

**Low Complexity Iterative Detection and Decoding in
Finite Geometry LDPC-coded MIMO Systems**

by

Dananjaya Nuwan Balasuriya

A Thesis submitted to the Faculty of Graduate Studies of
The University of Manitoba
in partial fulfilment of the requirements of the degree of

Master of Science

Department of Electrical and Computer Engineering
University of Manitoba
Winnipeg, Manitoba, Canada

Copyright © 2009 by Dananjaya Nuwan Balasuriya

THE UNIVERSITY OF MANITOBA
FACULTY OF GRADUATE STUDIES

COPYRIGHT PERMISSION

**Low Complexity Iterative Detection and Decoding in
Finite Geometry LDPC-coded MIMO Systems**

By

Dananjaya Nuwan Balasuriya

A Thesis/Practicum submitted to the Faculty of Graduate Studies of The University of
Manitoba in partial fulfillment of the requirement of the degree
Of

Master of Science

Dananjaya Nuwan Balasuriya©2009

Permission has been granted to the University of Manitoba Libraries to lend a copy of this thesis/practicum, to Library and Archives Canada (LAC) to lend a copy of this thesis/practicum, and to LAC's agent (UMI/ProQuest) to microfilm, sell copies and to publish an abstract of this thesis/practicum.

This reproduction or copy of this thesis has been made available by authority of the copyright owner solely for the purpose of private study and research, and may only be reproduced and copied as permitted by copyright laws or with express written authorization from the copyright owner.

Abstract

In multiple-input multiple-output (MIMO) antenna wireless communication systems, finite geometry low density parity check (FG-LDPC) channel codes can be used to achieve a very high reliability. In general, in a MIMO-LDPC system, joint detection and decoding is needed to guarantee the near-optimal performance and a practical approach to achieving this is by iterative joint detection and decoding (IJDD). But, the joint detection and decoding of FG-LDPC codes using the near-optimal belief propagation (BP) algorithm is prohibitively complex in MIMO systems.

In this thesis, a novel low complexity IJDD algorithm based on a simple multiple bit flipping (MBF) decoder is proposed for FG-LDPC coded MIMO systems where the MIMO detector and the FG-LDPC decoder iteratively exchange soft information. An important issue addressed here is the generation of soft-information from the binary outputs of the MBF decoder to be fed back to the MIMO detector. In particular, two methods are proposed to generate the soft feedback information from the decoder's bit vector output. Simulation results show that the proposed IJDD algorithm achieves a substantial reduction in decoding error probability compared to a cascaded detector and a decoder. We also compare the performance with BP based detector-decoders which are significantly more complex. The new algorithm provides a practical approach to joint detection and decoding of popular FG-LDPC codes in a MIMO system.

Acknowledgments

Support and guidance of many individuals are blended into this thesis.

First, I would like to express my sincere gratitude to my supervisors Prof. P. Yahampath and Prof. A. S. Alfa; without their support and guidance this thesis would not have been possible. Their patience, encouragement and invaluable advices throughout this period were the main forces behind this thesis.

Further, I am very grateful to Dr. Telex Ngatched, who introduced me to the field of channel coding, spending his valuable hours to guide me at my difficult times.

I am also very grateful to the Communications and Network Engineering Research Group at Robert Alan Kennedy Communications Laboratory. Working with them gave me an opportunity to experience the real research culture, sharing ideas of many individuals, which I experienced for the first time in my life.

Further, my deep gratitude is extended to all the Sri Lankan friends in Winnipeg who supported me in numerous ways to make my life in Winnipeg a very pleasant one.

Finally, I am forever indebted to my parents and to my only sister for the emotional care and support they have provided over the years, which has immensely contributed not only in the success of this thesis, but also in my total academic carrier. Also, I would like to say "thank you so much" to my wife Ganga, who accompanied me to Canada and stayed by my side throughout whatever the good or bad times, supporting, encouraging and looking after me as a wife, a sister and as my very best friend. She was a reservoir of patience. To four of them, I dedicate this thesis.

Contents

Abstract	i
Acknowledgments	ii
List of Tables	vii
List of Figures	viii
List of Acronyms	x
1 Introduction	1
1.1 An Overview of the Digital Communication System	2
1.2 An Overview of the Wireless Channel	3
1.3 Introduction to MIMO Systems	6
1.4 MIMO Systems with Channel Coding	7
1.5 Contribution of the Thesis	8
1.6 Outline of the Thesis	9

2	Fundamentals	11
2.1	MIMO System Model	11
2.1.1	The Transmitter	12
2.1.2	The MIMO Channel	13
2.1.3	The Receiver	15
2.2	Low Density Parity-Check Codes	17
2.2.1	Tanner Graphs	18
2.2.2	Encoding of LDPC Codes	20
2.2.3	Decoding of LDPC Codes	21
2.3	Finite Geometry LDPC Codes	30
3	Iterative Joint Detection and Decoding of LDPC Coded MIMO Sys-	
	tems	34
3.1	Suboptimal Detectors in IJDD	36
3.1.1	List Sphere Detection (LSD)	36
3.1.2	Minimum Mean Square Error Equalizer with Successive Interfer-	
	ence Cancellation	39
3.2	Individually Optimal Detector Based IJDD Algorithm	42
3.2.1	Three Level Tanner Graph	43
3.2.2	Tripartite Message Passing Algorithm	44
3.3	Simulation Results	47

4	Low Complexity IJDD of FG-LDPC Coded MIMO Systems	53
4.1	The Log Likelihood Domain Detector	54
4.2	The Feedback	58
4.2.1	Inverted LLR Soft Information (I-LSI)	58
4.2.2	Modified Inverted LLR Soft Information (MI-LSI)	59
4.3	The Proposed IJDD Algorithm	63
4.4	Computational Complexity	64
4.5	Simulation Results	66
5	Conclusions and Suggestions for Future Work	76
5.1	Summary and Conclusion	76
5.2	Possible Future Research Areas	79
	Bibliography	80
	Appendices	
A	Equivalent Representation of a Bandpass System	86
A.1	Equivalent Lowpass for a Bandpass Signal	86
A.2	Equivalent Lowpass for a Bandpass Channel	88
A.3	Equivalent Lowpass for a Bandpass System	88
B	Proof of (2.1), (2.2) and (2.3)	91
B.1	Proof of 2.1	91

B.2	Proof of 2.2	92
B.3	Proof of 2.3	94
C	Derivation of (2.6)	96
D	Generation of Finite Geometries	98
E	Derivation of (3.16)	100
F	Justification of the Independence Assumption	102
F.1	Independence Assumption for Bipartite BP Algorithm	102
F.2	Independence Assumption for Tripartite IJDD Algorithm	103
F.3	Independence Assumption for MBF Based Novel Algorithm	104
G	Localized Random Search Algorithm	105

List of Tables

4.1	Comparison of the average number of calculations per iteration of $255 \times$ 175 code at $SNR = 18$ dB	67
4.2	Comparison of the average number of calculations per iteration of $1023 \times$ 781 code at $SNR = 21$ dB	67

List of Figures

1.1	A digital communication system	2
2.1	The MIMO system model	12
2.2	A Tanner graph representation	19
3.1	Iterative joint detection and decoding	35
3.2	Three level example Tanner graph with 2x2 MIMO array	44
3.3	Three level Tanner graph with 2x2 MIMO array and lumped r nodes . .	45
3.4	Comparison of BER performance of joint and cascaded detection-decoding schemes for 63x37 FG-LDPC code with 2x2 MIMO antenna array	49
3.5	Comparison of BER performance of joint and cascaded detection-decoding schemes for 255x175 FG-LDPC code with 2x2 MIMO antenna array . . .	50
3.6	Comparison of BER performance of joint and cascaded detection-decoding schemes for 1023x781 FG-LDPC code with 2x2 MIMO antenna array . .	51
4.1	The receiver operating with MBF based IJDD	64

4.2	Frequency of occurrence of executed iterations for 255x175 FG-LDPC code (SNR=18 dB)	68
4.3	Frequency of occurrence of executed iterations for 1023x781 FG-LDPC code (SNR=21 dB)	69
4.4	Comparison of BER performance of different detection-decoding schemes for 255x175 FG-LDPC code with 2x2 MIMO antenna array	71
4.5	Comparison of BER performance of different detection-decoding schemes for 1023x781 FG-LDPC code with 2x2 MIMO antenna array	72
4.6	Comparison of BER performance of different detection-decoding schemes for 4095x3367 FG-LDPC code with 2x2 MIMO antenna array	73
4.7	Comparison of proposed decoder, with and without interleaver for 255x175 code	74
4.8	Comparison of proposed decoder, with and without interleaver for 1023x781 code	75
D.1	A sample euclidean geometry: $\mathcal{D} = 2, \mathcal{T} = 1$	99

List of Acronyms

AWGN	additive white Gaussian noise
BER	bit error rate
BF	bit flipping
BLAST	Bell labs layered space-time
BP	belief propagation
BPSK	binary phase shift keying
CDMA	code division multiple access
EXIT	extrinsic information transfer
FG-LDPC	finite geometric low density parity check
IJDD	iterative joint detection and decoding
ISI	inter-symbol interference
LDPC	low density parity check
LLR	log-likelihood ratio
LSD	list sphere detector
MAP	maximum a posteriori probability
MBF	multiple bit flipping
MIMO	multiple-input multiple-output
MMSE-SIC	minimum mean square error equalizer with successive interference cancellation
OFDM	orthogonal frequency division multiplexing
SDA	sphere decoding algorithm
SISO	single-input single-output
STBC	space-time block code

Chapter 1

Introduction

Today's high demand for high speed data communication over the wireless channels has generated new requirements. Communicating high volumes of data through limited capacity channels with minimum amount of errors, introduces the need of efficient source coding for signal compression and channel coding for error correction. Further the wireless technologies like multiple-input multiple-output (MIMO) systems have been a wide choice to improve the capacity and reliability of a channel.

In this introductory chapter, the basic elements in a digital communication system are introduced. Further, digital wireless communication system fundamentals will be followed by a brief discussion on MIMO channels and their advantages. The use of channel coding to combat the channel's impairments in MIMO systems will be discussed. Finally, the contributions of this thesis will be outlined.

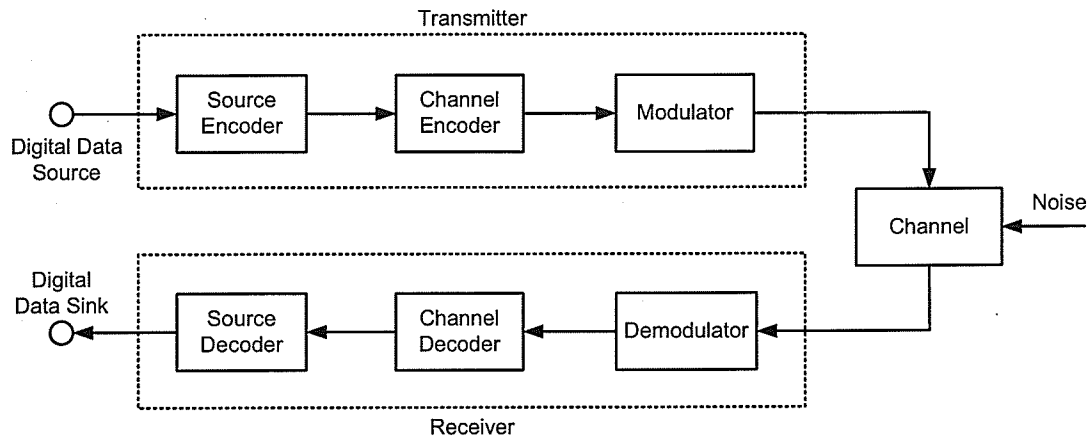


Figure 1.1: A digital communication system

1.1 An Overview of the Digital Communication System

A general communication system consists of three main components. The transmitter processes and converts the source information to a different format which is compatible with the channel. The channel is a medium to convey this signal to the receiver which recovers the original information. In any communication system, the modulator present at the transmitter converts the baseband information signal to a form which can travel a longer distances tolerating the channel impairments and the demodulator at the receiver extracts the baseband signal from the received signal. However in a digital communication system (Fig. 1.1), where the system deals with the signals which are discrete both in time and amplitude, more processing can be carried out in order to have a more efficient and reliable communication. This includes the source coding to eliminate the

redundancy in information and to compress the signals and channel coding which adds a controlled redundancy to the information, such that the original information can be recovered in case of a loss. Even with all these, there can be a mismatch between the recovered information at the receiver and the original information due to the following two reasons. First, the source coded information may be lossy compressed. Secondly the channel impairments may cause errors which are not completely eliminated by channel coding. Therefore the difference between the original signal and the recovered signal is a very important performance measure which in every digital communication system is the highest priority to be kept at an acceptable level.

The channel in a communication system can consist of a variety of media, namely twisted pair, coaxial cable, fiber optics or wireless communication with radio waves. In today's communication industry, wireless communication has become the most interesting communication area.

1.2 An Overview of the Wireless Channel

Radio waves are a kind of electro-magnetic waves which can carry energy over free space. The information can be embedded in these signals to be transmitted over a distance. However in a wireless channel, resources namely bandwidth and the transmit power are finite and special care is needed in sharing these resources in a multi-user, multi-system environment. Moreover it's of highest interest to efficiently use the bandwidth in wire-

less communication. In achieving this goal, the source coding plays a major role.

Further the information communicated must be reliable at the receiver end, hence channel coding plays the role of detecting and correcting the errors caused in the channel.

It is worthwhile to explore the causes of errors in the wireless channel. Wireless channel may have multiple paths for a signal to travel between a single transmitter and a single receiver. These multiple paths are created by 3 main phenomena in radio wave propagation.

- reflection
- refraction
- scattering

The multiple paths may vary in traveling distance, hence arriving at the receiver at different times. The signals traveling longer than the shortest path are said to be arriving with a *delay*. This delay causes multiple copies of the same signal to arrive at different times causing the symbols to interfere with the adjacent symbols which is known as inter-symbol interference (ISI). Whenever the channel is affected by ISI, the channel is said to be a frequency selective fading channel and the *coherence bandwidth* of the channel is smaller than the bandwidth of the signal. Coherence bandwidth is defined as the minimum frequency separation needed for two signals to undergo uncorrelated fading.

On the other hand the multiple paths received at the same time can have different

attenuations and phases, thus they can add up constructively or destructively at the receiver, which causes fading. Fading is two fold, namely fast fading and slow fading. Slow fading occurs whenever the *coherence time*, the time over which the channel stays constant is greater than the channel symbol time and fast fading otherwise.

Fading in communication systems can be stochastically modeled as a probability distribution of the magnitude of the fading coefficient. Rician and Raleigh [1] are the two most common models while some practical channels are more accurate to be modeled as Nakagami fading channels [2]. Moreover there are some empirical models such as Okumura-Hata model [2] which best fit some practical scenarios.

In wireless mobile communication, further impairments are added to the channel due to the mobility of the user [2]. The relative movement of the user causes a Doppler shift in frequency. With the multi-path signal, a range of frequencies are received at the receiver corresponding to one transmitted frequency, thus if the bandwidth of the signal is less than this frequency spread, frequency domain interference can occur.

Various measures are being taken to combat these adverse effects. Examples include the deployment of equalizers to mitigate ISI and use of diversity schemes to cope up with fading. Further, some multiple access schemes such as code division multiple access (CDMA) and orthogonal frequency division multiplexing (OFDM) provide ISI prevention themselves with their special properties. Apart from the fading effect, noise is introduced at the receiver antennas. Noise is usually modeled as additive white Gaussian noise (AWGN).

1.3 Introduction to MIMO Systems

Fading in wireless channels is a main cause of performance degradation, thus many schemes have been deployed to combat fading. One of the main such techniques is the diversity. Diversity can be three fold,

1. Frequency diversity
2. Time diversity
3. Space diversity

Frequency diversity refers to a technique where multiple copies of the same information are transmitted over different frequencies spaced more than the coherence bandwidth of the channel. Hence in case of a fading of one frequency, there will not be a complete loss of data.

Time diversity refers to a technique where multiple copies of the same information is transmitted over different time slots. Hence even when fading affects some time slots, the information has a higher probability to reach the destination. Channel coding is a very good example for time diversity where the check bits carrying the duplicate information are sent over different time slots. Channel coding provides a highly efficient method of deploying time diversity. However the proper design of channel codes and the decoding algorithms are required to ensure good performance.

However, both these diversity schemes add redundancy to the transmitted bit stream, hence threaten the efficiency in resource usage. As a remedy a third scheme, spacial

diversity has been proposed.

Spatial diversity is simply the use of multiple different paths to transmit the same information assuming that the probability of simultaneous fading in all the paths is very low. Spatial diversity can be easily achieved with MIMO antenna systems [3],[4]. Use of multiple antennas not only provide this reliability but also can be used to transmit multiple data streams through different antennas at the same time. This technique, known as spatial multiplexing, improves the system capacity. Further spatial diversity and spatial multiplexing can both be simultaneously achieved by utilizing a space-time block code (STBC) on top of the MIMO system [5]-[7]. Widely used STB codes such as the Alamouti code [8] and the Bell labs layered space-time (BLAST) code [9] provide exceptional performance in practical MIMO systems.

1.4 MIMO Systems with Channel Coding

As discussed in the previous section, multiple antennas add space diversity while channel codes provide time diversity. In most of the practical MIMO systems a space time code is deployed as the inner code and a channel code is utilized as the outer code to harness both these diversity advantages simultaneously [10]-[16].

Further, at the receiver, ideally the detection and decoding should be carried out jointly to obtain this total diversity gain advantage or otherwise the performance degradation can occur due to the lack of information transfer between dis-joint detection and

decoding processes. On the other hand such joint detection-decoding schemes are prohibitively complex when deployed with some of the channel codes such as low density parity check (LDPC) codes [17]-[21] due to their very large block length. However this issue can be partially resolved with the introduction of iterative joint detection and decoding (IJDD), where an information exchange between the two dis-joint sub systems occur in the form of a feedback.

Moreover a sub class of LDPC codes, finite geometric low density parity check (FG-LDPC) codes [22],[23] provides ease of encoding and also high performance due to their special structural properties. However the same properties add more complexity to decoding. Specially the belief propagation (BP) algorithm [17], which is the best performing algorithm for LDPC decoding becomes prohibitively complex. Therefore a simpler IJDD algorithm is required in order to benefit from the iterative joint decoding while gaining the advantages of FG-LDPC codes.

1.5 Contribution of the Thesis

In this thesis, a simplified IJDD algorithm is proposed as a solution to the above problem. The contribution of this thesis is basically two-fold. First a simulation is carried out to verify the performance gain in existing best performing tripartite message passing IJDD algorithm [24] in the FG-LDPC environment. Then, as a solution to the high complexity problem, a simple algorithm is proposed whose complexity rises only

linearly with the LDPC codeword length. In developing this algorithm, the complex message passing decoder is replaced by a simple decoder with the intention of simplifying the overall algorithm. The most important element of this thesis is the generation of soft feedback information from the decoder's output bit (hard) vector. An additional module is proposed to carryout this soft feedback information generation. Further, the performance of the proposed algorithm is investigated together with the computational complexity compared to the existing message passing algorithm.

1.6 Outline of the Thesis

The rest of the thesis is organized as follows. Chapter 2 introduces the fundamentals underlying the work in this thesis, namely the MIMO systems, LDPC codes, FG-LDPC codes and their decoding algorithms. In Chapter 3, a discussion of the existing methods for IJDD is presented. The BP based IJDD algorithms with simplified detector are first discussed. Moreover in Chapter 3, tripartite message passing algorithm consisting of an optimal detector and BP decoder, which is the existing algorithm with the highest performance is discussed. This algorithm's performance is verified by numerical simulations and compared with that of the disjoint detection-decoding scheme.

Any of the existing IJDD algorithms that will be discussed in Chapter 3 does not fit in FG-LDPC in MIMO environment due to their high complexity. To the author's knowledge, IJDD with FG-LDPC has not been analysed in any of the previous work.

Therefore in Chapter 4, a novel algorithm is proposed to combat this complexity issue. Further, the algorithm's novel components, the log likelihood domain detector, and most importantly the new feedback methods are discussed in detail. Moreover, a complexity analysis of the novel algorithm and the existing BP based methods are carried out and compared. In the final section of Chapter 4, a simulation is carried out for some FG-LDPC codes to investigate the performance of the proposed algorithm. Finally, Chapter 5 concludes the thesis with a discussion of possible future research paths in this area.

Chapter 2

Fundamentals

In this chapter, the main components present in the MIMO system studied in this thesis are discussed. Moreover, LDPC and FG-LDPC codes are discussed in detail. In these discussions, although we generally concentrate on the MIMO system, the LDPC decoding methods are presented in a single-input single-output (SISO) environment for simplicity.

