# COMMUNICATION SCIENCES INSTITUTE

## Random-like Space-Time Codes: Performance Analysis, Code Design and Iterative Detection

***by***

**Yuankai Wang**

**CSI-05-08-01**

USC VITERBI SCHOOL OF ENGINEERING
UNIVERSITY OF SOUTHERN CALIFORNIA
ELECTRICAL ENGINEERING — SYSTEMS
LOS ANGELES, CA  90089-2565

# RANDOM-LIKE SPACE-TIME CODES: PERFORMANCE ANALYSIS, CODE DESIGN AND ITERATIVE DETECTION

by

Yuankai Wang

A Dissertation Presented to the
FACULTY OF THE GRADUATE SCHOOL
UNIVERSITY OF SOUTHERN CALIFORNIA
In Partial Fulfillment of the
Requirements for the Degree
DOCTOR OF PHILOSOPHY
(ELECTRICAL ENGINEERING)

August 2004

# Dedication

To my family for their constant encouragement, support, and love.

# Acknowledgements

So many people have supported me during the development of this dissertation, and more generally to my graduate experience here at USC. A few words mentioned here cannot adequately express all my gratitude and appreciation.

I would like to thank my advisor, Professor Keith M. Chugg, for teaching me the fundamental essence of wireless communications. I have benefited tremendously from his keen insight and great guidance. Thanks for the challenging and relaxed atmosphere he provided; Thanks for his listening when he wanted to be heard! His creative thinking was an inspiration to me throughout my journey at USC, and his character made this journey deeply memorable. He is a great role model that I will always look up to in my life.

My heartfelt thanks also go to Professor P. Vijay Kumar and Professor Zhen Zhang. Discussions and collaborations with them are enjoyable, stimulating, and fruitful. I would also like to thank Professor Antonio Ortega and Professor Kenneth Alexander for serving on my dissertation committee. Their comments and suggestions have helped to make this a better thesis. Also thanks to Professor Charles L. Weber for his help and directions to my research.

Special thanks to Milly Montenegro, Mayumi Thrasher, Gerrielyn Ramos for making the work environment at CSI pleasurable.

I am also very thankful to many friends at CSI who have contributed significantly to my experience at USC over the years. Special thanks to Guangcai Zhou, Gregory Dubney, Jun Yang, Reza Omrani for their encouragement and invaluable help whenever needed. Thanks to Durai Thirupathi for those many times we spent together. Thanks to Robert Wilson for the sports time together on the track and for entertaining discussions about news and basketball games. Thanks to Mingrui Zhu, Paniz Ebrahimi, Terry Lewis, Yiling Chao, Jifeng Geng, Paul Kuo, Francis Lu, Pan-Sop Kim, Tom Halford, Jordan Melzer, Robert Weaver (I am sure I have forgotten some) for those technical and non-technical discussions. It has been a privilege to know such a great group of people.

Lastly, I would like to thank my family. Their love, support, and encouragement have been with me every single moment. This dissertation is dedicated to them as an inadequate but sincere expression of appreciation and love.

# Contents

# List Of Figures

# Abstract

Multipath fading can have a severe impact on the performance of wireless communication systems, and space-time codes have proven to be an effective technique to mitigate channel fading through the transmit diversity. Random-like codes, including turbo codes and LDPC codes, have demonstrated remarkable performance, which is typically within 1 dB of the Shannon limit on the AWGN channels.

The combining of random-like codes and space-time codes have been investigated, and several concatenated space time coding schemes were proposed. However, what is shown and known to date is essentially due to experimental demonstrations, and as a consequence, a number of basic questions are still unanswered from theoretic point of view. The goal of this dissertation is to investigate the performance analysis of random-like space-time codes, and develop efficient code construction and iterative detection.

The investigation begins with performance analysis of space-time codes. Based on an alternate representation for Gaussian Q-function, a lower bound on the pairwise error probability is obtained, and the transmit diversity is shown to be good design criterion. For finite alphabet MIMO systems, it is then proved that the Singleton upper bound on the rate-diversity tradeoff is asymptotically achievable.

Using the fundamental tradeoff between rate and diversity, performance analysis of random-like space-time codes is conducted. For BPSK modulation and a specific ensemble of LDPC codes, it is proved that the upper bound on the rate-diversity tradeoff can be asymptotically achieved with probability one. LDPC space-time codes are designed by constructing a two-dimensional array with bounded doubly-periodic correlation, and iterative decoding and detection are studied. Linear dispersion space-time codes with simplified decoding algorithm is also discussed.

# Chapter 1

# About this Dissertation

## 1.1 Introduction

The need for efficient and reliable data communication over noisy channels has been growing for decades, and the typical applications include telephone modems, wireless communications, internet data transfer and data storage devices etc.

The fundamental approach to the problems of efficiency and reliability in communication systems is contained in the noisy channel coding theorem developed by C.E.Shannon [Sha48]. Shannon's theorem states that over a noisy channel, if code rate $R$ is less than the channel capacity $C$, there exists a coding scheme of code rate $R$ with arbitrary small error probability. The proof is essentially nonconstructive and assumes infinite data block length. When it comes to practical systems, however, there are always some constraints, such as a delay constraint or a peak power constraint, and such constraints usually result in some limitation on the systems to approach the channel capacity. Therefore, a tradeoff has to be made among transmission rate, error probability, implementation complexity or other issues [CAC01].

To improve the system performance in terms of transmission rate and reliability, researchers and practicing communication engineers made some exciting progress in two fields over the past ten years. One is space time codes [Tel99, TSC98], which are designed for multiple transmit antenna systems over wireless fading channels; and the second is turbo codes (along with LDPC code and other random-like codes) [BGT93, RU01, Gal63] which were designed originally for additive white Gaussian noise (AWGN) channels and now developed for fading channels.

*A. Space-time codes.* The transmitted signal in wireless communications usually travels to the receiver via multiple paths, the gains and delays of which vary with time due to the mobility of the users and/or the reflectors in the environment. The changing strength of each path and the changing interference between these paths result in fading, and multipath fading can have a severe impact on the performance of wireless communication systems. An effective technique to mitigate channel fading is to exploit diversity through the use of multiple antennas at the transmitter and/or receiver [FG98, Tel99, MH99]. Information-theoretic aspects of transmit diversity are addressed in [FG98, Tel99], and the major conclusion is that the capacity grows at least linearly with the number of transmit antennas as long as the number of receive antennas is greater than or equal to the number of transmit antennas. Many space-time coding and modulation schemes have been suggested for known channel [TSC98, HH02a, LWKC02, LWKC03] and unknown channel [HM00] cases.

*B. Turbo codes and iterative detection.* In the 50 years since Shannon determined the capacity of noisy channels, the construction of capacity-approaching coding schemes has been the supreme goal of coding research. But it was not until the early 90s that we saw the first class of codes whose performance practically approaches Shannon's theoretical limit. In 1993, turbo codes were introduced along with experiments demonstrating their remarkable performance, which is typically within 1 dB of the Shannon limit on the AWGN channels [BGT93]. A few years later, the low-density parity-check (LDPC) codes re-emerged and exhibited similar characteristics and performance [RU01, LMSS01]. Both turbo codes and LDPC codes belong to the general class of concatenated codes employing pseudo-random encoders and iterative decoders, and iterative decoding of random-like codes has been shown to be a powerful method for approaching capacity on noisy channels.

While the decoding of these powerful random-like codes is the most well-known and celebrated special case of iterative detection, iterative detection itself is applicable to virtually every practical digital communication system and can provide significant gains in performance and/or complexity reduction. An example of these gains is the mitigation of like-signal interference in multiuser detectors. Furthermore, these significant gains can be achieved with hardware complexity that is either within today's technology or feasible in the near term [CAC01].

The great success of space-time codes and random-like codes motivates us to integrate them together and consider the performance analysis and code construction. The first attempt is to develop some appropriate performance criteria for space-time codes, and to present the tradeoff between performance parameters for multiple antenna systems in practice. A random-like space-time coding scheme is then studied and shown to be able to achieve the tradeoff.

## 1.2 Organization

This dissertation consists of 6 chapters, and each chapter is written in a self-contained manner. The dissertation is organized as following:

In Chapter 2, the system model for multi-antenna transmission is described, and performance analysis and some design criteria are given. Based on an alternate representation of Gaussian Q-function, we present a lower bound on the pair-wise error probability, and discuss the importance of diversity for space-time codes.

In Chapter 3, we show the Singleton upper bound on the achievable rate for a given transmit diversity, then prove this upper bound can be achieved asymptotically as the block length increases. Essentially there is a tradeoff between the rate and the diversity. An efficient clique-based code design algorithm is proposed and simulation results are given.

In Chapter 4, LDPC code ensembles are introduced, and several concatenated space-time coding schemes are described. We then prove that LDPC based space-time codes can asymptotically achieve the upper bound of rate-diversity tradeoff with probability one. Therefore, LDPC can be regarded as universal codes for multiple-input multiple-output Rayleigh fading channels.

In Chapter 5, algebraic design of LDPC space-time codes is proposed by constructing a two-dimensional array with bounded doubly-periodic correlation. Iterative detection is studied, and simulation results show the remarkable performance of random-like space-time codes.

In Chapter 6, linear dispersion space-time codes with decoupled decoding is considered. We present the conditions of basis matrices so that receiver can decode the symbols in the decoupled manner. Normalized transmission rate is considered.

In Chapter 7, we will draw conclusions, and illustrate some future work.

Generally, the framework of this dissertation can be described as: diversity is important for space-time codes, the rate-diversity tradeoff can be achieved asymptotically, random-like space-time codes achieve the rate-diversity tradeoff, algebraic construction of random-like space-time codes, and iterative decoding and detection can be practical tools for achieving this objective.

# Chapter 2

# Space-Time Codes and Performance Analysis

Wireless communication systems are of significant interest due to their ability to provide flexible voice and data services. While initial deployments such as digital cordless phone and second generation cellular systems focused on voice communications, current interest is in applications that provide both voice and data access. Examples include third generation (3G) cellular systems and broadband fixed wireless systems.

One key challenge in wireless communications is that the transmitted signal usually travels to the receiver via multiple paths, the gains and delays of which vary with time due to the mobility of the users and/or the reflectors in the environment. The changing strength of each path and the changing interference between these paths result in fading, and multipath fading can have a severe impact on the performance of wireless communication systems. An effective technique to mitigate channel fading is to exploit diversity, and examples of diversity are (but are not restricted to) temporal diversity, frequency diversity and antenna diversity. Antenna diversity is obtained through the use of multiple antennas at the transmitter and/or receiver [FG98, Tel99, MH99]. Information-theoretic aspects of transmit diversity are addressed in [FG98, Tel99], and the major conclusion is that the capacity grows at least linearly with the number of transmit antennas as long as the number of receive antennas is greater than or equal to the number of transmit antennas.

By the Chernoff bound on Gaussian Q-function, an upper bound on the pair-wise error probability (PWEP) is derived [TSC98], and the performance is shown to be determined by the difference matrix between the two codewords. The minimum rank among these matrices quantifies the *diversity gain*, while the minimum determinant quantifies the *coding gain*. However, it is not clear how tight this upper bound is, and how effective the design criteria are.

In this chapter, first we describe the system model, and present performance analysis and design criteria. Based on an alternate representation for Gaussian Q-function, we give a lower bound on the pair-wise error probability. Implications of the lower bound are also discussed.

## 2.1 System Model and Design Criteria

We consider a multiple-input multiple-output (MIMO) system employing $Q$ transmit antennas and $P$ receive antennas. At each time slot, $Q$ signals are transmitted simultaneously each from a different antenna, and the signal at each receive antenna is a noisy superposition of the $Q$ transmitted signals corrupted by Rayleigh fading. We assume the quasi-static fading channel model that the channel coefficient from transmit antenna $q$ to receive antenna $p$ is independently Rayleigh distributed and remains constant for one block length $T(T \geq Q)$. After one block length, the channel coefficients change to new independent random values which they remain constant for another block period, and so on. It is also assumed that the receiver has perfect channel state information (CSI), i.e., each channel realization $H$ of $\mathbf{H}$ is exactly known by the receiver but unknown at the transmitter.

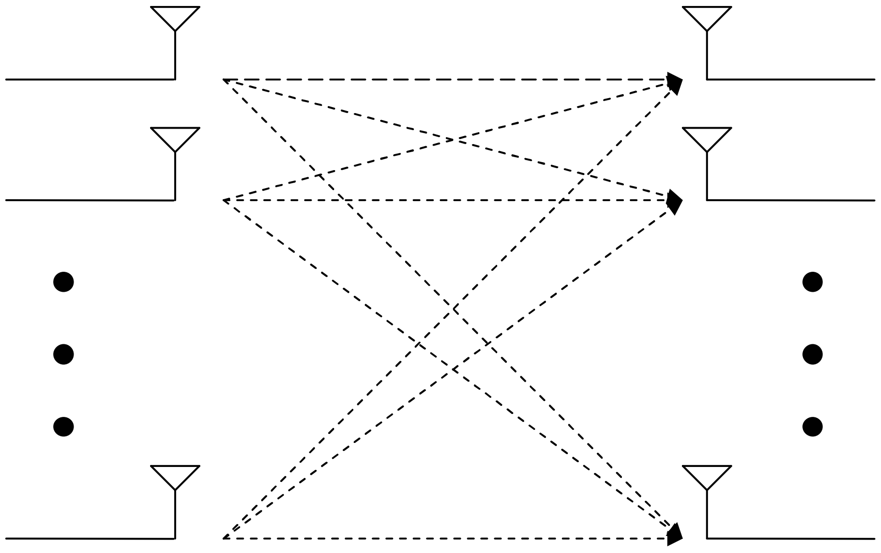

Figure 2.1: MIMO channel

Let $\mathcal{A}$ denote the signal alphabet (constellation) and $\mathcal{S} \subset \mathcal{A}^{QT}$ be a space-time code. Each element of the code is thus a $Q \times T$ matrix. Suppose that $S \in \mathcal{S}$ is the transmitted codeword (code matrix), the received signal after matched-filtering can be represented as

$$\mathbf{Y} = \sqrt{\rho}\mathbf{HS} + \mathbf{N} \tag{2.1.1}$$

where $\rho$ is the signal-to-noise ratio (SNR). The components $n_{p,t}$, $h_{p,q}$ of the noise matrix $N$ and the $(P \times Q)$ channel fading coefficient matrix $H$ respectively, are independent identically distributed, zero-mean complex Gaussian random variables having common density function:

$$f(x) = \frac{1}{\pi} e^{-|x|^2} \tag{2.1.2}$$

We also constrain the signal so that

$$\sum_{q=1}^{Q} |s_{qt}|^2 = 1, \text{ for } \ t = 1, 2, \cdots, T \tag{2.1.3}$$

With this normalization, $\rho = E_s/N_0$, where $E_s$ is the received energy per column of $Y$ at each receive antenna and $N_0/2$ is the spectral level of the AWGN.

