// linear combination of last $2L - i$ components, see Eq. (5.78)
$[m_i, \text{step}_i, n_i] = \text{Bestsymbol}\,(\text{sum}(i), g_{ii}, q)$	// best candidate symbol and phase index for s_{2L-1}
< **loop** >	
$M = p$ or q	// judge p-PSK or q-PSK constellation by index i
if $i < 2L$ {	
$\text{dist}_i^2 = \left\lvert g_{ii} e^{j\frac{2\pi}{M} m_i} + \text{sum}(i) \right\rvert^2 + \text{dist}_{i+1}^2$ }	// update squared distance $1 \le i < 2L$, see Eq. (5.77)
if $\text{dist}_i < R$ and $n_i \le M$ {	// check sphere radius and constellation size
$\mathbf{s}_i = e^{j\frac{2\pi}{M} m_i}$	//save the candidate symbol for s_i
if $i \neq 1$ {	// not reached $1st$ component s_1
$i = i - 1$	// move up
$\text{sum}(i) = \sum_{l=i+1}^{2L} g_{il} \cdot s_l$	// linear combination of last $2L - i$ components, see Eq. (5.78)
$M = p$ or q	// judge p-PSK or q-PSK constellation by index i
$[m_i, \text{step}_i, n_i] = \text{Bestsymbol}\,(\text{sum}(i), g_{ii}, M)$	// best candidate symbol and phase index for s_i
} else	// reach the first component
{ $\widehat{\mathbf{s}} = \mathbf{s}$	// best lattice point so far
$R = \text{dist}_1$	// update sphere radius
$i = i + 1$	// move down
$M = p$ or q	// judge p-PSK or q-PSK constellation by index i
$[m_i, \text{step}_i, n_i] = \text{Nextsymbol}\,(m_i, \text{step}_i, n_i)$	// next candidate symbol examined for s_i
}	
} else	
{ do {	
if $i == 2L$ return $\widehat{\mathbf{s}}$ and exit	// outside sphere and search terminated
$i = i + 1$	// move down
$M = p$ or q	// judge p-PSK or q-PSK constellation by index i
} while $n_i == M$	// while all candidate symbols examined
$[m_i, \text{step}_i, n_i] = \text{Nextsymbol}\,(m_i, \text{step}_i, n_i)$	// next candidate symbol examined for s_i
}	
goto < **loop** >	

To make this sphere decoding algorithm easier to understand and operate, we provide a detailed pseudocode in Table 5.2, 5.3 and 5.4 for our blind ML sphere decoder, which properly modifies the algorithms given in [?, 43].

5.3 Simulation Results

In this section, we provide several simulation examples to examine the performance of our new blind ML detection method for the Alamouti STBC channel. In all the tests, the transmitted signals are selected at random alternately from a Q-PSK ($p = 4$) and a T-PSK ($q = 3$) constellation as required by our signalling scheme. Different blocks of symbols consisting of different numbers of frames are transmitted for the tests. Here, we consider 10, 15 and 20 frames in one transmission block respectively, i.e., $L = 10, 15$ and 20 in Eq. (5.52). The SNR here is defined as the average transmitted symbol energy to noise ratio (E_s/N_0), and gradually increased from 0dB to 20dB. At the receiver, we jointly estimate the channel coefficients and the transmitted symbols using the SDR-ML detector and sphere decoder, where the number of randomization of the SDR-ML detector is 40, i.e., $M_{rand} = 40$. In implementation, we carry out 50 trials, in each of which the channel is randomly generated following an i.i.d. circular Gaussian distribution. At each SNR, the average normalized MSE $\left(\bar{\epsilon}_h^2 = \frac{1}{50}\sum_{k=1}^{50} \|\mathbf{h}_k - \hat{\mathbf{h}}_k\|^2/\|\mathbf{h}_k\|^2\right)$ between the true channel coefficients and their estimates is calculated and the average symbol error rate (SER) is also computed.

Example 1: The purpose of this example is to evaluate the average normalized MSE of the estimated channel vector over which the signals are transmitted. In Figure 5.10, the solid curves with square, circular and diamond marks show the average normalized MSE of our blind SDR-ML detector. The dash-dot curves with plus, asterisk and "x" marks show the average normalized MSE of our blind sphere decoder. Also, the dash curves with triangle marks show the corresponding average

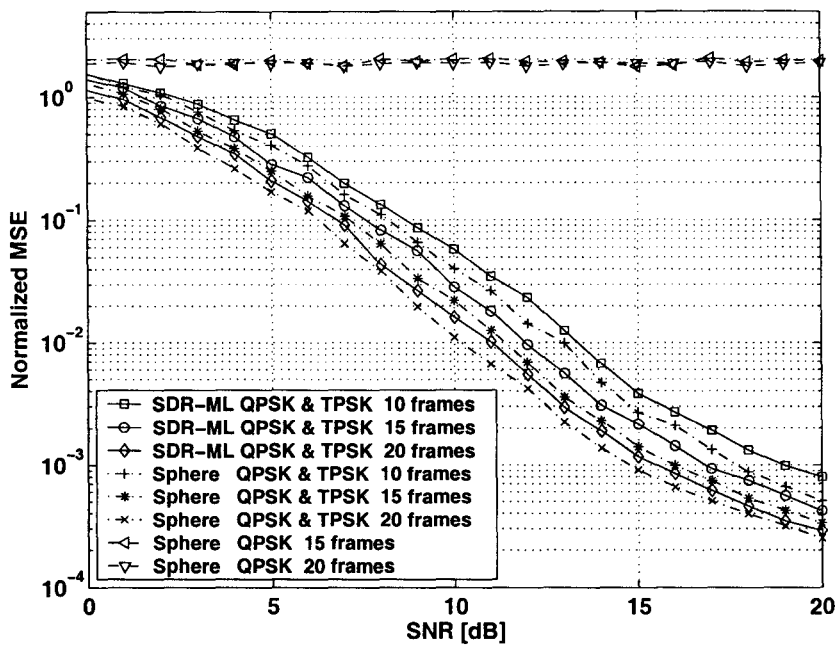

Figure 5.10: Channel normalized MSE vs. SNR using blind ML detection methods

normalized MSE of the channel estimates using blind sphere decoder which uses only one Q-PSK constellation.

From the solid and dash-dot curves, it can be observed that as the SNR increases, the average normalized MSE of the estimated channel coefficients quickly decreases, the longer is the transmission block, the smaller is the estimation error. On the contrary, as shown in the dash curves, no matter how long the transmission block is, the channel coefficients cannot be estimated with any degree of accuracy. This poor performance is due to the rotational ambiguity associated with the single signal constellation. Our signalling scheme employing two signal constellations eliminates such rotational ambiguity and thus offers substantially superior normalized MSE performance without using any pilot symbols.

Example 2: In this example, we are interested in the average SER performance of our signalling scheme equipped with the blind SDR-ML detector and the blind

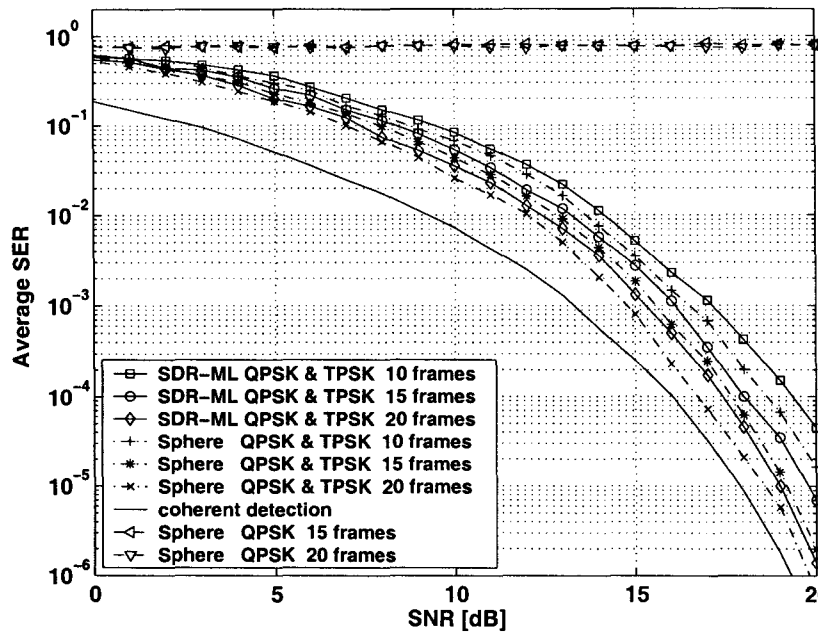

Figure 5.11: Average SER vs. SNR using blind ML detection methods

sphere decoder. For comparison purpose, the average SER performance of classical blind sphere decoder (which uses only one Q-PSK constellation) and the coherent ML detection (which necessitates perfect channel knowledge at the receiver) are also plotted. In Figure 5.11, the solid curves with square, circle, diamond marks represent the average SER of our blind SDR-ML detector. The dash-dot curves with plus, asterisk, "x" marks represent the average SER of our blind sphere decoder. Also, the dash curves with triangle marks are the average SER of classical blind sphere decoder, and the solid curve shows the average SER of coherent ML detector.