2.1 MIMO System Model

The main components of the system considered in this thesis are shown in Fig. 2.1. Here we consider a channel coded MIMO system with N_t and N_r transmitter and receiver antennas, respectively. We will be describing the transmitter, the MIMO channel and the receiver in this section. We are specially interested in the receiver as the main focus of this thesis is on the two functions of the receiver, the detection and decoding.

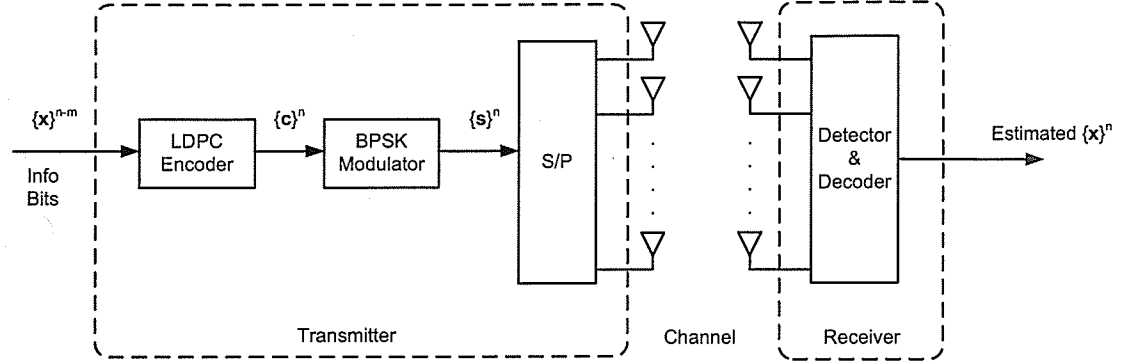


Figure 2.1: The MIMO system model

2.1.1 The Transmitter

The transmitter is responsible for the conversion of the information into a format which will ensure that the data is transferred to the receiver side and can be decoded with the minimal error probability. In this sense, both the channel coding and the modulation play a major role. Apart from those, the MIMO system itself adds redundancy to the information transfer so that the error probability is reduced. There are some forms of MIMO applications [25] where multiple antennas can be used to increase the capacity, but in this thesis we are only concerned with reducing the error probability.

At first, each consecutive block of $n - m$ information bits, \mathbf{x} is encoded by a $(n, n - m)$ binary channel code to produce an n bit channel codeword, \mathbf{c} . In this thesis we use binary FG-LDPC codes for this purpose, which will be described in detail in Section 2.3.

After encoding, the output of the channel encoder is modulated using a binary phase shift keying (BPSK) modulator to provide a symbol stream \mathbf{s} of length n . Consider-

ing the discrete time baseband equivalent of the wireless system (See Appendix A for details), let the modulation constellation be $\{-1, +1\}$. Hence the modulator uniquely maps the n bit channel codeword $\mathbf{c} \in \{0, 1\}^n$ to a n dimensional modulated signal vector $\mathbf{s} = (s_1, \dots, s_n)^T$, where $s_j \in \{-1, +1\}$. After modulation, the symbol stream needs to be distributed among the multiple transmission sessions $K = \lceil \frac{n}{N_t} \rceil$, such that $\mathbf{s} = \left((\tilde{\mathbf{s}}^{(1)})^T, \dots, (\tilde{\mathbf{s}}^{(K)})^T \right)^T$. Note that in the system considered in this thesis, extra, $n \bmod N_t$ padding bits are added to the K^{th} transmission session in each block. In fact one code block needs to be transmitted over K sessions of N_t symbols for each session. Each symbol is transmitted by a separate antenna in the N_t transmit antenna array. With the use of MIMO antenna array, there is a possibility to use space-time codes such as Alamouti codes or BLAST architecture to obtain an inner coding gain. However, we are interested in comparing disjoint (cascaded) and joint systems and the improvement made by the use of the space-time code affects both systems in a similar way. Hence, in this thesis we avoid the use of a space time code for simplicity and clarity.

2.1.2 The MIMO Channel

We consider a MIMO channel with N_t transmit antennas and $N_r (\geq N_t)$ receiver antennas. The modulated signal vector is sub-divided and the sub-blocks are transmitted by the transmitter antenna array as described in Section 2.1.1.

Practical channels are not perfect, in fact they consist of two main impairments. One of these is the fading, a phenomenon which randomly reduces or amplifies the signal

intensity at the receiver and fading can be represented by a channel gain coefficient matrix. Although the channel gains in a MIMO system in general are correlated, for simplicity we assume that the channel gains are uncorrelated in this thesis. Also, we assume that the channel gains are constant over a single transmission and the channel gains are completely known at the receiver.

As stated in Chapter 1, fading can be further described by the random distribution of channel gain magnitudes for which the most common models are the Rayleigh and Rician fading. Rayleigh fading occurs whenever there is no direct path between the transmitter and the receiver. However when there is a direct path between the transmitter and the receiver, the fading can be more accurately modeled as Rician fading. In this work, we select our fading model to be Rayleigh fading, thus the channel matrix corresponding to the l^{th} use of the channel, $H^{(l)}$ consist of $N_r \times N_t$ zero mean i.i.d. circularly symmetric complex Gaussian entries.

The other impairment is that the channel is affected by the Gaussian noise at the receiver antennas which in general is correlated. However in this work, as usual we consider the noise to be uncorrelated complex Gaussian with zero mean and variance σ^2 per real dimension. Let $(N_r \times 1)$ dimensional noise vector corresponding to the l^{th} transmission be denoted by $\tilde{\mathbf{n}}^{(l)}$.

Now we are in a position to state the relationship between the received values at the receiver antennas, $\tilde{\mathbf{r}}^{(l)}$, and the transmitted values $\tilde{\mathbf{s}}^{(l)}$ at the l^{th} use of the channel. The

received value at the l^{th} use of the channel is given by the $N_r \times 1$ dimensional vector,

$$\tilde{\mathbf{r}}^{(l)} = \mathbf{H}^{(l)}\tilde{\mathbf{s}}^{(l)} + \tilde{\mathbf{n}}^{(l)}.$$

Thus the received value vector \mathbf{r} corresponds to a single transmitted codeword to be collected over K uses of the channel is $\mathbf{r} = \left(\left(\tilde{\mathbf{r}}^{(1)} \right)^T, \dots, \left(\tilde{\mathbf{r}}^{(K)} \right)^T \right)^T$.

2.1.3 The Receiver

As discussed earlier, the received signal at the receiver antenna array is impaired by fading and the channel noise, thus the objective of the receiver is to estimate the transmitted information \mathbf{c} , while minimizing the corresponding error probability. Due to the fact that in the MIMO system discussed in this thesis, the channel code's output codeword length is very much larger than the number of antennas, each MIMO transmission delivers only a fraction of the entire codeword. As a result, an optimal receiver will have to estimate the transmitted information based on several MIMO transmissions.

In general this estimation is based on the minimization of either the bit error probability or the frame error probability. The estimate the receiver can make to minimize the probability of bit error is to maximize the a-posteriori probabilities (APPs), hence,

$$\hat{c}_j = \arg \max_{c_j \in \{0,1\}} P(c_j | \mathbf{r}, \mathbf{H}^{(1)}, \dots, \mathbf{H}^{(K)}) \quad j = 1, \dots, n.$$

To perform the above, in an ideal system, joint detection and decoding is used. However with the large block lengths in LDPC codes, it involves a prohibitively complex marginalization process [28], which cannot be accommodated in the system studied in this thesis.

Given that the implementation of the optimal joint detection and decoding is impossible, one obvious option in practical receiver design is to implement the disjoint receivers. The idea of disjoint detection and decoding, also known as cascaded detection-decoding is to separate the two coupled operations by ignoring the presence of the other. Such simplification is achieved at the cost of performance degradation in the receiver, because each detection is only capable of detecting a small fraction of a codeword and the correlation between these detected symbols (bits) and the rest of the codeword is neglected. In other words, with this disjoint scheme, the detector does not utilize knowledge about the code and the decoder does not use the knowledge of the channel. Hence, not all the available structure in the codeword is taken advantage of. Therefore due to the separation of the two functions, although they are optimal individually, as a whole they do not provide an optimal solution. In order to minimize this performance loss while retaining the low complexity, IJDD is used in practical receiver design [26]. IJDD is an iterative process derived directly from the concept of iterative decoding, also known as turbo decoding [27]-[30], in which soft information is exchanged between the detector and the channel decoder. Through exchanging of information with the channel decoder, the detector can explore the correlation of data bits in a codeword and improve its decision

based on the knowledge of the codeword inter-dependencies. In this thesis, we explore the IJDD schemes used in the general MIMO-LDPC systems and propose an IJDD algorithm to further reduce the complexity, thus it can be deployed in FG-LDPC coded MIMO systems which are too complex to decode with the existing IJDD techniques.

2.2 Low Density Parity-Check Codes

LDPC codes is a class of linear block codes which has the capability to achieve high error correcting performance, very close to Shannon's limit. LDPC codes were first discovered by Gallager [17] in 1960's, but unfortunately they were almost neglected for about forty years due to the lack of feasible decoding technologies. However, in late 90's they were again brought into prominence by Mackay and Neal [18]. Since then they have attracted a very high research interest and are accepted as a leading competitor to the commonly used high performing turbo codes.

A LDPC code is completely defined by its parity check matrix \mathcal{H} and like any other linear block code, any valid codeword \mathbf{c} belongs to the null space of \mathcal{H} . In other words \mathbf{c} is a valid codeword iff the syndrome vector $\mathbf{Z} = \mathbf{c}\mathcal{H}^T = \mathbf{0}$.

A binary LDPC code is said to be a *regular* LDPC code if the number of 1's along a row is a constant over all the rows in \mathcal{H} and the number of 1's along a column are a constant over all columns of \mathcal{H} . Further an LDPC code is a *systematic* code if the codeword's structure is either $[\mathbf{I} \ \mathbf{C}]$ or $[\mathbf{C} \ \mathbf{I}]$ where \mathbf{I} and \mathbf{C} are the information bit

vector and check bit vector of a codeword respectively. For the convenience, we only consider *regular systematic* LDPC codes in this thesis.

The key difference between the LDPC codes and the regular parity check codes is the sparse parity check matrix of LDPC codes. Similar to any other block code, LDPC code performance is highly dependent on its block length. Larger block lengths in the range of thousands of bits provide appealing performance than the shorter codes. However, decoding of such large block length LDPC codes have only been possible because of the sparse parity check matrix, which reduces the number of calculations in decoding. Due to the above properties, LDPC codes have been nominated for a myriad of communication standards and technologies such as Mobile WiMAX [31](IEEE 802.16e-2005) and 10GBase-T Ethernet [32](IEEE 802.3an.).

In early 80's a method of graphically representing the LDPC codes was introduced by Tanner and this graph is well known as the *Tanner graph* [33]. This provides an insight into a LDPC code and are very useful in code design and also decoding of LDPC codes.

2.2.1 Tanner Graphs

Tanner discovered the representation of a LDPC code using a bipartite graph consisting of bit (variable) nodes and check nodes at the edges of the graph. This structure can be directly derived from the parity check matrix. In this case, the m check nodes correspond to the m rows of \mathcal{H} and n bit nodes correspond to the n columns of \mathcal{H} . The nodes by edges are connected such that whenever the (j, i) position in \mathcal{H} is 1, the variable node

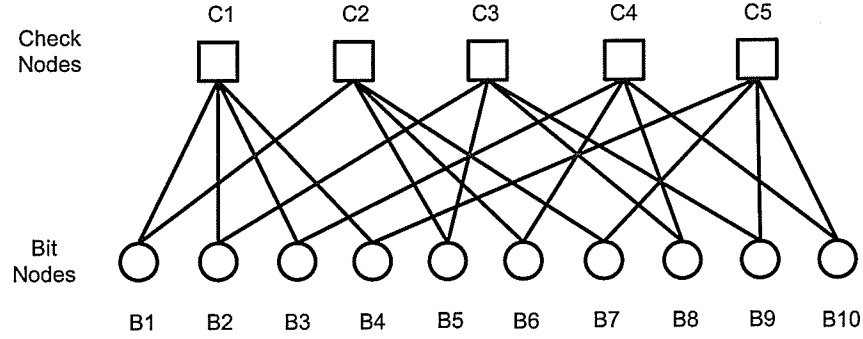


Figure 2.2: A Tanner graph representation

i is connected with check node j . In the Tanner graph, there exist connections only between nodes of different types. For the regular LDPC codes, the number of bit nodes connected to any of the check nodes is a constant and is equal to the row weight, w_r , of \mathcal{H} . Similarly the number of check nodes connected to each bit node is also a constant and is equal to the column weight, w_c . As an example consider the regular LDPC code given by,

$$\mathcal{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

The corresponding Tanner graph is shown in Fig. 2.2. The length of the shortest cycle, the number of edges it takes when starting from one node and returning to the same node via the shortest path is a very important parameter which is known as the *girth* of

the Tanner graph. In this example, the girth is six. Having a girth as high as possible is important in LDPC decoding to validate the independence assumption discussed in Chapters 3 & 4 (See Appendix F for details). Therefore, the Tanner graph not only provides a complete representation of the LDPC code, but also helps to decide the girth and the structure of the code easily.

The performance highly depends on the generation methods of LDPC codes and the decoding methods. There are a handful of methods in designing efficient LDPC codes and extrinsic information transfer (EXIT) chart based LDPC code generation [34] and geometry based LDPC code generation are two of the most commonly used. In this thesis we are interested in the LDPC codes generated based on finite geometries which will be discussed in Section 2.3.

2.2.2 Encoding of LDPC Codes

As in any other error correcting code, encoding process at the transmitter is to generate a set of additional bits (parity check bits) $\mathbf{p} = (p_1, p_2, \dots, p_m)$, based on the information bits $\mathbf{b} = (b_1, b_2, \dots, b_{n-m})$. This duplication of information provides a method to recover the original information in case of transmission errors.

In a systematic LDPC code, the information bits and the parity check bits are ordered as $[\mathbf{b} \ \mathbf{p}]$ to form a transmitted codeword. In order to encode an incoming set of information bits, the first step is to determine the generator matrix \mathcal{G} of size $(n - m) \times n$ such that $\mathcal{G}\mathcal{H}^T = 0$. This is usually achieved by reducing the \mathcal{H} to the form $[I \ P]$ by Gaussian

elimination, where I represents an identity matrix. Then \mathcal{G} can be written as $[P^T \ I']$ with I' being an identity matrix to match the dimensions of P^T . The codeword can be generated by multiplying the incoming information bit set by \mathcal{G} .

2.2.3 Decoding of LDPC Codes

LDPC decoding can be achieved by many methods and these decoding methods influence the performance of the code. These methods range from moderate to very good in performance and also from simple to very high in complexity. However, depending on the application, the decoding algorithm needs to be selected to achieve a trade-off between the complexity and the performance.

Belief propagation algorithm, which is also known as the sum-product algorithm, is an iterative message passing schemes which provides the best performance, very close to the Shannon's limit [18]. However, this method involves a large number of probability updates within each iteration, passed between bit and check nodes of a Tanner graph and hence is the most complex. The complexity of this algorithm increases rapidly with the block length. To cope with this issue many simplifications have been proposed. BP algorithm and its variants fall into the category of soft-in soft-out algorithms for LDPC decoding.

On the other hand, bit flipping (BF) is a very simple heuristic algorithm originally proposed by Gallager [17], which is a hard-in hard-out algorithm. It too is an iterative algorithm which has "hard-valued" inputs and outputs. However, the simplicity of this

decoding algorithm comes at a cost; a performance loss compared to the BP algorithm. In order to have a tradeoff between performance and complexity, a third algorithm is proposed [35], which is a hybrid of the two algorithms above and it makes use of the soft and hard information at the input to provide a hard bit vector at the output. This hybrid algorithm is further improved to have better performance without much added complexity by the introduction of the concept of multiple bit flipping within a single iteration.

Belief Propagation Algorithm

The BP algorithm iteratively calculates the probabilities of each node in a Tanner graph and these values are exchanged between bit nodes and check nodes to update and obtain a new set of probability values. This exchange of information can be viewed as a message passing between the two types of nodes, hence the BP is also known as a message passing algorithm.

Before presenting the BP algorithm for an isolated decoder, we need to define some notation to be used. Let \mathcal{N}_j denote the set of bits which participate in the j^{th} parity check and $\mathcal{N}_j \setminus i$ denote the set of all the elements of \mathcal{N}_j excluding i . Similarly \mathcal{M}_i and $\mathcal{M}_i \setminus j$ represents the set of checks in which bit i participate and the set of checks in \mathcal{M}_i excluding check j . Further in an iteration, let the message passed from the check node j to bit node i be $p_{ji}(c_i)$ and the message passed from bit node i to check node j be $q_{ij}(c_i)$. Here $c_i \in \{0, 1\}$. Moreover, let \mathbf{r} be the received value vector in a SISO channel.

Now we are in a position to present the probability domain BP algorithm.

Without the loss of generality we consider the message passing between bit node i and check node j . Initially, assuming Gaussian noise channel,

$$\begin{aligned} q_{ij}(1) = P_i &= Pr(c_i = 1|r_i) = \frac{1}{1 + e^{\frac{-2r_i}{\sigma^2}}}, \\ q_{ij}(0) &= 1 - q_{ij}(1), \end{aligned} \tag{2.1}$$

where σ^2 and r_i stand for the Gaussian noise variance and the i^{th} received value, respectively.

At any iteration the message passed from the check node j to the bit node i is

$$\begin{aligned} p_{ji}(1) &= \frac{1}{2} \left[1 - \prod_{i' \in \mathcal{N}_j \setminus i} (1 - 2q_{i'j}(1)) \right], \\ p_{ji}(0) &= 1 - p_{ji}(1). \end{aligned} \tag{2.2}$$

Derivation of these two equations is based on the probability of having an odd number of ones in other participating bits (in a parity check equation), given that the bit i is one and the probability of having an even number of ones in other participating bits, given that the bit i is zero [17]. This probability represents the probability of satisfying the j^{th} parity check equation, given that the bit i is either zero or one. It is an important thing to note that the message from the i^{th} bit node is excluded in this calculation in order to avoid the same information from looping back again.

Then,

$$\begin{aligned} q_{ij}(1) &= K_{ij} P_i \prod_{j' \in \mathcal{M}_i \setminus j} p_{j'i}(1), \\ q_{ij}(0) &= K_{ij} (1 - P_i) \prod_{j' \in \mathcal{M}_i \setminus j} p_{j'i}(0). \end{aligned} \quad (2.3)$$

Here K_{ij} is the normalizing constant. These two equations represent the probability of satisfying all the parity check equations where bit i is involved, given that the bit i is either zero or one [17]. Here too, the message from the j^{th} check bit is excluded from the calculation, in order to avoid the loop back of the same information.

Finally, in each and every iteration,

$$\begin{aligned} Q_i(1) &= K_i P_i \prod_{j \in M_i} p_{ji}(1), \\ Q_i(0) &= K_i (1 - P_i) \prod_{j \in M_i} p_{ji}(0), \end{aligned} \quad (2.4)$$

are calculated with K_i being a normalizing constant and the rule,

for every i ,

$$\hat{c}_i = \begin{cases} 1 & Q_i(1) > 0.5 \\ 0 & \text{otherwise,} \end{cases}$$

is used to generate the estimate $\hat{\mathbf{c}}$ for the transmitted bit vector. At the end of the iteration, the syndrome bit vector $\mathbf{Z} = \hat{\mathbf{c}}\mathcal{H}^T$ is generated. If the syndrome vector is not a null vector, further refinements are needed and the q_{ij} values are taken as inputs for the next iteration.

More detailed derivation of these probability calculation equations can be found in [17] and also presented in Appendix B.

In a binary coding scheme, each of these probabilities passed can assume two values, corresponding to the cases of the probability of the bit being either zero or one. This involves a huge number of messages passed, but this number can be halved by working in the log-likelihood domain, where the two messages passed between two nodes simultaneously are replaced by a single log-likelihood ratio (LLR) value.

LLR of a binary random variable u is defined as,

$$LLR(u) = \log \frac{P(u = 1)}{P(u = 0)},$$

which carries the information corresponding to both messages.

It is obvious that the sign of the LLR value determines the decoded value of the bit while the magnitude determines the reliability of this decision. Further, in the LLR domain, the probability domain multiplication operation becomes an addition. The addition in the probability domain must be represented in the LLR domain as a more complex operation involving the hyperbolic tangent function [36].

$$\text{Let } L(c_i) = \log \frac{P(c_i=1|r_i)}{P(c_i=0|r_i)}, L(p_{ji}) = \log \frac{p_{ji}(1)}{p_{ji}(0)}, \text{ and } L(q_{ij}) = \log \frac{q_{ij}(1)}{q_{ij}(0)}.$$

Then, the initialization in (2.1) becomes,

$$\begin{aligned} L(q_{ij}) = L(c_i) &= \log \frac{\left(1 + e^{\frac{-2r_i}{\sigma^2}}\right)^{-1}}{\left(1 + e^{\frac{2r_i}{\sigma^2}}\right)^{-1}} \\ &= \frac{2r_i}{\sigma^2}. \end{aligned} \quad (2.5)$$

The message passed from the check node j to the bit node i can be presented as,

$$L(p_{ji}) = -2 \tanh^{-1} \left[\prod_{i' \in \mathcal{N}_j \setminus i} \tanh \left(-\frac{1}{2} L(q_{i'j}) \right) \right]. \quad (2.6)$$

Derivation of this expression is given in detail in Appendix C.