Given one channel realization $H$ of $\mathbf{H}$, for any pair of codewords $S_1, S_2$, the squared Euclidean distance between the corresponding received matrices $Y_1, Y_2$ is given by [TSC98]:

$$\begin{aligned} d^2(S_1, S_2) &= \rho \cdot \mathrm{Tr}\left(H(S_1 - S_2)(S_1 - S_2)^\dagger H^\dagger\right) \\ &= \rho \cdot \sum_{q=1}^{Q} \lambda_q \sum_{p=1}^{P} \beta_{pq}^2 \end{aligned} \tag{2.1.4}$$

where $\{\lambda_q\}$ are the eigenvalues of $\Delta S \Delta S^\dagger$, $\Delta S = S_1 - S_2$ is the difference matrix, $U$ is the corresponding eigenvector matrix, and $\beta_{pq} = (HU)_{pq}$.

Let the codeword $S_1$ be transmitted, and $S_2$ denote the codeword selected by the decoder. Then the pair-wise error probability is given by:

$$P(\mathbf{S_1} \to \mathbf{S_2}|H) = Q\left(\frac{d(S_1, S_2)}{\sqrt{2}}\right) \tag{2.1.5}$$

By the Chernoff bound on Gaussian Q-function $Q(x) \leq \frac{1}{2}e^{-\frac{x^2}{2}}$, the pair-wise error probability given channel $H$ can be upper bounded by:

$$P(\mathbf{S_1} \to \mathbf{S_2}|H) \leq e^{\frac{d^2(S_1,S_2)}{4}} \tag{2.1.6}$$

For the quasistatic fading channel, (2.1.6) can be averaged over $H$ to obtain the bound on pair-wise error probability:

$$\begin{aligned} P(\mathbf{S_1} \to \mathbf{S_2}) &\leq \left(\prod_{q=1}^{r} \frac{1}{1+\frac{\rho}{4}\lambda_q}\right)^{P} \\ &\leq \left(\prod_{q=1}^{r} \lambda_q\right)^{-P} \left(\frac{\rho}{4}\right)^{-rP} \end{aligned} \qquad (2.1.7)$$

where $r$ is the rank of the matrix $\Delta S \Delta S^{\dagger}$, and $\lambda_1, \cdots, \lambda_r$ are the corresponding nonzero eigenvalues. Thus a diversity advantage of $rP$ and a coding advantage of $(\lambda_1\lambda_2\cdots\lambda_r)^{1/r}$ are achieved, and $r$ is usually called the transmit diversity. The design criteria for Rayleigh space-time codes were presented in [TSC98]:

1 *The Rank Criterion*: the transmit diversity gain is defined to be the minimum $r = \text{rank}(\mathbf{S_1} - \mathbf{S_2})$ over all pairs of distinct codewords $\mathbf{S_1}, \mathbf{S_2}$. In order to achieve the maximum diversity gain, the matrix $\mathbf{S_1} - \mathbf{S_2}$ has to be full rank.

2 *The Determinant Criterion*: the coding gain is defined to be the minimum $\eta = (\lambda_1\lambda_2\ldots\lambda_r)^{1/r}$ over all pairs of distinct codewords $\mathbf{S_1}, \mathbf{S_2}$. The design aim is making this as large as possible.

Based on the design criteria, space-time block codes from orthogonal designs are constructed in [TJC99], and space-time convolutional codes are studied in [ZWZC01].

## 2.2 Lower Bound on Pair-wise Error Probability

The noise in communications is usually modelled as Gaussian white noise, and the Gaussian Q-function plays an important role in performance analysis of all types of communication systems. The classical definition of Gaussian Q-function is given as:

$$Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{y^2}{2}} dy \tag{2.2.8}$$

An alternate definite integral form is presented in [Cra91] where Craig simplified the evaluation of average error probability for the two-dimensional AWGN channel. In particular,

$$Q(x) = \frac{1}{\pi} \int_0^{\pi/2} e^{-\frac{x^2}{2\sin^2\theta}} d\theta \tag{2.2.9}$$

By this alternate form of Gaussian-Q function as well as the Marcum-Q functions, Simon and Alouini presented a unified approach to the performance analysis of digital communication over generalized fading channels, such as Rayleigh fading, Rician fading or log normal fading [SA98].

Now the pair-wise error probability in (2.1.5) can be expressed in another form:

$$\begin{aligned} P(\mathbf{S_1} \rightarrow \mathbf{S_2}|H) &= \frac{1}{\pi}\int_0^{\pi/2} e^{-\frac{d^2(S_1,S_2)}{4\sin^2\theta}} d\theta \\ &= \frac{1}{\pi}\int_0^{\pi/2} \prod_{p,q} \exp\left(-\frac{\rho\lambda_q\beta_{pq}^2}{4\sin^2\theta}\right) d\theta \qquad (2.2.10) \end{aligned}$$

Averaging over Rayleigh fading channel $H$, the exact expression for PWEP is:

$$\begin{aligned} P(\mathbf{S_1} \rightarrow \mathbf{S_2}) &= \frac{1}{\pi}\int_0^{\pi/2}\int_0^{\infty} \prod_{p,q} 2\beta_{pq}\exp\left(-\frac{\rho\lambda_q\beta_{pq}^2}{4\sin^2\theta}\right)\exp(-\beta_{pq}^2)d\beta_{pq}d\theta \\ &= \frac{1}{\pi}\int_0^{\pi/2} \prod_{q=1}^{r}\left(\frac{\sin^2\theta}{\sin^2\theta+\rho\lambda_q/4}\right)^P d\theta \qquad (2.2.11) \end{aligned}$$

In (2.2.11), if we replace $\sin^2\theta$ in both numerator and denominator by 1, we obtain the upper bound as in the previous section; if we replace $\sin^2\theta$ only in the denominator by 1, we get the lower bound.

$$\kappa\left(\prod_{q=1}^{r}\frac{1}{1+\frac{\rho}{4}\lambda_q}\right)^P \leq P(\mathbf{S_1} \rightarrow \mathbf{S_2}) \leq \left(\prod_{q=1}^{r}\frac{1}{1+\frac{\rho}{4}\lambda_q}\right)^P \qquad (2.2.12)$$

where $\kappa = \frac{1}{\pi}\int_0^{\pi/2}(\sin^2\theta)^{rP}d\theta$. As we can see, the difference between the upper bound and lower bound is only a constant ratio $\kappa$, and $\kappa$ depends on the product $rP$ only. Some values of $\kappa$ are tabulated below. To some degree, we can say that the upper bound and the lower bound are very close.

| $rP$ | 4 | 6 | 8 | 10 | 12 |
|---|---|---|---|---|---|
| $\kappa$ | 0.2734 | 0.2256 | 0.1964 | 0.1762 | 0.1612 |

Considering the product in denominator,

$$\prod_{q=1}^{r}\left(1+\frac{\rho}{4}\lambda_q\right) = 1+\frac{\rho}{4}\sum_{q=1}^{r}\lambda_q+\cdots+\left(\frac{\rho}{4}\right)^r\prod_{q=1}^{r}\lambda_q \qquad (2.2.13)$$

For the coefficient of degree-1 term $\frac{\rho}{4}$, $\sum_{q=1}^{r}\lambda_q = \mathrm{Tr}\left((S_1-S_2)(S_1-S_2)^\dagger\right)$, is the squared Euclidean distance, while the last term $\prod_{q=1}^{r}\lambda_q$ is the determinant of $(S_1-S_2)(S_1-S_2)^\dagger$. We would like to make some notes here:

(1). When SNR $\rho$ is low, the trace (i.e., the Euclidean distance) appears to be the dominant factor, and the channel behaves like traditional AWGN channel. At moderate to high SNR, the diversity gain and coding gain (i.e. the determinant) dominate, and the channel is the type on which most of the existing space-time codes mainly focus. If we can construct space-time codes with good rank and determinant as well as good Euclidean distance, it would be a universal code which works for all the regions of SNR. Later we will show that rand-like space-time codes possess such properties.

(2). At some time during the development of space-time codes, there was some concern in the research community that the rank and determinant may not be the appropriate design criteria. Since the lower bound of PWEP is a constant ratio of the upper bound, this shows that, at moderate to high SNR the rank and determinant are indeed good design criteria.

# Chapter 3

# Trade-off Between Rate and Diversity

A fundamental trade-off in digital communication system design is that between throughput rate and performance. In an effort to formalize this trade-off, it is often necessary to introduce a proxy measure for performance. For example, Euclidean distance between signals is a common choice for additive white Gaussian channels while Hamming distance is a common choice for the binary symmetric channel. In both cases, the minimum distance is a good indicator of performance trends at moderate to high signal to noise ratio.

As shown in Chapter 2, transmit diversity is an appropriate measure for space-time codes design over Rayleigh fading channels. In addition to providing transmit diversity gain, MIMO systems can enable increased data transmission rate through spatial multiplexing [JP00]. This is particularly important for those systems that are equipped with large numbers of transmit antennas, since it may be advantageous to increase the transmission rate higher than that possible with full diversity codes, while a reasonable diversity gain can still be maintained [Gam02]. The diversity-multiplexing trade-off is essentially the trade-off between the error probability and the transmission rate, and information-theoretic aspects were addressed in [ZT02]. It is shown that multiple-input multiple-output (MIMO) communication systems can increase spectral efficiency through spatial multiplexing, and that diversity gain and multiplexing gain can be simultaneously obtained [JP00, ZT02]. The diversity-multiplexing trade-off for finite alphabet MIMO systems is addressed in this chapter.

For linear binary error correction codes, the Singleton and the Gilbert-Varsharmov bounds establish upper and lower limits, respectively, on the achievable code rate for a given minimum Hamming distance. A code that achieves the Singleton bound is called maximum distance separable (MDS).

The Singleton bound has been generalized to bound the rate of a MIMO system in Rayleigh fading in terms of the diversity achieved [KH00, Gam02, SKWD01]. Since the transmit diversity is determined by the minimum rank of code matrix difference, it is reasonable to refer to MIMO signal designs that achieve the generalized Singleton bounds as maximum rank separable (MRS) [Gab85].

While the high channel capacity due to multiple antennas generally requires the modulation size to be large, prior treatments on rate-diversity tradeoff and code design mainly focused on BPSK/QPSK. Using the properties of the binary field, a binary rank criterion is presented [JG00] for space time codes with BPSK/QPSK, but it is difficult to extend this result to arbitrary $M$-PSK modulations. Full diversity MRS space time codes are designed for arbitrary $M$-PSK modulation in [SR02], however the number of transmit antennas is restricted.

In this chapter, we generalize the Gilbert-Varsharmov bound for MIMO systems in Rayleigh fading. Using this lower bound on the achievable rate, together with the generalized Singleton bound, we show that MRS designs are asymptotically achievable for arbitrary signal constellation as the block size increases [WCY+03]. We also apply a code design methodology recently introduced in [CC], and demonstrate designs with substantial rate increase but with little or no performance degradation.

This chapter is organized as follows. Section 3.1 describes the Singleton bound on the achievable rate for a given transmit diversity. In section 3.2, we present a generalized Gilbert-Varsharmov lower bound, and show that the lower bound will approach the upper bound as the block size increases. An efficient clique-based code design algorithm and simulation results are given in section 3.3.

## 3.1 Singleton Bound

We consider a multiple-input multiple-output system employing $Q$ transmit antennas and $P$ receive antennas, and assume the quasi-static fading channel model that the channel coefficient from transmit antenna $q$ to receive antenna $p$ is independently Rayleigh distributed and remains constant for the block length $T(T \geq Q)$.

Let $\mathcal{A}$ denote the signal alphabet (constellation) and $\mathcal{S} \subset \mathcal{A}^{QT}$ be a space-time code. Each element of the code is thus a $Q \times T$ matrix.

Assuming that the receiver has perfect channel state information (CSI), i.e., each channel realization $H$ of $\mathbf{H}$ is exactly known by the receiver but unknown at the transmitter. The analysis of pairwise error probability shows that the performance criteria for space-time codes design are rank criterion and determinant criterion [TSC98].

In addition to providing diversity gain, MIMO systems can enable increased data transmission rate through spatial multiplexing [JP00, ZT02]. Here we consider such MIMO systems with coding symbol from a finite alphabet $\mathcal{A}$, and define two parameters as following:

**Definition 3.1** *(Transmit Diversity Gain) Transmit diversity gain $d$ of the code is defined as the minimum of rank of the difference matrix between any two code matrices.*

**Definition 3.2** *($M$-ary Symbol Rate) $M$-ary symbol rate $\eta$ of a code is*

$$\eta = \frac{\log_M |\mathcal{S}|}{T} \tag{3.1.1}$$

*where $|\mathcal{S}|$ means the size of the code, and $M$ denotes $|\mathcal{A}|$, the size of the alphabet set. Note that with sinc pulse shaping a spectral efficiency of $\eta \log_2 M$ bps/Hz can be achieved.*

The transmit diversity gain is an indication of the transmission reliability, and the symbol rate means the transmission speed. In the work on coding for block fading channels using a single transmit antenna [KH00], Knopp and Humblet presented a generalized version of Singleton bound on the maximum diversity for a given number of uncorrelated fading blocks and information rate. This idea was generalized in [Gam02, SKWD01] for space-time codes over MIMO block fading channels, resulting in:

$$\eta \leq Q - d + 1 \tag{3.1.2}$$

In traditional code design, codes which achieve the Singleton bound are referred to as maximum-distance separable (MDS), and MDS codes can be constructed under some restricted cases. For space-time codes, the minimum distance is replaced by minimum rank. Prior treatments on rate-diversity tradeoff mainly focused on BPSK/QPSK, and space-time codes have been constructed to achieve the upper bound [Gab85]. For systems with arbitrary finite alphabet, it is not known whether this upper bound would be obtained, i.e. whether we can always construct a code to achieve the upper bound.