From Fig. 5.11, it can be observed that when the block data consists of 20 frames, at an average SER of at the 10^{-4}, the difference in SNR requirement between our signalling scheme and that the coherent detection method is only 1.5 dB. At lower SER, the difference is even smaller. On the contrary, the dash curves show that the rotational ambiguity in classical signal transmission results in very poor average SER

performance due to the exploitation of only a single Q-PSK constellation.

In summary, the two simulation examples above verify our theoretic analysis. When only finite received signals are provided, the blind ML detection methods employing our signalling scheme can eliminate the rotational ambiguity and thus, achieve substantially better performances of channel estimation and symbol detection without the aid of pilot symbols.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In this thesis, we proposed a novel blind channel identification technique for Alamouti STBC channel by properly designing and transmitting signals. Using our signalling scheme, we proved that in the noise-free case, only two distinct pairs of symbols (two consecutive frames) are needed to uniquely determine the channel coefficients and decode the symbols, while in the case of complex Gaussian noise, if the pth-order and qth-order statistics (p and q being co-prime integers) of the received signals are available or can be estimated accurately, we are still able to uniquely determine the channel coefficients. In both cases, simple closed-form solutions were derived by exploiting specific properties of the Alamouti code and linear Diophantine equation theory.

However, when only a limited number of received data are available, under Gaussian noise environment, we suggest the use of the semi-definite relaxation randomization method and the sphere decoding method to implement blind ML detection so that the joint estimation of the channel and the transmitted symbols can be efficiently facilitated. Simulation results show that our blind ML estimation methods provide

superior the average normalized mean square error in channel estimation compared to the method using only one constellation and that the average symbol error rate is close to that of the coherent detector, particularly when the SNR is high.

As an extension of our signalling scheme to other channels, we applied a specific space-time coding technique to multi-input single-output system with an even number of transmitter antennas. We demonstrated that this system has an equivalent representation which consists of multiple Alamouti STBC subchannels. Hence, our blind channel estimation technique is also useful to the estimation of this particular space-time coded MISO communication system.

6.2 Future Work

There are many possibilities for future work in this area.

1. In this thesis, our signalling scheme is proposed for the estimation of single user Alamouti STBC channel. In the future, we may consider to apply it to multiple user scenario.

2. Here, we discuss the estimation of Alamouti STBC channel under flat fading environment. If Orthogonal Frequency Division Multiplexing (OFDM) technique is employed, further possibility may include extending the channel estimation from flat fading channel to frequency selective Alamouti STBC channel.

3. The idea of our signalling scheme may also be applicable to MIMO system with the generalized OSTBC, i.e., estimating the channel through a properly designed signalling scheme.

4. In addition, the idea of joint channel estimation and symbol detection opens up many research possibilities. In implementation of our blind ML estimation

methods, the SDR-ML detector and the sphere decoder are both found to be very slow in operation when the frame number in one observation block is beyond 20. To improve the performance of our blind ML estimation methods, there may exist other optimization algorithms which can efficiently handle the maximum likelihood estimation problem with large data size.

Appendix A

Proof of Theorem 1

To prove Theorem 1, we need the following lemmas and definitions.

Lemma 1 [39] *If* $\gcd(p,q) = 1$, *the following Diophantine equation*

$$pm + qn = k \tag{A.1}$$

has integer solutions with respect to variables m *and* n. *If* (m_0, n_0) *is a specific solution to Eq. (A.1), then, the set of all solutions can be characterized by*

$$m = m_0 + qt, \quad n = n_0 - pt \tag{A.2}$$

where t *is any integer.* ■

Proof: From $pm + qn = k$ and $pm_0 + qn_0 = k$, we have $p(m - m_0) + q(n - n_0) = 0$. Since $\gcd(p,q) = 1$, we deduce that p divides $n - n_0$. Let $n = n_0 - pt$, so that $m = m_0 + qt$. The required result follows from substituting these into Eq. (A.1). □

Definition 1 [39] *Let* m *be a natural number. If* $a - b$ *is a multiple of* m, *then we say that* a *and* b *are congruent mod* m, *and we write* $a \equiv b \ (mod\ m)$. ■

The congruence has the following fundamental properties [39]:

1. $a \equiv a \pmod{m}$ (*reflexive*);
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ (*symmetric*);
3. If $a \equiv b, b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ (*transitive*). ■

The above three properties show that congruence is an equivalence relation. The set of integers can be partitioned into equivalence classes so that integers in each class are congruent among themselves, and two integers from different classes are not congruent. We call these equivalence classes *residue classes.*

Definition 2 [39] *We denote by $\varphi(m)$ the number of residue classes (mod m) co-prime with m. This function $\varphi(m)$ is called Euler's function, and it may also be described as the number of all positive integers not exceeding m and prime with m.* ■

The Euler function has the following properties [39]:

1. Multiplicative property, i.e., If $\gcd(m, m') = 1$, then, $\varphi(mm') = \varphi(m)\varphi(m')$.
2. For any integers m, if the standard factorization is given by

$$m = p_1^{l_1} \cdots p_s^{l_s}, \quad p_1 < p_2 < \cdots < p_s \tag{A.3}$$

where $p_1, p_2, \cdots, p_s$ are prime number, then, we have

$$\varphi(m) = \varphi(p_1^{l_1}) \cdots \varphi(p_s^{l_s}) \tag{A.4}$$

3. For any integer m, we have

$$\varphi(m) = m \prod_{p|m} (1 - \frac{1}{p}) \tag{A.5}$$

where $p|m$ defines m is divisible by p, and p runs over the distinct prime divisors of m. ■

Example: $\varphi(12) = \varphi(2^2 \cdot 3^1) = 2^2 \cdot 3^1(1 - \frac{1}{2})(1 - \frac{1}{3}) = 4$.

Definition 3 [39] *If we select one member of each residue class co-prime with m:*

$$a_1, \ldots, a_{\varphi(m)}$$

then we call this set of integers a reduced residue system. ■

Lemma 2 [39] *Let $a_1, a_2, \ldots, a_{\varphi(m)}$ be a reduced residue system, and suppose that $\gcd(k, m) = 1$. Then $ka_1, ka_2, \ldots, ka_{\varphi(m)}$ is also a reduced residue system.* ■

Proof: Clearly we have $\gcd(ka_i, m) = 1$, so that each ka_i represents a residue class co-prime with m. If $ka_i \equiv ka_j \pmod{m}$, then, since $\gcd(k, m) = 1$, we have $a_i \equiv a_j \pmod{m}$. Therefore, the members ka_i represent distinct residue classes. □

Lemma 3 [39]*(Euler) If* $\gcd(k, m) = 1$, *then,* $k^{\varphi(m)} \equiv 1 \ (mod\ m)$. ■

Proof: From Lemma 2, we have:

$$\prod_{v=1}^{\varphi(m)} (ka_v) \equiv \prod_{v=1}^{\varphi(m)} a_v \pmod{m}$$

Since $\gcd(m, a_i) = 1$, it follows that $k^{\varphi(m)} \equiv 1 \pmod{m}$. □

In order to prove Theorem 1, we also need the following lemmas.

Lemma 4 [58] *Let two positive integers p and q be co-prime. Then, for any given integer k, there exists a unique pair of integers m and n such that*

$$k = pm + qn, \qquad for\ \ 0 \leq m < q \tag{A.6}$$

Furthermore, m and n can be explicitly determined by

$$m = kp^{\varphi(q)-1} - q\left\lceil \frac{kp^{\varphi(q)-1}}{q} \right\rceil \tag{A.7a}$$

$$n = \frac{k}{q}\left(1 - p^{\varphi(q)}\right) + p\left\lceil \frac{kp^{\varphi(q)-1}}{q} \right\rceil \tag{A.7b}$$

■

Proof: Since $\gcd(p, q) = 1$, by Lemma 1, there exists a pair of integers m and n satisfying Eq. (A.6). To prove the uniqueness of the solutions, suppose there exist two different pairs of m, n and m', n' with $0 \leq m, m' < q$ such that

$$k = pm + qn \tag{A.8a}$$

$$k = pm' + qn' \tag{A.8b}$$

From these two equations, we have $(m - m')p = (n' - n)q$. Since $\gcd(p, q) = 1$, q divides $m - m'$. Combing this with condition $0 \leq m, m' < q$ results in $m = m'$ and thus, $n = n'$. Therefore, the solution is unique. In the following, we prove that Eqs. (A.7a) and (A.7b) are true based on the Euclid algorithm (see Appendix C). From Eq. (A.6), we have

$$k \equiv pm \pmod{q} \tag{A.9}$$

Since $\gcd(p, q) = 1$, $p^{\varphi(q)-1}$ is also co-prime to q. Multiplying both sides of Eq. (A.9) by $p^{\varphi(q)-1}$ yields

$$\begin{aligned} p^{\varphi(q)-1}k &\equiv p^{\varphi(q)-1}pm \pmod{q} \\ &\equiv p^{\varphi(q)}m \pmod{q} \end{aligned} \tag{A.10}$$

By Lemma 3, we have $p^{\varphi(q)} \equiv 1 \pmod{q}$. Substituting this into Eq. (A.10) leads to

$$\begin{aligned} m &\equiv kp^{\varphi(q)-1} \pmod{q} \\ &= kp^{\varphi(q)-1} - q\left\lceil \frac{kp^{\varphi(q)-1}}{q} \right\rceil \end{aligned} \tag{A.11}$$

where $0 \leq m < q$. Substituting Eq. (A.11) into Eq. (A.6) yields

$$n = \frac{k}{q}\left(1 - p^{\varphi(q)}\right) + p\left\lceil \frac{kp^{\varphi(q)-1}}{q} \right\rceil \tag{A.12}$$