Then, the message passed from the bit node i to the check node j can be converted to LLR domain as,

$$L(q_{ij}) = L(c_i) + \sum_{j' \in \mathcal{M}_i \setminus j} L(p_{j'i}), \quad (2.7)$$

and

$$L(Q_i) = L(c_i) + \sum_{j' \in \mathcal{M}_i} L(p_{j'i}).$$

Finally, using the fact that the sign of the LLR completely define the hard bit decision,

$$\hat{c}_i = \begin{cases} 1 & L(Q_i) > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Although the number of messages are halved in the LLR domain, the computing of the hyperbolic tangent and the inverse hyperbolic tangent adds a lot of complexity. But this issue can be resolved with the use of a specific function as given in [36], which is outside the scope of this thesis.

Bit Flipping Algorithm

Gallager's bit flipping algorithm is one of the simplest and earliest proposed algorithms for the decoding of LDPC codes. It too is an iterative decoding algorithm, but instead of a systematic convergence as in the BP algorithm, it makes a guess of the transmitted codeword at each iteration, by looking at the results of the parity check calculations. In BF algorithm, decoder computes all the parity checks and determine the bits which are involved in more than a predetermined number of unsuccessful parity check equations and then flip those bits to generate an estimate for the transmitted codeword. The resultant estimate is used to calculate a fresh set of parity check results, and if any of these resultant checks are non-zero, we proceed to the next iteration for another set of flips. Whenever all the parity checks are satisfied (i.e. whenever all parity check syndrome bits are zero), the currently estimated codeword is accepted as the valid transmitted codeword.

Although it does not have a rapid convergence as in the BP algorithm, this algorithm's convergence is also at a reasonable rate. Furthermore, with a smaller set of bits participating in each parity check (i.e. with lower row weights), this decoding scheme tends to provide better convergence. This can be easily explained by the fact that, with fairly smaller row weights, most of the parity checks will contain one or no bits affected by transmission errors. Hence, when most of the parity checks in which a given bit is involved are unsuccessful, it's a clear indication that that bit is in error.

Hybrid BF Algorithm

FG-LDPC codes are a special class of LDPC codes which offer a low probability of decoding error, but also involves a high decoding complexity due to their special structure. We will be discussing FG-LDPC in detail in the next section. In decoding FG-LDPC codes, the use of BP algorithm is very complex due to the higher number of bits involved in parity check equations, resulting in a large number of messages passed within one iteration. On the other hand, while BF is very simple, the benefit of using it in FG-LDPC scenario is reduced by increased probability of decoding error. Moreover with high row weight of the FG-LDPC parity check matrix, the rate of convergence is reduced.

To cope with these two problems, a hybrid algorithm between soft-in soft-out and hard-in hard-out is proposed in [35], which provides very much high performance than the Gallager BF algorithm, but at a very less complexity compared to the optimal BP algorithm. This algorithm is further modified to provide even appealing performance

without much increment in the complexity [37]. The modified hybrid algorithm, which will be referred to as the multiple bit flipping (MBF) algorithm in the rest of the thesis, can be presented as follows. Similar to the Gallager BF algorithm this algorithm starts with the hard limited received vector and searches iteratively over the n dimensional binary space for a valid codeword. Let, $l_j = \min_{i \in \mathcal{N}_j} |y_i|$ and $u_j = \max_{i \in \mathcal{N}_j} |y_i|$, where $y_i = \log \frac{f(c_i=1|r_i)}{f(c_i=0|r_i)}$. In other words l_j and u_j stand for the minimum and the maximum reliabilities corresponding to the set of bits which involves in the j^{th} parity check. Now we are in a position to describe the MBF algorithm. Let the syndrome vector generated by the parity check at $(k-1)^{th}$ iteration be $\mathbf{Z}^{k-1} = \hat{\mathbf{c}}^{k-1} \mathbf{H}^T \neq 0$. Then we need to select a set of \mathcal{P} bits to be flipped to generate the estimate or the new candidate for the transmitted bit vector. It is observed that the number of nonzero syndrome bits is proportional to the number of errors on average, hence there should be more bits to be flipped whenever there are more errors. The number of bits to be flipped can hence be decided by $\mathcal{P} = \left\lceil \frac{w(\mathbf{Z}^{k-1})}{w_c} \right\rceil$ where $w(\mathbf{Z}^{k-1})$ and w_c stands for the weight of the syndrome vector at the $k-1$ stage and the column weight of \mathcal{H} , respectively.

In order to select those \mathcal{P} bits from the total of n bits, sub-metric value $\phi_{i,j}^k$ is calculated as

$$\phi_{i,j}^k = \begin{cases} |y_i| - \frac{l_j}{2} & \text{if } Z_j^{k-1} = 0 \\ |y_i| - \left(u_j + \frac{l_j}{2}\right) & \text{if } Z_j^{k-1} = 1, \end{cases}$$

for every check $j = 1, 2, \dots, m$ and $i \in \mathcal{N}_j$. Thereafter, $\phi_{i,j}^k$ is summed over all the checks to generate the metric value $\phi_i^k = \sum_{j \in \mathcal{M}_i} \phi_{i,j}^k$, $i = 1, \dots, n$. Finally, the

minimum \mathcal{P} number of ϕ_i^k values are selected (these are the most unreliable considering the received values and the code structure) and the corresponding bits are flipped to generate the new estimate bit vector. This procedure takes into account that the bits to be flipped are decided not only depending on the reliability of the bit being considered, but also on the reliabilities of the other bits involved in the same unsuccessful parity checks. As an example, if a bit is occupied in an unsuccessful parity check and if all the other bits in the same parity check have a high reliability, the bit being considered has a higher probability of being in error. Hence will be selected with a high probability for flipping.

2.3 Finite Geometry LDPC Codes

LDPC codes are observed to be a leading competitor to turbo codes and they are widely used in a variety of applications. However, there are only a very few solid analytic procedures to generate good LDPC codes (eg: EXIT chart based LDPC code generation) [34],[38]. In fact, foundation work by Gallager only proposes a semi-random method for generating LDPC codes. Therefore, most of the good LDPC codes are computer generated and as a result they lack any structure. Consequently, encoding is very hard. Therefore, lately a class of LDPC codes called finite geometry LDPC codes have attracted much attention due to their special structure. Due to their either cyclic or quasi cyclic nature, the encoding can be done in linear time with feedback shift

registers, based on their generator polynomials. This ability of linear time encoding is unique to FG-LDPC.

There are two families of finite geometric LDPC codes, namely euclidean and projective geometric LDPC codes. Based on these two families, there are four classes of LDPC codes. Construction of the FG-LDPC codes is totally based on lines and points of a finite geometry. Let G be the finite geometry consisting of n points and J lines which has the following fundamental structural properties:

1. Every line consists of w_r points.
2. Every point is intersected by w_c lines.
3. Any two points are connected by one and only one line.
4. Two lines are either parallel (i.e. they have no point in common) or they intersect at one and only one point.

As stated earlier, two families of finite geometries possess the above structural properties.

Further, for a given dimension and a given Galois field [22], there is a finite geometry which satisfies the above properties. Several parameters, those define that finite geometry are proven [22] to be functions of the dimension \mathcal{D} and the field parameter \mathcal{T} . These parameters are listed in Appendix D. After determining these parameters, the lines and points, hence the finite geometry, can be formed. A simple example is discussed in Appendix D. Moreover the corresponding FG-LDPC code's parity check matrix generation

procedure is as follows.

Let us form a $J \times n$ matrix H_G over the binary field whose rows and columns corresponds to the J lines and n points of the finite geometry G , respectively. Hence the $(j, i)^{th}$ element of H_G is "one" if and only if j^{th} line contains the i^{th} point and the matrix element is zero otherwise. This H_G represents the parity check matrix of the corresponding FG-LDPC code. From the structural properties described above, it follows that every two columns have only one "1" in common and also any two rows have only one "1" in common. Since w_c and w_r are small compared to J and n , it is obvious that the resultant H_G is a sparse matrix and the null space of the same gives a binary LDPC code of length n . However, all the rows in H_G generated by the finite geometry are not linearly independent. Hence, the rank of the matrix, \mathcal{R} is lesser than the number of rows. Therefore, this in turn provides a $(n, n - \mathcal{R})$ binary LDPC code with parity check matrix H_G . This FG-LDPC is known as a type-I FG-LDPC code. The transpose of H_G also satisfies the above finite geometric properties and hence the null space of H_G^T too provides a FG-LDPC code, which is well known as a type-II LDPC code.

Another important property of the FG-LDPC codes is the minimum Tanner graph cycle length (girth) being six. Using the above structural properties, it can be proven that cycles with length four do not occur. (This proof is beyond the scope of this thesis). This is very important in the decoding process, as it preserves the independence of bits as much as possible, and improves the code's performance. Specially, the higher girth

of the FG-LDPC codes are very important for BP decoding.

Apart from all these, a very interesting property of the FG-LDPC codes is their ability to expand or compress a given FG-LDPC code to provide different FG-LDPC codes. Specially, by expanding the code, the girth can be increased to dramatically improve the performance of that code. However, the expanding methods are beyond the scope of this thesis and will not be discussed.

Chapter 3

Iterative Joint Detection and Decoding of LDPC Coded MIMO Systems

As discussed in Chapter 2, IJDD is a technique to achieve a tradeoff between the high complexity and high performance of joint detection-decoding and the low complexity and low performance of disjoint (cascaded) sub-optimal schemes. It allows the system to approach near optimal performance, without much complexity.

The idea behind the IJDD is that the detector and the decoder are considered as two serial individually optimal subsystems where the detector output becomes the input for the decoder. Further the decoder output is fed back as an input to the detector, to provide a new estimate in an iterative fashion (Fig. 3.1). By using the refined informa-

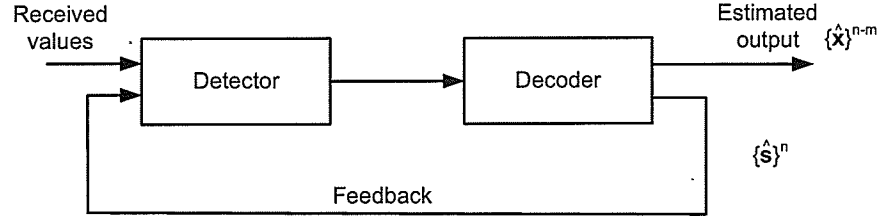


Figure 3.1: Iterative joint detection and decoding

tion of decoded bit values as feedback, the detector can provide an improved estimate compared to a standalone detector. However, when the number of antennas in the MIMO system is large, the length of the bit vector to be transmitted and detected in one use of the MIMO channel also becomes larger. Therefore, whenever an individually optimal detector is used as usual, it involves a marginalization over a large number of variables which is prohibitively complex [21]. This in turn increases the complexity of the overall IJDD system. As a solution to this issue, a large number of sub-optimal detectors are proposed, such as the list sphere detector (LSD) [39] and the minimum mean square error equalizer with successive interference cancellation (MMSE-SIC) [14]. All these sub-optimal detectors further reduce the overall performance from that of the individually optimal schemes. However, these allow us to keep the complexity of the overall IJDD system at an acceptable level.

3.1 Suboptimal Detectors in IJDD

In this section, we focus our attention on two widely used suboptimal detection schemes used in BP decoding based IJDD schemes, namely the list sphere detection and minimum mean square error equalization with successive interference cancellation.

3.1.1 List Sphere Detection (LSD)

In the optimal detector, the marginalization is carried out over the entire modulation signal constellation space (all possible valid combinations of the N_t bits transmitted in a single use of the channel), \mathcal{S}^{N_t} . Thus, the key idea behind LSD is to select a sub-space of this entire constellation space such that this sub-space contains the candidate bit vectors with a high probability. Then, the marginalization is carried out only over this subspace. Since LSD is directly derived from the sphere decoding algorithm (SDA), it is worthwhile to discuss the concept of SDA first.

In the optimal maximum likelihood detector, the estimate for the symbol vector is given by

$$\hat{\mathbf{s}} = \arg \min_{\mathbf{s} \in \mathcal{S}^{N_t}} \|\mathbf{r} - \mathbf{H}\mathbf{s}\|^2, \quad (3.1)$$

where \mathbf{r} and \mathbf{H} are the received vector and the channel gain matrix respectively. The index for the transmission (use of the channel) is omitted here for simplicity. Equation (3.1) involves an exhaustive search over the total space, \mathcal{S}^{N_t} . However, given the transmitted values, some of the candidates in this search space have very low probab-

ity of occurrence. Hence the search can be greatly simplified by confining to the high probability candidate set. These candidates satisfy the condition

$$d^2 \geq \|\mathbf{r} - \mathbf{H}\mathbf{s}\|^2, \quad (3.2)$$

where the sphere radius d is a parameter to be selected in order to have a tradeoff between the performance and the complexity. This idea of SDA is the foundation for the LSD algorithm discussed below. By “Q-R” decomposition of \mathbf{H} in (3.2)

$$\begin{aligned} d^2 \geq \|\mathbf{r} - \mathbf{H}\mathbf{s}\|^2 &= \left\| \mathbf{r} - [\mathbf{Q}_1 \ \mathbf{Q}_2] \begin{bmatrix} \mathbf{A} \\ \mathbf{0} \end{bmatrix} \mathbf{s} \right\|^2 \\ &= \left\| \begin{bmatrix} \mathbf{Q}_1^T \\ \mathbf{Q}_2^T \end{bmatrix} \mathbf{r} - \begin{bmatrix} \mathbf{A} \\ \mathbf{0} \end{bmatrix} \mathbf{s} \right\|^2 \\ &= \|\mathbf{Q}_1^T \mathbf{r} - \mathbf{A}\mathbf{s}\|^2 + \|\mathbf{Q}_2^T \mathbf{r}\|^2, \end{aligned} \quad (3.3)$$

where \mathbf{A} is a $N_t \times N_t$ upper triangular matrix and $\mathbf{Q} = [\mathbf{Q}_1 \ \mathbf{Q}_2]$ is a unitary matrix with \mathbf{Q}_1 and \mathbf{Q}_2 matrices consisting of the first N_t and last $N_r - N_t$ columns of \mathbf{Q} respectively.

Then, by letting $\check{\mathbf{s}} = \mathbf{A}^{-1}\mathbf{Q}_1^T \mathbf{r}$

$$d'^2 \geq \|\mathbf{A}(\check{\mathbf{s}} - \mathbf{s})\|^2, \quad (3.4)$$

where $d'^2 = d^2 - \|\mathbf{Q}_2^T \mathbf{r}\|^2$. Thereafter, by expanding the matrices in (3.4)

$$d'^2 \geq a_{N_t, N_t}^2 (s_{N_t} - \check{s}_{N_t})^2 + a_{N_t-1, N_t-1}^2 \left(s_{N_t-1} - \check{s}_{N_t-1} + \frac{a_{N_t-1, N_t}}{a_{N_t-1, N_t-1}} (s_{N_t} - \check{s}_{N_t}) \right)^2 + \dots \quad (3.5)$$

where $a_{i,j}$ denotes the (i, j) -th element of A . Right hand side of this inequality is a sum of different terms and with the addition of more terms, the inequality becomes tighter. If every term on the right hand side is considered as a separate necessary condition, starting from the first term, a set of inequalities can be derived as follows.

$$d'^2 \geq a_{N_t, N_t}^2 (s_{N_t} - \check{s}_{N_t})^2, \quad (3.6)$$

which implies,

$$\left[\check{s}_{N_t} - \frac{d'}{a_{N_t, N_t}} \right] \leq s_{N_t} \leq \left[\check{s}_{N_t} + \frac{d'}{a_{N_t, N_t}} \right]. \quad (3.7)$$

Now with the knowledge of the range of s_{N_t} we can consider the second term in (3.5),

which yields

$$\left[\check{s}_{N_t-1|N_t} - \frac{d'_{N_t-1}}{a_{N_t-1, N_t-1}} \right] \leq s_{N_t-1} \leq \left[\check{s}_{N_t-1|N_t} + \frac{d'_{N_t-1}}{a_{N_t-1, N_t-1}} \right], \quad (3.8)$$

where $\check{s}_{N_t-1|N_t} = \check{s}_{N_t-1} - \frac{a_{N_t-1, N_t}}{a_{N_t-1, N_t-1}} (s_{N_t} - \check{s}_{N_t})$ and $d'_{N_t-1} = d'^2 - (r_{N_t} - a_{N_t, N_t} s_{N_t})$. With the knowledge of s_{N_t} , (3.8) can be solved for a range of values of s_{N_t-1} .

Similarly, calculating in backward direction, all the constraints for the s_i , $i = 1, \dots, N_t$ values can be determined. Finally, the marginalization is carried out within the bound-

aries defined by these constraints. It is obvious that, with proper selection of d , these boundaries can be expanded or shrunk. Thus, d defines the marginalization space.

3.1.2 Minimum Mean Square Error Equalizer with Successive Interference Cancellation

MMSE-SIC is also a widely deployed technique to achieve the detection function in IJDD algorithms. The goal of the MMSE equalization is to minimize the mean square error between the transmitted signal vector \mathbf{s} and its estimate $\hat{\mathbf{s}}$

$$\min E \|\mathbf{s} - \hat{\mathbf{s}}\|^2. \quad (3.9)$$

The estimate $\hat{\mathbf{s}}$, which minimizes the MSE can be easily obtained by passing the received bit vector through an MMSE filter \mathbf{G}_{MMSE} such that

$$\hat{\mathbf{s}} = \mathbf{G}_{MMSE} \mathbf{r}. \quad (3.10)$$

The coefficients of the MMSE filter are selected to minimize (3.9) and are given by [40]

$$\mathbf{G}_{MMSE} = \mathbf{H}^H (\mathbf{H}\mathbf{H}^H + \sigma^2 \mathbf{I}_{N_r})^{-1}. \quad (3.11)$$

Here $(.)^H$ is the Hermitian operation and \mathbf{I}_{N_r} is an identity matrix of dimension N_r . However ISI present in the channel causes a performance degradation and a SIC is

usually deployed before the equalizer to reduce the effect of ISI. By using the a priori information fed back from the channel decoder, SIC calculates a modified received vector in which the interference from other bits at a given bit position are minimized. The a priori information provides the estimate

$$\tilde{x}_i = E[s_i] \quad i = 1, \dots, N_t, \quad (3.12)$$

and let

$$\tilde{\mathbf{x}}_i = [\tilde{x}_1, \dots, \tilde{x}_{i-1}, 0, \tilde{x}_{i+1}, \dots, \tilde{x}_{N_t}]^T, \quad (3.13)$$

which carries all the interfering symbol information corresponding to the bit position i .

The “soft-interference-cancelled” version of the received vector can be defined as

$$\tilde{\mathbf{r}}_i = \mathbf{r} - \mathbf{H}\tilde{\mathbf{x}}_i. \quad (3.14)$$

However, at the first iteration there will not be any a priori information available. Thus in a binary system, all the starting a priori information is taken as 0.5. Now the modified received vector $\tilde{\mathbf{r}}_i$ is fed back to the equalizer to calculate the best estimate

$$\hat{s}_i = \mathbf{w}_{i,MMSE}^H \tilde{\mathbf{r}}_i, \quad (3.15)$$

where the filter $\mathbf{w}_{i,MMSE}^H$ is selected to minimize the mean square error between the

transmitted signal s_i and the filter output \hat{s}_i .

It can be further proven that

$$\mathbf{w}_{i,MMSE} = \left(H\Delta_i H^H + \sigma^2 I_{N_r} \right)^{-1} H \mathbf{e}_i, \quad (3.16)$$

where Δ_i is a diagonal matrix with $\Delta_i = \text{COV}(\mathbf{s}_i - \tilde{\mathbf{x}}_i)$ and \mathbf{e}_i is an all zero column vector with a "1" only at position i . Derivation of (3.16) is discussed in detail in Appendix E. Further, the distribution of \hat{s}_i is well approximated by a Gaussian distribution and can be expressed as

$$\hat{s}_i = u_i s_i + \eta_i, \quad (3.17)$$

where $u_i = \mathbf{w}_{i,MMSE}^H \mathbf{H} \mathbf{e}_i$ and η_i is Gaussian distributed with zero mean and variance z_i^2 . Then it follows that

$$f(\hat{s}_i | s_i = \tilde{s}) = \frac{1}{\pi z_i^2} \exp \left[-\frac{\|\hat{s}_i - u_i \tilde{s}\|^2}{z_i^2} \right]. \quad (3.18)$$

The main difference between this method and the optimal methods is that, the bit-wise soft information is calculated here considering only the \hat{s}_j instead of the whole received vector. This is also the reason for the sub-optimality of this method. It is important to note that the decoder of these suboptimal detector based IJDD implementations is still the optimal BP decoder.