## 3.2 Asymptotic Data Rate

In this section, we will prove that the upper bound can be achieved asymptotically as block length $T$ increases. To prove this theorem, we show some properties of code matrices and use the ideas of sphere packing.

**Definition 3.3** *(r-ball) For a code matrix $S \in \mathcal{S}$, an $r$-ball centered at $S$ is defined as*

$$B_r(S) = \{W \in \mathcal{S} | rank(W - S) \leq r\},$$

*i.e., the neighboring matrices whose difference matrix with $S$ has rank $\leq r$.*

Since code design may be viewed as sphere packing, the volume of the $r$-ball is very important to determine the number of the codewords for space-time codes.

**Lemma 3.1** *Let $X$ be a complex $Q \times T$ matrix, and assume that $x_{ij}$ can take value from a finite alphabet set of size $u$. Let $r$ rows of $X$ be given, if we further require that the remaining $Q - r$ rows be the linear combinations of these fixed $r$ rows, the choice for the remaining $Q - r$ rows is upper bounded by $u^{(Q-r) \cdot u^r}$ .*

*Proof*: Without loss of generality, suppose that the first $r$ rows are given, and consider the first column of this $r \times T$ sub-matrix. Every entry can take only $u$ values, so the choice for this column is $u^r$. For each of these $u^r$ choices, since the first entry of the following $(r+1)^{st}$ row can take only $u$ values, the number of possible linear combinations is $u$, therefore the number of total possible linear combinations is $u^{u^r}$. Because the $(r+1)^{st}$ row is linear combination of those first $r$ rows, the number of choices for the $(r+1)^{st}$ is upper bounded by $u^{u^r}$. Considering all the remaining $(Q-r)$ rows, the number of choices is upper bounded by $(u^{u^r})^{Q-r}$, which is $u^{(Q-r)u^r}$. □

Denote $g(u, Q, r) = u^{(Q-r)\cdot u^r}$. Lemma 1 shows that the upper bound on the choice for the remaining $Q - r$ rows does not depend on the block length $T$. The next lemma shows how large the $r$-ball could be.

**Lemma 3.2** *($|B_r(S)|$, Volume of $r$-ball) For any matrix $S \in \mathcal{S}$, $|B_r(S)|$, the volume of $r$-ball is upper bounded by $\binom{Q}{r}M^{rT}g(M^2 - M + 1, Q, r)$, where the function $g$ is defined as above.*

*Proof*: Suppose that matrix $W$ satisfies the requirement, $\text{rank}(W - S) \leq r$. This means that, in the difference matrix $W - S$, at most $r$ rows are linearly independent, and the remaining rows are linear combinations of these. To select $W$, we first arbitrarily choose $r$ of $Q$ rows, so the number of choices is $\binom{Q}{r}M^{rT}$. Next, consider the difference matrix $W - S$, the corresponding $r$ rows have been fixed, and the element can take value from a set of at most $M(M-1)+1 = M^2 - M + 1$ numbers. From Lemma 1, the choice for the remaining $Q - r$ rows in $W$ is at most $g(M^2 - M + 1, Q, r)$. Therefore, $|B_r(S)|$ is upper bounded by $\binom{Q}{r}M^{rT}g(M^2 - M + 1, Q, r)$. □

Based on Lemmas 1 and 2, we obtain the following lower bound on the code size $|\mathcal{S}|$.

**Theorem 3.1** *(Lower Bound on $|\mathcal{S}|$) For MIMO communication systems with $Q$ transmitter antennas and block length $T$, given the requirement of transmit diversity gain $d$, we can construct a code $\mathcal{S}^*$ with the following property:*

$$\frac{M^{QT}}{\binom{Q}{d-1} M^{(d-1)T} g(M^2 - M + 1, Q, d-1)} \leq |\mathcal{S}^*| \tag{3.2.3}$$

*Proof*: To meet the requirement of transmit diversity gain $d$, we consider the $r$-ball where $r = d-1$, and its volume is $\leq \binom{Q}{d-1} M^{(d-1)T} g(M^2-M+1, Q, d-1)$. We first select a matrix $S_0$, and find the $B_{d-1}(S_0)$; Among the remaining matrices, we can select another matrix $S_1$ and find $B_{d-1}(S_1)$. This procedure can be repeated, and we can obtain a code $\mathcal{S}^* = \{S_0, S_1, \cdots\}$. The total volume is $M^{QT}$, therefore $|\mathcal{S}^*| \geq \frac{M^{QT}}{\binom{Q}{d-1} M^{(d-1)T} g(M^2-M+1,Q,d-1)}$, and this is a lower bound on $|\mathcal{S}|$. □

The asymptotic rate then results from Theorem 1.

**Theorem 3.2** *(Asymptotic Rate $\eta$) For MIMO communication systems with $Q$ transmit antennas and block length $T$, given the transmit diversity gain to be $d$,*

$$\lim_{T \to \infty} \eta = Q - d + 1 \tag{3.2.4}$$

*Proof*: From (3.2.3), we have

$$\begin{aligned}
\lim_{T\to\infty} \eta &= \lim_{T\to\infty} \frac{\log_M |\mathcal{S}_T|}{T} \\
&\geq (Q-d+1) - \lim_{T\to\infty} \frac{\log_M \left[\binom{Q}{d-1} g(M^2-M+1, Q, d-1)\right]}{T} \\
&= Q-d+1
\end{aligned}$$

Combining with (3.1.2), we get the asymptotic rate $\lim_{T\to\infty} \eta = Q-d+1$. $\square$

Theorem 2 implies that, asymptotically, there is linear relationship between the transmit diversity gain and the symbol rate, and the sum of these two parameters is $Q+1$. In the terminology of [ZT02], the total degrees of freedom for this system is $Q+1$, and we can make tradeoff between transmit diversity gain and the symbol rate.

Besides the Singleton type bound, there is another intuitive comparison of the bound (3.2.3) with Gilbert-Varsharmov bound in error correction codes [MS77]. Let $n$ be the codeword length, $k$ the dimension of the code, and $d_{min}$ the minimum Hamming distance. For an $[n, k, d_{min}]$ binary code, the Gilbert-Varsharmov bound says that:

$$\frac{2^n}{\sum_{i=0}^{d_{min}-1} \binom{n}{i}} \leq 2^k \qquad (3.2.5)$$

By relating $(Q, \eta, d)$ with $(n, k, d_{min})$ respectively, we observe the similarity between these two bounds. For example, $\eta$ and $k$ are related with size of the code, the total

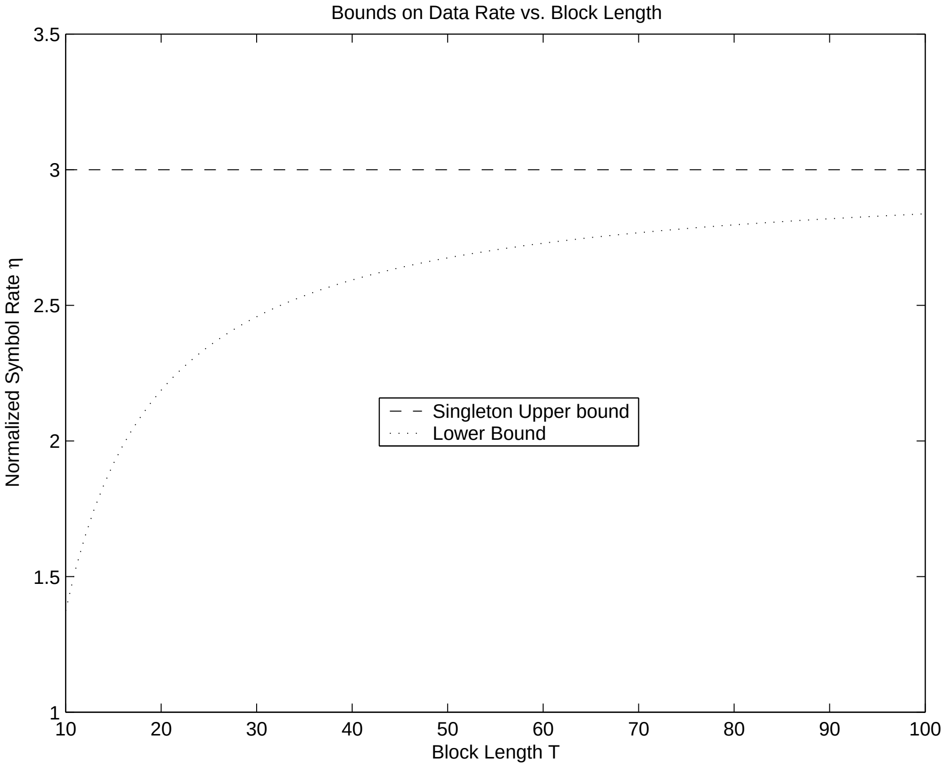

Figure 3.1: Bounds on data rate vs. block length, BPSK (M=2), 4-Tx (Q=4), d=2.

volumes are $M^{QT}$ and $2^n$, and the denominators are $\binom{Q}{d-1}M^{(d-1)T}g(M^2 - M + 1, Q, d-1)$ and $\sum_{i=0}^{d_{min}-1}\binom{n}{i}$ respectively.

For the case of BPSK ($M = 2$), 4-Tx ($Q = 4$) and transmit diversity $d = 2$, the Singleton upper bound on data rate is 3. We plot the lower bound on data rate in Fig. 3.1. The convergence speed of lower bound to the Singleton upper bound is proportional to $1/T$ where $T$ is block length.

## 3.3 Clique-based Design Algorithm and Simulation Results

Assuming that the receiver has perfect channel state information (CSI), i.e., each channel realization $H$ of $\mathbf{H}$ is exactly known by the receiver but unknown at the transmitter, a closed-form expression for pairwise error probability is [LWKC02]:

$$\begin{aligned} P(S_1 \to S_2) &= \frac{1}{\pi}\int_0^{\pi/2} \prod_{q=1}^{r} \left(\frac{\sin^2\theta}{\sin^2\theta + \zeta\lambda_q}\right)^P d\theta \\ &= \frac{1}{2}\left\{1 - \sum_{q=1}^{g} \mu_q \sum_{p=1}^{m_q} \kappa_{pq} \sum_{k=0}^{p-1} \binom{2k}{k} \left(\frac{1-\mu_q^2}{4}\right)^k\right\} \end{aligned}$$

where $\mu_q = \sqrt{\frac{\zeta\lambda_q}{1+\zeta\lambda_q}}$, $\zeta = \frac{\rho}{4Q}$, $\lambda_q, q = 1, 2, \cdots, r$ are the non-zero eigenvalues of $(S_1 - S_2)(S_1 - S_2)^\dagger$, $g$ is the number of distinct nonzero eigenvalues, and $m_q$ and $\kappa_{pq}$ are the related multiplicity and partial fraction expansion coefficients.

While the determinant criterion is defined over complex number domain, traditional code design is carried in binary or discrete domain. In [LWKC02] the relationship is presented between the sum of the complex eigenvalues and the Hamming distance in discrete domain. For BPSK and two code matrices $S_1, S_2$, the constraint is:

$$\sum_q \lambda_q = 4d_H(S_1, S_2) \tag{3.3.6}$$

where $d_H$ is the Hamming-distance metric. The coding gain, i.e., the determinant, is usually defined as $\left(\prod_{q=1}^{r} \lambda_q\right)^{1/r}$.

To design the space-time block codes with high data rate or good performance, it is advantageous to integrate together the transmit diversity, Hamming distance and the closed-form pair error rate expression. We present a clique-based algorithm to find good space-time block codes. Considering every possible matrix as a node in a graph, we make a connection between a pair of matrices if they satisfy the pairwise conditions: At a given SNR level, the pairwise error probability is lower than a threshold; Transmit diversity gain is greater than a given number; and/or Hamming distance is larger than the preset value. In practice, we can also consider the pairwise error probability only.

The code design algorithm is then formulated as finding the largest connected subgraph (or clique), i.e., the so called clique problem. The general class of clique problems is known to be NP-Hard, however they can be solved efficiently by some optimal search algorithm [CC].

We consider a system with 4-Tx 4-Rx antennas, frame length 4 and BPSK modulation, and the simulation results are shown in Fig. 3.2. The orthogonal design can provide full diversity with 16 code matrices. By the clique-based algorithm, we can find a code of 42 matrices which satisfies the transmit diversity gain 3 and has performance degradation of 0.3-0.4dB compared with orthogonal design. Through the clique-based algorithm, we can also find a code of 16 matrices with transmit diversity gain 3, and the code has 0.3-0.4 dB gain compared to orthogonal design. If we only consider the pairwise error probability in our algorithm, we can find a

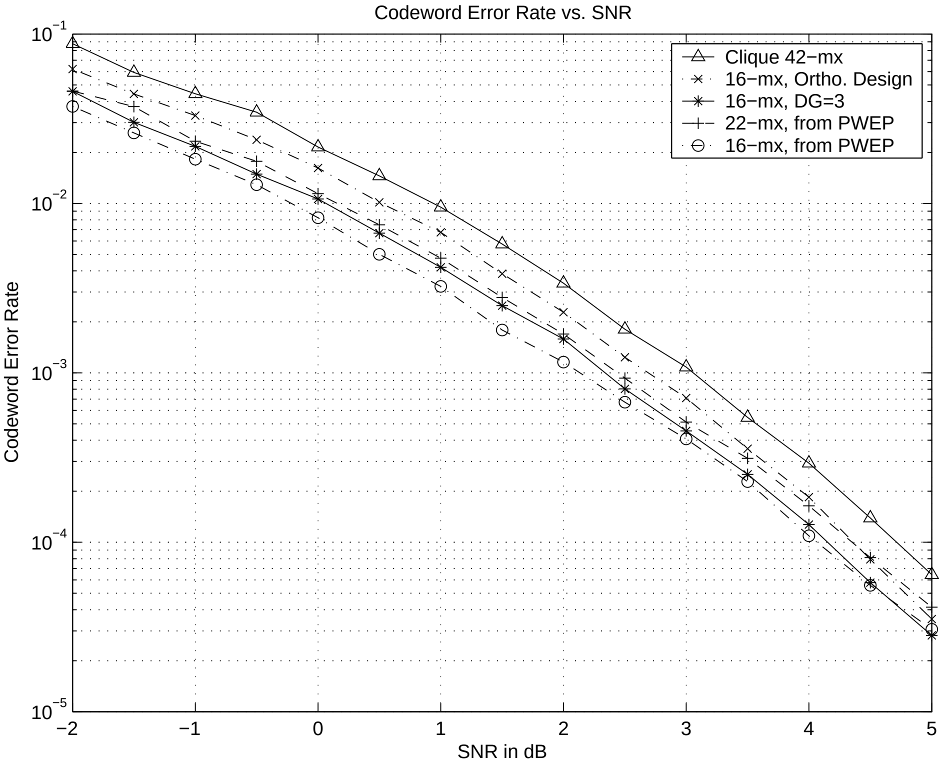

Figure 3.2: Codeword error rate vs. SNR, BPSK, 4-Tx 4-Rx antennas.

code of 16 matrices with further improved performance; a code of 22 matrices is also found, and the simulation result is shown in Fig. 3.2.

