Performance Analysis of Low Density Parity Check Code for Next Generation Communication System

Major Project Report

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology

In

Electronics And Communication Engineering

(Communication Engineering)

By

Ardeshana Mayankkumar A.

(08MECC01)

Department of Electronics & Communication Engineering

Institute of Technology

Nirma University

Ahmedabad-382 481

May 2010

Performance Analysis of Low Density Parity Check Code for Next Generation Communication System

Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology

In

Electronics And Communication Engineering

(Communication Engineering)

By

Ardeshana Mayankkumar A.

(08MECC01)

Under the Guidance of

Dr. D. K. Kothari

Department of Electronics & Communication Engineering

Institute of Technology

Nirma University

Ahmedabad-382 481

May 2010

Declaration

This is to certify that

i) The thesis comprises my original work towards the degree of Master of Technology in Communication Engineering at Nirma University and has not been submitted elsewhere for a degree.

ii) Due acknowledgement has been made in the text to all other material used.

-Ardeshana Mayankkumar Arvindbhai

Certificate

This is to certify that the Major Project entitled **"Performance Analysis of Low Density Parity Check Code for Next Generation Communication System"** submitted by **Ardeshana Mayankkumar A. (08MECC01)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Communication Engineering of Nirma University, Ahmedabad is the record of work carried out by him under our supervision and guidance. In our opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Date :

Place : Ahmedabad

Internal Guide	External Guide
(Dr. D. K. Kothari) Associate Professor, EC	(Amit Saparia) Team leader Transmission Plan. and Optim., Nokia Siemens Networks Pvt. Ltd.
HOD	Director
(Prof. A. S. Ranade) Professor, EC	(Dr. K Kotecha) Director, IT, NU

Acknowledgements

I am deeply indebted to my thesis guide Dr. D. K. Kothari for his constant guidance and motivation. He has devoted significant amount of his valuable time to plan and discuss the thesis work. Without his experience and insights, it would have been very difficult to do quality work.

My sincere thanks to Director of Institute of Technology, Dr K Kotecha and Prof. A. S. Ranade Head of Electrical Engineering Department for allowing me to undertake this thesis work and their constant encouragement.

My special and sincere thanks to Prof. Mehul Naik and Prof. Y. N. Trivedi and all the members of review committee for their critical review and suggestions during my dissertation work.

I wish to thank all my batchmates for their delightful company which kept me in good humor throughout the year.

Last, but not the least, no words are enough to acknowledge constant support and sacrifices of my family members because of whom I am able to complete the degree program successfully.

- Ardeshana Mayankkumar Arvindbhai

08MECC01

Abstract

Channel coding provides the means of patterning signals so as to reduce their energy or bandwidth consumption for a given error performance. Low density Parity Check (LDPC) codes have been shown to have good error correcting performance which enables efficient and reliable communication. LDPC codes have linear decoding complexity but performance approaching close to shannon capacity with iterative probabilistic decoding algorithm. It has drawn the significant attention of researchers due to these reasons.

In this dissertation, the performance of different error correcting code such as convolution, Reed Solomon (RS), hamming, block code are evaluated based on different parameters like code rate, bit error rate (BER), Eb/No, complexity, coding gain and compare with LDPC code. In general, message passing algorithm and the sum-product algorithm are used to decode the message. We showed that logarithmic sum-product algorithm with long block length code reduces multiplication to addition by introducing logarithmic likelihood ratio so that it achieves the highest BER performance among all the LDPC decoding algorithms. By applying min sum algorithm we achieved further reduction in complexity and improvement of decoding performance. The main contribution of this thesis is to modify min sum algorithm in such a way that decoding performance can be improved with a shorter block length code and reasonable complexity.

The astonishing performance combined with proposed modified min sum decoding algorithm make these codes very attractive for the next generations digital broadcasting system (ABS - S). This reduces the complexity of decoder with a significant performance improvement as compared to the DVB - S2 standard.

Contents

List of Figures

List of Tables

Nomenclature

G	The generator matrix for a linear block code
H	The parity check matrix for a linear block code
N	Number of columns in H (Bit nodes)
M	Number of row in H (Parity check node)
W_c, W_v	Column and row weight of an H parity check matrix
R	Code rate
$I_{M\times M}$	$M \times M$ Idenity matrix
v	Information message
C	Codeword bit
C	Channel capacity
$\mathrm{P}\left(\frac{X_i}{Y_i}\right)$	Estimate of the symbol X_i after knowing that a given symbol Y_i
$\mathrm{E}_{j,i}$	Messages sent from check node j to bit node i
$\mathrm{M}_{j,i}$	Messages sent from the bit node i to the check node j
$\mathrm{LLR}(y_i)$	LLR of priori message probabilities
E_b/N_0	Ratio of energy per bit to the spectral noise density
$P_{j,i}^{ext}$	Probability that the parity-check equation is satisfied if bit i is a 1
$P_{j,i'}^{int}$	Current estimate, available to check j, of the probability that bit i is a 1
$M_{j,i'}$	LLR of $P_{j,i'}^{int}$
$S_{j,i'}$	Sign of $M_{j,i'}$
$\beta_{j,i}$	Magnitude of $M_{j,i'}$
L_i	The total LLR of the i-th bit
$\hat{\gamma}$	Correction factor
$m1$	minimunm value of $M_{j,i'}$
$m2$	sum - minimum value of $M_{j,i'}$