However, most of the practical situations considered in prior work in this area and

the work in this thesis deal with a fairly small antenna array due to cost effectiveness and also due to the space constraints. The near optimal schemes, which uses IJDD based on the individually optimal maximum a posteriori probability (MAP) detector, can still be deployed with manageable complexity in small antenna array based MIMO systems. Thus we do not come across the need for these suboptimal detectors. Further, in this thesis our main focus is on FG-LDPC coded systems and the interest is in the reduction of the complexity of the decoder. Hence a small antenna array with the optimal MAP detector is considered. Therefore, the IJDD implementations with MAP based individually optimal detectors are discussed in the next section.

3.2 Individually Optimal Detector Based IJDD Algorithm

In this section, the main existing implementation of IJDD with individually optimal detector is explored. However, it is worth to note that there are many improvements and simplifications of the IJDD algorithm based on this approach, but for simplicity only the main algorithm is presented in this thesis.

This IJDD algorithm is completely based on the BP decoder operating with the tripartite message passing algorithm [24]. Before moving on to the algorithm it is worthwhile to describe the tripartite representation of the joint system.

3.2.1 Three Level Tanner Graph

In chapter 2, we discussed the two level Tanner graph representing the check nodes and the bit nodes and also the message passing between these two levels to carry-out the decoding in an iterative fashion. Three level Tanner graph is a simple extension of the two level Tanner graph with the addition of the third level to represent the received value nodes. Thus, in the tripartite Tanner graph, the structure of the top part consisting of bit nodes and check nodes clearly follows the channel code (LDPC) structure, and it is identical to the bipartite Tanner graph when the channel code representation is taken alone. However, with the MIMO channel, the third set of nodes is added to represent the received values. This third level consists of altogether KN_r nodes representing all the values received by N_r receiver antennas in K uses of the channel. The connections are present between these bottom two levels' nodes to depict the information transfer paths or the inter-relationships. Since the signal transmitted by an antenna (corresponding to a particular bit) is received by all N_r receiver antennas, any given bit node is connected to N_r corresponding received value nodes as shown in Fig. 3.2. Similarly every received value contains the information of all the bits transmitted in the same use of the channel and thus all the bit nodes corresponding to the same transmission are connected to all the received values corresponding to the same use of the channel.

However, in passing messages between the bit nodes and the received value nodes along the connections defined earlier, there will be short loops due to the structure of the MIMO channel. This poses a threat to the independence assumption described in Ap-

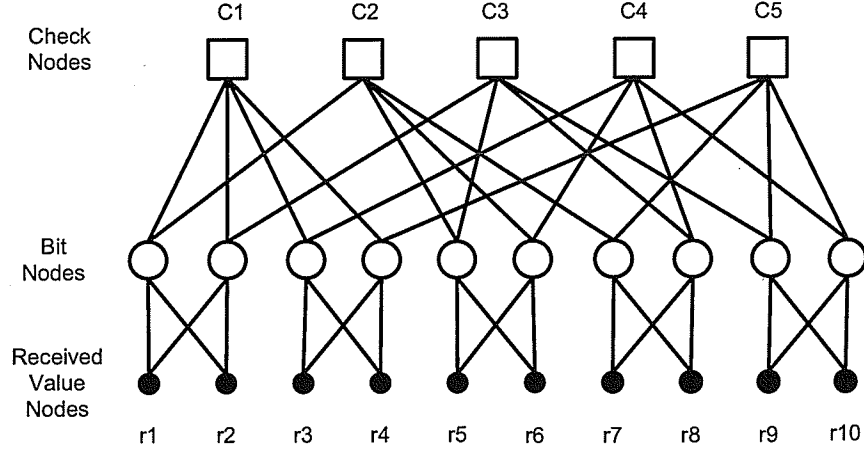


Figure 3.2: Three level example Tanner graph with 2x2 MIMO array

pendix F, which seriously affect the performance of the IJDD algorithm. In order to cope with this situation, short loops in the bottom half of the Tanner graph need to be eliminated. This can be easily achieved by the lumping of the received value nodes so that there exists only a single node at the received value node level corresponding to each use of channel as shown in Fig. 3.3 [41]. This results in a short-loop-free Tanner graph, which can provide a very much low bit error rate (BER) in detection-decoding.

3.2.2 Tripartite Message Passing Algorithm

After presenting the tripartite Tanner graph representation of the LDPC coded MIMO system, now we are in a position to describe the tripartite message passing algorithm used in the IJDD based on BP decoder.

As usual, the messages passed in the top half of the Tanner graph (i.e. the messages passed between the check nodes and the bit nodes) are identical to those in the two level

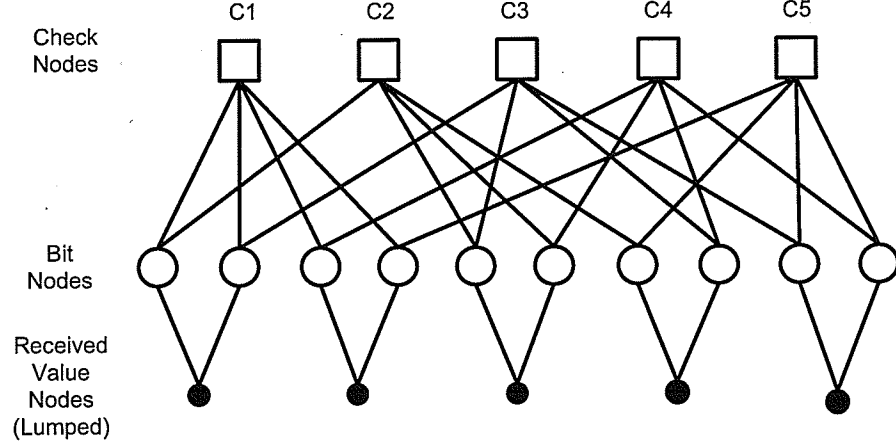


Figure 3.3: Three level Tanner graph with 2x2 MIMO array and lumped r nodes

Tanner graph except for the fact that the a priori probabilities contained in the bit node to check node message is updated in each iteration. This update is carried out through the utilization of the knowledge of the channel and hence the messages are passed from bit nodes to received value nodes. Then a set of messages will be generated and passed from received value nodes back to the bit node to update the a priori probability of the bit.

Without loss of generality, let's consider the bit node i , check node j and the received value node (r-node) k for the discussion of the passed messages. First, the message from the check node j to bit node i is the probability of satisfying j^{th} parity check equation with either one or zero at the i^{th} bit position. Using the same notation used in presenting the BP algorithm in Chapter 1

$$p_{ji}(1) = \frac{1}{2} \left[1 - \prod_{i' \in \mathcal{N}_j \setminus i} (1 - 2q_{i'j}(1)) \right] \quad (3.19)$$

$$p_{ji}(0) = 1 - p_{ji}(1).$$

The product of such messages at the bit node i provides the message from bit node i to check node j , which in turn is the probability of satisfying all the parity check equations given the bit i being either zero or one, given by

$$\begin{aligned} q_{ij}(1) &= K_{ij} \lambda_{ki} \prod_{j' \in \mathcal{M}_i \setminus j} p_{j'i}(1) \\ q_{ij}(0) &= K_{ij} \lambda_{ki} \prod_{j' \in \mathcal{M}_i \setminus j} p_{j'i}(0), \end{aligned} \quad (3.20)$$

where λ_{ki} are the a priori probabilities discussed below. At the bottom half of the tripartite Tanner graph, the update of a priori probabilities takes place using the information passed from the bit nodes to the r-nodes given by

$$\begin{aligned} \pi_{ik}(1) &= K_{ik} \prod_{j' \in \mathcal{M}_i} p_{j'i}(1) \\ \pi_{ik}(0) &= K_{ik} \prod_{j' \in \mathcal{M}_i} p_{j'i}(0). \end{aligned} \quad (3.21)$$

Then the updated a priori conditional probability message λ representing the probability of the bit i being one or zero given the received value vector, can be represented as

$$\lambda_{ki}(c_i) = \sum_{C^i} f(\mathbf{r}|C^i, c_i) \prod_{C_{i'}^i} \pi_{i'k}(C_{i'}^i). \quad (3.22)$$

Here C^i is the set of all valid codeword combinations for the other bits, when the bit position i is set to c_i . Further, in these equations K_{ij} and K_{ik} are the normalizing constants and the message from the i^{th} node is omitted in calculating the message for the i^{th} node, in order to avoid the error propagation. As usual, at the end of each iteration the resultant soft values are hard decoded and parity checked for a null syndrome vector. Finally, the key difference between the tripartite message passing in the MIMO channel scenario and the bipartite message passing in the SISO scenario can be summarized as follows. In the SISO case, each bit is connected to one r-node and therefore the update of the probabilities in a given bit node does not change the probabilities of neighboring bits. But in the case of MIMO systems, due to the fact that more than one bit is connected to a given r-node the update of one bit's probability information does affect the other bits connected to the same r-node. Thus, in each and every iteration, the a priori probabilities should also be updated.

Many improvements have been added to the tripartite message passing method to improve the performance by carrying out the IJDD in a non-binary Galois field ($GF(q)$, $q > 2$) [10]. These approaches benefit from the fact that in non-binary fields, the short loops in the structure are eliminated.

3.3 Simulation Results

Numerical simulations for,

1. Cascaded detector and decoder system

2. Iterative joint detector-decoder system

are carried out for three FG-LDPC codes of three different block lengths 63, 255, and 1023 with equal row and column weights 8, 16, and 32 respectively. Further, for this simulation a 2×2 antenna array is considered. The channel coefficients are assumed to be uncorrelated Rayleigh distributed and channel noise is assumed to be uncorrelated complex additive white Gaussian. The results are presented in Fig. 3.4 - Fig. 3.6. It can be seen that the tripartite message passing algorithm provides a low probability of error compared to the cascaded schemes. It is worth to note that the three different 63x37, 255x175 and 1023x781 FG-LDPC codes considered here have the code rates 0.58, 0.64 and 0.76, respectively. Since, with increased code rates the BER performance decreases, high code rate codes need a higher SNR value for a given BER performance, than the SNR value needed for a code with a lower code rate. Therefore, if different codes are compared, it is very important to consider the codes with similar code rates.

However the IJDD based on tripartite message passing suffers from a serious problem due to its large number of interconnections between the three levels, which causes the number of messages to be passed within one iteration to be very large. Therefore this algorithm is proven to be highly complex. Specially with the increased block length, the complexity is prohibitively high. Similarly, the systems using FG-LDPC codes which have a larger column weight and a larger row weight also introduces the same complexity issue as it is required to pass a relatively huge number of messages in that

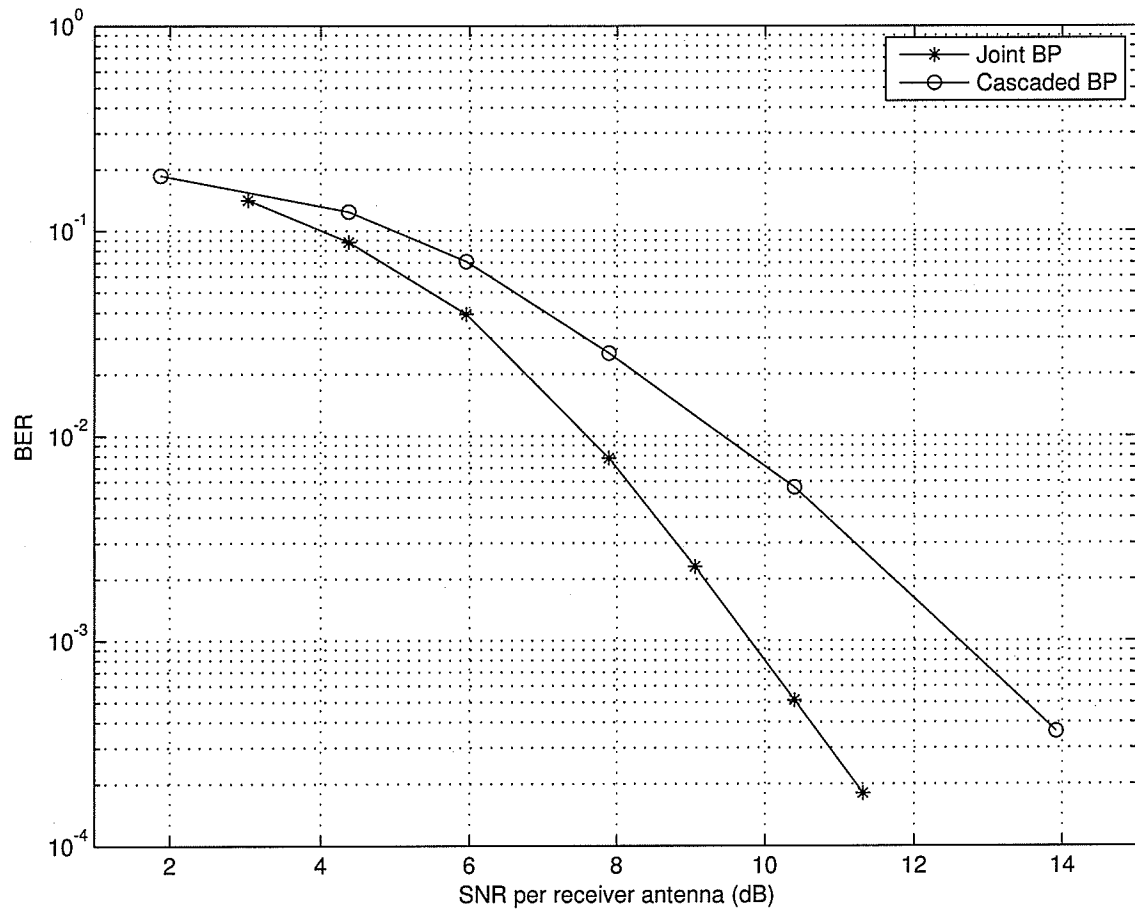


Figure 3.4: Comparison of BER performance of joint and cascaded detection-decoding schemes for 63x37 FG-LDPC code with 2x2 MIMO antenna array

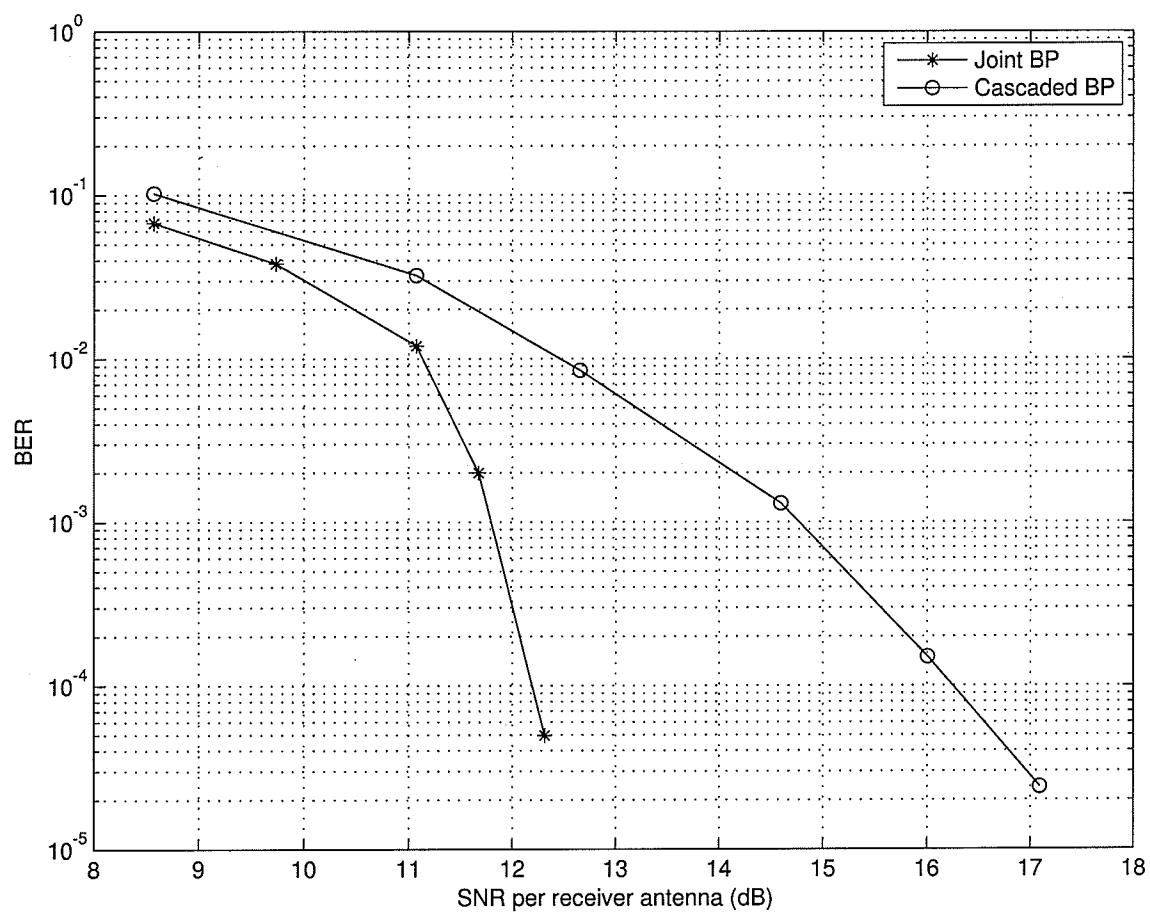


Figure 3.5: Comparison of BER performance of joint and cascaded detection-decoding schemes for 255x175 FG-LDPC code with 2x2 MIMO antenna array

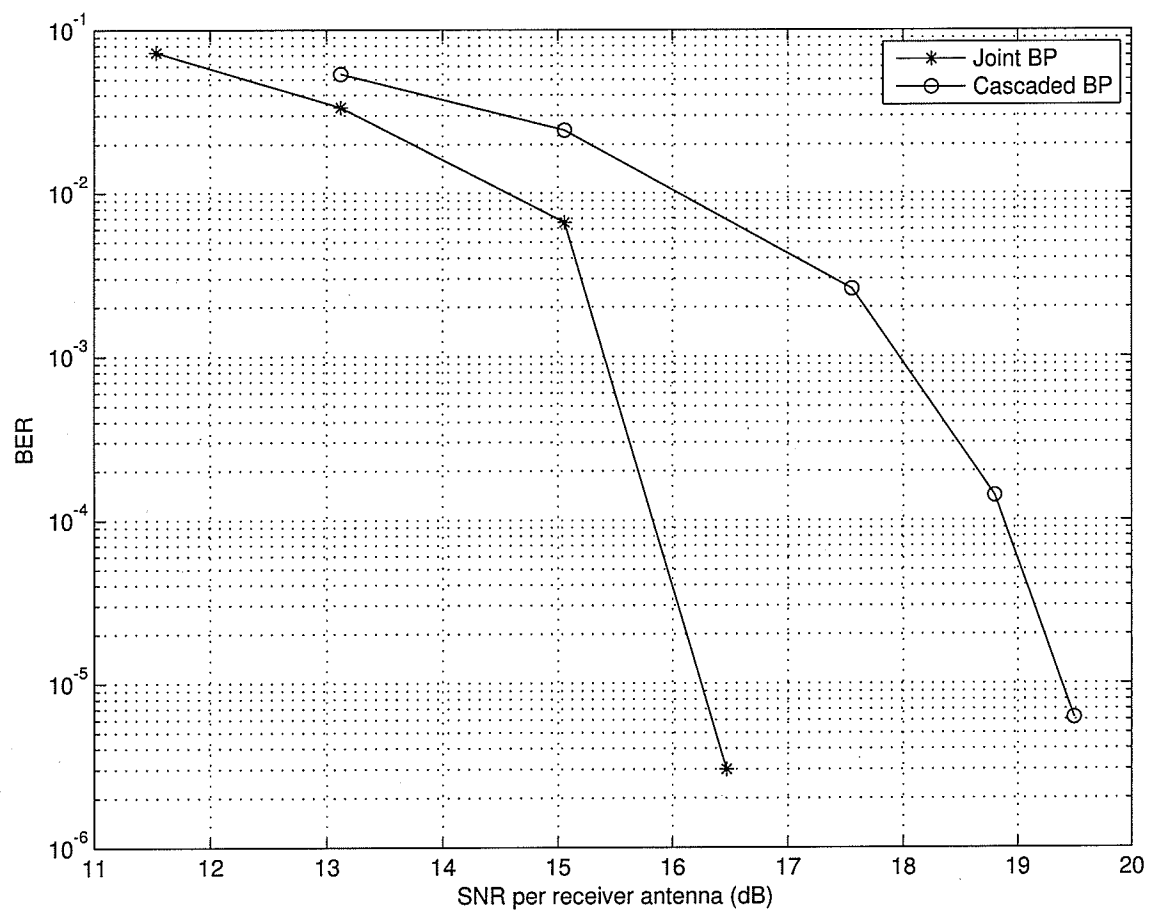


Figure 3.6: Comparison of BER performance of joint and cascaded detection-decoding schemes for 1023x781 FG-LDPC code with 2x2 MIMO antenna array

case too. This is a result of their denser parity check matrix which results in a Tanner graph with higher number of interconnections. In this thesis, we consider the iterative joint detection and decoding of FG-LDPC coded MIMO systems. It is obvious that the existing algorithm can not be practically used in this case due to its unmanageable complexity. Therefore, a simpler algorithm replacing the BP based tripartite message passing algorithm is proposed to achieve a tradeoff between the complexity and the performance. The proposed algorithm not only provides a manageable simplicity in the case of FG-LDPC codes, but can also be utilized in general LDPC coded system to further simplify the decoding process with only a small degradation in performance.