# Chapter 4

# LDPC Space-Time Codes: Performance Analysis

In the 50 years since Shannon determined the capacity of noisy channels, the construction of capacity-approaching coding schemes has been the supreme goal of coding research. But it was not until the early 90s that we saw the first class of codes whose performance practically approaches Shannon's theoretical limit. In 1993, turbo codes were introduced along with experiments demonstrating their remarkable performance, which is typically within 1 dB of the Shannon limit on the AWGN channels. A few years later, the low density parity check codes re-emerged and exhibited similar characteristics and performance. Both turbo codes and LDPC codes belong to the general class of concatenated codes employing pseudo-random encoders and iterative decoders, and iterative decoding of random-like codes has been shown to be a powerful method for approaching capacity on noisy channels.

While the decoding of these powerful random-like codes is the most well-known and celebrated special case of iterative detection, iterative detection itself is applicable to virtually every practical digital communication system and can provide significant gains in performance and/or complexity reduction. An example of these gains is the mitigation of like-signal interference in multiuser detectors. Furthermore, these significant gains can be achieved by with hardware complexity that is either within today's technology or feasible in the near term [CAC01].

The combining of random-like codes and space-time codes have been investigated, and several concatenated space time coding schemes are proposed [GN02, tBKA02]. Simulation results strongly suggest that such concatenated schemes are some promising solutions to highly efficient data transmission over Rayleigh fading channels. However, what is shown and known to date is essentially due to experimental demonstrations, and as a consequence, a number of basic questions are still unanswered from theoretic point of view. In this chapter, we will offer some theoretical justification of these schemes, and consider their practical relevance as well.

This chapter is organized as follows. First we give a general introduction about the LDPC codes and some concatenated space time coding schemes. Then the LDPC based space time codes is shown to achieve the rate-diversity tradeoff with probability one, and finally we discuss LDPC as universal codes for MIMO Rayleigh fading channels.

## 4.1 Low-Density Parity-Check Codes

Low-density parity-check codes were first introduced by Gallager in his thesis [Gal63] in 1961, but were subsequently neglected by the coding community until they were rediscovered shortly after the invention of turbo codes in the mid-1990s. The reason why LDPC codes were forgotten is partly due to that Gallager's codes were ahead of time. In 1961, the $N^2-$cost in memory for explicit storage in the process would have been unattainable, so computational resources were (temporarily) a big problem. Given the limited processing capabilities of the time, Gallager's codes were simply considered impractical [Mac99] [FKJ$^+$01]. Today's technology has made it feasible, and VLSI chips for LDPC codes are now commercially available.

For parity-check codes, the parity check matrix represents a set of linear homogeneous modulo 2 equations called parity-check equations, and the set of codewords is the set of the solutions of these equations [MS77]. Low-density parity-check codes are codes specified by the parity check matrix containing mostly 0's and only a small number of 1's. In particular, an $(n, j, k)$ LDPC code is a code of block length $n$ with the parity check matrix $H$, where each column contains a small fixed number, $k \geq 3$, of 1's and each row contains a small fixed number, $j$, of 1's. It follows that the parity check matrix $H$ has $nk/j$ rows and thus a rate $R \geq 1 - \frac{k}{j}$.

Another convenient way to specify LDPC codes is graph representation. Let's consider a bipartite graph with $n$ variable nodes on the left and $m = \frac{nk}{j}$ check nodes on the right. Each variable node corresponds to one bit of the codeword, i.e., to one column of $H$, and each check node corresponds to one parity-check equation, i.e., to one row of $H$. Edges in the graph connect variable nodes to check nodes and are in one-to-one correspondence with the non-zero entries of $H$. The sum-product decoding algorithms work iteratively, and information is exchanged between the neighboring nodes in the graph by passing messages along the edges. When the graph is cycle-free, the optimality of sum-product decoding algorithm can be proved [Tan81].

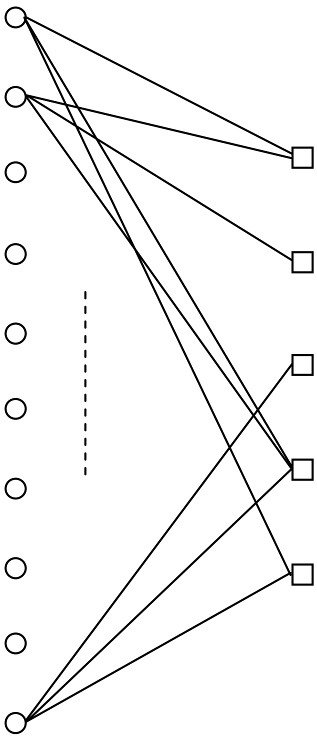

Figure 4.1: Graph representations of LDPC codes. There are 10 variable nodes on the left and 5 check nodes on the right.

For a parity-check code of long block length, it is usually impractical to calculate exactly the distance function or even the minimum distance because of the enormous number of codewords involved. It is often simpler to analyze the average distance function of an ensemble of code; the statistics of an ensemble permit one to average over quantities that are not tractable in individual codes. From the ensemble average, one can then make statistical statement about the member codes.

Following Gallager's definition on LDPC codes, there have been some variants, and different ensembles have been defined [LMSS01], [LS02b], [Mac99]. Here we consider 4 ensembles which are presented and well studied in [LS02a].

Let H be a collection of binary parity-check matrices of size $M \times N$, where $M \leq N$. Every such matrix defines a code of rate $R \geq 1 - \frac{M}{N}$. Let $k$ and $l$ be given numbers, independent of $N$. The four ensembles of codes are as given as following:

- Ensemble A: Matrix $H$ is chosen with uniform probability from the ensemble of $M \times N$ (0,1)-matrices having row sums equal $l$ and column sums equal $k$.

- Ensemble B: Matrix $H$ is chosen with uniform probability from the ensemble of $M \times N$ (0,1)-matrices having column sums equal $k$.

- Ensemble C: Matrix $H$ is chosen with uniform probability from the ensemble of $M \times N$ (0,1)-matrices having row sums equal $l$.

- Ensemble D: Matrix $H$ is generated starting from the all-zero matrix by flipping each entry with probability $l/n = k/m$.

As shown in [LS02a], from D to A, the performance appears to become better while theoretical analysis becomes more difficult.

Some well-known results about LDPC are summarized in following. On the distance properties, we have:

- The minimum distance grows linearly in block length $n$ [Gal63] [LS02a];
- The average distance distribution converges to binomial distribution whenever $k$ or $j$ goes to $\infty$ [LS02a].

About the message-passing decoding algorithm, we have [RU01]:

- [Concentration Around Ensemble Average] the behavior of the individual codes concentrates around the ensemble; the concentration speed is exponential in block length;
- [Convergence of Ensemble Average to Cycle-free Case] The ensemble average converges to the cycle-free case; the convergence speed is known to be of order $\frac{1}{n}$, and is likely to be polynomial at best.

## 4.2 Concatenated Space-Time Coding Schemes

Space-time block codes (STBC) and space-time trellis codes (STTC) have been extensively studied during the past several years. While STBC can provide diversity gain, its main goal is not to provide additional coding gain; while STTC can provide coding gain as well as diversity gain, its coding gain still needs further improvement. In order to obtain the near-capacity performance, concatenated space-time coding schemes have to be used for MIMO Rayleigh fading channels.

Concatenated space-time codes have been addressed in [GN02],[tBKA02], and three typical concatenated schemes are:

- Direct transmission of random-like codes;
- A concatenated scheme with STBC as the inner code;
- A concatenated scheme with STTC as the inner code.

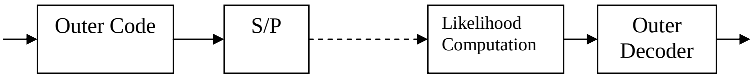

Figure 4.2: Direct transmission scheme

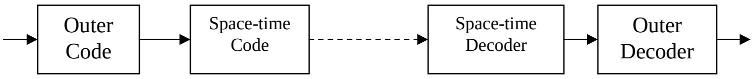

Figure 4.3: Space-time concatenation schemes

The direct transmission scheme may be thought of as a concatenated system where the inner space-time codes is a trivial serial to parallel (S/P) converter. The transmit sequences for this scheme imitate the equiprobable i.i.d. sequences from a finite alphabet, and we will focus on this scheme in this chapter.

The modulation considered in this chapter is BPSK. One of the difficulties for space-time codes design is that, the diversity and coding advantage criteria apply to complex domain, but traditional code design is working in discrete domain. For BPSK modulation, the discrete domain is the field $F_2 = \{0, 1\}$ of integers modulo 2. Modulation is performed by mapping the symbol $x \in F_2$ to the constellation point $s \in \{+1, -1\}$ according to the rule $s = (-1)^x$. In [JG00], Hammons and El Gamal developed binary rank criteria to guarantee that the space time code achieves some degree of diversity, which can be stated as:

**Proposition 4.1** *(Hammons and El Gamal, 2000) Let $\mathcal{C}$ be a binary linear $Q \times N$ space-time code with $N \geq Q$. Suppose that the minimum binary rank of the nonzero codeword in $F_2$ is $d$, then the space-time code achieves transmit diversity $d$ (in the complex signal domain).*

When rank criterion is concerned, we can concentrate on the field $F_2$ first, and based on this proposition the space time code will obtain the transmit diversity accordingly.

## 4.3 Rate-Diversity Tradeoff for S/P of LDPC

In this section, we consider the following MIMO systems: BPSK, $Q$ transmit antennas, direct transmission of LDPC code by S/P conversion, and the LDPC codes are from ensemble B, where parity check matrix $H$ is chosen with uniform probability from the ensemble of $M \times N$ (0,1)-matrices having column sums equal $k$. Now the *transmission rate of the whole system* is $\eta = QR$, where $R \geq 1 - \frac{M}{N}$. On the rate-diversity tradeoff of the system, we have the following theorem:

**Theorem 4.1** *Let the LDPC coding rate be R, and the system transmission rate be $\eta = QR$. For every fixed k, there is a constant $\beta_k$ so that the transmit diversity $d \geq Q(1-R)\beta_k + 1$ can be achieved with probability one. Furthermore, $\beta_k \sim 1 - e^{-k}/\log 2$ as $k \to \infty$*

Combining with the Singleton upper bound $d = Q(1-R)+1 = (Q-\eta)+1$, we see that the following transmit diversity gain is achievable with probability one,

$$(Q-\eta)\beta_k + 1 \leq d \leq (Q-\eta)+1$$

The diversity given in theorem 1 approaches the bound quickly and closely, even for relatively small $k$ such as 3 or 4.

To prove theorem 1, let's first consider the simple case $Q = 2$. Suppose a codeword $c$ is divided into two parts $c_1$ and $c_2$, where where $c_1$ and $c_2$ are column vectors and transmitted over two antennas respectively, and we want to show that rank-one is not likely. Rank-one has two cases: $c_2 = 0$ or $c_1 = c_2$. By the parity check matrix $H = [H_1, H_2]$ and the parity check equation $Hc = 0$, we have $H_1c_1 = 0$, or $[H_1 + H_2]c_1 = 0$. Then our question can be described in another way, whether the null space of $H_1$ or $H_1 + H_2$ is zero with probability one, i.e. whether the matrix $H_1$ or $H_1 + H_2$ is full rank. Such questions have been partly answered by researchers in mathematics. In [Cal97], the lower bound $\beta_k n$ is determined for the number of random binary vectors of length $n$ with weight $k$ to obtain a dependent set of vectors with probability one. More information can be found in related papers [Cal96, BKW97].

Let $S_{n,k}$ denote the set of binary vectors of length $n$ having $k$ 1's, and $u_1, u_2, \cdots, u_m$ be vectors chosen uniformly at random from $S_{n,k}$. Let $r$ be the rank of the set $\{u_1, u_2, \cdots, u_m\}$, and denote by $s = m - r$ (equivalently, $s$ is the dimension of the kernel of the matrix having columns $u_1, u_2, \cdots, u_m$). Denote by $p_{n,k}(m)$ be be the probability that $u_1, u_2, \cdots, u_m$ are linearly dependent. An exact expression for $E(2^s)$ can be determined by a Markov chain derived from a suitable random walk. Define

$$x_0 = 0, x_i = x_{i-1} + u_i \tag{4.3.1}$$

(so the steps in the walk correspond to flipping $k$ random bits).

We associate with this random walk the following Markov chain: define $y_i$ to be the weight of $x_i$. Then $y_0, y_1, y_2, \cdots, y_m$ is a Markov chain with states $\{0, 1, 2, \cdots, n\}$. The transition matrix $A$ for this chain, with $A = \{a_{pq}\}$, where $a_{pq}$ is the probability of moving from state $q$ to state $p$ is given by

$$a_{pq} = \binom{q}{\frac{k-p+q}{2}} \binom{n-q}{\frac{k+p-q}{2}} / \binom{n}{k} \tag{4.3.2}$$

Some results from [Cal97] are summarized as following:

**Theorem 4.2** *(Calkin 1997)*

**(1)** *The eigenvalues $\lambda_i$ and corresponding eigenvector $e_i$ of $A$, $i = 0, 1, \cdots, n$ are given by*

$$\lambda_i = \sum_{t=0}^{k} (-1)^t \binom{i}{t} \binom{n-i}{k-t} / \binom{n}{k} \tag{4.3.3}$$

*and the $j - th$ component of $e_i$ is given by*

$$e_i(j) = \sum_{t=0}^{j} (-1)^t \binom{i}{t} \binom{n-i}{j-t} \tag{4.3.4}$$

**(2)** *Let $U$ be the matrix whose columns are $e_0, e_1, \cdots, e_n$, then $U^2 = 2^n I$, and if $\Lambda$ is the diagonal matrix of eigenvalues, then $A = \frac{1}{2^n} U \Lambda U$*

**(3)** $|\lambda_i| \leq 1, \lambda_i = (-1)^k \lambda_{n-i}$. *Let $0 < c < \frac{1}{2}$, if $i = cn$, then*

$$\lambda_i = \left(1 - \frac{2i}{n}\right)^k - \frac{4\binom{k}{2}}{n} \left(1 - \frac{2i}{n}\right)^{k-2} \frac{i}{n} \left(1 - \frac{i}{n}\right) + O\left(\frac{k^3}{c^2 n^2}\right) \tag{4.3.5}$$

The eigenvalues and eigenvectors are related to the binary Krawtchouk polynomials:

$$K_l^{(i)}(x) = \sum_{t=0}^{l} (-1)^t \binom{x}{t} \binom{i-x}{l-t} \tag{4.3.6}$$

For a survey of properties of Krawtchouk polynomials, see [MS77, KL01].