□

Lemma 5 [58] *Let two positive integers p and q be co-prime, s_p and s_q denote two symbols chosen from p-PSK and q-PSK constellations, respectively, i.e., $s_p \in \mathcal{S}_p$ and $s_q \in \mathcal{S}_q$. Suppose*

$$s_p s_q = \exp\left(j\frac{2\pi k}{pq}\right), \quad \text{for } 0 \leq k < pq \tag{A.13}$$

then, s_p and s_q can be uniquely determined by

$$s_p = \exp\left(j\frac{2\pi}{p}\left(\frac{k}{q}\left(1 - p^{\varphi(q)}\right) + p\left\lceil \frac{kp^{\varphi(q)-1}}{q} \right\rceil\right)\right) \tag{A.14a}$$

$$s_q = \exp\left(j\frac{2\pi}{q}\left(kp^{\varphi(q)-1} - q\left\lceil \frac{kp^{\varphi(q)-1}}{q} \right\rceil\right)\right) \tag{A.14b}$$

where $0 \leq \left(kp^{\varphi(q)-1} - q\left\lceil \frac{kp^{\varphi(q)-1}}{q} \right\rceil\right) < q$. ■

Proof: From Lemma 4, for any given k, there exists a pair of s_p and s_q satisfying Eqs. (A.14) and (A.6). Therefore, we have

$$\begin{aligned} \exp\left(j\frac{2\pi k}{pq}\right) &= \exp\left(j\frac{2\pi(mp+nq)}{pq}\right) \\ &= \exp\left(j\frac{2\pi m}{q}\right)\exp\left(j\frac{2\pi n}{p}\right) \end{aligned}$$

That is, such a pair of s_p and s_q is a solution to Eq. (A.49). In the following, we will prove the uniqueness of the solutions. To do that, suppose there exists a different pair of symbols $s'_p \in \mathcal{S}_p$ and $s'_q \in \mathcal{S}_q$ satisfying Eq. (A.49). Hence, $s_p s_q = s'_p s'_q$. Let

$$s_p = \exp\left(j\frac{2\pi n}{p}\right),\ 0 \le n < p \quad \text{and} \quad s_q = \exp\left(j\frac{2\pi m}{q}\right),\ 0 \le m < q \tag{A.15a}$$

$$s'_p = \exp\left(j\frac{2\pi n'}{p}\right),\ 0 \le n' < p \quad \text{and} \quad s'_q = \exp\left(j\frac{2\pi m'}{q}\right),\ 0 \le m' < q \tag{A.15b}$$

Then, we have

$$\exp\left(j2\pi\left(\frac{n}{p}+\frac{m}{q}\right)\right) = \exp\left(j2\pi\left(\frac{n'}{p}+\frac{m'}{q}\right)\right) \tag{A.16}$$

This is equivalent to

$$(n-n')q \equiv (m'-m)p \pmod{pq} \tag{A.17}$$

Therefore, $m'-m \equiv 0 \pmod{q}$ and $n-n' \equiv 0 \pmod{p}$. Since $0 \le m, m' < q$ and $0 \le n, n' < p$, we have $m = m'$ and $n = n'$. □

Lemma 6 [58] *Let $s_{pn} \in \mathcal{S}_p$ and $s_{qn} \in \mathcal{S}_q$ for $n = i, i+1$ be four symbols respectively chosen from p-PSK and q-PSK constellations, p and q being co-prime positive integers. Define $a_{i1} = \frac{1}{2}\left(s_{p(i+1)}s^*_{pi} + s_{q(i+1)}s^*_{qi}\right)$ and $a_{i2} = \frac{1}{2}\left(s_{pi}s_{q(i+1)} - s_{qi}s_{p(i+1)}\right)$. Then, we have*

$$|a_{i1}|^2 + |a_{i2}|^2 = 1 \tag{A.18}$$

■

Proof: From the definition of a_{i1} and a_{i2}, we have

$$\begin{aligned} |a_{i1}|^2 &= \frac{1}{4}\left(s_{p(i+1)}s_{pi}^* + s_{q(i+1)}s_{qi}^*\right)^H\left(s_{p(i+1)}s_{pi}^* + s_{q(i+1)}s_{qi}^*\right) \\ &= \frac{1}{4}\left[2 + s_{p(i+1)}s_{pi}^* s_{q(i+1)}^* s_{qi} + s_{p(i+1)}^* s_{pi} s_{q(i+1)} s_{qi}^*\right] \qquad \text{(A.19a)} \\ |a_{i2}|^2 &= \frac{1}{4}\left(s_{pi}s_{q(i+1)} - s_{qi}s_{p(i+1)}\right)^H\left(s_{pi}s_{q(i+1)} - s_{qi}s_{p(i+1)}\right) \\ &= \frac{1}{4}\left[2 - s_{pi}s_{p(i+1)}^* s_{qi}^* s_{q(i+1)} - s_{pi}^* s_{p(i+1)} s_{qi} s_{q(i+1)}^*\right] \qquad \text{(A.19b)} \end{aligned}$$

Adding both sides of the two equations above yields $|a_{i1}|^2 + |a_{i2}|^2 = 1$. □

Lemma 7 [58] *Let $s_{pn} \in \mathcal{S}_p$ and $s_{qn} \in \mathcal{S}_q$ for $n = i, i+1$ be four symbols respectively chosen from p-PSK and q-PSK constellations, p and q being co-prime positive integers. Also, let $a_{i1} = \frac{1}{2}\left(s_{p(i+1)}s_{pi}^* + s_{q(i+1)}s_{qi}^*\right)$ and $a_{i2} = \frac{1}{2}\left(s_{pi}s_{q(i+1)} - s_{qi}s_{p(i+1)}\right)$, where $a_{i1} \triangleq |a_{i1}|e^{j\theta_{i1}}, \theta_{i1} \in [-\pi, \pi)$ with $\alpha \triangleq \arccos|a_{i1}|$ and $a_{i2} \triangleq |a_{i2}|e^{j\theta_{i2}}, \theta_{i2} \in [-\pi, \pi)$. Then, the solutions of the following equation*

$$\left|\frac{a_{i2}}{a_{i1} - \exp(j\omega)}\right|^2 = 1 \qquad \text{(A.20)}$$

with respect to variable ω with $0 \le \omega < 2\pi$ can be expressed by

$$\omega = \theta_{i1} \pm \alpha - 2l\pi \qquad \text{(A.21)}$$

Furthermore, for such ω, we have

$$\frac{a_{i2}}{a_{i1} - \exp(j\omega)} = \begin{cases} \exp\left(j\left(\theta_{i2} - \theta_{i1} + \frac{\pi}{2}\right)\right), & \omega = \theta_{i1} + \alpha - 2l\pi \\ \exp\left(j\left(\theta_{i2} - \theta_{i1} - \frac{\pi}{2}\right)\right), & \omega = \theta_{i1} - \alpha - 2l\pi \end{cases} \qquad \text{(A.22)}$$

where $l = 0, -1$. ■

Proof: Eq. (A.20) is equivalent to

$$\begin{aligned} |a_{i2}|^2 &= \left|a_{i1} - \exp(j\omega)\right|^2 \\ &= a_{i1}^H a_{i1} - a_{i1}^H \exp(j\omega) - a_{i1}\exp(-j\omega) + 1 \\ &= |a_{i1}|^2 - |a_{i1}|\Big\{\exp[j(\omega-\theta_{i1})] + \exp[-j(\omega-\theta_{i1})]\Big\} + 1 \\ &= |a_{i1}|^2 - 2|a_{i1}|\cos(\theta_{i1}-\omega) + 1 \end{aligned} \tag{A.23}$$

where $0 \leq \omega < 2\pi$. Using Eq. (A.18) in Lemma 6 results in

$$1 - |a_{i1}|^2 = |a_{i1}|^2 - 2|a_{i1}|\cos(\theta_{i1}-\omega) + 1 \tag{A.24}$$

which can be further simplified as

$$\cos(\theta_{i1}-\omega) = |a_{i1}| = \cos\alpha \tag{A.25}$$

Therefore, we get

$$\omega = \theta_{i1} \pm \alpha - 2l\pi \tag{A.26}$$

If $\omega = \theta_{i1} + \alpha - 2l\pi$, then, we have

$$-\pi - 2l\pi \leq \theta_{i1} + \alpha - 2l\pi < \frac{3\pi}{2} - 2l\pi \tag{A.27}$$

since $\theta_{i1} \in [-\pi, \pi)$ and $\alpha \in [0, \pi/2]$. Hence, for $0 \leq \omega < 2\pi$, the possible values for l are 0 and -1. Similarly, when $\omega = \theta_{i1} - \alpha - 2l\pi$, the possible values for l are also 0 and -1.