Chapter 4

Low Complexity IJDD of FG-LDPC Coded MIMO Systems

Due to the special properties of FG-LDPC codes discussed in Chapter 2, they have recently captured a high research interest. While providing the ease of encoding due to their special cyclic and quasi-cyclic structures, FG-LDPC codes perform better than regular LDPC codes due to their dense parity check matrix and the extended short loop free structure. In practical MIMO systems, FG-LDPC codes can be utilized as the outer or the channel code in order to harness this performance advantage and to simplify the encoding. However this performance gain comes at a cost; it will increase the overall complexity due to the increased number of calculations, when deployed along with BP decoder based IJDD as discussed in Chapter 3. As a remedy for this situation, a simplified IJDD algorithm which retains the benefits of FG-LDPC codes, while reducing the

complexity of detector-decoder system is proposed in this chapter. This novel algorithm is based on the simple multiple bit flipping decoder and thus its overall complexity is greatly reduced from that of the BP based IJDD systems. The proposed IJDD system has a similar functional structure as BP based IJDD algorithm, but with the individually optimal detector and a MBF decoder. Further, the output of the decoder is fed back to the detector input to be used in the next iteration. Meanwhile, at each and every iteration the resultant decoder output is parity checked to identify whether the estimated decoder output is a valid codeword or it needs to be further refined. However, unlike in tripartite message passing algorithm discussed in Chapter 3, the output of the MBF decoder deployed here is a binary (hard bit) vector while the required feedback to the detector is a soft value. Therefore, there should be some mechanism to generate the soft values from the hard bit vector output of the decoder. In this chapter, together with the proposed IJDD algorithm, the two novel components, the log likelihood domain detector and the feedback mechanism are developed.

4.1 The Log Likelihood Domain Detector

The detector in this algorithm is capable of accepting the received values from the channel and the fed back information from the decoder output to provide a soft output. In order to further simplify the calculation by reducing the number of operations, the algorithm is developed in log likelihood domain.

First, the LLR value for the j -th bit computed by the soft-channel detector can be defined as

$$\begin{aligned} \text{LLR}_j(s_j|\mathbf{r}) &= \log \frac{f(s_j = +1|\mathbf{r})}{f(s_j = -1|\mathbf{r})} = \log \left(\frac{\sum_{\mathbf{s}: s_j = +1} f(\mathbf{s}, \mathbf{r})}{\sum_{\mathbf{s}: s_j = -1} f(\mathbf{s}, \mathbf{r})} \right) \\ &= \log \left(\frac{\sum_{\mathbf{s}: s_j = +1} f(\mathbf{r}|\mathbf{s})P(\mathbf{s})}{\sum_{\mathbf{s}: s_j = -1} f(\mathbf{r}|\mathbf{s})P(\mathbf{s})} \right), \end{aligned} \quad (4.1)$$

where $j = 1, \dots, n$, and each sum involves all the possible codewords with $s_j = \pm 1$. Clearly, this involves a prohibitively complex marginalization process, which is computationally unmanageable for long LDPC codes. Further, the complexity of this marginalization increases exponentially with increments in the block length. Therefore, an approximation is needed to cope with this situation. In the proposed algorithm, the approximation comes from the fact that in IJDD, the detector operates on a received sub-vector corresponding to a single use of the channel at a time. Note that s_j (i.e., the j -th element of \mathbf{s}) is the i -th element of $\tilde{\mathbf{s}}^{(l)}$, where

$$i = ((j - 1) \bmod N_t) + 1,$$

and

$$l = (j \div N_t) + 1,$$

i.e., $\tilde{\mathbf{s}}_i^{(l)} = s_j$.

Now to simplify (4.1), we assume that $\text{LLR}_j(s_j|\mathbf{r}) \simeq \text{LLR}_j(s_j|\tilde{\mathbf{r}}^{(l)})$, and hence

$$\text{LLR}_j(s_j|\mathbf{r}) \simeq \log \left(\frac{\sum_{\tilde{\mathbf{s}}^{(l)}: \tilde{s}_i^{(l)}=+1} f(\tilde{\mathbf{r}}^{(l)}|\tilde{\mathbf{s}}^{(l)}) P(\tilde{\mathbf{s}}^{(l)})}{\sum_{\tilde{\mathbf{s}}^{(l)}: \tilde{s}_i^{(l)}=-1} f(\tilde{\mathbf{r}}^{(l)}|\tilde{\mathbf{s}}^{(l)}) P(\tilde{\mathbf{s}}^{(l)})} \right), \quad (4.2)$$

where the sums now only involves 2^{N_t-1} terms. With a small number of antennas, this marginalization is computationally manageable. It is worthwhile to note that with the above simplification, the correlation of the bits in the rest of the codewords is neglected within a single detection operation, causing a performance degradation. However as in any other IJDD algorithm, a partial compensation for this loss is obtained by feedback.

As usually done with belief-propagation decoding [17], assume that \tilde{s}_i has independent elements (this independent assumption is further discussed in Appendix F). It then follows that

$$\text{LLR}_j(s_j|\mathbf{r}) \simeq \log \frac{P(s_j = +1)}{P(s_j = -1)} + L_e(s_j|\mathbf{r}), \quad (4.3)$$

where,

$$L_e(s_j|\mathbf{r}) = \log \left(\frac{\sum_{\tilde{\mathbf{s}}^{(l)}: \tilde{s}_i^{(l)}=+1} f(\tilde{\mathbf{r}}^{(l)}|\tilde{\mathbf{s}}^{(l)}) \prod_{t:t \neq i} P(\tilde{s}_t^{(l)})}{\sum_{\tilde{\mathbf{s}}^{(l)}: \tilde{s}_i^{(l)}=-1} f(\tilde{\mathbf{r}}^{(l)}|\tilde{\mathbf{s}}^{(l)}) \prod_{t:t \neq i} P(\tilde{s}_t^{(l)})} \right). \quad (4.4)$$

Now, in order to develop an iterative detector-decoder algorithm, (4.3) can be written in the iterative form

$$L^{k+1}(s_j|\mathbf{r}) = L^k(s_j) + L_e^k(s_j|\mathbf{r}), \quad (4.5)$$

where $L^{k+1}(s_j|\mathbf{r}) = \text{LLR}_j(s_j|\mathbf{r})$ is the LLR value passed to the decoder by the soft-

detector in the k -th iteration, $L^k(s_j) = \log \left(\frac{P(\tilde{s}_j=+1)}{P(\tilde{s}_j=-1)} \right)$ is the *intrinsic information* of j -th bit in \mathbf{c} , and $L_e^k(s_j|\mathbf{r})$ plays the role of *extrinsic information*, determined by the code structure and MIMO channel. As in any other iterative algorithm, the intrinsic information is excluded to avoid the error propagation.

As described in Chapter 2, a $N_t \times N_r$ MIMO channel with uncorrelated Rayleigh fading and *iid* AWGN is considered and the channel realization is assumed to be completely known to the decoder. Therefore, for the l^{th} use of the channel we have

$$f(\tilde{\mathbf{r}}^{(l)}|\tilde{\mathbf{s}}^{(l)}) = \frac{1}{(\sqrt{2\pi}\sigma)^{2N_r}} \exp \left(-\frac{\|\tilde{\mathbf{r}}^{(l)} - \mathbf{H}^{(l)}\tilde{\mathbf{s}}^{(l)}\|^2}{2\sigma^2} \right).$$

Using (4.4) and (4.5), an expression for extrinsic information can be obtained. However, this equation contains probabilities and further simplification is required before its utilization in the LLR domain IJDD algorithm. It can be shown that the LLR and binary bit probabilities are related as follows

$$\begin{aligned} P(s = +1) &= \frac{e^{L(s)}}{1 + e^{L(s)}} = \frac{e^{\frac{L(s)}{2}}}{e^{\frac{-L(s)}{2}} + e^{\frac{L(s)}{2}}}, \\ P(s = -1) &= \frac{1}{1 + e^{L(s)}} = \frac{e^{\frac{-L(s)}{2}}}{e^{\frac{-L(s)}{2}} + e^{\frac{L(s)}{2}}}, \end{aligned}$$

Then (4.4) can be represented as

$$L_e^k(s_j|\mathbf{r}) = \log \left(\frac{\sum_{\tilde{\mathbf{s}}^{(l)}: \tilde{s}_i^{(l)}=+1} \exp \left(-\frac{\|\tilde{\mathbf{r}}^{(l)} - \mathbf{H}^{(l)}\tilde{\mathbf{s}}^{(l)}\|^2}{2\sigma^2} + \sum_{t, t \neq i} \tilde{s}_t^{(l)} \frac{L_f^k(\tilde{s}_t^{(l)})}{2} \right)}{\sum_{\tilde{\mathbf{s}}^{(l)}: \tilde{s}_i^{(l)}=-1} \exp \left(-\frac{\|\tilde{\mathbf{r}}^{(l)} - \mathbf{H}^{(l)}\tilde{\mathbf{s}}^{(l)}\|^2}{2\sigma^2} + \sum_{t, t \neq i} \tilde{s}_t^{(l)} \frac{L_f^k(\tilde{s}_t^{(l)})}{2} \right)} \right). \quad (4.6)$$

where $L_f^k(\tilde{s}_t^{(l)})$, the feedback information from the output of the decoder, is defined in the next section.

4.2 The Feedback

The feedback in (4.6), $L_f^k(\tilde{s}_t^{(l)})$, plays a major role in the proposed algorithm. Further, as discussed earlier, hard bits-to-soft information conversion is needed for feedback. As our main goal is to retain the simplicity of BF-decoding, we propose two simple heuristic methods of feedback conversion whose complexity is only linear in LDPC code block length.

4.2.1 Inverted LLR Soft Information (I-LSI)

In BF, a bit is inverted if its LLR value is deemed close to zero (hence unreliable) and also if it participates in parity check equations where the other bits are more reliable. Hence, if the decoder output in a given iteration is assumed correct, then the new information available at the decoder output can be fed back to the detector by inverting

the sign of the LLR values of the flipped bits. Based on this idea, feedback LLR-values are generated as

$$L_f^{k+1}(s_j) = \begin{cases} -L^k(s_j|\mathbf{r}) & \text{if } s_j \text{ is flipped} \\ L^k(s_j|\mathbf{r}) & \text{otherwise.} \end{cases} \quad (4.7)$$

Through this hard-to-soft conversion, the information at the output of the decoder is clearly conveyed to the soft feedback to the detector. Thus with this conveyed knowledge of the correlation of bits, the resultant algorithm is expected to perform better than the cascaded detector and decoder.

4.2.2 Modified Inverted LLR Soft Information (MI-LSI)

However, a weakness of the above approach is that, while it correctly feeds the new information at the decoder output back to the detector in the form of a sign change, one still assumes that the magnitudes of the LLR values of the flipped bits remain unchanged. Note that, as the BF algorithm is a search algorithm, it typically flips some bits erroneously, which will eventually be corrected at a later iteration. Although, this usually works for a hard bit vector, the incorrect sign changes in the soft information leads to error accumulation in the feedback loop if the magnitudes of the LLRs are retained while the signs are inverted. Therefore, we need to ensure that when a bit is erroneously flipped, this decision is not “hard-encoded” into the LLR magnitude fed back to the detector. In order to accomplish this, the rule in (4.7) can be improved as

follows.

$$L_f^{k+1}(s_j) = -\lambda_j L^k(s_j|\mathbf{r}) \text{ if } s_j \text{ is flipped} \quad (4.8)$$

where $\lambda_j \geq 0$ is a value selected to depict the reliability of the bit inversion decision as below.

For the computation of λ_j , three possibilities are considered.

1. *M-ILSI-1*

λ_j corresponding to multiple bits flipped within a single iteration are chosen from the interval $[0, 1]$, uniformly spaced such that the bits flipped with high certainty are given a higher λ value while the bits flipped with low certainty are given low λ values. This step makes sure that the high reliable flipping are provided with only a sign change while the low reliable flipping are given a higher chance to be reconsidered by decreasing the magnitude. Decision of the reliability is taken by the metric value ϕ_j^k , calculated in the MBF iteration step.

2. *M-ILSI-2*

However in the above update rule, equi-spaced selection of λ_j does not take into account the relative values of the reliability metric values. As an example, when one metric value is far less than the others, it is a clear indication that the flipped result is highly reliable. But the above assignment of equi-spaced λ fails to capture such relatively high reliabilities.

On the other hand if a flipped bit value is proven to be highly reliable by its

low metric value, it is reasonable to increase its reliability in the fed back LLR magnitude rather than retaining the same magnitude. These effects can be easily achieved by the use of following rule for the λ_j selection.

$$\lambda_j = \frac{\tilde{\phi}^k - \phi_j^k}{\frac{1}{\mathcal{P}} \sum_{j=1}^{\mathcal{P}} (\tilde{\phi}^k - \phi_j^k)},$$

with $\phi_j^k, j = 1, \dots, \mathcal{P}$ being the reliability values of those bits flipped by the BF-decoder in the iteration k and $\tilde{\phi}^k = \max_j \{\phi_j^k\}$. The difference metric value in the numerator effectively maps the $\phi_j^k \in (-\infty, \infty)$ to a set in $[0, \infty)$, and the division by the average effectively scales this set of values. Therefore the low metric values (i.e. the values corresponding to the high reliable flipped bits) are now mapped to $\lambda_j > 1$ and high metric values (corresponding to the low reliable flipped bits) are now mapped to $\lambda_j < 1$. This mapping ensures that high reliable flippings are given a boost by increasing the magnitude of the LLR while reducing the magnitude for low reliable flippings so that they have a high chance to be rechecked. Further the relative reliabilities are taken care of.

It is expected the first λ_j selection to yield a noticeable improvement from the sign inversion method and the second selection method to provide a further improvement.

3. *M-ILSI-3*

Stochastic perturbation is widely used in optimization [42]. Whenever a function,

whose roots to be determined are affected by random noise, a random iterative search for roots is proven to be a better approach over a deterministic iterative search. In every iteration, the random search method randomly selects a search direction and search interval, opposed to deterministic searches such as the Newton-Rapson method. Localized random search algorithm in [42] is such an improved random search method and is presented in Appendix G.

In the context of MBF based IJDD algorithm, the decoding is a localized search algorithm which finds a $\hat{\mathbf{c}}$ to satisfy $\mathbf{Z} = \hat{\mathbf{c}}\mathcal{H}^T = 0$, which is a root finding process. Further, flippings can be viewed as addition of another bit vector to the current candidate, $\hat{\mathbf{c}}$. Thus, if the feedback is selected randomly, then a random vector can be added to the current candidate to generate the new candidate exactly the same way as in the modified localized random search algorithm presented in Appendix G. In other words, the localized random search algorithm in [42] can be easily modified and adopted to fit the proposed IJDD algorithm to find the local root of $\mathbf{Z} = 0$, by a controlled random selection of feedback values.

This can be implemented with selecting the λ_j from a random distribution. The choice of the probability distribution is important and we consider two possibilities,

- (a) λ_j uniformly distributed in $[0, 1]$ so that $|L_f^{k+1}(s_j)|$ is randomly distributed between $[0, |L^k(s_j|\mathbf{r})|]$,
- (b) λ_j exponentially distributed such that $P(0 < \lambda_j < 1) \simeq 1$.

The two extremes cases of this approach correspond to fixed-detection ($\lambda_j = 0$) and the update rule (4.7) [$\lambda_j = 1$].

The use of magnitudes which are exponentially distributed ensures that the flipped LLRs are more likely to be assigned smaller reliability values. This can be expected to yield improved results compared to uniformly distributed values, as it better reflects our increased uncertainty about the flipped bits.

4.3 The Proposed IJDD Algorithm

Now the overall IJDD algorithm based on MBF decoder can be presented as follows.

1. Initially $L_f^k(\tilde{s}_t^{(l)})$ are assumed to be zero (equal a priori probabilities).
2. The $L_j^k(s_j|\mathbf{r})$ values for $j = 1, \dots, n$ are calculated using (4.5) and (4.6) in the detector.
3. The resultant $L_j(s_j|\mathbf{r})$ are passed on to the MBF decoder as the reliabilities of the channel outputs and the decoder outputs a set of hard decoded outputs (bits) $\hat{\mathbf{c}}^k$.
4. Decoder output, the estimated bit vector $\hat{\mathbf{c}}^k$ is used to calculate the syndrome vector $\mathbf{Z}^k = (\hat{\mathbf{c}})^k \mathcal{H}^T$ which if it is a null vector, the estimate is accepted as the transmitted codeword and the algorithm is stopped. If \mathbf{Z}^k is not a null vector, then it proceeds to the next iteration.
5. In the case of non zero \mathbf{Z}^k , the $\hat{\mathbf{s}}^k$ values are converted to a set of soft LLR values,

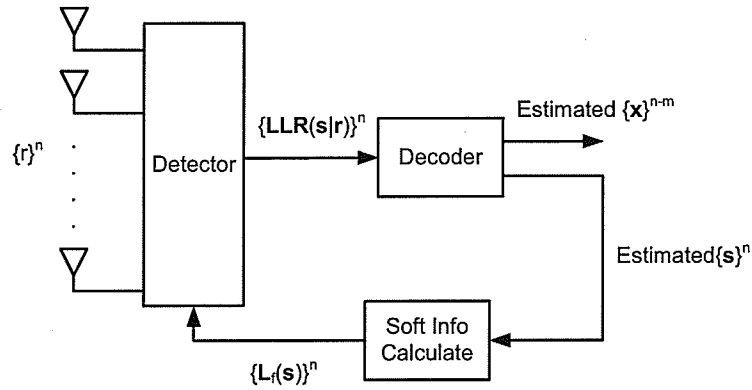


Figure 4.1: The receiver operating with MBF based IJDD

$L_f^{k+1}(\tilde{s}_t^{(l)})$, which reflects the bit value information in \hat{s}^k and they are fed back as inputs to the detector calculation in step 2.

4.4 Computational Complexity

The main goal of the proposed algorithm is to simplify the overall IJDD with the simplified decoder so that it is computationally manageable in a FG-LDPC environment. Therefore, it is worthwhile to analyse the computational complexity of the proposed detection-decoding algorithm and compare it to the complexity of two other algorithms with BP decoding listed below.

1. cascaded BP receiver, where the detection and decoding are performed in a disjoint fashion with a BP based decoder.
2. IJDD receiver with BP decoder.

In this analysis we assume the complexity of additions, inversions and comparisons are almost the same, which will be generally referred to as additions. Also the complexity of multiplications and divisions are the same, which will be referred to as multiplications. With the row and column weights of \mathcal{H} being w_r and w_c respectively, first the detector can be analyzed as follows.

In (4.6) there are $[(2N_t + 4N_r + 4N_t N_r)2^{N_t-1} + 4] \times n$ total number of calculations at the detector within a single iteration. However in the comparison with the BP based algorithms, it is sufficient to compare only the decoder and feedback, since the same log likelihood domain detector can be used in both.

Therefore we focus on the MBF decoder discussed in Chapter 2 and feedback, in this comparison. Let the number of bits selected to be flipped in a given iteration of the MBF decoder be \mathcal{P} . Within this iteration there will be $\sum_{i=n-\mathcal{P}}^{n-1} i = \mathcal{P}n - \frac{\mathcal{P}}{2}(\mathcal{P} + 1)$ comparisons to select the \mathcal{P} least reliable positions. Then we need to update a maximum of w_c syndrome bits per selected position, in which the selected position participate. If bit by bit updating is selected, this will require $w_c \times \mathcal{P}$ additions. At the next step the reliability metric parameter ϕ_n should be updated w_r times for each of the above updated $w_c \times \mathcal{P}$ syndrome bits. Therefore, all together there will be $\mathcal{P}n - \frac{\mathcal{P}}{2}(\mathcal{P} + 1) + \mathcal{P}w_c w_r$ additions in the MBF decoder.