We can compute the probability that $u_1, u_2, \cdots, u_t$ sum to 0, which is the $00-th$ coefficient in $A^t$ and is equal to

$$\frac{1}{2^n}\sum_{i=0}^{n}\lambda_i^t\binom{n}{i} \tag{4.3.7}$$

If $u_1, u_2, \cdots, u_m$ are vectors with $k$ 1's chosen independently at random, then the expected number of subsequences $u_{a_1}, u_{a_2}, \cdots, u_{a_t}$ which sum to 0 is

$$E(2^s) = \frac{1}{2^n}\sum_{t=0}^{m}\binom{m}{t}\sum_{i=0}^{n}\lambda_i^t\binom{n}{i} = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}(1+\lambda_i)^m \tag{4.3.8}$$

Define

$$f(\alpha,\beta) = -\ln 2 - \alpha\ln(\alpha) - (1-\alpha)\ln(1-\alpha) + \beta\ln(1+(1-2\alpha)^k) \tag{4.3.9}$$

and let $(\alpha_k, \beta_k)$ be the root of

$$\begin{aligned} f(\alpha,\beta) &= 0 \\ \frac{\partial f(\alpha,\beta)}{\partial\alpha} &= 0 \end{aligned} \tag{4.3.10}$$

**Lemma 4.1** *If $\beta < \beta_k$, and $m < \beta n$, then $\frac{1}{2^n}\sum_i\binom{n}{i}(1+|\lambda_i|)^m \to 1$ as $n \to \infty$; If $\beta > \beta_k$, and $m > \beta n$, then $\frac{1}{2^n}\sum_i\binom{n}{i}(1+|\lambda_i|)^m \to \infty$ as $n \to \infty$*

*Proof*: see Appendix A □

*Complete the proof of Theorem 1.* Now consider that $u_1, u_2, \cdots, u_t$ sum to 0. Each of these vectors is either directly from the original parity-check matrix $H$, or is a sum of different columns in $H$ (in case $Q = 2$, this corresponds to the situation of $H_1 + H_2$). Some vectors of $u_1, u_2, \cdots, u_t$ may contain the same column in the original parity-check matrix $H$, but such column is cancelled in the sum. So the probability that $u_1, u_2, \cdots, u_t$ sum to 0 is

$$\frac{1}{2^n}\sum_{i=0}^{n} \lambda_i^{t'} \binom{n}{i} \leq \frac{1}{2^n}\sum_{i=0}^{n} \lambda_i^{t} \binom{n}{i} \tag{4.3.11}$$

where $t' \geq t$.

$P(2^s > 1) < E(2^s) - 1$. The minimum rank is at least $\frac{M\beta_k}{N/Q} + 1$ and this completes the proof. □

While the theorem is proved only for BPSK modulation and for a specific ensemble of LDPC codes, we believe that it should still hold for general modulations and random-like codes, although formal proofs could be substantially more complex.

## 4.4 LDPC as Universal Good Code

In coding community, there have been different perspectives on whether there are good and practical codes, and whether there are universal codes. We first explain what we are meaning by these terms.

Shannon's coding theorem states that for any channel there exist families of block codes that achieve arbitrary small probability of error at any rate up to the channel capacity, and such code families are usually referred to as "*very good*" codes. By another term"*good*" codes, we mean the code families that achieve arbitrary small probability of error at data rates up to some maximum rate that may be less than the channel capacity. By "*practical*" code we mean code families which can be encoded and decoded in time and space polynomial in the block length [Mac99].

Shannon's proof was nonconstructive and employed random codes for which there is no practical encoding and decoding algorithm. The convectional view is that there are few known constructive code that are good, fewer still that are practical, and none at all that are both practical and very good. It seems to be widely believed that while almost any random linear code is good, codes with structure allowing practical coding are likely to be bad.

Another closely related question is whether there is a single code to be good for any channel. At a given decoding complexity, codes with consistently good proximity to capacity over a class of channels are usually referred to as "*universal*" codes [KW02]. It was anticipated that to achieve very good performance on a new channel, a new custom-designed code would be needed.

It appears that the invention of turbo codes and the rediscovery of LDPC codes have some revolutionary effect on the field of error correction codes, and researchers are now re-considering these issues mentioned above. In his work on good error-correcting codes based on very sparse matrices [Mac99], David MacKay proved that LDPC codes have two important properties for binary symmetric channels (BSC): 1. Because the codes are constructed from sparse matrices, they have simple and practical decoding algorithms; 2. These code are "*very good*" in spite of their simple construction. Furthermore, MacKay also proved that the same codes are in fact also good for any ergodic symmetric channel, which in some sense means that these codes are universal.

At about the same time, Richard Wesel conducted some work on universal trellis codes [KW02], [WLS00]. Following the compound channel theorem which indicates that a single code can provide reliable communication on all linear Gaussian vector channels [RV68], Wesel designed some universal space-time trellis codes, serial concatenated codes as universal codes for periodic erasures, and LDPC codes as universal codes for OFDM.

In the same paper on good error-correcting codes based on very sparse matrices [Mac99], David MacKay further wrote "*we are optimistic that they (LDPC codes) will be excellent codes for channel with bursts and fades*". When it comes to MIMO Rayleigh fading channel, we observe that LDPC codes work well for all the SNR regions:

- At low SNR, the MIMO Rayleigh fading channel behaves like AWGN channel, and LDPC codes work well due to their properties on minimum distance and average distance distributions.
- At moderate to high SNR, LDPC based space-time codes can achieve the rate-diversity trade-off, which means they could also be working well.

Therefore, it is safe to say that LDPC codes are good and universal, in the sense that they work for BSC, AWGN and MIMO Rayleigh fading channels.

However, our arguments here should not be interpreted into the extreme case that there is no need to study and construct new codes. On the contrary, any specific application has its own requirement and its own issues to consider, and new codes are always worth of investigation. Pseudo-random construction of codes work well, particularly for long block lengths, but more structured algebraic constructions are desirable both in order to describe codes compactly and to control their distance and other theoretic parameters more precisely [FKJ$^+$01]. All of these will continue to keep the fields of error-correction codes active and prospective. An example is that, within the family of LDPC codes, algebraic construction can still be found by finite geometry [KLF01] or by optical orthogonal codes [OLMK03a].

# Chapter 5

# LDPC Space-Time Codes: Code Design and Iterative Detection

Turbo codes and LDPC codes achieved success due to their remarkable performance. In last chapter, it has been proven that LDPC space-time codes can asymptotically achieve the Singleton upper bound of rate-diversity tradeoff with probability one, and we believe this property still holds for general modulations and random-like codes.

The performance of LDPC codes is relatively well understood so far, but it remains open how we can design these codes efficiently. Gallager only provided a class of pseudorandom LDPC codes [Gal63]. Pseudorandom constructions work well, particularly for long block codes. On other hand, more structured algebraic constructions are desirable both in order to describe codes compactly and to control their distance and graph-theoretic parameters more precisely. Finite geometries has been studied for design of LDPC codes, and we will investigate the algebraic constructions in this chapter.

While the decoding of these powerful random-like codes is the most well-known and celebrated special case of iterative detection, iterative detection itself is applicable to virtually every practical digital communication system and can provide significant gains in performance and/or complexity reduction. The core of the iterative detection structure is a soft-input soft-output (SISO) module that implements the maximum a posteriori (MAP) algorithm. In this chapter, we will describe how the likelihoods of the transmitted bits are computed from the received signals, and how the iterative decoding algorithm works for LDPC codes.

This chapter is organized as follows. First we design the LDPC space-time codes by constructing 2-dimensional array whose doubly-periodic correlation is bounded by 1, and show that such codes have the desired rank properties. Then the computation of likelihoods for transmitted bits is presented, and iterative decoding algorithm of LDPC is described. Finally we show simulation results and draw some conclusions.

## 5.1 Algebraic Design of LDPC Space-Time Codes

In previous chapter, we consider the ensemble of LDPC codes where the column weight is constant. Regular LDPC codes whose row weight is also constant will be considered in this section. LDPC codes are specified by the sparse parity check matrix containing mostly 0's and only a small number of 1's. The real inner product of any two rows, i.e. the "ones" in common between any two rows, is not greater than 1 so that the associated Tanner graph of the code has better minimum cycle length. In addition, it is desired that the parity-check matrices have the rank properties as described in the above. To satisfy these requirements, we construct the parity-check matrix by designing a 2-dimensional array whose doubly-periodic correlation is bounded by 1 and then mapping the array to the parity-check matrix.

Such 2-dimensional arrays also find applications in mobile radio, frequency-hopping spread-spectrum communications, and radar and sonar systems. In a frequency-hopping radar or sonar system [GT84], the signal consists of one or more frequencies for transmission at consecutive time intervals. When this signal is reflected from the target and received by the observer, it is shifted in both time and frequency. The observer can determine the amounts of the shifts and hence determine the distance and velocity. As a frequency-hop pattern, the Costas array has optimum ambiguity function.

Another closely related code is optical orthogonal code (OOC) [MZKZ95] [OLMK03b]. An OOC is a family of (0,1) sequences with good auto- and cross-correlation properties, i.e., the autocorrelation of each sequence exhibits the "thumbtack" shape and the cross correlation between any two sequences remains low throughout. Its study has been motivated by an application in a code-division multiple-access fiber optical channel. The use of OOC's enables a large number of asynchronous users to transmit information efficiently and reliably. The thumbtack shape of autocorrelation facilitates the detection of the desired signal, and the low cross correlation reduces the interference from unwanted users.

To design the LDPC space-time codes, we first construct a 2-dimensional array whose doubly-periodic correlation is bounded by 1. Let $p$ be a prime, $\alpha$ be a primitive element of $F_p$ [Hun74] [Nic99] [Rib01] . The $p \times (p-1)$ matrix $A$ is defined:

$$A(i,j) = \begin{cases} 1 & \text{if } i = \alpha^j, \\ 0 & \text{otherwise.} \end{cases}$$

It is known that doubly-periodic correlation of $A$ is bounded by 1 due to the construction [GT84] [MZKZ95]. Using matrix $A$, we can construct a $p \times p(p-1)$ sub-matrix:

- start from 1st row, and simply append all the remaining rows, we get a row vector of length $p(p-1)$;
- start from 2nd row, append all remaining rows (the original 1st row is now in the last, cyclic shift), we get a row vector of length $p(p-1)$
- repetition of this process leads to $p$ such vectors in total. With these $p$ vectors, we get a sub-matrix with $p$ rows and $p(p-1)$ columns.

Next, we shift $A$ to the left by one column; and by repeating the above steps, we get another sub-matrix. In this way, we may obtain $j (j < p-1)$ sub-matrices in total. If we put these sub-matrices together, we get a $jp \times p(p-1)$ parity-check matrix where there are $p-1$ ones in each row and $j$ ones in each column. Through this construction, the codeword length is $p(p-1)$, and the coding rate is roughly $1 - \frac{j}{p-1}$.

We illustrate the above algebraic construction by an example.

*Example:* Let $p = 5, \alpha = 2$. From the table, we obtain matrix $A$ where the bottom-left is assumed to be position $(0,0)$.

| $j$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $2^j$ | 1 | 2 | 4 | 3 |

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

About the doubly-periodic correlation, for any shift $\tau_1, \tau_2$,

$$\sum_{i=0}^{4} \sum_{j=0}^{3} A(i,j)A(i \oplus_5 \tau_1, j \oplus_4 \tau_2) \leq 1$$

If we let $j = 3$, we get a $15 \times 20$ matrix, where each row has four 1's, each column has three 1's, and the correlation of any two rows is at most one. This matrix is then used as the parity-check matrix. The matrix can also be written in another form:

$$\begin{pmatrix} A & P_LA & P_L^2A & P_L^3A & P_L^4A \\ AP_R & P_LAP_R & P_L^2AP_R & P_L^3AP_R & P_L^4AP_R \\ AP_R^2 & P_LAP_R^2 & P_L^2AP_R^2 & P_L^3AP_R^2 & P_L^4AP_R^2 \end{pmatrix} \tag{5.1.1}$$

where $P_L$ and $P_R$ are permutation matrices,

$$P_L = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}, P_R = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

In the following, we will consider the properties of codes designed in the above. Specifically, we will consider the minimum cycle length of the associated bipartite graph, and study the rank property of the parity check matrix.

As we know, the parity-check matrix also specifies a bipartite graph with $n$ variable nodes on the left and $m$ check nodes on the right. Each variable node corresponds to one bit of the codeword, i.e., to one column of $H$, and each check node corresponds to one parity-check equation, i.e., to one row of $H$. Edges in the graph connect variable nodes to check nodes and are in one-to-one correspondence with the non-zero entries of $H$. When the graph is cycle-free, the optimality of sum-product decoding algorithm can be proved [Tan81]. Generally the graph is not cycle-free, and we want the minimum cycle length to be large. For the above construction, we have the following theorem.