Acronyms

ABS - S	Advanced Broadcasting System-Satellite
ACM	Adaptive Coding and Modulation
APSK	Amplitude Phase Shift Key
AWGN	Additive White Gaussian Noise
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit Error Rate
BPSK	Binary Phase Shift Key
CCM	Constant Coding and Modulation
DVB	Digital Video Broadcasting
DVB - DSNG	Digital Satellite News Gathering
ECC	Error Correcting Code
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
LDPC	Low Density Parity Check Code
LLR	Log Likelihood Ratio
MAP	Maximum A Posteriori
ML	Maximum Likelihood
MMS	Modified Min Sum
PSD	Power Spectral Density
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Key
SNR	Signal to Noise Ratio
SPA	Sum Product Algorithm
VCM	Variable Coding and Modulation

Chapter 1

Introduction

Efficient and reliable digital data communication system are required for faithful data transmission. The channel coding is therefore employed to minimize the error rate & thus increase the reliability of the system. At the same time it improves the system efficiency. The channel coding is correlated with the source information and the channel capacity which is stated in the Shannon theorems as follows :
"*If the information rate of a given source does not exceed the capacity of a given channel, then there exists a coding technique that makes possible error free transmission through this unreliable channel [1].*"

1.1 Error Correcting Codes

Coding techniques are used to control error in modern digital communication system. Without error correcting code data is required to be retransmitted if error has been detected in the received data. Retransmission adds delay, cost and reduces system throughput. The error correcting code can therefore be used to detect and correct errors in the received data thereby increasing system throughput, speed and reducing power consumption. They are specially suitable for long distance one way communication channels such as satellite to satellite and deep space communication. They are also used in wireless communication and storage devices. Several error correction

codes have been developed over time to encode and decode, sending and receiving data respectively. They differ in correcting error performance, computation and complexity.

It has been mentioned how the introduction of FEC schemes increases the complexity of the transmitter and receiver. In particular the receiving equipment has to take care of correcting the possible errors, a task that can be computational demanding. For this reason, when real systems are designed, the choice of the code used cannot be based exclusively on the coding performances but also hardware requirements must be considered. Hence, it is important to develop codes that are capable of good performances without making the encoding and decoding processes intractable from an implementation point of view.

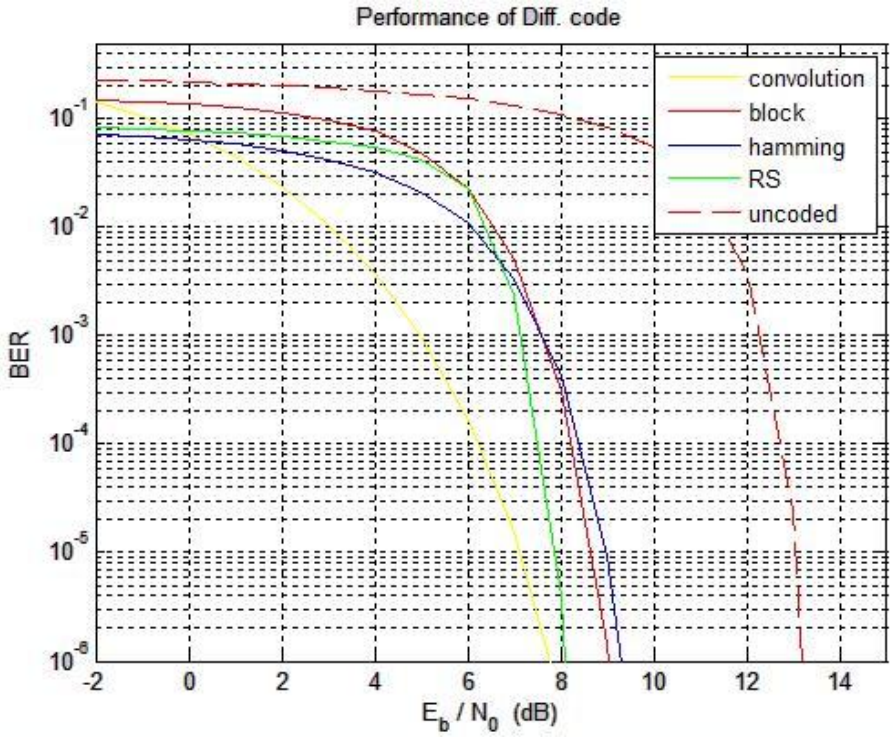


Figure 1.1: BER Performance of different Error Correcting code

The error correcting codes can be classified in two major category namely linear block codes and the convolution codes. Convolution codes differ from block codes in the sense that the encoder output is constructed not only from a single input but also using some previous encoder inputs. Clearly memory is required to store previous inputs for further use. The encoder for a block codes divides the information sequence into message blocks and transforms each message independently to discrete symbols, called codeword. Convolutional codes are used extensively in numerous applications in order to achieve reliable data transfer, including digital video and mobile communication [2]. It is well suited for channels with random errors, in general the reed - solomon code is well suited to correct the burst output errors. Figure 1.1 shows the BER performance of different error correcting codes. The comparison of the same for coding gain, E_b/N_0, BER, complexity and application is given in table 1.1.