For the I-LSI feedback we need the sign inversion for \mathcal{P} positions, hence \mathcal{P} additions and for M-ILSI-1 or M-ILSI-2 feedback we require $2\mathcal{P} - 3$ additions and $2\mathcal{P}$ multiplications. Further for M-ILSI-3 feedback we require \mathcal{P} multiplications. These clearly show a linear

behavior with n . Further, with \mathcal{P} value decreasing and tending to reach one after some number of iterations, average number of calculations per iteration is very much lesser. On the other hand, in BP algorithm there are $n(3w_c + 1)$ additions and $12nw_c - 5n - 6m$ multiplications per iteration [35]. Moreover, there is no feedback in the disjoint BP based algorithm and no feedback conversion in the BP based IJDD algorithm. Thus, it is obvious that the number of calculations in the BP based algorithm in general are very much higher. Further it's very important to note that multiplications are more expensive in implementing than the additions. In the BP based algorithms, the number of multiplications are huge compared to the proposed algorithm. Therefore the proposed algorithm is computationally very efficient.

4.5 Simulation Results

In order to investigate the performance and the complexity of the novel algorithm, it is simulated together with the joint tripartite message passing algorithm and the disjoint BP algorithm for the MIMO-LDPC system introduced in Section 1.3. Simulation results show that the average number of flippings for 255x175 FG-LDPC code at SNR=18 dB (Mid value of the range) is observed to be 6 approximately. Then the average number of calculations needed in the decoder and the feedback within an iteration for the 255x175 FG-LDPC coded system can be summarized as in Table. 4.1.

Similarly, the average number of flippings for the 1023x781 code at SNR=21 dB

Table 4.1: Comparison of the average number of calculations per iteration of 255×175 code at $SNR = 18$ dB

Algorithm	Additions	Multiplications
Proposed IJDD with I-LSI feedback	3051	0
Proposed IJDD with MI-LSI-1 or -2 feedback	3054	12
Proposed IJDD with MI-LSI-3 feedback	3045	6
Tripartite message passing IJDD or Cascaded BP	12495	46155

(Mid value of the range) is observed to be 11, thus the average number of calculations needed in the decoder and the feedback within an iteration for this FG-LDPC coded system is summarized in Table. 4.2.

Table 4.2: Comparison of the average number of calculations per iteration of 1023×781 code at $SNR = 21$ dB

Algorithm	Additions	Multiplications
Proposed IJDD with I-LSI feedback	22462	0
Proposed IJDD with M-ILSI-1 or -2 feedback	22470	22
Proposed IJDD with M-ILSI-3 feedback	22451	11
Tripartite message passing IJDD or Cascaded BP	99231	381579

Secondly, the histograms for the occurrence of the number of iterations for the same two codes are observed for $SNR=18$ dB and $SNR=21$ dB respectively and the results are shown in Fig. 4.2 and Fig. 4.3.

It is observed that the average number of iterations are within the same order of magnitude. Hence it is clearly verified by the results that the overall number of operations in the proposed algorithm are very much less than the BP based algorithms.

However, convergence is a little slower in the proposed algorithm than BP based al-

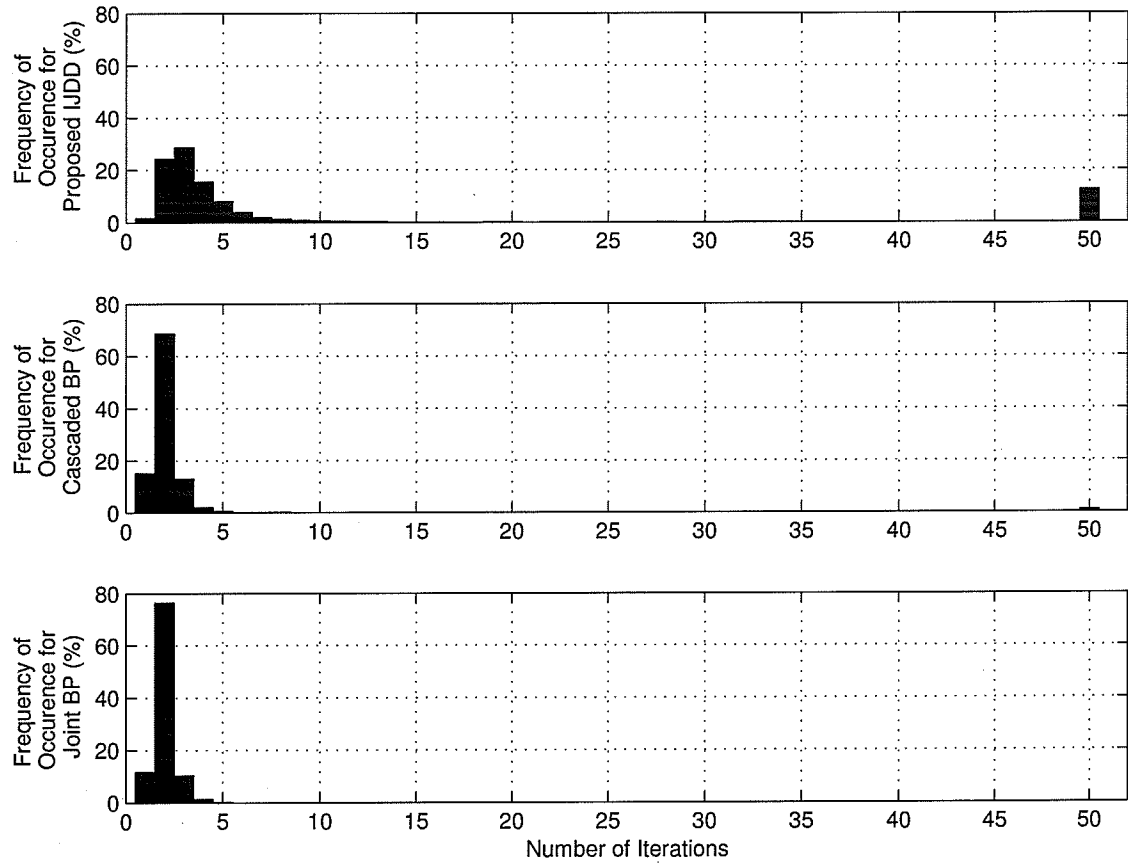


Figure 4.2: Frequency of occurrence of executed iterations for 255x175 FG-LDPC code (SNR=18 dB)

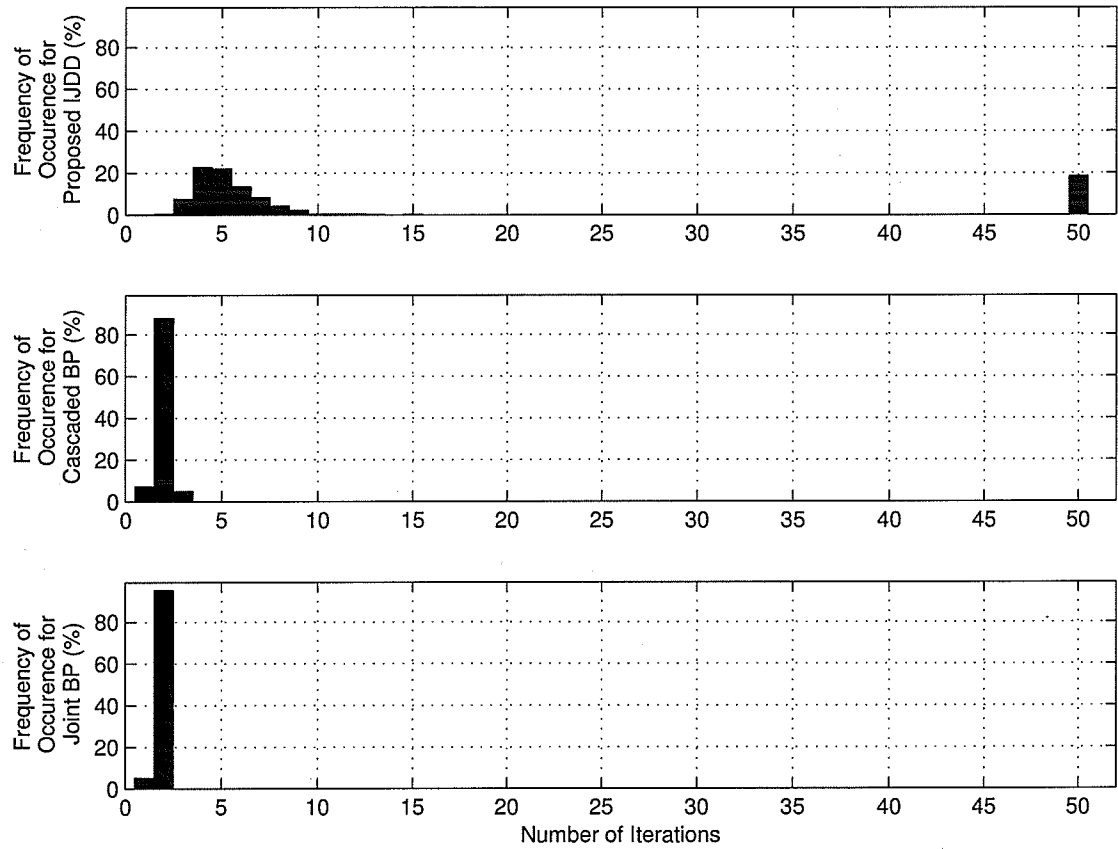


Figure 4.3: Frequency of occurrence of executed iterations for 1023x781 FG-LDPC code (SNR=21 dB)

gorithms and also there is a higher probability for a non-convergence, but still nearly 80-90% of the time it is converging at the selected mid SNRs. With the dramatic reduction in complexity, this minor adverse effect of non-convergence can be neglected and the new algorithm can be well accepted. Further, this non-convergence can be overcome without much added complexity by the use of a loop detection mechanism in the MBF decoder.

Next we focus our attention on the BER performance of the novel algorithm in the above simulation scenario. A comparison with ,

1. disjoint algorithm with MBF decoding (cascaded MBF)
2. disjoint algorithm with BP decoding (cascaded BP)
3. tripartite message passing algorithm (joint BP),

is shown in Fig. 4.4, Fig. 4.5 and Fig. 4.6 and it clearly depicts the superior performance of the proposed algorithm over the cascaded MBF. Although it does not perform better than BP based algorithms, the proposed algorithm's performance lies within few decibels from the BP based algorithms.

Finally in order to investigate the validity of the independence assumption we have made in deriving (4.6), a system in which the bits from two consecutive LDPC codewords are interleaved to decrease correlation among parity bits in a codeword is considered. That is, bits from two different codewords are transmitted over the two antennas, at a time. The BER performance of interleaved systems are compared with non-interleaved

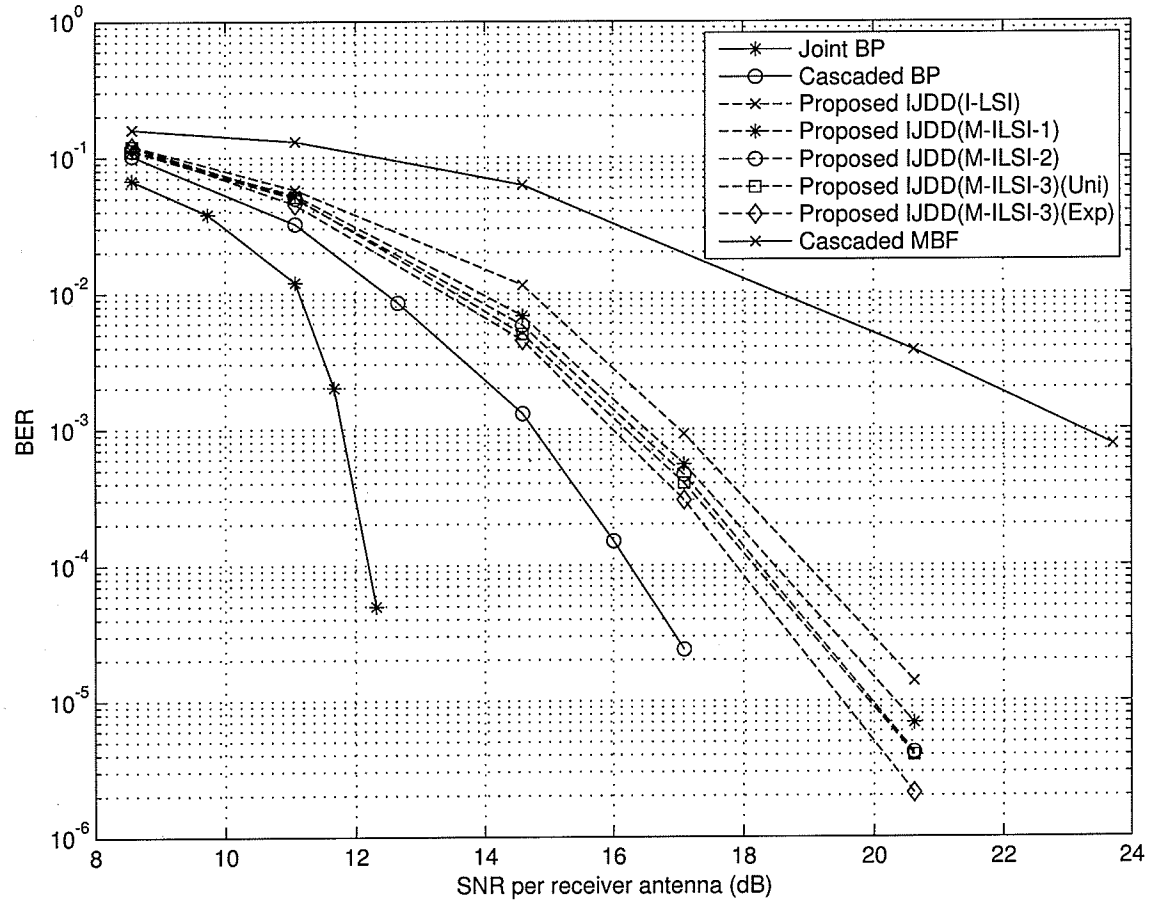


Figure 4.4: Comparison of BER performance of different detection-decoding schemes for 255x175 FG-LDPC code with 2x2 MIMO antenna array

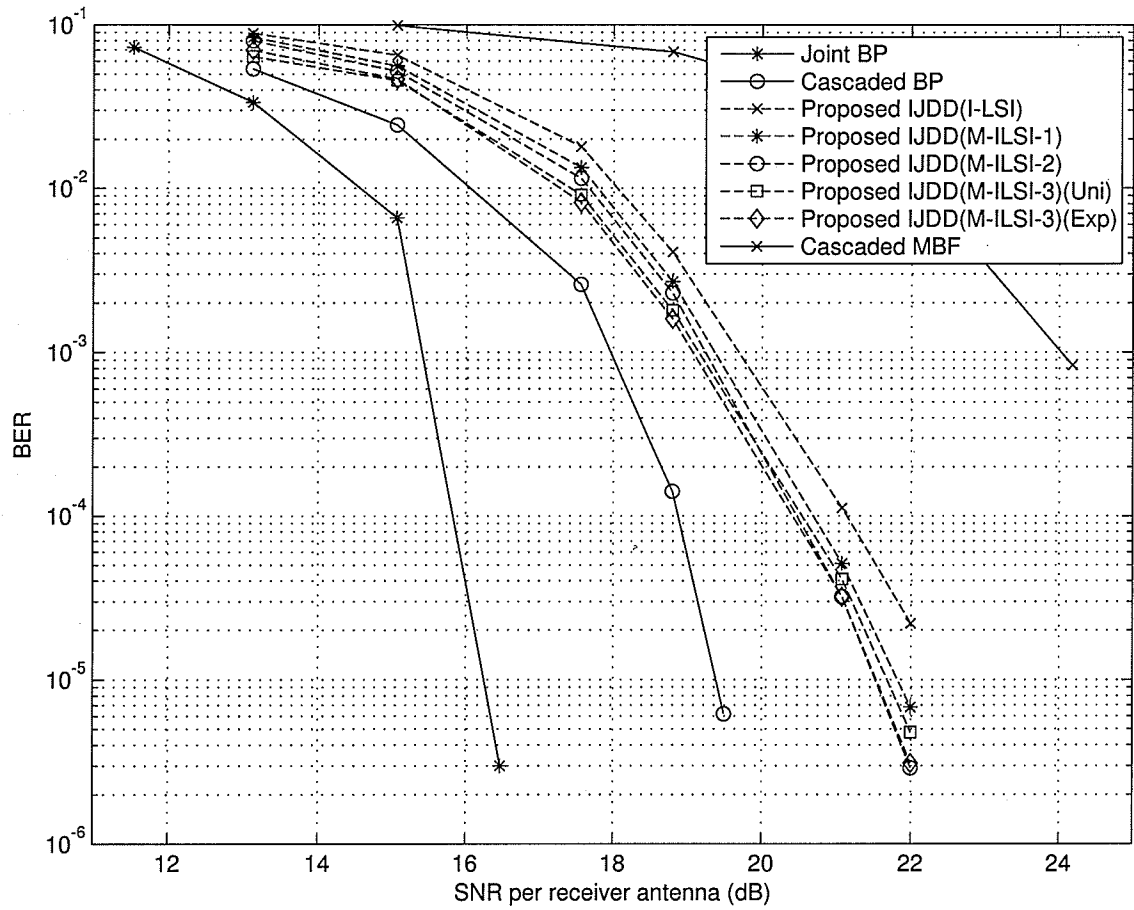


Figure 4.5: Comparison of BER performance of different detection-decoding schemes for 1023x781 FG-LDPC code with 2x2 MIMO antenna array

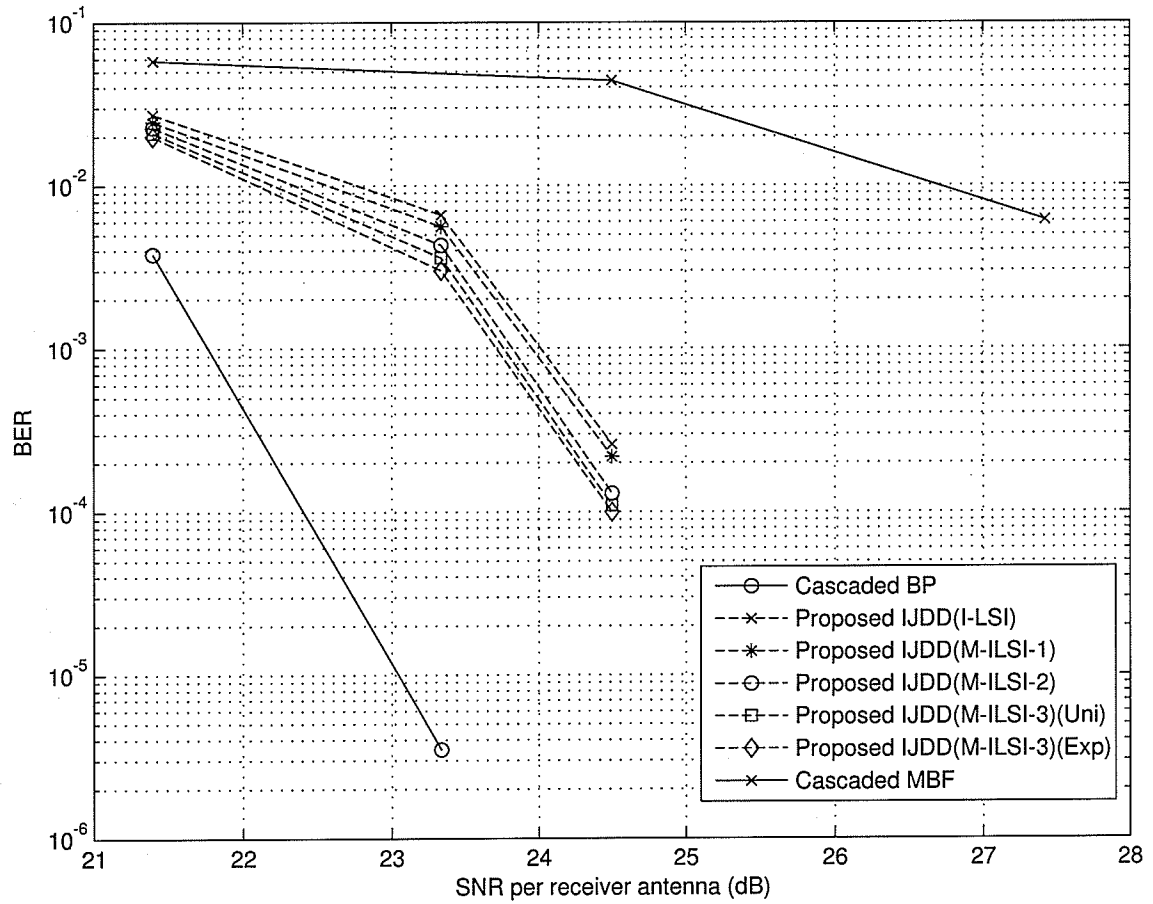


Figure 4.6: Comparison of BER performance of different detection-decoding schemes for 4095x3367 FG-LDPC code with 2x2 MIMO antenna array