**Theorem 5.1** *The bipartite graphs associated to the codes presented here have minimum cycle length greater than or equal to 6.*

*Proof*: By the construction, the correlation of any two rows is upper-bounded by 1, i.e., there are no two "ones" in common. Therefore, there is no cycle of length 4, and the minimum cycle length is greater than or equal to 6. □

With regarding the rank property, it was indicated by Gallager [Gal63] that, at least $j-1$ rows are linearly dependent in the $jp \times p(p-1)$ parity-check matrix constructed in the above, therefore the rank of the parity-check matrix is at most $jp-j+1$. Simulation results show that, the matrices given by our construction usually have rank of at least $jp-j$ which is very close to the upper bound, and they satisfy the requirement for multiple antenna transmission. To study the rank property of the matrix, we may inspect the upper-left part in 5.1.1. For the special case of $\begin{pmatrix} A & P_L A \\ AP_R & P_L A \end{pmatrix}$, we have the following theorem.

**Theorem 5.2** *If $\alpha = 2$ is a primitive element of $F_p$ and used to construct the parity-check matrix, then $\begin{pmatrix} A & P_L A \\ AP_R & P_L A \end{pmatrix}$ has rank $2p-2$.*

*Proof*: ( + stands for $\oplus_p$ in the proof.) This matrix has $2p-2$ columns. Suppose it has rank less than $2p-2$, which means we could choose the columns

$\{x_1, \cdots, x_n\}(0 < n < p-1)$ from the left half and choose the columns $\{y_1, \cdots, y_n\}$ from the right half, such that

$$\begin{aligned} \alpha^{x_i} &= \alpha^{y_i} + 1 \qquad (5.1.2) \\ \alpha^{x_i+1} &= \alpha^{y_i+1} + 1, i = 1, \cdots, n \end{aligned}$$

and 1 is not in the set $\{\alpha^{y_i+1} + 1 : i = 1, \cdots, n\}$.

From 5.1.2, we also get $\alpha^{x_i+1} = \alpha^{y_i+1} + \alpha$, so the two sets $\{\alpha^{y_i+1} + 1 : i = 1, \cdots, n\}$ and $\{\alpha^{y_i+1} + \alpha : i = 1, \cdots, n\}$ need to be equal. Since 1 is not in the former set, this is not possible when $\alpha = 2$, contradiction. Therefore, the matrix has rank $2p - 2$ □

Although we could not completely prove the rank properties of our construction, simulation results show that such construction usually has the desired properties. Based on the result that LDPC space-time codes can asymptotically achieve the rate-diversity trade-off with probability one, it is reasonable to believe that our construction can achieve the tradeoff in finite length.

To design LDPC codes with long code length, such as $p(p^m - 1)$ with $m \geq 1$, we can also use another design which is derived from the above algorithm. The idea of both algorithms are similar. For more details, please refer [MZKZ95] [OLMK03b].

## 5.2 Iterative Detection and Simulation Results

Iterative detection may be regarded as a technique employing a soft-input soft-output algorithm that is iterated several times to improve the error performance of a transmission scheme, with the aim of approaching true maximum-likelihood decoding (MLD), with less complexity. In this section, we present a suboptimal detection algorithm for the direct transmission scheme, i.e. S/P of LDPC codes.

Basically, there are two methods in the receiver soft information processing:

- Iterative Decoding: Assuming that all the constellation points are equally likely, we compute the likelihoods of the transmitted bits, and use them for the iterative decoding the LDPC codes;

- Iterative Demodulation-Decoding: this is an improved version of decoding algorithm. Due to the use of soft-input soft-output decoder of LDPC codes, we can obtain an estimate of the probabilities of the transmitted bits, and use them as *a priori* information in the demodulation process. This way we obtain an iterative demodulation-decoding algorithm.

Using the iterative demodulation-decoding algorithm can obtain better performance over the iterative decoding algorithm, at the expense of increased hardware complexity that is either within today's technology or feasible in the near term. However, in this chapter we mainly focus on the iterative decoding algorithm to reduce the receiver complexity.

We now describe how the likelihoods of the individual bits are computed from the received signal. Consider the following MIMO systems: BPSK, $Q$ transmit antennas and $P$ receive antennas. At time $t$, the received signal after matched-filtering can be represented as

$$\mathbf{y} = \sqrt{\rho}\mathbf{H}\mathbf{b} + \mathbf{n} \tag{5.2.3}$$

where $\mathbf{y}$ is the received vector of $P \times 1$, $\mathbf{b}$ is the transmitted vector of $Q \times 1$, $\rho$ is the signal-to-noise ratio, $\mathbf{n}$ is the noise vector, and the $(P \times Q)$ channel fading coefficient matrix $H$ is known at the receiver. The likelihood for the $l$th element of $\mathbf{b}$, $b_l$, is given by

$$\begin{aligned} \wedge(b_l) &= \frac{P(b_l = 1|\mathbf{y})}{P(b_l = 0|\mathbf{y})} \\ &= \frac{P(b_l = 1, \mathbf{y})}{P(b_l = 0, \mathbf{y})} \end{aligned} \tag{5.2.4}$$

which can also be written as:

$$\wedge(b_l) = \frac{\sum_{\mathbf{b}:b_l=1} P(\mathbf{b}, \mathbf{y})}{\sum_{\mathbf{b}:b_l=0} P(\mathbf{b}, \mathbf{y})} \tag{5.2.5}$$

Assuming that all the constellation points are equally likely, we can write:

$$\begin{aligned}\wedge(b_l) &= \frac{\sum_{\mathbf{b}:b_l=1} P(\mathbf{y}|\mathbf{b})}{\sum_{\mathbf{b}:b_l=0} P(\mathbf{y}|\mathbf{b})} \\ &= \frac{\sum_{\mathbf{b}:b_l=1} \exp\left(-\frac{|\mathbf{y}-\sqrt{\rho}\mathbf{H}\mathbf{b}|^2}{N_0}\right)}{\sum_{\mathbf{b}:b_l=0} \exp\left(-\frac{|\mathbf{y}-\sqrt{\rho}\mathbf{H}\mathbf{b}|^2}{N_0}\right)} \end{aligned} \tag{5.2.6}$$

The likelihoods are then sent to the iterative decoder of LDPC codes. Iterative decoding algorithm of LDPC codes is described as following [MN97].

Let $\mathbf{H}$ be the parity-check matrix, and $\mathbf{x}$ be the codeword with $\mathbf{Hx} = 0$. We refer to the elements of $\mathbf{x}$ as bits and to the rows of $\mathbf{H}$ as checks. We denote the set of bits $n$ that participate in check $m$ by $N(m) \equiv \{n : \mathbf{H}_{mn} = 1\}$. Similarly we define the set of checks in which bit $n$ participates as $M(n) \equiv \{m : \mathbf{H}_{mn} = 1\}$. We denote a set $N(m)$ with $n$ excluded by $N(m)\backslash n$.

The algorithm has two alternating parts, in which quantities $q_{mn}$ and $r_{mn}$ associated with each nonzero element in $\mathbf{H}$ matrix are iteratively updated. The quantity $q^x_{mn}$ is the probability that bit $n$ of $\mathbf{x}$ is $x$, given the information obtained via checks other than check $m$. The quantity $r^x_{mn}$ is the probability of check $m$ being satisfied if bit $n$ of $\mathbf{x}$ is considered fixed at $x$ and the other bits have a separable distribution given by the probabilities $\{q_{mn'} : n' \in N(m)\backslash n\}$. This algorithm would give the exact posterior probabilities of all the bits if the associated bipartite graph has no cycles. This algorithm can be described:

- *Initialization*: The variables $q_{mn}^0$ and $q_{mn}^1$ are initialized to the values $f_n^0$ and $f_n^1$, based on the likelihoods from the demodulation processing.

- *Horizontal step*: we define $\delta q_{mn} = q_{mn}^0 - q_{mn}^1$ and compute for each $m, n$:

  $$\delta r_{mn} = \prod_{n' \in N(m) \backslash n} \delta q_{mn'}$$

  then set $r_{mn}^0 = (1 + \delta r_{mn})/2$, and $r_{mn}^0 = (1 - \delta r_{mn})/2$

- *Vertical step*: for each $n$ and $m$ and for $x = 0, 1$, we update:

  $$\delta q_{mn}^x = \alpha_{mn} f_n^x \prod_{m' \in M(n) \backslash m} r_{m'n}^x$$

  where $\alpha_{mn}$ is chosen such that $q_{mn}^0 + q_{mn}^1 = 1$. We can also update the following quantities $q_n^0$ and $q_n^1$ given by:

  $$q_n^x = \alpha_n f_n^x \prod_{m \in M(n)} r_{mn}^x$$

  These quantities are used to create a tentative bit-by-bit decoding $\hat{\mathbf{x}}$; if $\mathbf{H}\hat{\mathbf{x}} = 0$, the decoding algorithm stops. Otherwise, the algorithm repeats from the horizontal step. A failure is declared if some maximum number of iterations occurs without a valid decoding.

We present simulation results for MIMO systems with 4 transmit antennas and 4 receive antennas. We assume the quasi-static Rayleigh fading channel model, where

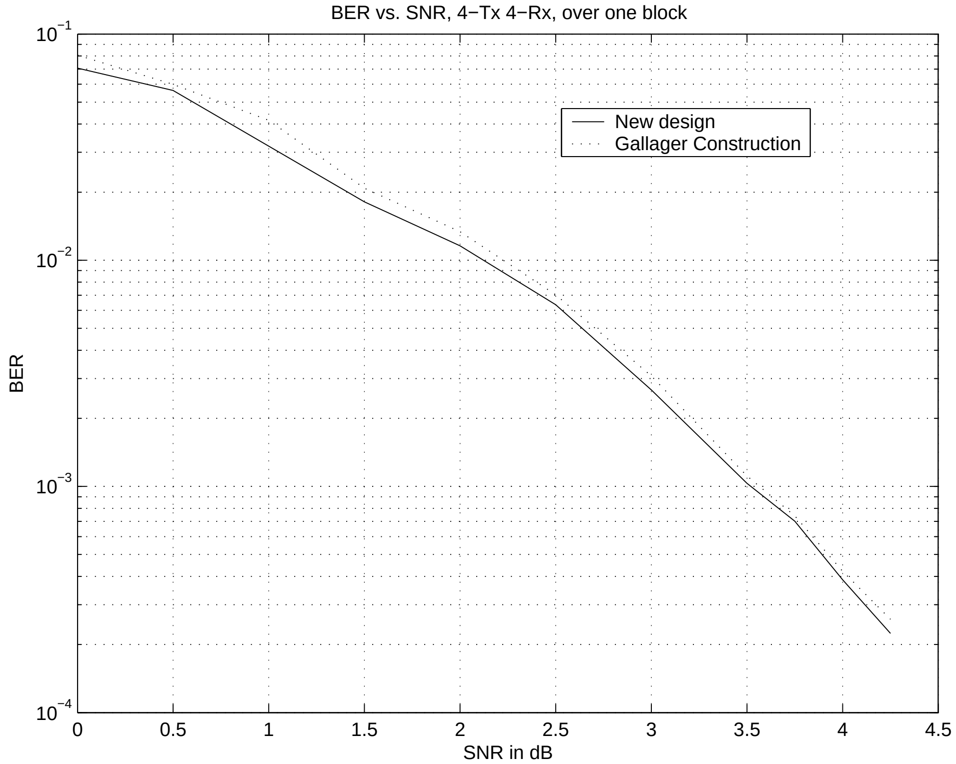

Figure 5.1: Bit Error Rate vs. SNR, BPSK, 4-Tx 4-Rx antennas, over one fading block.

the channel coefficients remain constant for one block length and then change to new independent random values for another block period.

We designed LDPC codes of rate 0.278, and the system transmission rate is 1.112 after the S/P conversion. For the iterative decoding algorithm, the maximum number of iterations is set to be 100. The bit error rates for coding over one fading block of length 330 are shown in Figure 5.1. The simulation result for Gallager construction is also shown, and the performance gain of our new design is about 0.1dB. It is worth noting that, the error floor of LDPC codes from algebraic construction is generally lower than the error floor of LDPC codes from random

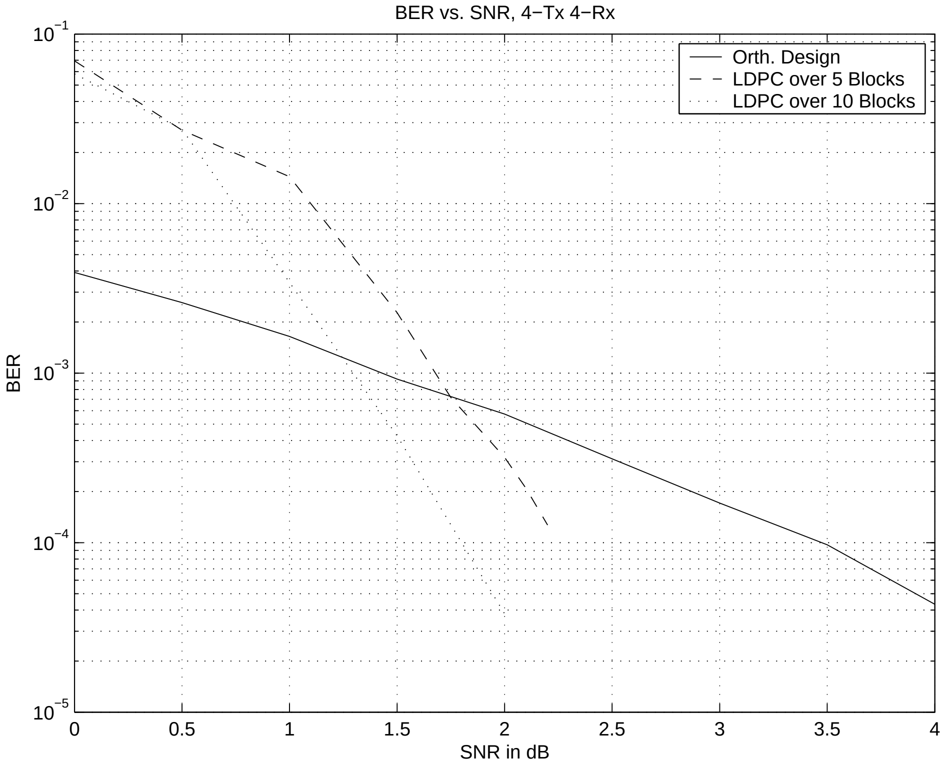

Figure 5.2: Bit Error Rate vs. SNR, BPSK, 4-Tx 4-Rx antennas, over multiple fading blocks.

construction. For fiber optical communications where bit error rate is about $10^{-12} \sim 10^{-15}$, error floor would be of concern.