In addition, using Eq. (A.26), we have

$$\begin{aligned}\frac{a_{i2}}{a_{i1}-\exp\left(j\omega\right)} &= \frac{a_{i2}}{a_{i1}-\exp\left(j(\theta_{i1}\pm\alpha)\right)} \\ &= \frac{a_{i2}}{\exp(j\theta_{i1})\big(|a_{i1}|-\exp(\pm j\alpha)\big)} \\ &= \frac{a_{i2}}{\exp(j\theta_{i1})\big(|a_{i1}|-\cos(\alpha)\mp j\sin(\alpha)\big)} \\ &= \frac{\pm j\, a_{i2}}{\exp(j\theta_{i1})\sqrt{1-|a_{i1}|^2}} \end{aligned} \tag{A.28}$$

where we have used $|a_{i1}| = \cos\alpha$. By Lemma 6, $\sin\alpha = \sqrt{1-|a_{i1}|^2} = |a_{i2}|$ for $\alpha \in [0, \frac{\pi}{2}]$. From the definition of $a_{i1} = |a_{i1}|e^{j\theta_{i1}}$ and $a_{i2} = |a_{i2}|e^{j\theta_{i2}}$, Eq. (A.28) can be further reduced to

$$\begin{aligned}\frac{a_{i2}}{a_{i1}-\exp\left(j\omega\right)} &= \begin{cases} \frac{j\,|a_{i2}|\exp(j\theta_{i2})}{\exp(j\theta_{i1})\,|a_{i2}|}, & \omega = \theta_{i1}+\alpha-2l\pi \\ \frac{-j\,|a_{i2}|\exp(j\theta_{i2})}{\exp(j\theta_{i1})\,|a_{i2}|}, & \omega = \theta_{i1}-\alpha-2l\pi \end{cases} \\ &= \begin{cases} j\exp\big(j(\theta_{i2}-\theta_{i1})\big), & \omega = \theta_{i1}+\alpha-2l\pi \\ -j\exp\big(j(\theta_{i2}-\theta_{i1})\big), & \omega = \theta_{i1}-\alpha-2l\pi \end{cases} \\ &= \begin{cases} \exp\Big(j\big(\theta_{i2}-\theta_{i1}+\frac{\pi}{2}\big)\Big), & \omega = \theta_{i1}+\alpha-2l\pi \\ \exp\Big(j\big(\theta_{i2}-\theta_{i1}-\frac{\pi}{2}\big)\Big), & \omega = \theta_{i1}-\alpha-2l\pi \end{cases} \end{aligned}$$

where $l = 0, -1$. This completes the proof of Lemma 7.

□

We are now in a position to prove Theorem 1 [58].

Proof of Theorem 1: First, we rewrite Eqs. (4.43) as

$$s_{pi}s_{qi}a_{i1} + a_{i2} = s_{pi}s_{q(i+1)} \tag{A.29a}$$

$$s_{pi}s_{qi}a_{i1} - a_{i2} = s_{qi}s_{p(i+1)} \tag{A.29b}$$

Particularly when $a_{i1} = 0$, the above equations are reduced to

$$s_{pi}s_{q(i+1)} = a_{i2} \tag{A.30a}$$

$$s_{qi}s_{p(i+1)} = -a_{i2} \tag{A.30b}$$

Using Lemma 5, from Eq. (A.30a), we can uniquely determine s_{pi} and $s_{q(i+1)}$ as

$$s_{pi} = \exp\left(j\frac{2\pi}{p}\left(\frac{k_1}{q}\left(1-p^{\varphi(q)}\right)+p\left\lceil\frac{k_1 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{A.31a}$$

$$s_{q(i+1)} = \exp\left(j\frac{2\pi}{q}\left(k_1 p^{\varphi(q)-1}-q\left\lceil\frac{k_1 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{A.31b}$$

where k_1 satisfies $\exp\left(j\frac{2\pi k_1}{pq}\right) = a_{i2}$, $k_1 \in [0, pq)$. Similarly, we can also uniquely determine s_{qi} and $s_{p(i+1)}$ from Eq. (A.30b) as

$$s_{p(i+1)} = \exp\left(j\frac{2\pi}{p}\left(\frac{k_2}{q}\left(1-p^{\varphi(q)}\right)+p\left\lceil\frac{k_2 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{A.32a}$$

$$s_{qi} = \exp\left(j\frac{2\pi}{q}\left(k_2 p^{\varphi(q)-1}-q\left\lceil\frac{k_2 p^{\varphi(q)-1}}{q}\right\rceil\right)\right) \tag{A.32b}$$

where k_2 satisfies $\exp\left(j\frac{2\pi k_2}{pq}\right) = -a_{i2}$, $k_2 \in [0, pq)$. This proves Statement 1.

In the following we will prove Statement 2. Since $s_{pi}, s_{p(i+1)} \in \mathcal{S}_p$ and $s_{qi}, s_{q(i+1)} \in \mathcal{S}_q$, the products $s^*_{pi}s_{p(i+1)}$ and $s^*_{qi}s_{q(i+1)}$ are still in $\mathcal{S}_p$ and $\mathcal{S}_q$, respectively. Let

$$s^*_{pi}s_{p(i+1)} = \exp\left(j2\pi\ell_p/p\right), \quad 0 \le \ell_p < p \tag{A.33a}$$

$$s^*_{qi}s_{q(i+1)} = \exp\left(j2\pi\ell_q/q\right), \quad 0 \le \ell_q < q \tag{A.33b}$$

From Eqs. (A.33), we have

$$s_{p(i+1)} = \exp\left(j\,2\pi\ell_p/p\right) s_{pi}, \quad 0 \le \ell_p < p \tag{A.34a}$$

$$s_{q(i+1)} = \exp\left(j\,2\pi\ell_q/q\right) s_{qi}, \quad 0 \le \ell_q < q \tag{A.34b}$$

Substituting Eqs. (A.34a) and (A.34b) into Eqs. (A.29b) and (A.29a) results in

$$s_{pi}s_{qi}\Big(a_{i1} - \exp\left(j\,2\pi\ell_p/p\right)\Big) = a_{i2}, \quad 0 \le \ell_p < p \tag{A.35a}$$

$$s_{pi}s_{qi}\Big(a_{i1} - \exp\left(j\,2\pi\ell_q/q\right)\Big) = -a_{i2}, \quad 0 \le \ell_q < q \tag{A.35b}$$

Now, we can claim $a_{i1} \neq \exp\left(j\frac{2\pi\ell_p}{p}\right)$ and $a_{i1} \neq \exp\left(j\frac{2\pi\ell_q}{q}\right)$. Otherwise, if $a_{i1} = \exp\left(j\frac{2\pi\ell_p}{p}\right)$ for $0 \le \ell_p < p$, then, a_{i2} in Eq. (A.35b) must be equal to zero. As a result, Eq. (A.29a) becomes

$$s_{pi}s_{qi}\exp\left(j\,2\pi\ell_p/p\right) = s_{pi}s_{q(i+1)}, \quad 0 \le \ell_p < p \tag{A.36}$$

Since $s_{pi} \neq 0$, from Eq. (A.36), we get

$$s_{qi}\exp\left(j\,2\pi\ell_p/p\right) = s_{q(i+1)}, \quad 0 \le \ell_p < p \tag{A.37}$$

Let $s_{qi} = \exp\left(j\,2\pi\ell_{qi}/q\right)$ and $s_{q(i+1)} = \exp\left(j\,2\pi\ell_{q(i+1)}/q\right)$. Then, Eq. (A.37) is expressed as

$$\exp\left(j\frac{2\pi\ell_{qi}}{q}\right)\exp\left(j\frac{2\pi\ell_p}{p}\right) = \exp\left(j\frac{2\pi\ell_{q(i+1)}}{q}\right), \quad 0 \le \ell_p < p \tag{A.38}$$

which is equivalent to

$$p\,\ell_{qi} + q\,\ell_p \equiv p\,\ell_{q(i+1)} \pmod{p\,q}, \quad 0 \le \ell_p < p \tag{A.39}$$

Therefore, we have

$$\ell_p\, q \equiv 0 \pmod{p}, \quad 0 \leq \ell_p < p \tag{A.40}$$

Since p and q are co-prime, the above equation holds only if $\ell_p \equiv 0 \,(\mathrm{mod}\, p)$. Combing this with $0 \leq \ell_p < p$ yields $\ell_p = 0$ and as a result, $a_{i1} = 1$ and $a_{i2} = 0$. With these a_{i1}, a_{i2} and Eqs. (A.29), we get $s_{qi} = s_{q(i+1)}$ and $s_{pi} = s_{p(i+1)}$ and we further have $\mathbf{z}_i = \mathbf{z}_{i+1}$, since $\mathbf{z}_i = \mathbf{S}_i\mathbf{h}$ and $\mathbf{z}_{i+1} = \mathbf{S}_{i+1}\mathbf{h}$ in Eqs. (4.35), which contradicts with the assumption in Theorem 1 that $\mathbf{z}_i$ and $\mathbf{z}_{i+1}$ are two distinct received signal vectors. Therefore, $a_{i1} \neq \exp\left(j\, 2\pi\ell_p/p\right)$ and Eq. (A.35a) can be rewritten as

$$s_{pi}s_{qi} = \frac{a_{i2}}{a_{i1} - \exp\left(j\frac{2\pi\ell_p}{p}\right)}, \quad 0 \leq \ell_p < p \tag{A.41}$$

Similarly, we can prove $a_{i1} \neq \exp\left(j\, 2\pi\ell_q/q\right)$ and thus, Eq. (A.35b) can be rewritten as

$$s_{pi}s_{qi} = \frac{-a_{i2}}{a_{i1} - \exp\left(j\frac{2\pi\ell_q}{q}\right)}, \quad 0 \leq \ell_q < q \tag{A.42}$$