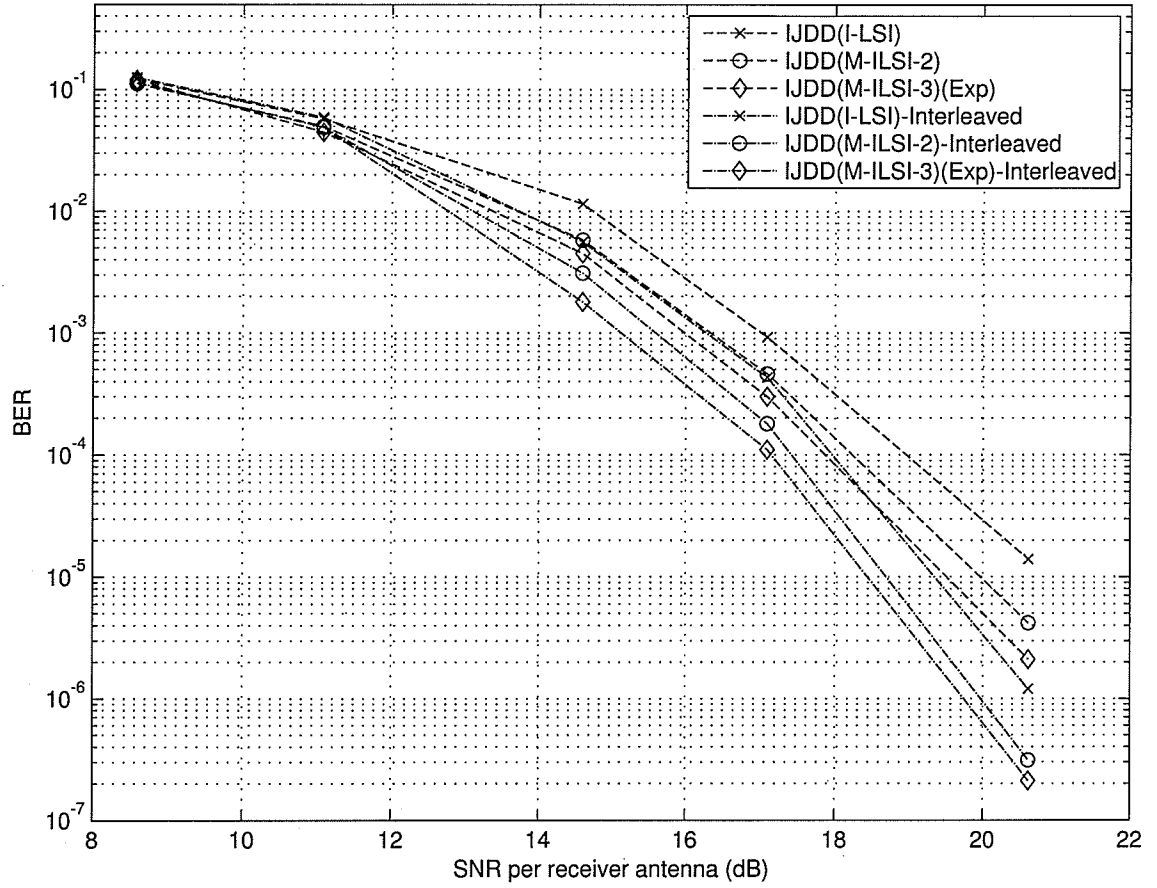


Figure 4.7: Comparison of proposed decoder, with and without interleaver for 255x175 code

systems in Fig. 4.7 and Fig. 4.8. This simulation results show that the interleaving provides only a minor BER performance improvement compared to the non-interleaved system. Therefore, there is only a little improvement gained by considering two independent bits instead of two correlated bits in an use of the channel, which justifies that the correlation is weak.

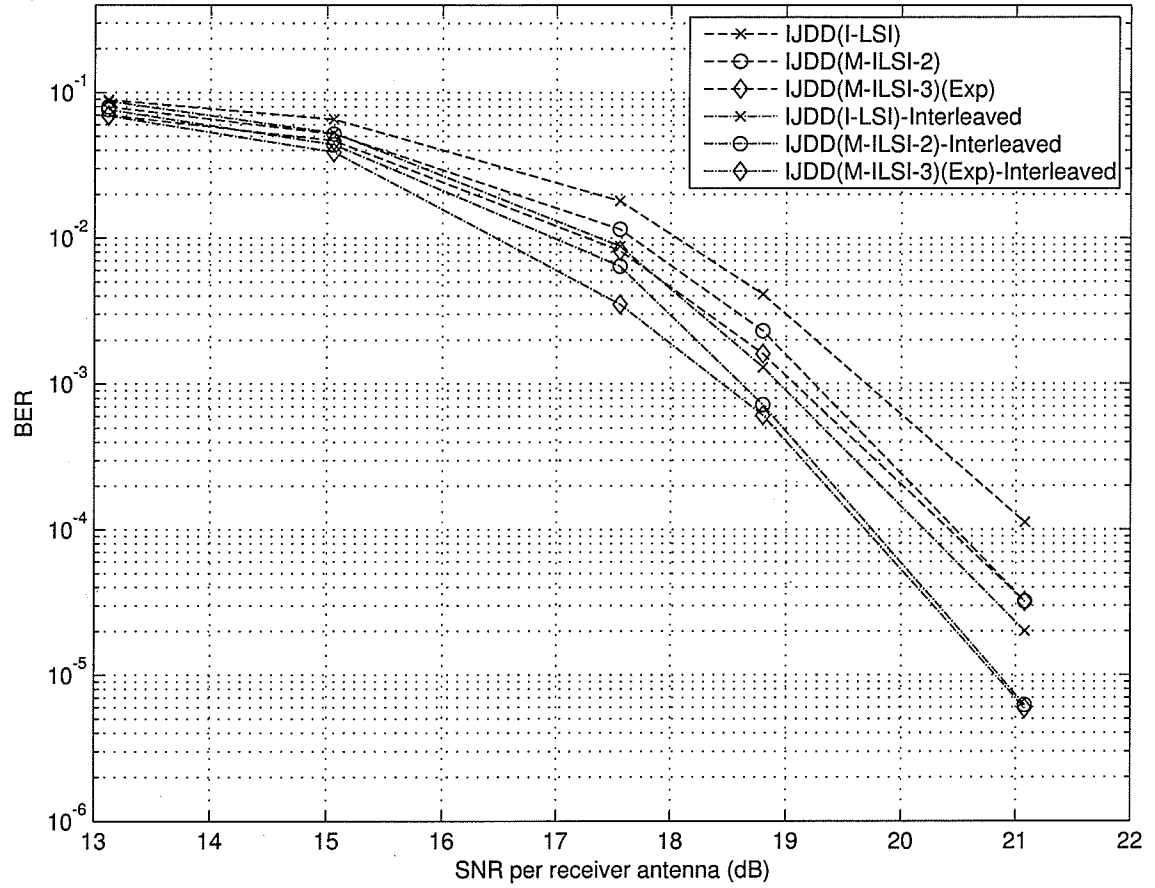


Figure 4.8: Comparison of proposed decoder, with and without interleaver for 1023x781 code

Chapter 5

Conclusions and Suggestions for Future Work

5.1 Summary and Conclusion

In today's wireless communication systems, LDPC coded MIMO channels are deployed to harness the temporal diversity gain of LDPC codes and the space diversity and spatial multiplexing gains of MIMO channels. FG-LDPC codes provide additional means of reliability with their special structure and also they are efficient in encoding. Hence FG-LDPC coded MIMO systems can provide an excellent error-rate performance. Incorporating FG-LDPC codes in a MIMO system ideally requires joint detection and decoding or IJDD for a near optimal performance. However both are unattainable with the existing BP based algorithms due to the complexity issues. Therefore in this thesis,

a simplified algorithm has been proposed for IJDD of FG-LDPC coded MIMO systems.

The contributions of this thesis are two fold.

- First an iterative joint detection and decoding algorithm is proposed based on the MBF decoder. In this algorithm the output of the decoder is fed-back to the detector to be used in the next iteration's calculation. Hence the detector makes use of the correlation of bits in a codeword, which is explored by the decoder. Further this IJDD scheme performs acceptably well and has a complexity comparable to the MBF decoder. Therefore the introduction of the MBF decoder has made this algorithm possible to be deployed in FG-LDPC coded systems.
- Secondly, the introduction of MBF decoder is not straightforward. In fact a special mechanism is needed to convert the hard bit vector output of the decoder to a soft information to be fed back. Four such conversion methods are proposed.
 1. Taking in to account that the sign of the soft information LLR represents the bit decision, working in the backward direction the bit decision at the detector output is represented as a sign change in the original soft LLR information. This feedback does not change the reliability of the modified bits. Thus, whenever a bit is flipped erroneously and corrected in a later iteration which is very usual in LDPC, the erroneous sign change in the soft information cannot be removed easily.
 2. The second method proposes a feedback where the soft information corre-

sponding to the changed bits are also assigned new magnitudes together with the sign changes. These magnitudes are generated such that the less reliable bits' current magnitudes are reduced, increasing their chances to be corrected, if in error. On the other hand more reliable bits are kept at nearly the same previous magnitude.

3. In the third proposal, together with decreasing the LLR magnitude corresponding to the less reliable bits, a magnitude increment is provided for more reliable bits confirming the decision of the decoder.
4. Finally a stochastic perturbation technique is adopted to provide a controlled random magnitude to the flipped bits.

Moreover, a separate independent assumption is used to simplify the calculation in the detector. Experimental results indicate that the proposed IJDD algorithm provides a substantial error rate improvement compared to a cascaded detector and a bit-flipping decoder. Further the second and third feedback methods prove to be providing better performance than the sign inverted feedback. The simulation for a bit interleaved system shows that the independence assumption used here is reasonably acceptable, even though it is weak compared to the original independent assumption in BP algorithm.

5.2 Possible Future Research Areas

Modifying the proposed algorithm in order to have a better BER performance and a lower complexity will be an interesting research path. In order to focus on simplification of the decoder and to highlight the key units of the proposed algorithm, we have assumed a BPSK modulation. However, this can be further extended to higher-order modulation schemes. Further the FG-LDPC code may be defined in a non-binary Galois field to eliminate short loops in the Tanner graph [20] which strengthens the independence assumption. However, the MBF decoder should be modified in such a way that instead of bit flipping, bit changing is used which will lead to an interesting research path. Incorporating these extensions can be expected to improve the system performance. Furthermore, an optimized feedback calculation method will be the greatest challenge in improving this novel IJDD algorithm.

Bibliography

- [1] J.G. Proakis and M. Salehi, *Digital communications*, McGraw-Hill, 5th ed., 2008.
- [2] A. Goldsmith, *Wireless communications*, Cambridge University Press, 2nd ed., 2005.
- [3] G. J. Foschini and M. J. Gans "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Communications*, vol. 6, pp. 311 – 335, Mar. 1998.
- [4] E. Telatar "Capacity of multi-antenna Gaussian channels," *European Transactions on Telecommunications*, vol. 10, no. 6, pp. 585 – 595, Nov./Dec. 1999.
- [5] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744 - 765, Mar. 1998.
- [6] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1456 - 1467, Jul. 1999.

- [7] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 7, pp. 1169 - 1174, Jul. 2000.
- [8] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451 - 1458, Oct.1998.
- [9] G. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Technical Journal*, pp. 41 - 59, Autumn 1996.
- [10] F. Guo and L. Hanzo, "Low complexity non-binary LDPC and modulation schemes communicating over MIMO channels.," in *Proc. of the IEEE Conference on Vehicular Technology*, vo. 2, pp. 1294 - 1298, Sept. 2004.
- [11] A. Sanderovich, M. Peleg and S. Shamai, "LDPC coded MIMO multiple access with iterative joint decoding," *IEEE Trans. Info. Theory*, vol. 51, no. 4, pp. 1437 - 1450, Apr. 2005.
- [12] A. Matache, C. Jones, and R. Wesel, "Reduced complexity MIMO detectors for LDPC coded systems," *Military Communications Conference (MILCOM 2004)*, vol. 2, pp. 1073 - 1079, Nov. 2004.
- [13] J. Zheng and B. D. Rao, "LDPC-coded MIMO Systems with unknown block fading channels: Soft MIMO detector design, channel estimation, and code optimization," *IEEE Trans. Commun.*, vol. 54, no.4, pp. 1504 - 1518, Apr. 2006.

- [14] K.C. Hwang, S. Park, M. June, S.Y. Yoon "Iterative joint detection and decoding of MIMO-OFDM wireless communications," *40th IEEE ACSSE*, Oct. 2006.
- [15] G. Li, I.J. Fair and W.A. Krzymien, "Low-density parity-check codes for space-time wireless transmission," *IEEE Trans. Wireless. Comm.*, vol. 5, iss. 2, pp. 312 – 322, Feb. 2006.
- [16] G.J. Byers and F. Takawira, "Non-binary and concatenated LDPC codes for multiple-antenna systems," in *Proc. IEEE AFRICON*, pp. 83 – 88, Sept. 2004.
- [17] R. Gallager, "Low-Density Parity-Check Codes," *IRE Trans on Info. Theory*, vol. 8, pp. 21 – 28, Jan. 1962.
- [18] D.J. Mackay and R.M. Neal, "Near Shannon limit performance of low-density parity-check codes," *IEE Electronic Letters*, vol. 32, iss. 18, pp. 1645 – 1646, Aug. 1996.
- [19] D.J. Mackay, "Good error-correcting codes based on very sparse matrices," *IEE Trans in Info. Theory*, vol. 45, no. 2, pp. 399 – 431, Mar. 1999.
- [20] M.C. Davey and D.J.C. Mackay, "Low density parity check codes over $GF(q)$," *IEEE Inform. Theory Workshop*, June 1998.
- [21] S. Lin and D.J. Costello, *Error control coding*, Prentice-Hall, 2003.

- [22] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711 - 2736, Nov. 2001.
- [23] H. Tang, J. Xu, S. Lin, and K. Abdel-Ghaffar, "Codes on finite geometries," *IEEE Trans. Inform. Theory*, vol. 51, no. 2, pp. 572 - 596, Feb. 2005.
- [24] P. Meshkat and H. Jafarkhani, "Space-time low-density parity-check codes," in *Proc. of the 36th Asilomar Conference on Signals, Systems and Computers*, vol. 2, iss. 3, pp. 1117 - 1121, Nov. 2002.
- [25] H.M. Karkhanechi and B.C. Levy, "Spatial multiplexing and diversity gain in OFDM-based MIMO systems," in *Proc. IEEE Wireless Tech. Topical Conf.*, pp. 299 - 301, Oct. 2003.
- [26] H. Futaki and T. Ohtsuki, "Low-density parity-check (LDPC) coded MIMO systems with iterative turbo decoding," in *Proc. IEEE 58th Vehicular Tech. Conf.*, Oct. 2003.
- [27] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo Codes," in *Proc. IEEE Int. Conf. Commun. ICC93*, Geneva, Switzerland, pp. 1064 - 1070, May 1993.
- [28] J. Boutros and G. Caire, "Iterative multiuser joint decoding: Unified framework and asymptotic analysis," *IEEE Trans. Inform. Theory*, vol 48, no 7, pp. 1772 - 1793, Jul. 2002.

- [29] S. Benedetto and G. Montorsi, "Unveilling Turbo codes: Some results on parallel concatenated coding schemes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 409 – 428, Mar. 1996.
- [30] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 429 – 445, Mar. 1996.
- [31] IEEE standard for local and metropolitan area networks - part 16: air interface for fixed and mobile broadband wireless access systems, 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005, 2006.
- [32] IEEE standard 802.3 -2005/Cor 1-2006 IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks., 802.3 -2005/Cor 1-2006, 2006.
- [33] M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, No. 5, pp. 533 – 547, Sept. 1981.
- [34] S. ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," *IEEE Trans. Commun.*, vo. 52, no. 4, pp. 670 – 678, Apr. 2004.
- [35] Z.Liu and D.A.Pados, "A decoding algorithm for finite-geometry LDPC Codes," *IEEE Trans. on Comm.*, vol. 53, iss. 3, pp. 415 – 421, Mar. 2005.

- [36] S. Gounai, T. Ohtsuki and T. Kaneko, "Modified belief propagation decoding algorithm for low-density parity check code based on oscillation," in *Proc. IEEE 63rd Vehicular Tech. Conf.*, vol. 3, pp. 1467 – 1471, May 2006.
- [37] T. Ngatched, F. Takawira & M. Bossert, "An improved decoding algorithm for finite-geometry LDPC Codes," *IEEE Trans. on Comm.*, Volume 57, No 2, pp. 302 – 306, Feb. 2009.
- [38] Y. Yang, X. Changqing, Z. Haibin, "Design of low-density parity-check codes using linear programming for modulation and detection," in *Proc. IEEE 62nd Vehicular Tech. Conf.*, pp. 532 – 535, Sept. 2005.
- [39] M. Tsai, S. Yousefi, "Fixed-complexity list-type iterative detection and decoding of LDPC-coded V-BLAST systems," *24th Biennial Symp. on Comm, Kingston, ON*, June 2008.
- [40] S. Verdu, *Multiuser detection*, Cambridge University Press, 2nd ed., 1998.
- [41] J. Pearl, *Probabilistic reasoning in intelligent systems*, Morgan Kaufmann, 1988.
- [42] J.C. Spall, *Introduction to stochastic search and optimization*, John Wiley & sons Inc., 1st ed., 2003.

Appendix A

Equivalent Representation of a Bandpass System

A.1 Equivalent Lowpass for a Bandpass Signal

Many of the signals in communication systems are real bandpass signals whose frequency response can be represented with a bandwidth $2B$ centered around $f_c (\gg 2B)$. Since they are real signals, their frequency response is symmetric around the origin but the positive frequency components are not necessarily symmetric around f_c . Let's represent a bandpass signal $s(t)$ with a center carrier f_c , as

$$s(t) = s_I(t) \cos(2\pi f_c t) - s_Q(t) \sin(2\pi f_c t), \quad (\text{A.1})$$

where $s_I(t)$ and $s_Q(t)$ representing two real baseband signals with a bandwidth of B each. $s_I(t)$ and $s_Q(t)$ are known as the *in-phase* and *quadrature* components of $s(t)$. Then define a complex baseband signal $s_l(t) = s_I(t) + js_Q(t)$ with a bandwidth B . With this definition, we can observe that

$$\begin{aligned} s(t) &= \operatorname{Re}\{s_l(t) \cos(2\pi f_c t)\} - \operatorname{Im}\{s_l(t) \sin(2\pi f_c t)\} \\ &= \operatorname{Re}\{s_l(t) e^{j2\pi f_c t}\}. \end{aligned} \quad (\text{A.2})$$

This representation is called the *complex lowpass representation* of the bandpass signal $s(t)$ and the signal $s_l(t)$ is known as the *equivalent low pass signal* or the *complex envelope* for the signal $s(t)$. Further with the Fourier transform, it can be shown that

$$S(f) = \frac{1}{2} [S_l(f - f_c) - S_l^*(-f - f_c)]. \quad (\text{A.3})$$

It is important to note that $S_l(f - f_c)$ and $S_l^*(-f - f_c)$ are not necessarily symmetric around $f = f_c$ and $f = -f_c$ respectively.

An alternative representation

$$s_l(t) = a(t) e^{j\phi(t)}, \quad (\text{A.4})$$

where $a(t) = \sqrt{s_I^2(t) + s_Q^2(t)}$ and $\phi(t) = \tan^{-1} \left(\frac{s_Q(t)}{s_I(t)} \right)$, yeilds

$$s(t) = \operatorname{Re}\{a(t) e^{j\phi(t)} e^{j2\pi f_c t}\} = a(t) \cos(2\pi f_c t + \phi(t)). \quad (\text{A.5})$$

A.2 Equivalent Lowpass for a Bandpass Channel

Let's consider a real channel with impulse response $h(t)$. Let Fourier transform of $h(t)$ be $H(f)$. Similar to the bandpass signal, the channel's frequency response is symmetric around the origin, but not symmetric around the carrier frequency f_c . Similar to the baseband signals it can be written as

$$h(t) = 2\text{Re}\{h_l(t)e^{j2\pi f_c t}\}, \quad (\text{A.6})$$

where $h_l(t)$ represents the equivalent lowpass channel impulse response. Further, in the frequency domain

$$H(f) = H_l(f - f_c) + H_l^*(-f - f_c). \quad (\text{A.7})$$

Note that the extra factor of 2 in (A.6) is to avoid a fraction in equation (A.7).

A.3 Equivalent Lowpass for a Bandpass System

Now we are in a position to describe the lowpass equivalent of a total bandpass system.