The bit error rates for our new codes across 5 fading blocks and 10 fading blocks are shown in Figure 5.2. The bit error rate for orthogonal design of rate 1 is also shown. For LDPC space-time codes, we can see that the bit error rate decreases quickly around 1.0-2.0dB, and more fading blocks provide additional diversity.

# Chapter 6

# Space-Time Block Codes with Decoupled Decoding

In previous chapters, random-like space-time codes have been considered. These codes usually have large codeword length, employ iterative decoding/detection, and are capable of approaching the channel capacity. In this chapter, we will consider another space-time block code. Such code usually has short codeword length, and employs simple maximum-likelihood decoding algorithm.

Early uses of multiple transmit antennas in a scattering environment achieve reliability through diversity, where redundant information is sent or received on two or more antennas in the hope that at least one path from the transmitter reaches the receiver. To keep the transmitter and receiver complexity low, linear processing is often preferred. Orthogonal designs were developed to achieve full diversity, and each symbol can be decoded in a completely decoupled manner [TJC99]. However, the normalized transmission rate is equal or less than one.

To achieve the high data rates promised by multiple transmit antennas, BLAST (Bell Labs Layered Space-Time) was developed. BLAST and its further versions usually break the original data stream into substreams that are transmitted on the individual antennas. The receiver decodes the substreams using a sequence of nulling and canceling steps. The decoding complexity is usually higher than that of orthogonal design.

Linear dispersion (LD) codes, where data streams are dispersed in linear combinations over space and time [HH02b], can be regarded an intermediate scheme. LD codes subsume, as special cases, both of the above codes. They are simple to encode, and can be decoded in a variety of ways.

In this chapter, we first describe orthogonal design and quasi-orthogonal design. We then present the conditions on which LD codes can be decoded in the decoupled manner. An upper bound on the coding rate is also presented.

## 6.1 Orthogonal and Quasi-Orthogonal Designs

In this section, we describe the application of orthogonal designs to coding for MIMO systems. Unfortunately, these designs only exist in a small number of dimensions, as explained in the following.

*Real Orthogonal Designs*

A real orthogonal design of size $n$ is an $n \times n$ orthogonal matrix with entries the indeterminates $\pm x_1, \pm x_2, \cdots, \pm x_n$. The existence problem for orthogonal design is known as the Hurwitz-Radon problem, and was completely settled by Radon in another context at the beginning of last century. In fact, an orthogonal design exists if and only if $n = 2, 4, 8$.

Examples of orthogonal designs are the 2 × 2 design

$$\begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$$

the 4 × 4 design

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ -x_3 & x_4 & x_1 & -x_2 \\ -x_4 & -x_3 & x_2 & x_1 \end{pmatrix}$$

the 8 × 8 design

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ -x_2 & x_1 & x_4 & -x_3 & x_6 & -x_5 & -x_8 & x_7 \\ -x_3 & -x_4 & x_1 & x_2 & x_7 & x_8 & -x_5 & -x_6 \\ -x_4 & x_3 & -x_2 & x_1 & x_8 & -x_7 & x_6 & -x_5 \\ -x_5 & -x_6 & -x_7 & -x_8 & x_1 & x_2 & x_3 & x_4 \\ -x_6 & x_5 & -x_8 & x_7 & -x_2 & x_1 & -x_4 & x_3 \\ -x_7 & x_8 & x_5 & -x_6 & -x_3 & x_4 & x_1 & -x_2 \\ -x_8 & -x_7 & x_6 & x_5 & -x_4 & -x_3 & x_2 & x_1 \end{pmatrix}$$

To illustrate how the decoding works, let's take the example of 2 × 2 design.

$$\begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} = x_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = x_1 A_1 + x_2 A_2$$

The matrices $A_1$ and $A_2$ satisfy the following equalities:

$$\begin{aligned} A_1 A_1^T &= A_2 A_2^T = I, && (6.1.1) \\ A_1 A_2^T &= -A_2 A_1^T, && (6.1.2) \end{aligned}$$

Now assume the received signal is:

$$Y = H(x_1 A_1 + x_2 A_2) + N \tag{6.1.3}$$

The decoding algorithm is to minimize the trace of the matrix:

$$\begin{aligned} & \left(Y - H(x_1 A_1 + x_2 A_2)\right)\left(Y - H(x_1 A_1 + x_2 A_2)\right)^T && (6.1.4) \\ = \; & YY^T - Y(x_1 A_1 + x_2 A_2)^T H^T - H(x_1 A_1 + x_2 A_2) Y^T \\ & + H\left(x_1^2 A_1 A_1^T + x_1 x_2 (A_1 A_2^T + A_2 A_1^T) + x_2^2 A_2 A_2^T\right) H^T && (6.1.5) \\ = \; & YY^T - \left(x_1 (Y A_1^T H^T + H A_1 Y^T) - x_1^2 H\right) \\ & - \left(x_2 (Y A_2^T H^T + H A_2 Y^T) - x_2^2 H\right) && (6.1.6) \end{aligned}$$

The cross term $x_1 x_2$ disappears in (6.1.6) due to the condition in (6.1.2), and decoding of $x_1$ and $x_2$ can be completely decoupled. In fact, condition (6.1.2) can be interpreted as anti-commuting, and it is sufficient for completely decoupled decoding. Condition (6.1.1) is related with the full transmit diversity, and it has to be removed if we want to increase the transmission rate.

*Complex Orthogonal Designs*

Complex orthogonal design of size $n$ only exists for $n = 2$; For $n = 4$, the transmission rate can be only up to $\frac{3}{4}$. [TJC99]

*Quasi-Orthogonal Designs*

To increase the transmission rate for systems with 4 transmit antennas, quasi-orthogonal designs is proposed [Jaf01]

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2^* & x_1^* & -x_4^* & x_3^* \\ -x_3^* & -x_4^* & x_1^* & -x_2^* \\ x_4 & -x_3 & -x_2 & x_1 \end{pmatrix}$$

With this design, the normalized transmission rate is 1, and the receiver is to minimize a metric of sums $f_{14}(x_1, x_4) + f_{23}(x_2, x_3)$, where $f_{14}$ is independent of $x_2$ and $x_3$, and $f_{23}$ is independent of $x_1$ and $x_4$. Therefore, the receiver can find the pair $(x_1, x_4)$ and pair $(x_2, x_3)$ independently, while the symbols in the same pair have to be decoded jointly. We can call this partially decoupled decoding.

We summarize the comparison between orthogonal and quasi-orthogonal space time block codes.

- Orthogonal space-time block codes [TJC99]:
  - Full diversity, completely decoupled decoding;
  - For square matrix, real symbols, rate-1 only for 2, 4, 8 transmit antennas;
  - For square matrix, complex symbols, rate-1 for 2-Tx, rate 3/4 for 4-Tx, rate 1/2 for 8-Tx; the general upper bound is rate $\leq 3/4$ when more than 2-Tx.
- Jafarkhani's quasi-orthogonal space-time block codes [Jaf01]:
  - focus on complex symbols (real symbols solved in orthogonal case);
  - half diversity, partially decoupled decoding (in pairs);
  - rate 1 for 4-Tx, rate 3/4 for 8-Tx

## 6.2 LD Codes with Partially Decoupled Decoding

In this section, we consider the LD codes, and further develop the idea of partially decoupled decoding. To simplify the description, we only consider the real numbers; for complex numbers, the idea can be generalized.

Assume that $\{A_1, A_2, A_3, \cdots A_I\}$ are the basis matrices, symbols $\{x_1, x_2, x_3, \cdots x_I\}$ are going to be transmitted. For LD space-time codes, the transmitted code matrix is

$$S = \sum_{i=1}^{I} x_i A_i$$

From last section, it is known that, if $A_i A_j^T = -A_j A_i^T, i \neq j$, then decoding is completely decoupled, and the normalized data rate can be up to 1.

Now let's put the basis matrices into different groups:

$$\begin{aligned} M_{k1} &= \{A_1, A_2, \cdots, A_k\} \\ M_{k2} &= \{A_{k+1}, A_{k+2}, \cdots, A_{2k}\} \\ &\vdots \end{aligned}$$

We can see that, if any matrix from one group anti-commutes with any matrix from a distinct group, then $(x_1, x_2, \cdots, x_k)$, $(x_{k+1}, x_{k+2}, \cdots, x_{2k})$, $\cdots$ can be decoded independently. Therefore, the receiver can decode in the partially decoupled manner. For normalized data rate $\eta$, we have the following proposition:

- For $k = 1$, i.e. completely decoupled, $\eta \leq 1$;
- For $k = 2$, i.e. decoding in pairs, $\eta \leq 2$;
- For $k = 3$, $\eta \leq 3$;
- and so on.

We notice that, based on orthogonal design, removing the condition of full transmit diversity (while completely decoupled decoding is kept) does not increase the data rate.

The sketch of proof for the above proposition is as following. Let's consider the case of square matrix $n \times n$. Due to the property of anti-commuting, the first columns from distinct groups have to be orthogonal to each other. If all of them are non-zero, then there are at most $n$ dimensions, hence at most $n$ groups. If one of the first columns is zero, the remaining columns in that matrix can take from only one dimension, hence at most $n$ groups in total. Based on similar arguments, the proposition can be proved.

If we want to design the LD space-time codes with some degree of transmit diversity, there is another version of rate-diversity tradeoff. Combining this tradeoff and decoupled decoding will also be important both in theory and in practice.

# Chapter 7

# Conclusions and Future Work

The basic framework to integrate space-time codes and random-like codes has been developed. While the focus of this dissertation was on LDPC space-time codes with BPSK modulation, the performance analysis about rate-diversity tradeoff is believed to be true for general modulations and random-like codes.

The first step in our development was to find some appropriate performance criteria for multiple antenna systems over fading channels. Based on an alternate representation for Gaussian Q-function, a lower bound on the pair-wise error probability was obtained. Since the lower bound is a constant ratio of the upper bound, the transmit diversity which is indicated by these bounds is indeed good design criterion at moderate to high SNR. For finite alphabet MIMO systems, it was then shown that there is a fundamental tradeoff between the data rate and the transmit diversity, and the Singleton upper bound on the rate-diversity tradeoff is asymptotically achievable. This fundamental tradeoff can be used as criterion to evaluate and design space-time codes.

Performance analysis of random-like space-time codes was then conducted. For BPSK modulation and a specific ensemble of LDPC codes, it was proved that the upper bound on the rate-diversity tradeoff can be asymptotically achieved with probability one. Based on this property as well as the properties of minimum distance and average distance distributions, LDPC codes can be regarded as universal good codes.

Algebraic design of LDPC space-time codes was proposed by constructing a two-dimensional array with bounded doubly-periodic correlation, the associated bipartite graph was analyzed in terms of minimum cycle length, and the rank property of the parity-check matrix was considered. Iterative detection was studied, and simulation results show the remarkable performance of random-like space-time codes. Linear dispersion space-time codes with simplified decoding algorithm was also discussed.

In short, the materials in Chapters 3 and 4 demonstrate the fundamental tradeoff between rate and diversity for MIMO systems, and the materials in Chapter 5 demonstrate the algebraic design and iterative decoding of random-like space-time codes. It is clear that this investigation has raised more questions than it has definitively answered. There are several areas which warrant further detailed investigation:

- *Efficient Design of Codes on Graphs*: The algebraic design presented in Chapter 5 works well for LDPC codes with moderate block length, but it involves a great amount of matrix operations for large block length. Graphic model has been introduced to describe codes, therefore it would be interesting if we can find algebraic construction for graphs that have the useful properties and at the same time are suitable for iterative decoding.

- *ad-hoc Wireless Networks*: In MIMO systems, all the transmit antenna are located in one terminal (the transmitter), hence they can fully cooperate in the encoding process. Similarly, all the receive antenna can fully cooperate in the decoding process. However, if the antenna are equipped in different terminals and these terminals are not static, this is the scenario of ad-hoc mobile wireless networks [GK00]. These ad-hoc networks initially found application primarily in military settings, but are recently penetrating certain commercial arenas such as home networking. For multi-source multi-destination wireless networks and wireless networks with cycles, there are still a lot of work to be conducted on the capacity analysis.

- *Network Coding in Wireless Networks*: In contrast to infrastructure networks that employ the direct wireless transmission between mobiles and a base station, ad-hoc networks have gravitated toward cascade transmission between source and destination terminals via several intermediate relay terminals. If there are parallel relay terminals, the ideas in space-time codes design can be employed, and new performance criteria and design methods have to be investigated.

# Reference List

[BGT93] C. Berrou, A. Glavieux, and P. Thitmajshima. Near Shannon limit error-correcting coding and decoding: Turbo-codes. In *Proc. International Conf. Communications*, pages 1064–1070, May 1993.

[BKW97] J. Blomer, R. Karp, and E. Welzl. The rank of sparse random matrices over finite fields. Random Structures and Algorithms, pages 407–419, 1997.

[CAC01] K. M. Chugg, A. Anastasopoulos, and X. Chen. *Iterative Detection: Adaptivity, Complexity Reduction and Applications.* Kluwer Academic Publishers, 2001.

[Cal96] N. J. Calkin. Dependent sets of constant weight vectors in GF(q). Random Structures and Algorithms, pages 49–53, 1996.

[Cal97] N. J. Calkin. Dependent sets of constant weight binary vectors. Combinatorics, Probability and Computing, pages 263–271, 1997.

[CC] O. Coskun and K. Chugg. Combined coding and training for unknown ISI channels. *Submitted to IEEE Trans. Commununication.*

[Cra91] J. W. Craig. A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations. In *Proc. IEEE Military Comm. Conf.*, pages 571 –575, November 1991.

[FG98] Gerard J. Foschini and M. Gans. On limits of wireless communications in fading environment when using multiple antennas. *Wireless Personal Commun.*, 6:311–335, 1998.

[FKJ$^+$01] B. J. Frey, R. Koetter, G. D. Forney Jr., F. R. Kschischang, R. J. McEliece, and D. A. Spielman. Introduction to the special issue on codes on graphs and iterative algorithms. *IEEE Trans. Information Theory*, 47:493–497, February 2001.

[Gab85] E. M. Gabidulin. Theory of codes with maximum rank distance. Probl. Inform. Transm., pages 1–12, July 1985.

[Gal63] R. G. Gallager. *Low-Density Parity-Check Codes.* MIT Press, Cambridge, MA, 1963.