Combining Eqs. (A.41) and (A.42) results in

$$\exp\left(j\frac{2\pi\ell_p}{p}\right) + \exp\left(j\frac{2\pi\ell_q}{q}\right) = 2\, a_{i1} \tag{A.43}$$

for $0 \leq \ell_p < p$ and $0 \leq \ell_q < q$. In addition, since the product $s_{pi}s_{qi}$ still belongs to PSK constellation in Lemma 5, from Eqs. (A.41) and (A.42), we can get

$$\left|\frac{a_{i2}}{a_{i1} - \exp\left(j\frac{2\pi\ell_p}{p}\right)}\right|^2 = \left|\frac{-a_{i2}}{a_{i1} - \exp\left(j\frac{2\pi\ell_q}{q}\right)}\right|^2 = 1 \tag{A.44}$$

where $0 \leq \ell_p < p$ and $0 \leq \ell_q < q$. For notation simplicity, let $\omega_p \triangleq 2\pi\ell_p/p$ and $\omega_q \triangleq 2\pi\ell_q/q$. By Lemma 7, we have

$$\omega_p = \theta_{i1} \pm \alpha - 2l_1\pi, \quad 0 \leq \omega_p < 2\pi \tag{A.45a}$$

$$\omega_q = \theta_{i1} \pm \alpha - 2l_2\pi, \quad 0 \leq \omega_q < 2\pi \tag{A.45b}$$

where $l_1 = 0, -1$ and $l_2 = 0, -1$.

Now, we consider the following cases for all possible values of ω_p, ω_q for l_1 and l_2. **Case 1**: $\omega_p = \theta_{i1} + \alpha - 2l_1\pi$ and $\omega_q = \theta_{i1} + \alpha - 2l_2\pi$. In this case, we have $\omega_p = \omega_q + 2(l_2 - l_1)\pi$. This is equivalent to

$$\ell_q\, p + (-\ell_p)\, q = -(l_2 - l_1)p\, q. \tag{A.46}$$

Therefore, we have $\ell_q p \equiv 0(\text{mod } q)$ and $\ell_p q \equiv 0(\text{mod } p)$. Since $\gcd(p, q) = 1$, $\ell_p \equiv 0(\text{mod } q)$ and $\ell_q \equiv 0(\text{mod } p)$. Combining with $0 \leq \ell_p < p$ and $0 \leq \ell_q < q$ yields $\ell_p = 0$ and $\ell_q = 0$. Substituting these into Eq. (A.43) results in $a_{i1} = 1$ and as a result, by Lemma 6, $a_{i2} = 0$. Thus, from Eqs. (A.29), we further get

$$s_{pi} = s_{p(i+1)}, \quad s_{qi} = s_{q(i+1)} \tag{A.47}$$

which contradicts with our assumption in Theorem 1. Therefore, Case 1 cannot happen.

Case 2: $\omega_p = \theta_{i1} - \alpha - 2l_1\pi$ and $\omega_q = \theta_{i1} - \alpha - 2l_2\pi$. Similar to Case 1, Case 2 cannot happen either.

Therefore, in order to prove Statement 2 of Theorem 1, we only need to consider the following cases according to all the possible conditions of θ_{i1} and α so that the corresponding ℓ_p and ℓ_q can be uniquely determined

Case 3: $e^{jp(\theta_{i1}+\alpha)} = 1$, $e^{jq(\theta_{i1}-\alpha)} = 1$, $\omega_p = \theta_{i1} + \alpha - 2l_1\pi$ and $\omega_q = \theta_{i1} - \alpha - 2l_2\pi$. In this case, we will discuss all the following possible values of l_1 and l_2.

a. If $0 \leq \theta_{i1} + \alpha < 2\pi$ and $0 \leq \theta_{i1} - \alpha < 2\pi$, i.e., $\alpha \leq \theta_{i1} < 2\pi - \alpha$, then $l_1 = 0$ and $l_2 = 0$. Otherwise, either $l_1 = -1$ or $l_2 = -1$. This results in $2\pi \leq \omega_p < 4\pi$ or $2\pi \leq \omega_q < 4\pi$, which contradicts with the angle constraints given in Eqs. (A.45). Therefore, we have $\ell_p = \frac{\omega_p p}{2\pi} = \frac{(\theta_{i1}+\alpha)p}{2\pi}$, $\ell_q = \frac{\omega_q q}{2\pi} = \frac{(\theta_{i1}-\alpha)q}{2\pi}$.

b. If $-\alpha \leq \theta_{i1} < \alpha$, then $l_1 = 0$ and $l_2 = -1$. Otherwise, either $l_1 = -1$ or $l_2 = 0$. This yields $2\pi \leq \omega_p < 4\pi$ or $\omega_q < 0$, which also contradicts with the angle constraints given in Eqs. (A.45). Therefore, we have $\ell_p = \frac{\omega_p p}{2\pi} = \frac{(\theta_{i1}+\alpha)p}{2\pi}$, $\ell_q = \frac{\omega_q q}{2\pi} = \frac{(\theta_{i1}-\alpha+2\pi)q}{2\pi}$.

c. If $-2\pi + \alpha \leq \theta_{i1} < -\alpha$, then, $l_1 = -1$ and $l_2 = -1$. Otherwise, either $l_1 = 0$ or $l_2 = 0$. This leads to $\omega_p < 0$ or $\omega_q < 0$, which also contradicts with the angle constraints given in Eqs. (A.45). Therefore, we have $\ell_p = \frac{\omega_p p}{2\pi} = \frac{(\theta_{i1}+\alpha+2\pi)p}{2\pi}$ and $\ell_q = \frac{\omega_q q}{2\pi} = \frac{(\theta_{i1}-\alpha+2\pi)q}{2\pi}$.

Case 4: $e^{jp(\theta_{i1}-\alpha)} = 1$, $e^{jq(\theta_{i1}+\alpha)} = 1$, $\omega_p = \theta_{i1} - \alpha - 2l_1\pi$ and $\omega_q = \theta_{i1} + \alpha - 2l_2\pi$. Similar to Case 3, we will discuss all the following possible values of l_1 and l_2.

a. If $\alpha \leq \theta_{i1} < 2\pi - \alpha$, then, $l_1 = 0$ and $l_2 = 0$. Otherwise, either $l_1 = -1$ or $l_2 = -1$. This results in $2\pi \leq \omega_p < 4\pi$ or $2\pi \leq \omega_q < 4\pi$, which also contradicts with the angle constraints given in Eqs. (A.45). Therefore, we have $\ell_p = \frac{\omega_p p}{2\pi} = \frac{(\theta_{i1}-\alpha)p}{2\pi}$, $\ell_q = \frac{\omega_q q}{2\pi} = \frac{(\theta_{i1}+\alpha)q}{2\pi}$.

b. If $-\alpha \leq \theta_{i1} < \alpha$, then, $l_1 = -1$ and $l_2 = 0$. Otherwise, either $l_1 = 0$ or $l_2 = -1$. This yields $\omega_p < 0$ or $2\pi \leq \omega_q < 4\pi$, which also contradicts with the angle constraints given in Eqs. (A.45). Therefore, we have $\ell_p = \frac{\omega_p p}{2\pi} = \frac{(\theta_{i1}-\alpha+2\pi)p}{2\pi}$, $\ell_q = \frac{\omega_q q}{2\pi} = \frac{(\theta_{i1}+\alpha)q}{2\pi}$.

c. If $-2\pi + \alpha \leq \theta_{i1} < -\alpha$, then, $l_1 = -1$ and $l_2 = -1$. Otherwise, either $l_1 = 0$ or $l_2 = 0$. This yields $\omega_p < 0$ or $\omega_q < 0$, which also contradicts with the angle constraints given in Eqs. (A.45). Therefore, we have $\ell_p = \frac{\omega_p p}{2\pi} = \frac{(\theta_{i1}-\alpha+2\pi)p}{2\pi}$, $\ell_q = \frac{\omega_q q}{2\pi} = \frac{(\theta_{i1}+\alpha+2\pi)q}{2\pi}$.

Therefore, from the above four cases we can uniquely determine ℓ_p and ℓ_q as $\ell_p = \omega_p p/2\pi$ and $\ell_q = \omega_q q/2\pi$. Now, by Lemma 7 we can get

$$\frac{a_{i2}}{a_{i1} - \exp\left(j\omega_p\right)} = \begin{cases} \exp\left(j\left(\theta_{i2} - \theta_{i1} + \frac{\pi}{2}\right)\right), & \ell_p = \frac{(\theta_{i1}+\alpha-2l\pi)p}{2\pi} \\ \exp\left(j\left(\theta_{i2} - \theta_{i1} - \frac{\pi}{2}\right)\right), & \ell_p = \frac{(\theta_{i1}-\alpha-2l\pi)p}{2\pi} \end{cases} \tag{A.48}$$

where $l = 0, -1$. Furthermore, from Eq. (A.41) we have

$$s_{pi}s_{qi} = \frac{a_{i2}}{a_{i1} - \exp\left(j\omega_p\right)} = \exp\left(j\frac{2\pi k}{p\,q}\right), \quad 0 \leq k < p\,q \tag{A.49}$$

Combining Eqs. (A.48) and (A.49), we can uniquely determine k as

$$k = \begin{cases} \frac{\left(\theta_{i2}-\theta_{i1}+\frac{\pi}{2}\right)p\,q}{2\pi} \mod p\,q, & \text{if } \ell_p = \frac{(\theta_{i1}+\alpha-2l\pi)p}{2\pi} \\ \frac{\left(\theta_{i2}-\theta_{i1}-\frac{\pi}{2}\right)p\,q}{2\pi} \mod p\,q, & \text{if } \ell_p = \frac{(\theta_{i1}-\alpha-2l\pi)p}{2\pi} \end{cases} \tag{A.50}$$

where $l = 0, -1$. Therefore, by Lemma 5 we can uniquely determine the symbols s_{pi} and s_{qi}, i.e., Eqs. (4.45a) and (4.45b), and furthermore, with a pair of the unique ℓ_p and ℓ_q, we can uniquely determine the symbol $s_{p(i+1)}$ and $s_{q(i+1)}$ from Eqs. (A.34); i.e., Eqs. (4.45c) and (4.45d). This completes the proof of Theorem 1.