Table 1.1: Comparison of different Error Correcting Code

Code	E_b/N_0**(db)**	**Coding Gain(db)**	**BER**	**Complexity**	**Application**
Uncoded	13				
Block	9.3	3.7	10^{-6}	very less	CD - ROM
Hamming	9	4	10^{-6}	less	
Convolution	7.5	5.5	10^{-6}	more	Cellular
RS	8	5	10^{-6}	more	Satellite

It is seen that convolution code has better coding gain compared to other code. However it has more computational complexity. So better codes are usually more complicated and have higher complexity [3]. This realization has lead to the development of better error correction codes and the subject of information theory to meet shannon's condition.

1.2 Thesis Organization

The rest of the thesis is organized as follows.

Chapter 2 is describe the LDPC codes. The different parameters which characterizes the LDPC codes are presented. Representation of LDPC code and methods for constructing LDPC codes are also discussed, followed by algorithm for 4 cycle removal in a tanner graph.

Chapter 3 explain encoding of LDPC codes using different methods like using G matrix, dense method and sparse LU decomposition method. Throughout this thesis Binary Phase Shift Keying (BPSK) modulation is used with Additive White Gaussian Noise (AWGN) channel.

Chapter 4 describes the iterative *Bit flipping Algorithm* and *Sum product Algorithm* which are used to decode the LDPC code and decoding performance of said LDPC code is evaluated. I proposed an algorithm based on sum - minimum value among extrinsic information from the variable nodes into consideration. The purposed algorithm make correction factor varies with different iteration which leads to better decoding performance. In

chapter 5, I have applied the LDPC codes concatenated with BCH codes in DVB - S2 standard which is used in satellite communication system. The performance is evaluated in terms of BER. I have also applied the LDPC codes in combination with the algorithm proposed in 4 to ABS - S system and evaluated its decoding performance.

Finally, in chapter 6 concluding remarks and scope of future work is presented.

Chapter 2

Low Density Parity Check Code

Low-density parity-check(LDPC) code was first proposed by Gallager in the 1963s but it was forgotten for the next few years until the discovery of Turbo codes because of high computation complexity. LDPC codes are linear codes whose parity check matrix contains only a few 1_s in comparison to the amount of 0_s. The most significant difference between LDPC codes and classical block codes lies in the manner [4] they are decoded. Classical block codes are generally decoded with Maximum Likelihood (ML) ratio and so are usually short and designed algebraically to make this task less complex. LDPC codes, however, are decoded iteratively using a graphical representation of their parity-check matrix and so decoding is very complex. LDPC codes mainly have two advantages and distinctions from other traditional codes. First, LDPC codes use the soft value of each bit in decoding. Secondly, it uses iterative decoding scheme based on graph model [5].

2.1 Characteristics of LDPC Codes

2.1.1 Near - capacity approaching Performance

According to shannon's theorem, with the long and random codes better channel capacity can be achieved. As the LDPC codes have large block length, therefore can

attain near capacity performance. Chung and Forney in [6] have demonstrated that LDPC code performs within 0.0045 dB of the Shannon limit at a bit error rate of 10^{-6} with block length of 10^7. The LDPC code works very well at high code rates as well as low code rates. This is demonstrated through simulation in chapter 4.

2.1.2 Sparse Parity Check Matrix

A sparse matrix is a matrix populated with few ones in each row and column. More precisely, the ratio of nonzero entries into that matrix is kept low. This is the reason why they are called $low-density$. Sparseness generally makes the code little complex but gives better error performance. Here the direction of constructing matrices is opposite to the normal one : design H and then calculate G.

2.1.3 Large Hamming distance

The Hamming distance between any two codewords is the number of bits with which the words differ from each other and the minimum distance of a code is the smallest hamming distance between two codewords. The larger the distance better the performance of a code. Some facts can help LDPC codes achieve this goal. First, any two columns have an overlap of at most one. Secondly, the sparse property allows us to avoid over-lapping. Less over - lapping means high independence among different coded bits. This condition provides good decoding ability in LDPC code and results in low bit error rate [5] [7].

2.1.4 Complexity

LDPC code have linear decoding complexity. The complexity per bit(= No of iterations $\times$ Operations per bit per iteration) is independent of the block length. Therefore, the total complexity is linear in the block length. The Encoding, in general, is performed by matrix multiplication and so complexity is quadratic in the code length [8].

2.2 LDPC Representation

2.2.1 Matrix Representation :

LDPC code is a binary linear block code that can be denoted as $N \times M$ code. where N is the code length , M is parity check. For a matrix to be called low-density the two conditions $W_c <<$ N and $W_r <<$ M must be satisfied. W_c is the column weight (number of nonzero elements in a column of the parity-check matrix), and W_r is the row weight (number of nonzero elements in a row of the parity-check matrix).