[Gam02] H. El Gamal. On the roubustness of space-time coding. *IEEE Trans. Signal Processing*, 50:2417–2428, October 2002.

[GK00] P. Gupta and P. R. Kumar. The capacity of wireless networks. *IEEE Trans. Information Theory*, 46(2):388–404, March 2000.

[GN02] V. Gulati and K. R. Narayanan. Concatenated space-time codes for quasi-static fading channels: Constrained capacity and code design. In *Proc. Globecom Conf.*, 2002.

[GT84] S. W. Golomb and H. Taylor. Constructions and properties of costas arrays. *Proc. IEEE*, 72(9):1143–1163, September 1984.

[HH02a] B. Hassibi and B. Hochwald. High-rate codes that are linear in space and time. *IEEE Trans. Information Theory*, 48(7):1804–1824, July 2002.

[HH02b] B. Hassibi and B. M. Hochwald. High-rate codes that are linear in space and time. *IEEE Trans. Information Theory*, 48(7):1804–1824, 2002.

[HM00] B. Hochwald and T. Marzetta. Unitary space-time modulation for multiple-antenna communication in Rayleigh flat fading. *IEEE Trans. Information Theory*, 46:543–565, March 2000.

[Hun74] T. W. Hungerford. *Algebra.* springer, 1974.

[Jaf01] H. Jafarkhani. A quasi-orthogonal space-time block code. *IEEE Trans. Commununication*, 49(1):1–4, January 2001.

[JG00] A. R. Hammons Jr. and H. El Gamal. On the theory of space-time codes for PSK modulation. *IEEE Trans. Information Theory*, 46:524–542, March 2000.

[JP00] R. W. Heath Jr. and A. Pauraj. Switching between spatial multiplexing and transmit diversity based on constellation distance. In *Proc. Allerton Conf. Commun., Control, Comp.*, October 2000.

[KH00] R. Knopp and P. A. Humblet. On coding for block fading channels. *IEEE Trans. Information Theory*, 46:189–205, January 2000.

[KL01] I. Krasikov and S. Litsyn. A survey of binary Krawtchouk polynomails. Codes and Association Schemes, 55:199–212, 2001.

[KLF01] Y. Kou, S. Lin, and M. P. Fossorier. Low-density parity-check codes based on finite geometries: A rediscovery of and new results. *IEEE Trans. Information Theory*, 47:2711–2736, November 2001.

[KW02] C. Kose and R. D. Wesel. Universal space-time trellis codes. In *Proc. Globecom Conf.*, pages 1108–1112, 2002.

[LMSS01] M. G. Luby, M. M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. Improved low-density parity-check codes using irregular graphs. *IEEE Trans. Information Theory*, 47:585–598, February 2001.

[LS02a] S. Litsyn and V. Shevelev. Distance distribution in ensembles of irregular LDPC codes. *Submitted to IEEE Trans. Information Theory*, January 2002.

[LS02b] S. Litsyn and V. Shevelev. On ensembles of LDPC codes: Aysmptotic distance distributions. *IEEE Trans. Information Theory*, 48:887–908, April 2002.

[LWKC02] H. Lu, Y. Wang, P. Kumar, and K. Chugg. On pairwise error problity of space-time codes. In *Proc. IEEE Symposium on Information Theory*, pages 330–330, July 2002.

[LWKC03] H. Lu, Y. Wang, P. V. Kumar, and K. M. Chugg. Remarks on space-time codes including a new lower bound and an improved code. *IEEE Trans. Information Theory*, 49(10), October 2003.

[Mac99] D. J. C. Mackay. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Information Theory*, 45:399–431, March 1999.

[MH99] T. Marzetta and B. Hochwald. Capacity of mobile multiple-antenna communication link in a Rayleigh flat fading. *IEEE Trans. Information Theory*, 45:139–157, January 1999.

[MN97] D. Mackay and R. Neal. Near shannon limit performance of low density parity check codes. *IEE Electronics Letters*, 33(6):457–458, March 1997.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* North-Holland, New York, 1977.

[MZKZ95] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev. New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. Information Theory*, 41(2):448–455, March 1995.

[Nic99] W. K. Nicholson. *Introduction to Abstract Algebra.* wiley, 1999.

[OLMK03a] R. Omrani, H. Lu, O. Moreno, and P. Kumar. Construction of LDPC codes from optical orthogonal codes. In *Proc. IEEE Symposium on Information Theory*, 2003.

[OLMK03b] R. Omrani, H. Lu, O. Moreno, and P. V. Kumar. Construction of low density parity check codes from optical orthogonal codes. In *Proc. IEEE Symposium on Information Theory*, 2003.

[Rib01] P. Ribenboim. *Classical Theory of Algebric Numbers.* springer, 2001.

[RU01] T. J. Richardson and R. L. Urbanke. The capacity of low-density parity-check codes under message-passing decoding. *IEEE Trans. Information Theory*, 47:599–618, February 2001.

[RV68] W. L. Root and P. P. Varaiya. Capacity of classes of Gaussian channels. SIAM J. Appl. Math., pages 1350–1393, November 1968.

[SA98] M. K. Simon and M. Alouini. A unified approach to the performance analysis of digital communication over generalized fading channels. *Proc. IEEE*, 86:1860–1877, September 1998.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, July 1948.

[SKWD01] W. Shi, C. Komninakis, R. D. Wesel, and B. Daneshrad. Robustness of space-time Turbo codes. In *Proc. International Conf. Communications*, pages 1700–1705, 2001.

[SR02] B. A. Sethuraman and B. Rajan. Optimal STBC over PSK signal sets from cyclotomic field extensions. In *Proc. International Conf. Communications*, pages 1783–1787, 2002.

[Tan81] R. Tanner. A recrusive approach to low complexity codes. *IEEE Trans. Information Theory*, 27:533–547, September 1981.

[tBKA02] S. ten. Brink, G. Kramer, and A. Ashikhmin. Design of LDPC codes for mulit-antenna modulation and detection. *Submitted to IEEE Trans. Communications*, June 2002.

[Tel99] I. Telatar. Capacity of multi-antenna Gaussian channels. *European Trans. Telecommun.*, 10:585–595, Nov./Dec. 1999.

[TJC99] V. Tarokh, H. Jafarkhani, and A. R. Calderbank. Space-time block codes from orthogonal designs. *IEEE Trans. Information Theory*, 45(5):1456–1467, July 1999.

[TSC98] V. Tarokh, N. Seshadri, and A. R. Calderbank. Space-time codes for high data rate wireless communication: Performance criterion and code construction. *IEEE Trans. Information Theory*, 44(2):744–765, March 1998.

[WCY$^+$03] Y. Wang, K. M. Chugg, J. Yang, Z. Zhang, and P. Kuo. On the tradeoff between perfomance and rate for finite alphabet MIMO systems. In *Proc. IEEE Symposium on Information Theory*, 2003.

[WLS00] R. D. Wesel, X. Liu, and W. Shi. Trellis codes for periodic erasures. *IEEE Trans. Commununication*, 48:938–946, June 2000.

[ZT02] L. Zheng and D. Tse. Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels. Submitted to IEEE Trans. Information Theory, January 2002.

[ZWZC01] G. Zhou, Y. Wang, Z. Zhang, and K. Chugg. On space-time convolutional codes for PSK modulation. In *Proc. International Conf. Communications*, pages 1122–1126, 2001.

# Appendix A

## *Proof of Lemma 4.1*

In this appendix, we will prove that:

If $\beta < \beta_k$, and $m < \beta n$, then $\frac{1}{2^n}\sum_i \binom{n}{i}(1+|\lambda_i|)^m \to 1$ as $n \to \infty$;

If $\beta > \beta_k$, and $m > \beta n$, then $\frac{1}{2^n}\sum_i \binom{n}{i}(1+|\lambda_i|)^m \to \infty$ as $n \to \infty$

where $(\alpha_k, \beta_k)$ is the root of

$$\begin{aligned} f(\alpha,\beta) &= 0 \\ \tfrac{\partial f(\alpha,\beta)}{\partial \alpha} &= 0 \end{aligned} \tag{A.0.1}$$

and

$$f(\alpha,\beta) = -\ln 2 - \alpha \ln(\alpha) - (1-\alpha)\ln(1-\alpha) + \beta \ln(1+(1-2\alpha)^k) \tag{A.0.2}$$

*Proof*: Since our value of $\beta_k$ is less than 1, we may assume that $\frac{m}{n} < 1-\delta$ for some $\delta > 0$. We shall show:

- The extreme tails of the sum are small.

- The middle range of the sum contributes 1 to sum.

- The rest of the sum is small if $\frac{m}{n} < \beta < \beta_k$, and is large if $\frac{m}{n} > \beta > \beta_k$

1. There is an $\epsilon > 0$ so that

$$\frac{1}{2^n}\sum_{i=0}^{\epsilon n}\binom{n}{i}(1+|\lambda_i|)^m \to 0 \text{ as } n \to \infty \tag{A.0.3}$$

Indeed,

$$\begin{aligned} \tfrac{1}{2^n}\textstyle\sum_{i=0}^{\epsilon n}\binom{n}{i}(1+|\lambda_i|)^m &< 2^{m-n}\textstyle\sum_{i=0}^{\epsilon n}\binom{n}{i} \\ &< n\epsilon 2^{m-n}\tbinom{n}{\epsilon n} \end{aligned} \tag{A.0.4}$$

and provided that $\epsilon$ is sufficiently small, this tends to 0.

Similarly,

$$\frac{1}{2^n}\sum_{i=(1-\epsilon)n}^{n}\binom{n}{i}(1+|\lambda_i|)^m \to 0 \text{ as } n \to \infty \tag{A.0.5}$$

2. We now show that the middle range of the sum contributes 1 to $E(2^s)$. Indeed, in the range $\frac{n}{2} - n^{4/7} < i < \frac{n}{2} + n^{4/7}$,

$$(1+\lambda_i)^m = (1 + o\left(\frac{1}{n}\right)^m = 1 + o(n) \tag{A.0.6}$$

we have

$$\frac{1}{2^n}\sum_{i=\frac{n}{2}-n^{4/7}}^{\frac{n}{2}+n^{4/7}}\binom{n}{i}(1+|\lambda_i|)^m \sim \frac{1}{2^n}\sum_{i=\frac{n}{2}-n^{4/7}}^{\frac{n}{2}+n^{4/7}}\binom{n}{i} \to 1 \text{ as } n \to \infty \tag{A.0.7}$$

We then show that we can widen the interval about the middle:

$$\frac{1}{2^n}\sum_{i=\frac{n}{2}(1-\epsilon)}^{\frac{n}{2}(1+\epsilon)}\binom{n}{i}(1+|\lambda_i|)^m \to 1 \tag{A.0.8}$$

Since $|\lambda_i| = |\lambda_{n-i}|$, it suffices to show that

$$\frac{1}{2^n}\sum_{i=\frac{n}{2}(1-\epsilon)}^{\frac{n}{2}-n^{4/7}}\binom{n}{i}(1+|\lambda_i|)^m \to 0 \tag{A.0.9}$$

In this range,

$$|\lambda_i| < \epsilon^k + \frac{\binom{k}{2}}{n}\epsilon^{k-2} + O\left(\frac{k^3}{n^2}\right) \tag{A.0.10}$$

hence

$$(1+|\lambda_i|)^m < e^{n\epsilon^k} e^{\binom{k}{2}\epsilon^{k-2}} \tag{A.0.11}$$

and since $k \geq 3$, the $n\epsilon^k$ term in the exponent is dominated by the $-n\epsilon^2$ term from the binomial coefficient, provided that $\epsilon$ is sufficiently small.

3. We now consider the remainder of the sum, or rather, the part in $(0, \frac{n}{2})$.

Define

$$f(\alpha,\beta) = -\ln 2 - \alpha\ln(\alpha) - (1-\alpha)\ln(1-\alpha) + \beta\ln(1+(1-2\alpha)^k) \tag{A.0.12}$$

Then if $f(\frac{i}{n}, \frac{m}{n}) < \gamma < 0$, the corresponding term of the sum is exponentially small, and if $f(\frac{i}{n}, \frac{m}{n}) > \gamma > 0$, the corresponding term of the sum is exponentially large. Therefore, if $f(\alpha, \frac{m}{n}) < \gamma < 0$ for all $\alpha \in (\epsilon, \frac{1}{2}(1-\epsilon))$, then we have:

$$\frac{1}{2^n}\sum_{i=\epsilon n}^{\frac{n}{2}(1-\epsilon)}\binom{n}{i}(1+|\lambda_i|)^m < ne^{\gamma n+o(n)} \to 0 \tag{A.0.13}$$

and if $f(\alpha, \frac{m}{n}) > \gamma > 0$ for some $\alpha \in (\epsilon, \frac{1}{2}(1-\epsilon))$, then we have:

$$\frac{1}{2^n}\sum_{i=\epsilon n}^{\frac{n}{2}(1-\epsilon)}\binom{n}{i}(1+|\lambda_i|)^m > \binom{n}{\alpha n}(1+\lambda_{\alpha n})^m 2^{-n} e^{\gamma n+o(n)} \to \infty \tag{A.0.14}$$

Now let $\beta_k$ be so that if $\beta < \beta_k$, then $f(\alpha,\beta) < 0$ for all $\alpha \in (\epsilon, \frac{1}{2}(1-\epsilon))$, and if $\beta > \beta_k$, then there is an $\alpha \in (\epsilon, \frac{1}{2}(1-\epsilon))$ such that $f(\alpha,\beta) > 0$. Thus we wish find $(\alpha_k, \beta_k)$ such that:

$$f(\alpha,\beta) = 0 \text{ and } \frac{\partial f(\alpha,\beta)}{\partial \alpha} = 0 \tag{A.0.15}$$

First we observe that $\alpha_k = e^{-k}$ and $\beta_k = 1 - \frac{e^{-k}}{\log 2}$ are close to a root, and there is no other root $\alpha$ in $(0, 1/2)$ and $\beta$ in $(0, 1)$. [Cal97]

As $k$ goes to $\infty$, the value of $\beta_k$ is asymptotic to

$$1 - \frac{e^{-k}}{\log 2} - \frac{1}{2\log 2}\left(k^2 - 2k + \frac{2k}{\log 2} - 1\right) e^{-2k} + O(k^4)e^{-3k} \tag{A.0.16}$$

□

This completes the proof for the theorem.