□

Appendix B

Proof of Theorem 2

To prove Theorem 2, we first establish the following lemmas.

Lemma 8 [58] *If a random variable, denoted by x, is complex circular Gaussian with zero-mean and variance $2\sigma^2$ then*

$$\mathrm{E}[x^k] = 0 \qquad \textit{for any } k \in \mathbb{Z}^{\dagger} \tag{B.1}$$

where $\mathrm{E}[\cdot]$ is the expectation operator and $\mathbb{Z}^{\dagger}$ denotes the positive integer set. ■

Proof: Let x_R and x_I respectively denote the real and image part of x, i.e., $x = x_R + jx_I$, with $x_R \sim \mathcal{N}(0, \sigma^2)$ and $x_I \sim \mathcal{N}(0, \sigma^2)$. We write the binomial expansion of the kth power of x as

$$x^k = (x_R + jx_I)^k = \sum_{l=0}^{k} \binom{k}{l} x_R^l j^{k-l} x_I^{k-l} \tag{B.2}$$

Taking expectation of both sides of Eq. (B.2), since x_R and x_I are independent with each other, we have

$$\begin{aligned} \mathrm{E}[x^k] &= \mathrm{E}\left[\sum_{l=0}^{k}\binom{k}{l}x_R^l j^{k-l}x_I^{k-l}\right] \\ &= \sum_{l=0}^{k}\binom{k}{l}j^{k-l}\mathrm{E}[x_R^l]\,\mathrm{E}[x_I^{k-l}] \end{aligned} \tag{B.3}$$

Since $x_R \sim \mathcal{N}(0,\sigma^2)$ and $x_I \sim \mathcal{N}(0,\sigma^2)$, it can be verified that $\mathrm{E}[x_R^l] = \mathrm{E}[x_I^l] = 0$ if l is odd integer. For this reason, the proof can be carried out in two cases:

1. When k is odd integer, one of l and $k-l$ must be odd and thus, we have

   $$\mathrm{E}[x_R^l] = 0 \quad \text{or} \quad \mathrm{E}[x_I^{k-l}] = 0, \quad \text{for} \quad l = 0, \cdots, k$$

   Therefor, Eq. (B.3) can be further deduced to

   $$\mathrm{E}[x^k] = \sum_{l=0}^{k}\binom{k}{l}j^{k-l}\mathrm{E}[x_R^l]\,\mathrm{E}[x_I^{k-l}] = 0 \tag{B.4}$$

   for k is odd integer.

2. When k is even integer, Eq. (B.3) can be rewritten as

   $$\mathrm{E}[x^k] = \sum_{l=0}^{k}\binom{k}{l}j^{k-l}\mathrm{E}[x_R^l]\,\mathrm{E}[x_I^{k-l}] \tag{B.5}$$

   $$= \sum_{n=0}^{k/2-1}\binom{k}{2n+1}j^{k-2n-1}\mathrm{E}[x_R^{2n+1}]\,\mathrm{E}[x_I^{k-2n-1}] \tag{B.6}$$

   $$+ \sum_{n=0}^{k/2}\binom{k}{2n}j^{k-2n}\mathrm{E}[x_R^{2n}]\,\mathrm{E}[x_I^{k-2n}] \tag{B.7}$$

   where the term (B.6) is zero since $\mathrm{E}[x_R^{2n+1}] = 0$ for $l = 2n+1$, $n =$

$0, \cdots, k/2-1$. The following task is to prove the term (B.7) is zero for $l = 2n, n = 0, \cdots, k/2$. Since we assumed $x_R \sim \mathcal{N}(0, \sigma^2)$, its probability density function is expressed by

$$f(x_R) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{x_R^2}{2\sigma^2}\right) \tag{B.8}$$

Therefore, from the definition of expectation, we get

$$\begin{aligned} \mathrm{E}[x_R^{2n}] &= \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} x_R^{2n} \exp\left(-\frac{x_R^2}{2\sigma^2}\right) \mathbf{d}x_R \\ &= \frac{1}{\sigma\sqrt{2\pi}} \left[\int_{-\infty}^{\infty} x_R^{2n-1} \mathbf{d}\exp(-x_R^2/2\sigma^2)\right](-\sigma^2) \\ &= -\frac{\sigma}{\sqrt{2\pi}} \left[x_R^{2n-1} e^{-\frac{x_R^2}{2\sigma^2}}\Big|_{-\infty}^{\infty} - \int_{-\infty}^{\infty} \exp\left(-\frac{x_R^2}{2\sigma^2}\right) \mathbf{d}x_R^{2n-1}\right] \end{aligned} \tag{B.9}$$

Since the first term in bracket is zero, Eq. (B.9) can be further derived

$$\begin{aligned} \mathrm{E}[x_R^{2n}] &= \frac{\sigma}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{x_R^2}{2\sigma^2}\right)(2n-1)x_R^{2n-1} \mathbf{d}x_R \\ &= \sigma^2(2n-1)\frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} x_R^{2(n-1)} \exp\left(-\frac{x_R^2}{2\sigma^2}\right) \mathbf{d}x_R \\ &= \sigma^2(2n-1)\mathrm{E}[x_R^{2(n-1)}] \\ &= \sigma^4(2n-1)(2n-3)\mathrm{E}[x_R^{2(n-2)}] \\ &\vdots \\ &= \sigma^{2n}(2n-1)!! \end{aligned} \tag{B.10}$$

where $E[x_R^0] = 1$ and $(2n-1)!! = (2n-1)(2n-3)\cdots 1$. Therefore, the term (B.7)

has the following derivation:

$$\begin{aligned}
&\sum_{n=0}^{k/2}\binom{k}{2n} j^{k-2n}\mathrm{E}[\,x_R^{2n}\,]\,\mathrm{E}[\,x_I^{k-2n}\,] \\
&= \sum_{n=0}^{k/2}\binom{k}{2n}(-1)^{\frac{k}{2}-n}(2n-1)!!\,\sigma^{2n}\,(k-2n-1)!!\,\sigma^{k-2n} \\
&= \sigma^k\sum_{n=0}^{k/2}(-1)^{\frac{k}{2}-n}\frac{k!}{(2n)!(k-2n)!}(2n-1)!!\,(k-2n-1)!! \\
&= \sigma^k\sum_{n=0}^{k/2}(-1)^{\frac{k}{2}-n}\frac{k!}{(2n)!!(k-2n)!!} \\
&= \sigma^k\sum_{n=0}^{k/2}(-1)^{\frac{k}{2}-n}\frac{k!}{2^n\,n!\,2^{\frac{k}{2}-n}\,(\frac{k}{2}-n)!}, \qquad \text{(B.11)}
\end{aligned}$$

where $(2n)!! = 2^n\,n!$ and $(k-2n)!! = 2^{\frac{k}{2}-n}\,(\frac{k}{2}-n)!$. Let $k = 2l$, by the property of $(2l)! = (2l)!!\,(2l-1)!!$, the right side of Eq. (B.11) becomes

$$\begin{aligned}
&\sigma^{2l}\sum_{n=0}^{l}(-1)^{l-n}\frac{(2l)!!(2l-1)!!}{2^l n!(l-n)!} \\
&= \sigma^{2l}\left[\sum_{n=0}^{l}(-1)^{l-n}\frac{l!}{n!(l-n)!}\right](2l-1)!! \\
&= \sigma^{2l}\left[\sum_{n=0}^{l}\binom{l}{n}1^n\,(-1)^{l-n}\right](2l-1)!! \\
&= \sigma^{2l}(1-1)^l(2l-1)!! \\
&= 0 \qquad \text{(B.12)}
\end{aligned}$$

Since both terms (B.6) and (B.7) are zero and as a result, Eq. (B.5) is zero for even integer k, i.e., $\mathrm{E}[\,x^k\,] = 0$, for even k.

Therefore, from these two proofs, we have $\mathrm{E}[\,x^k\,] = 0$ for any positive integer k.