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

$(8, 4)$ *Code with* $Wc = 2,\ Wr = 4$

2.2.2 Graph Representation :

Tanner graphs, which are essentially Bipartite graphs, can be used to represent LDPC Codes. These graphs also help to describe the decoding algorithm. The tanner graph consists of two types of nodes namely bit nodes and parity check nodes. An edge between a bit node to a check node exists if that bit is included in the corresponding parity-check equation. The number of edges in the tanner graph is equal to the number of ones in the parity-check matrix which is shown in figure 2.1

Tanner graphs are bipartite graphs that means that the nodes of the graph are separated into two distinctive sets and edges are only connecting nodes of two different types. Tanner graph of the code consists N bit nodes and $(1 - M) \times N$ check nodes. Total number of nodes in the tree is therefore $(2 - M) \times N$. In this graph a cycle is

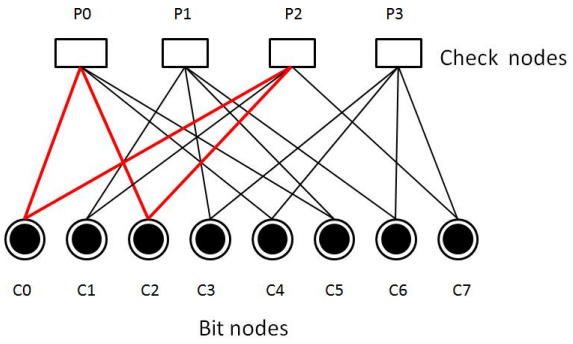


Figure 2.1: Tanner graph corresponding to the (8,4) regular code

formed by a path starting from a node and ending at the same node. The length of cycle is given by the number of edges in the path. Smallest cycle in a tanner graph is called Girth.

2.3 Regular and Irregular LDPC codes

A LDPC code is called *Regular* if Tanner graph is both left and right-regular, means number of one's are constant for every column(W_c) and number of one's are constant for every row (W_r) respectively. The code rate is defined as the ratio of the number of information bits to the total number of bits in the codeword. This is also given by the ratio of the number of check nodes to the number of bit nodes in the code in tanner graph. *i.e.* R = $\frac{M}{N}$

For *Regular Code*

$$W_r = W_c \left(\frac{N}{M}\right) \tag{2.1}$$

When the numbers of 1s in each row or column are not constant than the code is called a *irregular* LDPC code.

For *Irregular Code*

$$M\left(\sum_i h_i \times i\right) = N\left(\sum_i v_i \times i\right) \tag{2.2}$$

For an irregular parity-check matrix we designate the fraction of columns of weight i by v_i and the fraction of rows of weight i by h_i. Where v and h are called the degree distribution of the code. The parity-check matrix shown below is irregular with degree distribution $h_3 = \frac{1}{2}, h_4 = \frac{1}{2}\ and\ v_1 = \frac{1}{4}, v_2 = \frac{3}{2}$. Tanner graph of (8,4) irregular code is shown in figure 2.2. In general, the BER performance of irregular LDPC codes are better than regular LDPC codes [9].

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

$(8, 4)\ irregular\ code$

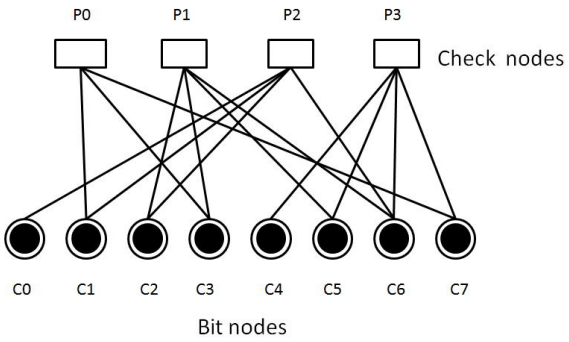


Figure 2.2: Tanner graph corresponding to the (8,4) irregular code

2.4 4 Cycle Removal

The smallest possible girth is four in a tanner graph. In figure 2.1 defined path C0 → P0 → C2 → P2 → C0 is an example for a short cycle. These short cycle should be avoided in the construction of LDPC codes since they are bad for decoding

performance. The Four-loop detection algorithm is used for removing short cycle [10]. The algorithm is explained in figure 2.3.

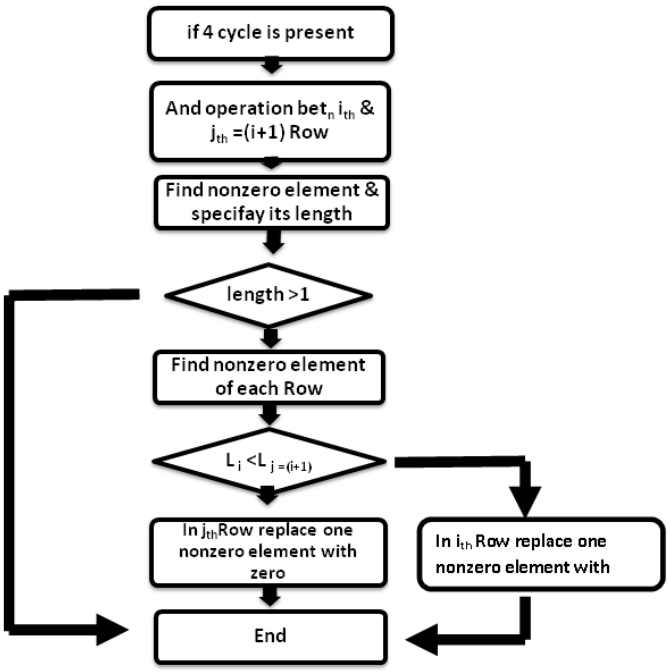


Figure 2.3: Flowchart of 4 Cycle Removal

a. Find the set of all bit nodes N to which the jth check node is connected.