With both $s(t)$ and $h(t)$ being real, the channel output $r(t)$ is a real signal with $r(t) = s(t) * h(t)$. The Fourier transform yields $R(f) = H(f)S(f)$. This concludes that $R(f)$ is also a bandpass signal, thus the complex low pass representation of $r(t)$ is

$$r(t) = \text{Re}\{r_l(t)e^{j2\pi f_c t}\}, \quad (\text{A.8})$$

with $r_l(t)$ representing the lowpass equivalent of $r(t)$. Then considering that $R(f) = H(f)S(f)$,

$$R(f) = \frac{1}{2} [H_l(f - f_c) + H_l^*(-f - f_c)] [S_l(f - f_c) + S_l^*(-f - f_c)]. \quad (\text{A.9})$$

With the expansion of (A.9) and the fact that $H_l(f - f_c)S_l^*(-f - f_c) = 0$ and $H_l^*(-f - f_c)S_l(f - f_c) = 0$, it implies that

$$R(f) = \frac{1}{2} [H_l(f - f_c)S_l(f - f_c) + H_l^*(-f - f_c)S_l^*(-f - f_c)]. \quad (\text{A.10})$$

Further, given (A.2) and (A.3), (A.8) implies,

$$R(f) = \frac{1}{2} [R_l(f - f_c) + R_l^*(-f - f_c)]. \quad (\text{A.11})$$

Now by equating the terms at positive frequencies in the two representations of $R(f)$, (A.10) and (A.11)

$$R_l(f - f_c) = H_l(f - f_c)S_l(f - f_c),$$

or equivalently

$$R_l(f) = H_l(f)S_l(f). \quad (\text{A.12})$$

In the time domain we have an equivalent given by

$$r_l(t) = h_l(t) * s_l(t), \quad (\text{A.13})$$

which is the equivalent lowpass signal for the received bandpass signal. Finally, the received signal can be represented as

$$r(t) = \text{Re} \left\{ (s_l(t) * h_l(t)) e^{j2\pi f_c t} \right\}. \quad (\text{A.14})$$

The main advantage of these baseband equivalents of a bandpass system is the ability to analyze them in baseband without the carrier components.

Appendix B

Proof of (2.1), (2.2) and (2.3)

B.1 Proof of 2.1

Consider a Gaussian noise channel with noise variance σ^2 . Assuming BPSK modulation, the source bit vector $\{0, 1\}^n$ is mapped to the symbol vector $\{-1, +1\}^n$, thus $P(c_i = 1|r_i) = P(s_i = +1|r_i)$ and $P(c_i = 0|r_i) = P(s_i = -1|r_i)$.

Then,

$$\begin{aligned} P(c_i|r_i) &= \frac{f(r_i|s_i)Pr(s_i)}{f(r_i)} \\ &= \frac{\frac{1}{2}\exp\left(-\frac{(r_i-s_i)^2}{2\sigma^2}\right)}{\frac{1}{2}\exp\left(-\frac{(r_i-1)^2}{2\sigma^2}\right) + \frac{1}{2}\exp\left(-\frac{(r_i+1)^2}{2\sigma^2}\right)} \\ &= \frac{\exp\left(\frac{r_i s_i}{\sigma^2}\right)}{\exp\left(\frac{r_i}{\sigma^2}\right) + \exp\left(-\frac{r_i}{\sigma^2}\right)} \\ &= \frac{1}{\exp\left(\frac{r_i(1-s_i)}{\sigma^2}\right) + \exp\left(-\frac{r_i(1+s_i)}{\sigma^2}\right)} \end{aligned}$$

$$= \frac{1}{1 - \exp\left(-\frac{2r_i s_i}{\sigma^2}\right)}. \quad (\text{B.1})$$

Therefore,

$$P(c_i = 1|r_i) = \frac{1}{1 - \exp\left(-\frac{2r_i}{\sigma^2}\right)}, \quad (\text{B.2})$$

$$\begin{aligned} P(c_i = 0|r_i) &= \frac{1}{1 - \exp\left(\frac{2r_i}{\sigma^2}\right)} \\ &= 1 - \frac{1}{1 - \exp\left(-\frac{2r_i}{\sigma^2}\right)} \\ &= 1 - P(c_i = 1|r_i). \end{aligned} \quad (\text{B.3})$$

B.2 Proof of 2.2

Lemma: Consider a sequence of n independent binary digits $\mathbf{a} = a_1, \dots, a_n$ and $P(a_k = 1) = p_k$. Then the probability that \mathbf{a} contains an even number of 1's is

$$\frac{1}{2} + \frac{1}{2} \prod_{k=1}^n (1 - 2p_k). \quad (\text{B.4})$$

Proof by Induction: Let the boolean sum of the bits in a L bit vector be z_L . Then the event that the number of 1's is even is represented by $z_L = 0$.

• $n=2$

$$P(z_2 = 0) = P(a_1 + a_2 = 0)$$

$$\begin{aligned}
&= p_1 p_2 + (1 - p_1)(1 - p_2) \\
&= \frac{1}{2} + \frac{1}{2} (1 - 2p_1)(1 - 2p_2)
\end{aligned} \tag{B.5}$$

$$= \frac{1}{2} + \frac{1}{2} \prod_{k=1}^2 (1 - 2p_k). \tag{B.6}$$

Therefore (B.4) is true for $n = 2$.

- Assume that (B.4) holds for $n = L - 1$, i.e.

$$P(z_{L-1} = 1) = \frac{1}{2} - \frac{1}{2} \prod_{k=1}^{L-1} (1 - 2p_k). \tag{B.7}$$

- For $n = L$,

$$\begin{aligned}
P(z_L = 0) &= P(z_{L-1} + a_L = 0) \\
&= \frac{1}{2} + \frac{1}{2} [1 - 2P(z_{L-1} = 1)] (1 - 2p_L) && \{\text{by B.6}\} \\
&= \frac{1}{2} + \frac{1}{2} \left[1 - 2 \left\{ \frac{1}{2} - \frac{1}{2} \prod_{k=1}^{L-1} (1 - 2p_k) \right\} \right] (1 - 2p_L) && \{\text{by B.7}\} \\
&= \frac{1}{2} + \frac{1}{2} \prod_{k=1}^L (1 - 2p_k).
\end{aligned}$$

Therefore (B.4) is proved by induction.

Then the probability of having an odd number of 1's

$$\frac{1}{2} - \frac{1}{2} \prod_{k=1}^n (1 - 2p_k). \tag{B.8}$$

When the i^{th} bit is 1, let the event of satisfying the j^{th} parity check be $Z_j|c_i = 1$. This is identical to the event of having an odd number of 1's in other contributing bits. Then from (B.8) with the notation used in Section 2.2.3

$$\begin{aligned} p_{ji}(1) &= P(Z_j|c_i = 1, \mathbf{r}) \\ &= \frac{1}{2} - \frac{1}{2} \prod_{i' \in \mathcal{N}_j \setminus i} (1 - 2q_{i'j}(1)), \end{aligned} \quad (\text{B.9})$$

where $q_{i'j}$ are the probability messages representing bit probabilities.

B.3 Proof of 2.3

Let the event of satisfying all parity checks be \mathbf{Z} and with the bits assumed uncorellated,

$$P(\mathbf{Z}|c_i, \mathbf{r}) = \prod_{j' \in \mathcal{M}_i} P(Z_{j'}|c_i, \mathbf{r}). \quad (\text{B.10})$$

With Bayes' rule

$$\begin{aligned} P(c_i|\mathbf{r}, \mathbf{Z}) &= \frac{P(c_i)P(\mathbf{Z}|c_i, \mathbf{r})}{P(\mathbf{Z})} \\ &= \frac{1}{P(\mathbf{Z})} P(c_i) \prod_{j' \in \mathcal{M}_i} P(Z_{j'}|c_i, \mathbf{r}) \quad \{\text{from (B.10)}\} \\ &= \frac{1}{P(\mathbf{Z})} P(c_i) \prod_{j' \in \mathcal{M}_i} p_{j'i}(c_i). \end{aligned} \quad (\text{B.11})$$

Let,

$$\check{p}_{ij}(c_i) = K_{ij} P(c_i) \prod_{j' \in \mathcal{M}_i \setminus j} p_{j'i}(c_i), \quad (\text{B.12})$$

where K_{ij} is the normalizing constant explained in Section 2.2.3.

Finally in order to have an iterative algorithm,

$$q_{ij}(c_i) \rightarrow \check{p}_{ij}(c_i). \quad (\text{B.13})$$

However note that probability message from i^{th} node is ignored here and this elimination of extrinsic information is needed in avoiding error propagation.

Appendix C

Derivation of (2.6)

It's trivial that

$$\tanh \left[\frac{1}{2} \log \frac{p_1}{p_0} \right] = p_1 - p_0 = 1 - 2p_0. \quad (\text{C.1})$$

Let

$$p_{ji}(1) = \frac{1}{2} - \frac{1}{2} \prod_{i' \in \mathcal{N}_j \setminus i} [1 - 2q_{i'j}(1)], \quad (\text{C.2})$$

which can be re-arranged as

$$1 - 2p_{ji}(1) = \prod_{i' \in \mathcal{N}_j \setminus i} [1 - 2q_{i'j}(1)]. \quad (\text{C.3})$$

From (C.1) and (C.3),

$$\begin{aligned} \tanh \left[\frac{1}{2} L(p_{ji}) \right] &= 1 - 2p_{ji}(0) \\ &= -[1 - 2p_{ji}(1)] \end{aligned}$$

$$\begin{aligned}
&= - \prod_{i' \in \mathcal{N}_j \setminus i} [1 - 2q_{i'j}(1)] \\
&= - \prod_{i' \in \mathcal{N}_j \setminus i} -\tanh \left[\frac{1}{2} L(q_{i'j}) \right].
\end{aligned}$$

Therefore

$$L(p_{ji}) = -2 \tanh^{-1} \left\{ \prod_{i' \in \mathcal{N}_j \setminus i} \tanh \left[-\frac{1}{2} L(q_{i'j}) \right] \right\}. \quad (\text{C.4})$$

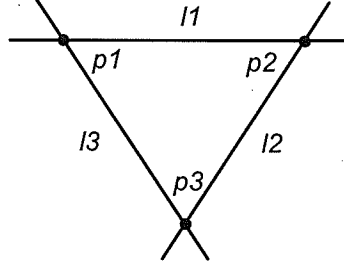
Appendix D

Generation of Finite Geometries

Let, $\text{EG}(\mathcal{D}, 2^T)$ be a \mathcal{D} dimensional euclidean geometry over the $\text{GF}(2^T)$, where \mathcal{D} and T are positive integers. Then each point in this euclidean space is a \mathcal{D} -tuple over $\text{GF}(2^T)$. Further all zero \mathcal{D} -tuple, $\mathbf{0} = (0, 0, \dots, 0)$ is called the origin and the origin point is not considered in forming the euclidean geometry. The euclidean geometry has the following parameter values [22]:

- There are $2^{\mathcal{D}T}$ points.
- There are $2^{(\mathcal{D}-1)T} (2^{\mathcal{D}T} - 1) / (2^T - 1)$ lines.
- Each line consists of 2^T points.
- For any point there are $2^{(\mathcal{D}-1)T} / (2^T - 1)$ lines intersecting at that point.
- Every line has $2^{(\mathcal{D}-1)T} - 1$ lines parallel to it.

Consider an example $\text{EG}(2, 2^1)$. Then

Figure D.1: A sample euclidean geometry: $\mathcal{D} = 2$, $\mathcal{T} = 1$

- There are 4 points (including the origin).
- There are 6 lines.
- Each line consists of 2 points.
- For any point there are 3 lines intersecting at that point.
- Every line has one lines parallel to it.

As usual, the origin and the three lines passing through the origin are ignored. Now the euclidean geometry can be shown as in Fig. D.1 with the three points $p1, p2, p3$ and the three lines $l1, l2, l3$. The corresponding EG-LDPC code's parity check matrix can be generated as [22]

$$\mathcal{H} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Appendix E

Derivation of (3.16)

From Section 3.1.2 we have $\hat{s}_i = \mathbf{w}_{i,MMSE}^H \tilde{\mathbf{r}}_i$ s.t. $E[\|\mathbf{s} - \hat{\mathbf{s}}\|^2]$ is a minimum. An optimal value for $\mathbf{w}_{i,MMSE}^H$ can be calculated using the principle of orthogonality.

Hence

$$\begin{aligned} E[(\mathbf{w}_{i,MMSE}^H \tilde{\mathbf{r}}_i - s_i) \tilde{\mathbf{r}}_i^H] &= 0 \\ \Rightarrow \mathbf{w}_{i,MMSE}^H E(\tilde{\mathbf{r}}_i \tilde{\mathbf{r}}_i^H) - E(s_i \tilde{\mathbf{r}}_i^H) &= 0 \\ \Rightarrow \mathbf{w}_{i,MMSE}^H &= E(s_i \tilde{\mathbf{r}}_i^H) E(\tilde{\mathbf{r}}_i \tilde{\mathbf{r}}_i^H)^{-1}. \end{aligned} \tag{E.1}$$

With $\tilde{\mathbf{r}}_i = \mathbf{r} - \mathbf{H}\tilde{\mathbf{x}}_i = \mathbf{H}(\mathbf{s} - \tilde{\mathbf{x}}_i) + \mathbf{n}$,

$$\begin{aligned} E(\tilde{\mathbf{r}}_i \tilde{\mathbf{r}}_i^H) &= E[\{\mathbf{H}(\mathbf{s} - \tilde{\mathbf{x}}_i) + \mathbf{n}\} \{\mathbf{H}(\mathbf{s} - \tilde{\mathbf{x}}_i) + \mathbf{n}\}^H] \\ &= E[\{\mathbf{H}(\mathbf{s} - \tilde{\mathbf{x}}_i) + \mathbf{n}\} \{(\mathbf{s} - \tilde{\mathbf{x}}_i)^H \mathbf{H}^H + \mathbf{n}^H\}] \end{aligned}$$

$$\begin{aligned}
&= E \left[\mathbf{H}(\mathbf{s} - \tilde{\mathbf{x}}_i)(\mathbf{s} - \tilde{\mathbf{x}}_i)^H \mathbf{H}^H \right] + \underbrace{E \left[\mathbf{n}(\mathbf{s} - \tilde{\mathbf{x}}_i)^H \mathbf{H}^H \right]}_0 + \underbrace{E \left[\mathbf{H}(\mathbf{s} - \tilde{\mathbf{x}}_i) \mathbf{n}^H \right]}_0 + E \left[\mathbf{n} \mathbf{n}^H \right] \\
&= \mathbf{H} \text{COV}(\mathbf{s} - \tilde{\mathbf{x}}_i) \mathbf{H}^H + \sigma^2 \mathbf{I}_{N_r} \\
&= \mathbf{H} \Delta_i \mathbf{H}^H + \sigma^2 \mathbf{I}_{N_r}.
\end{aligned} \tag{E.2}$$

Also

$$\begin{aligned}
E \left[s_i \tilde{\mathbf{r}}_i^H \right] &= E \left[s_i (\mathbf{s} - \tilde{\mathbf{x}}_i)^H \mathbf{H}^H + s_i \mathbf{n}^H \right] \\
&= E \left(s_i s_i^H \mathbf{h}_i^H \right) + \underbrace{E \left[s_i (\mathbf{s} - \tilde{\mathbf{x}}_i)^H \mathbf{H}_{\setminus i}^H \right]}_0 + \underbrace{E \left(s_i \mathbf{n}^H \right)}_0 \\
&= E \left(s_i s_i^H \right) \mathbf{h}_i^H \\
&= E_s \mathbf{e}_i^T \mathbf{H}^H \\
&= \mathbf{e}_i^T \mathbf{H}^H.
\end{aligned} \tag{E.3}$$

Here \mathbf{h}_i , $\mathbf{H}_{\setminus i}$, $\mathbf{x}_{\setminus i}$ and \mathbf{e}_i are the i^{th} column of \mathbf{H} , \mathbf{H} matrix excluding the i^{th} column, sub vector \mathbf{x} excluding the i^{th} element and a N_t dimensional column vector of all zeros except a 1 at i^{th} position, respectively. Further, E_s is the average signal energy which is set to one in this work.

Then with (E.1), (E.2) and (E.3),

$$\mathbf{w}_{i,MMSE} = \left(\mathbf{H} \Delta_i \mathbf{H}^H + \sigma^2 \mathbf{I}_{N_r} \right)^{-1} \mathbf{H} \mathbf{e}_i.$$

Appendix F

Justification of the Independence Assumption

F.1 Independence Assumption for Bipartite BP Algorithm

- Given the received values, initially the bits are statistically independent.
- The independence holds until the message passing between the two levels reaches the closure of a loop. In practical LDPC codes design, girth is selected to be fairly high so that the loop closure occurs only after a fairly large number of iterations. Therefore the independence property is preserved up to a fairly large depth.
- However In practical codes, infinite *girth* is not possible, thus a loop closure occurs

after some iterations and dependencies appear. But at that point, the bit values are more refined and the uncertainties are reduced. With the reduced uncertainty the mutual information is also reduced, reducing the bit dependencies. Further, the resultant bit vector at this stage can again be considered as a new received value set with lesser uncertainty.

Therefore the independence assumption is well justified for the bipartite BP algorithm.

F.2 Independence Assumption for Tripartite IJDD

Algorithm

- In tripartite message passing algorithm, by lumping of received value nodes, the short loops between the received value nodes and bit nodes are eliminated. Further the code is designed to have a higher *girth*. Therefore there are no short loops, thus similar to the bipartite algorithm, the independence is preserved until the closure of a loop.
- Whenever the dependencies appear, the bit values are more refined, even than the bipartite algorithm due to the high rate of convergence in IJDD. Therefore the mutual information and hence the dependencies, are greatly reduced.

F.3 Independence Assumption for MBF Based Novel

Algorithm

Since the proposed MBF based IJDD algorithm does not use any message passing along the edges of a Tanner graph, the independence assumption can be justified as follows.

- In the MBF algorithm, the information transfer follows a similar way as in BP message passing. Therefore if the LDPC code has a Tanner graph which is free of short loops, then the same information does not get transferred to two separate bit nodes until a loop closes, preserving the independence.
- With high code rates, the fraction of independent information bits (compared to dependent parity bits) is large and therefore, the independence assumption holds for majority of bits in a codeword.
- In MBF decoding, a fair amount of uncertainty is reduced at each iteration so that the mutual information and hence the correlation between bits is also reduced.

Therefore the independence assumption can be assumed to hold, even though it is weaker than for the BP algorithm. The simulations in Section 4.5 for a bit interleaved system where the bits are truly independent, is observed to be having only a minor improvement, which further justify the independence assumption.

Appendix G

Localized Random Search

Algorithm

Consider a root finding process of an equation $g(\theta) = 0$. Then the iterative localized random search algorithm is as follows [42]:

Step 0: (Initiaization) Initial guess $\hat{\theta}_0 \in \Theta$ is selected either randomly or with prior information.

Step 1: $\hat{\theta}_{new} = \hat{\theta}_k + \mathbf{d}_k$ where \mathbf{d}_k is an independent random vector.

if $\hat{\theta}_{new} \notin \Theta$, then include θ_{new} in set Θ , otherwise repeat **Step 1**.

Step 2: If $|g(\hat{\theta}_{new})| < |g(\hat{\theta}_k)|$, $\hat{\theta}_{k+1} = \hat{\theta}_{new}$, otherwise $\hat{\theta}_{k+1} = \hat{\theta}_k$.

Step 3: Stop when the maximum number of iterations reached or a predefined stopping criterion is reached, otherwise return to **Step 1**.

This algorithm can be easily modified to suit the MBF decoder. The modified algorithm in the context of the MBF decoder is as follows:

Step 0: (Initialization) Initial guess for the codeword is $\hat{\mathbf{c}}^0$.

Step 1: $\hat{\mathbf{c}}_{new} = \hat{\mathbf{c}}^k + \mathbf{d}_k$, where \mathbf{d}_k is a random bit vector depicting the bit positions to be inverted. If $\hat{\mathbf{c}}_{new}$ has been considered in an earlier iteration repeat **Step 1**, otherwise go to **Step 2**.

Step 2: $\hat{\mathbf{c}}^{k+1} = \hat{\mathbf{c}}_{new}$.

Step 3: If the maximum number of iterations are reached or $\mathbf{Z}^{k+1} = \hat{\mathbf{c}}^{k+1} \mathbf{H}^T = \mathbf{0}$, then stop. Otherwise go to **Step 1**.

It is important to note that **Step 2** here is different from that of the original localized random search algorithm that $\hat{\mathbf{c}}_{new}$ is accepted without checking the closeness of $\hat{\mathbf{c}}_{new} \mathbf{H}^T$ to zero. This measure is important to account for the fact that $\hat{\mathbf{c}}_{new} \mathbf{H}^T$ is not a smooth function even near a local root point. However, it can be shown by simulation that this root search converges.