□

Lemma 9 [58] *Let two positive integers p and q be co-prime and α and β be two complex numbers. Then, there exists a complex number x satisfying*

$$x^p = \alpha \tag{B.13a}$$

$$x^q = \beta \tag{B.13b}$$

if and only if α and β meet the following conditions:

$$|\alpha|^{1/p} = |\beta|^{1/q} \tag{B.14a}$$

$$\arg(\beta)p - \arg(\alpha)q \equiv 0 \mod 2\pi \tag{B.14b}$$

Furthermore, under the above two conditions, x is uniquely determined by

$$x = |\alpha|^{1/p} e^{j\theta} \tag{B.15}$$

where $\theta = \frac{\arg(\beta)+2m\pi}{q} = \frac{\arg(\alpha)+2n\pi}{p}$ for $0 \leq m < q$ and $0 \leq n < p$, with such integers m and n uniquely determined by

$$m = (-k)p^{\varphi(q)-1} - q\left\lceil \frac{(-k)p^{\varphi(q)-1}}{q} \right\rceil \tag{B.16a}$$

$$n = \frac{k}{q}\left(1 - p^{\varphi(q)}\right) - p\left\lceil \frac{(-k)p^{\varphi(q)-1}}{q} \right\rceil \tag{B.16b}$$

Here $k = \frac{\arg(\beta)p - \arg(\alpha)q}{2\pi}$. ■

Proof: Let $x = |x|e^{j\theta}$, $\alpha = |\alpha|e^{j\arg(\alpha)}$ and $\beta = |\beta|e^{j\arg(\beta)}$. Then, Eqs. (B.13a) and (B.13b) have a unique solution if and only if Condition (B.14a) and the following

conditions are satisfied,

$$p\theta = \arg(\alpha) + 2n\pi \tag{B.17a}$$

$$q\theta = \arg(\beta) + 2m\pi \tag{B.17b}$$

where $0 \leq \theta, \arg(\alpha), \arg(\beta) < 2\pi$, $0 \leq m < q$ and $0 \leq n < p$. Notice that Eqs. (B.17) have a unique solution with respect to variables m and n iff the following Diophantine equation has a unique solution,

$$\frac{\arg(\beta)p - \arg(\alpha)q}{2\pi} = qn - pm, \quad \text{for } 0 \leq m < q \text{ and } 0 \leq n < p \tag{B.18}$$

Using Lemma 4, Eq. (B.18) has a unique solution iff $\frac{\arg(\beta)p-\arg(\alpha)q}{2\pi}$ is an integer. Following the proof of Lemma 4, we can have the unique solution of Eqs. (B.16) as required. □

Proof of Theorem 2: First, we prove that Eqs. (4.49) are true. From the channel model of Eq. (4.48), we raise the first received signal to its pth power, i.e.,

$$\begin{aligned} z^p(1) &= \Big[s_p h_1 + s_q h_2 + \xi(1)\Big]^p \\ &= \sum_{k=0}^{p} \binom{p}{k} \Big(s_p h_1 + s_q h_2\Big)^k \xi^{p-k}(1) \end{aligned} \tag{B.19}$$

where $\binom{p}{k}$ denotes the binomial coefficient. Taking the expectation of both sides of Eq. (B.19) over random variables s_p, s_q and $\xi(1)$, we have

$$\begin{aligned} \mathrm{E}[z^p(1)] &= \sum_{k=0}^{p} \binom{p}{k} \mathrm{E}\Big[(s_p h_1 + s_q h_2)^k \xi^{p-k}(1)\Big] \\ &= \sum_{k=0}^{p-1} \binom{p}{k} \mathrm{E}\Big[(s_p h_1 + s_q h_2)^k\Big] \mathrm{E}\Big[\xi^{p-k}(1)\Big] + \mathrm{E}\Big[(s_p h_1 + s_q h_2)^p\Big] \end{aligned} \tag{B.20}$$

Since the noise $\xi(1)$ is complex white Gaussian and independent with the transmitted symbols s_p and s_q, using Lemma 8 results in $\mathrm{E}[\xi^l(1)] = 0$ for $l = 1, \cdots, p$, the summation term in Eq. (B.20) is thus zero. Taking binomial expansion to the second term in Eq. (B.20) yields

$$\begin{aligned}
\mathrm{E}\Big[(s_p h_1 + s_q h_2)^p\Big] &= \sum_{l=0}^{p} \binom{p}{l} \mathrm{E}\Big[(s_p h_1)^l (s_q h_2)^{p-l}\Big] \\
&= h_2^p \,\mathrm{E}[s_q^p] + \sum_{l=1}^{p-1} \binom{p}{l} \mathrm{E}\left[(s_p h_1)^l (s_q h_2)^{p-l}\right] + h_1^p \,\mathrm{E}[s_p^p] \\
&= \sum_{l=1}^{p-1} \binom{p}{l} \mathrm{E}\left[(s_p h_1)^l (s_q h_2)^{p-l}\right] + h_1^p \qquad \text{(B.21)} \\
&= \sum_{l=1}^{p-1} \binom{p}{l} h_1^l h_2^{p-l} \mathrm{E}[\, s_p^l\,] \mathrm{E}[\, s_q^{p-l}\,] + h_1^p \qquad \text{(B.22)} \\
&= h_1^p \qquad \text{(B.23)}
\end{aligned}$$

where $\mathrm{E}[s_p^p] = 1$, and $\mathrm{E}[s_q^p] = 0$ since $\gcd(p, q) = 1$. The derivation from (B.21) to (B.22) is under the assumption that s_p and s_q are independently selected from $\mathcal{S}_p$ and $\mathcal{S}_q$, respectively. Since $\mathrm{E}[s_p^l] = 0$ for $l = 1, \cdots, p-1$, the summation term in Eq. (B.22) is zero, and Eq. (B.23) is thus derived. Therefore, combining Eq. (B.20) and Eq. (B.23), we have

$$h_1^p = \mathrm{E}\Big[(s_p h_1 + s_q h_2)^p\Big] = \mathrm{E}[z^p(1)] \qquad \text{(B.24)}$$

By the same token, we have

$$h_1^q = (-1)^q \mathrm{E}[z^q(2)] \qquad \text{(B.25)}$$

Now using Lemma 9, we can prove the statement for h_1 in Theorem 2. Similarly, we can prove the statement for h_2 in Theorem 2. □

Appendix C

Euclid Algorithm

The Euclid Algorithm is designed to compute the greatest common divisor for two integers a and b (not zero) from the following situations:

1. If a is divisible by b, namely $b|a$, then $\gcd(a,b) = b$. This is indeed so because no number (b, in particular) may have a divisor greater than the number itself (for non-negative integers).

2. If $a = bt + r$, for integers t and r, then $\gcd(a,b) = \gcd(b,r)$. Indeed, every common divisor of a and b also divides r. Thus $\gcd(a,b)$ divides r. But, of course, $\gcd(a,b)|b$. Therefore, $\gcd(a,b)$ is a common divisor of b and r and hence $\gcd(a,b) = \gcd(b,r)$. The reverse is also true because every divisor of b and r also divides a.

For example, let $a = 294$, $b = 66$.

$294 = 66 * 4 + 30$	$\gcd(294,66) = \gcd(66,30)$
$66 = 30 * 2 + 6$	$\gcd(66,30) = \gcd(30,6)$
$30 = 6 * 5$	$\gcd(30,6) = 6$

Therefore, $\gcd(294,66) = 6$.

For any pair a and b, the algorithm is bound to terminate since every new step generates a similar problem (that of finding gcd) for a pair of smaller integers. We have the following corollary:

Corollary 1 *For every pair of whole numbers a and b, there exist two integers x and y such that $ax + by = \gcd(a, b)$.* ■

For example: $294 * (-2) + 66 * 9 = 6$.

Note that any linear combination $ax + by$ is divisible by any common factor of a and b. In particular, any common factor of a and b also divides $\gcd(a, b)$. In a "reverse" application, any linear combination $ax + by$ is divisible by $\gcd(a, b)$.

One of the uses of the Euclidean algorithm is to solve the Diophantine equation $ax+by = c$. This is solvable (for x and y) whenever $\gcd(a, b)$ divides c. If we keep track of the quotients in the Euclidean algorithm while finding $\gcd(a, b)$, we can reverse the steps to find x and y. For p and q being co-prime integers, i.e., $\gcd(p, q) = 1$, we can reverse the steps to find m and n to satisfy the Diophantine equation $mp + nq = k$ for any given integer k since $\gcd(p, q)$ divides any integer.

Bibliography

[1] I. Teletar, "Capacity of multi-antenna Gaussian channels," *European Trans. Telecommun.*, vol. 10, pp. 585–595, Nov. 1999.

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

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

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

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

[6] B. Hassibi and B. M. Hochwald, "How much training is needed in a multiple-antenna wireless link?," *IEEE Trans. Inform. Theory*, vol. 49, pp. 951–964, Apr. 2003.

[7] C. Budianu and L. Tong, "Channel estimation for space-time orthogonal block codes," *IEEE Trans. Signal Processing*, vol. 50, pp. 2515–2528, Oct. 2002.

[8] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE J. Select. Areas Commun.*, vol. 18, pp. 1169–1174, Jul. 2000.

[9] H. Jafarkhani and V. Tarokh, "Multiple transmit antenna differential detection from generalized orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 47, p. 2626-2631, 2001.

[10] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat-fading," *IEEE Trans. Inform. Theory*, vol. 46, pp. 543–564, Mar. 2000.

[11] B. L. Hughes, "Differential space-time modulation," *IEEE Trans. Inform. Theory*, vol. 46, p. 2567-2578, Nov. 2000.

[12] A. J. van der Veen, "Algebraic methods for deterministic blind beamforming," *in Proc. of the IEEE*, vol. 86, pp. 1987–2008, Oct. 1998.