b. For each bit node i in N ($N \neq i$), find all the check nodes M, that are connected to that nodes.

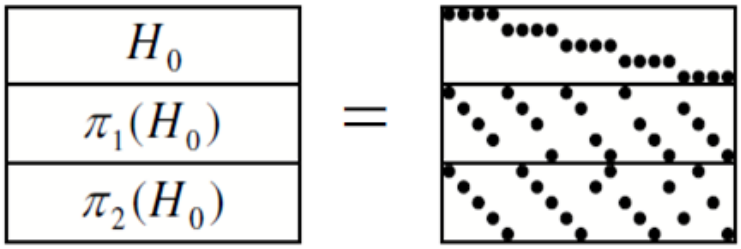
c. For each check node j in M ($M \neq j$), find all the bit nodes N, that are connected to that node.

d. If any ith bit node are in M then a four loop is detected and the edge should be removed.

2.5 Construction of LDPC Code

2.5.1 Gallagers Construction

The original LDPC codes proposed by Gallager with a fixed column weight (W_c) and a fixed row weight (W_r).The parity-check matrix is divided horizontally into W_c blocks with $\frac{M}{Wc}$ rows in each block and containing a single 1 in each column. Every other block of rows is a randomly chosen column permutation of this first block, H_0 as shown in figure 2.4. Where $\pi_i(H_0)$ denotes a column permutation of H_0 [11].



π_1 = {1,5,9,13,2,6,10,17,3,7,14,18,4,11,15,19,8,12,16,20}
π_2 = {1,6,12,18,2,7,11,16,3,8,13,19,4,9,14,17,5,10,15,20}

Figure 2.4: (20,15)Code with Wc=3,Wr=4 Gallagers Construction

2.5.2 MacKay Neal Construction

The Mackay Neal construction method for LDPC codes can be used to avoid cycles of length 4, called 4-cycles, by checking each pair of columns in H to see if they overlap in two places. In one of the method, H is generated with weight j per column and uniform weight i per row for avoiding four cycle or girth larger than six [12]. Figure 2.5 shows one of the Mackay construction which uses identity matrix and rotate it with column permutation of the first block.

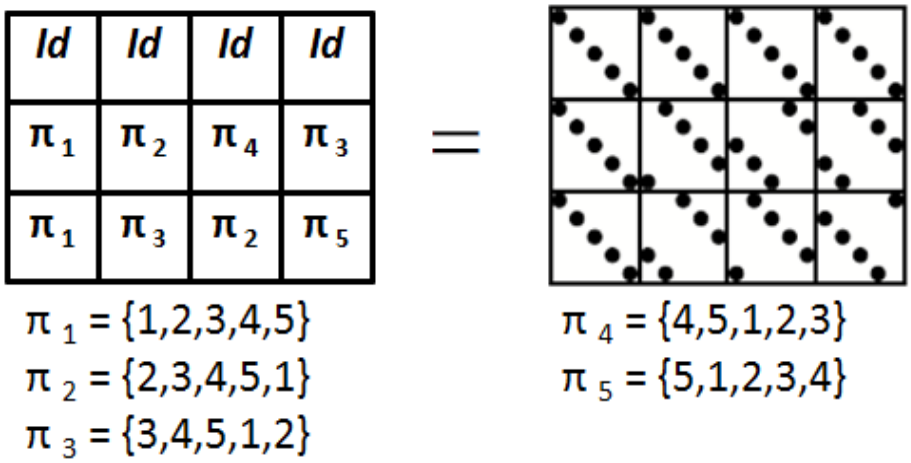


Figure 2.5: (20,15)Code with Wc=3,Wr=4 MacKay's construction

2.6 Summary

LDPC codes are a class of block codes which can be decoded using iterative probabilistic decoding algorithm and codes are based on tanner graph. Random constructions connect rows and columns of a LDPC code matrix without any predefined pattern. Gallager, MacKay and Neal construction were random construction of LDPC which are based on column permutation. Mackay prove that short cycle (Girth 4) should be avoided in the construction of LDPC codes since they are bad for decoding performance. Random constructions have flexibility in design and construction but lack row - column connections regularity, which increase decoder interconnection complexity.