[13] L. Tong and S. Perreau, "Multichannel blind identification: from subspace to maximum likelihood methods," *in Proc. of the IEEE*, vol. 86, pp. 1951–1968, Oct. 1998.

[14] D. N. Godard, "Self-recovering equalization and carrier tracking in two-dimensional data communication systems," *IEEE Trans. Commun.*, vol. 28, pp. 1867–1875, Nov. 1980.

[15] J. R. Treichler and M. G. Agee, "A new approach to multipath correction of constant modulus signals," *IEEE Trans. Acoustics, Speech, Signal Processing*, vol. 31, pp. 349–472, Apr. 1983.

[16] C. R. J. Jr., P. Schniter, T. J. Endres, J. D. Behm, D. R. Brown, and R. A. Casas, "Blind equalization using the constant modulus criterion: A review," *in Proc. of the IEEE*, vol. 86, pp. 1927-1950, Oct. 1998.

[17] G. Xu, H. Liu, L. Tong, and T. Kailath, "A least-squares approach to blind channel identification," *IEEE Trans. Signal Processing*, vol. 43, pp. 2982–2993, Dec. 1995.

[18] A. L. Swindlehurst and G. Leus, "Blind and semi-blind equalization for generalized space-time block codes," *IEEE Trans. Signal Processing*, vol. 50, Oct. 2002.

[19] P. Stoica and G. Ganesan, "Space-time block codes: trained, blind and semi-blind detection," *Digital Signal Processing*, vol. 13, pp. 93–105, 2003.

[20] A. J. van der Veen, S. Talwar, and A. Paulraj, "A subspace approach to blind space-time signal processing for wireless communication systems," *IEEE Trans. Signal Processing*, vol. 45, pp. 173–190, Jan. 1997.

[21] A. J. van der Veen, A. Paulraj, "An analytical constant modulus algorithm," *IEEE Trans. Signal Processing*, vol. 44, pp. 1136–1155, May 1996.

[22] G. B. Giannakis and S. D. Halford, "Blind fractionally spaced equalization of noisy FIR channel: Direct and adaptive solutions," *IEEE Trans. Signal Processing*, vol. 45, pp. 2277–2292, Sept. 1997.

[23] C. B. Papadias and D. T. M. Slock, "Fractionally spaced equalization of linear polyphase channels and related blind techniques based on multichannel linear prediction," *IEEE Trans. Signal Processing*, vol. 47, pp. 641–654, Mar. 1997.

[24] Z. Ding and Z.-Q. Luo, "A fast linear programming algorithm for blind equalization," *IEEE Trans. on Commun.*, vol. 48, pp. 1432–1436, Sept. 2000.

[25] Z.-Q. Luo, M. Meng, K. M. Wong, and J.-K. Zhang, "A fractionally spaced blind equalizer based on linear programming," *IEEE Trans. Signal Processing*, vol. 50, pp. 1650–1660, Jun. 2002.

[26] D. Brillinger, "The identification of polynomial systems by means of higher-order spectra," *J. Sound Vib.*, vol. 20, pp. 301–313, 1970.

[27] J. G. Proakis, *Digital Communications*, 4th ed, McGraw-Hill, New York, 2000.

[28] B. Friedlander and B. Porat, "Asymptotically optimal estimation of MA and ARMA parameters of non-Gaussian processes from higher-order moments," *IEEE Trans. Automat. Control*, vol. 35, pp. 27–35, Jan. 1990.

[29] B. Porat and B. Friedlander, "Blind equalization of digital communication channels using high-order moments," *IEEE Trans. Signal Processing*, vol. 39, pp. 522-526, 1991.

[30] J. M. Mendel, "Tutorial on higher-order statistics (spectra) in signal processing and system theory: Theoretical results and some applications," *in Proc. of the IEEE*, vol. 79, pp. 278-305, Mar. 1991.

[31] Shang-Ho Tsai, Xiaoli Yu, and C. Jay Kuo, "Channel diagonalization using a full-rate space-time block code," *in Proc. IEEE Global Telecommun. Conf.*, vol. 5, pp. 2951–2955, Dallas, TX, Nov. 2004.

[32] Y. Sung, L. Tong, and A. Swami, "Blind channel estimation for space-time coded WCDMA," *EURASIP J. Wireless Commun. Networking*, vol. 2004, pp. 322–334, Dec. 2004.

[33] S. Zhou, B. Muquet, and G. B. Giannakis, "Subspace-based (semi-) blind channel estimation for block precoded space-time OFDM," *IEEE Trans. Signal Processing*, vol. 50, pp. 1215–1228, May 2002.

[34] S. Shahbazpanahi, A. B. Gershman, and J. H. Manton, "Closed-form channel estimation for blind decoding of orthogonal space-time block codes," *in Proc. IEEE Int. Conf. Commun.*, vol. 1, pp. 603–607, Paris, France, Jun. 2004.

[35] S. Shahbazpanahi, A. B. Gershman, and J. H. Manton, "Blind decoding of orthogonal space-time block codes using closed-form channel estimation," *accepted for publication in IEEE Trans. Signal Processing*, 2004.

[36] W.-K. Ma, P. C. Ching, T. N. Davidson, and X.-G. Xia, "Blind maximum-likelihood decoding for orthogonal space-time block codes: A semidefinite relaxation approach," *in Proc. IEEE Global Telecommun. Conf.*, vol.5, pp. 2094–2098, San Francisco, USA, Dec. 2003.

[37] W.-K. Ma, B.-N. Vo, T. N. Davidson, and P. C. Ching, "Blind ML detection of orthogonal sapce-time block codes: Efficient, high-performance implementations," *IEEE Trans. Signal Processing*, to appear.

[38] S. Shahbazpanahi, A. B. Gershman, and J. H. Manton, "A relaxed maximum likelihood approach to blind channel estimation and symbol detection in MIMO systems with orthogonal space-time block codes," *in Proc. IEEE Vehicular Technology Conf., Spring 2004*, vol. 1, pp. 289–293, Milan, Italy, May 2004.

[39] L.-K. Hua, *Introduction to Number Theory.* Springer-Verlag, 1982.

[40] S. Verdu, "Computational complexity of optimum multiuser detection," *Algorithmica*, vol. 4, pp. 303-312, 1989.

[41] W.-K. Ma, T. N. Davidson, K. M. Wong, Z.-Q. Luo, and P. C. Ching, "Quasi-maximum-likelihood multiuser detection using semi-definite relaxation with application to synchronous CDMA," *IEEE Trans. Signal Processing*, vol. 50, pp. 912–922, Apr. 2002.

[42] W.-K. Ma, P. C. Ching, and Z. Ding, "Semidefinite relaxation based multiuser detection for M-ary PSK multiuser systems," *IEEE Trans. Signal Processing*, vol. 52, pp. 2862–2872, Oct. 2004.

[43] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2201–2214, Aug. 2002.

[44] L. Lampe, R. Schober, V. Pauli, and C. Windpassinger, "Multiple-symbol differential sphere decoding," *to appear in IEEE Trans. Commun.*, Dec. 2005.

[45] J. Luo, K. Pattipati, P. Willet, and F. Hasegawa, "Near-optimal multiuser detection in synchronous CDMA using probabilistic data association," *IEEE Commun. Lett.*, vol. 5, pp. 361–363, Sept. 2001.

[46] C. Helmberg, F. Rendl, R. J. Vanderbei, and H. Wolkowicz, "An interior point method for semidefinite programming," *SIAM J. Optim.*, vol. 6, no. 2, pp. 342–361, 1996.

[47] M. X. Goemans and D. P. Williamson, "Improved approxiamation algorithms for maximum cut and satisfiability problem using semi-definite programming," *J. ACM*, vol. 42, pp. 1115–1145, 1995.

[48] Y. E. Nesterov, "Semidefinite relaxation and nonconvex quadratic optimization," *Optim. Methods Software*, vol. 9, pp. 140–160, 1998.

[49] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1639-1642, 1999.

[50] O. Damen, A. Chkeif, and J.-C. Belfiore, "Lattice code decoder for space-time codes," *IEEE Commun. Lett.*, vol. 4, pp. 2201–2214, 2000.

[51] O. Damen, H. E. Gamal, and G. Caire, "On maximum likelihood detection and the search for the closest lattice point," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2389–2402, 2003.

[52] C. P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Programming*, vol. 66, pp. 181–191, 1994.

[53] L. Babai, "On Lovász' lattice reduction and the nearest lattice point problem," *Combinatorica*, vol. 6, no. 1, pp. 1-13, 1986.

[54] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, pp. 463-471, 1985.

[55] W. H. Mow, "Maximum likelihood sequence estimation from the lattice viewpoint," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1591-1600, Sept. 1994.

[56] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications," *ACM SIGSAM Bull.*, vol. 15, pp. 37-44, Feb. 1981.

[57] L. Zhou, J.-K. Zhang, and K. M. Wong, "Blind unique identification of Alamouti space-time coded channel via signal design and transmission technique," *in Proc. Eighth Int. Symp. Signal Processing and Its Applications*, Sydney, Australia, Aug. 2005.

[58] L. Zhou, J.-K. Zhang, and K. M. Wong, "A novel signalling scheme for blind unique identification of Alamouti space-time block coded channel," *submitted to IEEE Trans. Signal Processing*, Oct. 2005.