Chapter 3

LDPC Encoding

The encoding of LDPC code is similar to that of the linear block code. From a given parity check matrix H, generator matrix G is derived. The parity check matrix is converted into systematic form $H = [P^T_{N-M\times M} \mid I_{M\times M}]$. From G matrix, codeword is obtained as C = vG where v is the information bit. The drawback of this approach is that, unlike H, the matrix G will most likely not be sparse. The encoding process complexity is of the order of (N^2) for block length N [13]. However for arbitrary parity-check matrices a good approach is to avoid constructing G at all and instead to encode using backward substitution with H. This approach is called as *Dense Encoding Method* [14].

In this method, the parity check matrix H partition into $M \times M$ left part A, and $M \times N$ right part B. If A is non - singular than rearranging the column to make singular. Same way partition the codeword x into $N - M$ information bits, s, and M parity check bits, c.

Now all parity check equations are satisfied if $Hx = 0$.

$$[A \mid B][\frac{c}{s}] = 0$$

From this, we get

$$Ac + Bs = 0$$

so,

$$c = A^{-1}Bs$$

Solving for the parity check bits c requires time of the order of $M \times (N - M)$, when $M < N - M$. If number of one in a row of B is constant then compute c = $A^{-1}z$, where z = Bs. The total time in this case is of the order M^2 which is better than previous method. In these approaches the time complexity is high. The Lower - Upper triangular (LU) decomposition method is on the other hand a fast encoding approach. This is described in following section.

3.1 Fast Encoding of General Low-Density Parity-Check Codes

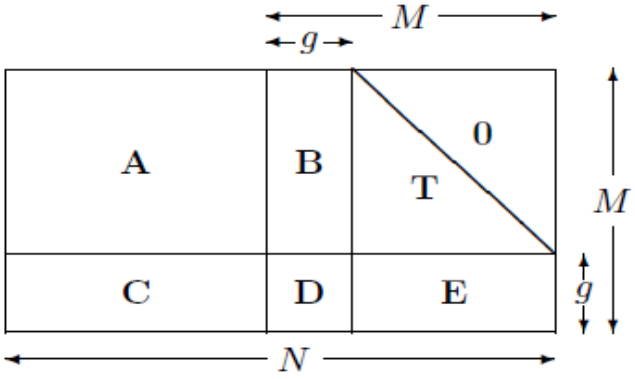


Figure 3.1: H matrix in approximate lower-triangular form

By row interchange and column interchange, the parity-check matrix can be put into approximate lower triangular form [15] as shown in figure 3.1. The matrix T is a lower triangular matrix has 1s everywhere on the diagonal with size $(M-g)\times(M-g)$. Six matrices of parity check matrix named A, B, T, C, D and E are very sparse because the original matrix H was very sparse. Time is reduced by N + g^2 , where g is the small fraction of N and the source vector s of length K = N - M which can be encoded into a transmission $t = [s; P1; P2]$ as follows where P_1 , P_2 are parity bit. Table 3.1 shows different LDPC encoding schemes.

Table 3.1: Summary of the different LDPC encoding schemes

Encoding scheme	**Description**	**Comments**
Using Generator matrix	$H \Rightarrow G; c = vG$	H and G not a sparse. Bad error performance
Dense encoding	$[A \mid B][\frac{c}{s}] = 0$;$Ac+Bs = 0; c = A^{-1}Bs$	A must be a non-sigular.weak error performance.less complex
LU decomposition		High complexity, Fast

3.2 Minimum BER achievable by coded BPSK systems in AWGN Channel

According to shannon's limit, the BER corresponding to channel capacity limit gives the minimum E_b/N_0 required for communication and it depends on a given bit error rate P, and a code rate R [16]. Let H_2 denote the entropy of a binary symmetric source :

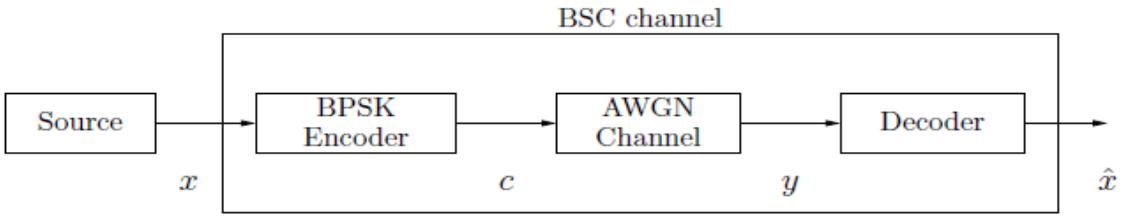


Figure 3.2: The binary-input gaussian-output channel

$$\begin{aligned} (P,R) &= R(1-H_2(p)) \\ &= R(1+plog_2(p)+(1-p)log_2(1-p)) \\ (P,R) &= C\left(R\frac{E_b}{N_0}\right) \end{aligned} \tag{3.1}$$

The graph in 3.3 for different values of are show the minimum bit error probabilities for the binary input with additive white Gaussian noise output. For the AWGN channel represented by R = 0.1, 0.5, 0.9, 0.99 (AWGN) notice that the AWGN input perform better than the binary input modulation. As the rate increases coding gain is

also increasing and tends to optimal value. The binary input curve is moving toward the BPSK curve, whereas the AWGN curve is moving toward shannon's limit of -1.6 db (appendix A).

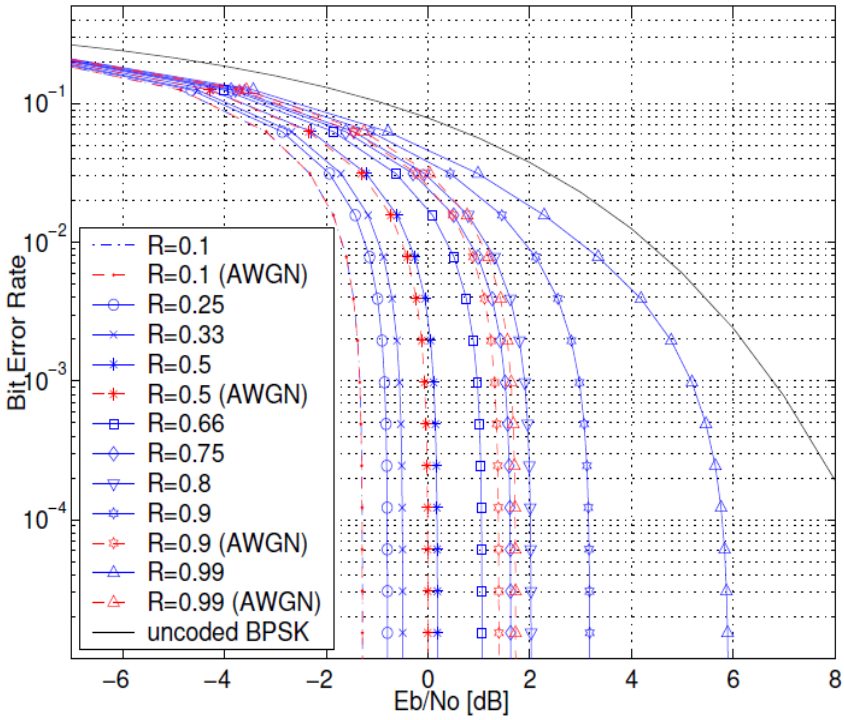


Figure 3.3: Minimum bit error probability for coded BPSK modulations

3.3 Summary

The weak point of LDPC codes is their encoding process: a sparse parity check matrix does not have necessarily a sparse generator matrix. Moreover, it appears to be particularly dense. So encoding by a G matrix yields to an N^2 complexity processing. Richardson demonstrated fast encoding method by which the encoding cost can be reduced from N^2 to a cost of $N + g^2$. Where N = block length, g is the small fraction of N.

Chapter 4

LDPC Decoding

LDPC code decoding is archived through iterative processing based on tanner graph, to satisfy parity check conditions named as *Message Passing Algorithm*. The *Message Passing Algorithm* is based on *Belief Propagation* which are used to decode LDPC code iteratively. In some algorithms, such as bit-flipping decoding, the messages are binary and in others, such as belief propagation decoding, the messages are probabilities which represent a level of belief about the value of the codeword bits. The bit-flipping decoding is one kind of hard decoding which accepts binary bit as input. The sum product algorithm is one kind of soft decoding which accepts input bit probabilities.

4.1 Bit flipping Algorithm

In *bit flipping Algorithm* decoder detects hard decision for each received bit as an input. Each bit node sends a message to each connected check node. The check node determines that its parity-check equation are fulfilled if the modulo-2 sum of the incoming bit values is zero. If parity-check equation are not fulfilled than each check node sends a message to each connected bit node. Each bit node has 3 type of information, out of them first is the original bit received and other two are suggestions from the check nodes. The majority rule is used to take the decision. If the

majority of the messages received by a bit node are different from its received value the bit node changes (flips) its current value. This process is continue until all of the parity-check equations are satisfied, or until maximum number of iterations are defined.

The algorithm is explained on the basis of the previous code (8,4) with regular H matrix and its tanner graph. Let us assume transmitted codeword C=[1 1 0 0 1 0 1 0] which passes through channel, during transmission one error is assumed to occur at bit C3 which flipped to 1. So received codeword C=[1 1 0 1 1 0 1 0]. In the first step, initial parity from bit node is calculated. After that each bit node send message to each connected parity node and each parity node send updated message to bit node. Messages sent and received by the bit nodes is as shown in below, where $[f_0....f_3]$ are parity check node and $[C_0...C_7]$ are bit node.

For f_0

$C_0 \rightarrow 1, f_0 \rightarrow 1$

$C_2 \rightarrow 0, f_0 \rightarrow 0$

$C_4 \rightarrow 1, f_0 \rightarrow 1$

$C_5 \rightarrow 0, f_0 \rightarrow 0$

For f_1

$C_1 \rightarrow 1, f_1 \rightarrow 0$

$C_3 \rightarrow 1, f_1 \rightarrow 0$

$C_5 \rightarrow 0, f_1 \rightarrow 1$

$C_6 \rightarrow 1, f_1 \rightarrow 0$

For f_2

$C_0 \rightarrow 1, f_2 \rightarrow 1$

$C_1 \rightarrow 1, f_2 \rightarrow 1$

$C_2 \rightarrow 0, f_2 \rightarrow 0$

$C_7 \rightarrow 0, f_2 \rightarrow 0$

For f_3

$C_3 \rightarrow 1, f_3 \rightarrow 0$

$C_4 \rightarrow 1, f_3 \rightarrow 0$

$C_6 \rightarrow 1, f_3 \rightarrow 0$

$C_7 \rightarrow 0, f_3 \rightarrow 1$

The decision is then taken using majority rules as shown in table 4.1. The decision is validated by performing parity check. For number of bit errors are more than one, as many iterations are required for parity check operations.

The bit-flipping algorithm has following benefits:

- Once a solution has been found, than additional iterations are avoided.
- Failure to converge to a codeword is always detected.

Table 4.1: Majority rule to take decision

Bit node	Received bit	Sent message from check node	Decision
C_0	1	$f_0 \rightarrow 1, f_2 \rightarrow 1$	1
C_1	1	$f_1 \rightarrow 1, f_2 \rightarrow 1$	1
C_2	0	$f_0 \rightarrow 1, f_2 \rightarrow 0$	0
C_3	1	$f_1 \rightarrow 1, f_3 \rightarrow 0$	0
C_4	1	$f_0 \rightarrow 1, f_3 \rightarrow 0$	1
C_5	0	$f_0 \rightarrow 0, f_1 \rightarrow 1$	0
C_6	1	$f_1 \rightarrow 0, f_3 \rightarrow 0$	1
C_7	0	$f_2 \rightarrow 0, f_3 \rightarrow 1$	0

4.2 Sum Product Algorithm

The sum-product algorithm (SP) is a soft decision algorithm which accepts the probability of each received bit as input. In [17] the SP algorithm estimates the input bit probabilities using *intrinsic* (knowledge before an event) and *extrinsic* (knowledge after an event) information. A *Priori Probabilities* refers to what was known about the bit before observing the outcome of the event A. It is denoted by

$$P_{priori}(x_i = 1/A)$$

Posterior probability $P(X_i/Y_i)$ is normally calculated by updating the *prior* probability by using Bayes' theorem which is an estimate of the symbol X_i after knowing that a given symbol Y_i appeared at the channel output which is denoted by

$$P\left(\frac{X_i}{Y_i}\right) = \frac{P(X_i)P\left(\frac{Y_i}{X_i}\right)}{P(Y_i)}$$

$$where\ X_i = transmitted\ bit \tag{4.1}$$

$$Y_i = received\ bit \tag{4.2}$$

In sum-product decoding algorithm *Priori* and *Posterior* probability are expressed as log-likelihood function. *'Likelihood'* allows us to estimate unknown parameters based on known outcomes. In case of binary the probability of variable x is expressed as Log likelihood ratios (LLR) and is represented by equation 4.3 and 4.4 for bit 1 and 0 respectively.

$$LLR(x) = log\left(\frac{P(x=1)}{P(x=0)}\right) = log\frac{P}{1-P}, \text{if } x = 1 \tag{4.3}$$

$$LLR(x) = log\left(\frac{P(x=0)}{P(x=1)}\right) = log\frac{1-P}{P}, \text{if } x = 0 \tag{4.4}$$

If p ≥ 0.5 or (p$(x = 0) \geq$ p$(x = 1)$) then LLR(x) is positive
If p ≤ 0.5 or (p$(x = 1) \leq$ p$(x = 0)$) then LLR(x) is negative, Thus the sign of LLR(x) provides the hard decision for x and the magnitude $|LLR(x)|$ is the reliability of this decision. The aim of SP decoding algorithm is to maximize the *a - Posteriori Probability* (MAP) for each codeword bit. Extrinsic information for bit i received from the parity-check nodes which is independent of the a priori probability information for the receiver bit i, but depend on the a priori probabilities of the other codeword bits. The a *priori* information is obtained from the channel and extrinsic information is obtained from other nodes in a decoding procedure as given in [18].

$$LLR^{post}(x) = LLR^{prior}(x) + LLR^{extr}(x) \tag{4.5}$$

Important notations :

- $E_{j,i}$ = Messages sent from check node j to bit node i.
- $M_{j,i}$ = Messages sent from the bit node i to the check node j.
- LLR(y_i) = LLR of priori message probabilities.

In case of an Additive White Gaussian Noise (AWGN) channel.

$$LLR(y_i) = \frac{2y_i}{\sigma^2} \tag{4.6}$$

where σ^2 is the noise variance and y_i(0,1) is the received bit. Sum-product algorithm of LDPC decoding requires the knowledge of noise variance of a Gaussian channel. If the assumed noise variance is smaller than that of the true value, the performance of decoding degrades. LLR(y_i) is the received probability. $E_{j,i}$ is the LLR of the probability that bit i causes parity-check j to be satisfied. The probability that the parity-check equation is satisfied if bit i is a zero is thus 1 - $P^{ext}_{j,i}$.

$$E_{j,i} = LLR(P^{ext}_{j,i}) = log\left(\frac{1 - P^{ext}_{j,i}}{P^{ext}_{j,i}}\right) \tag{4.7}$$

where $P^{ext}_{j,i}$ is the probability that the parity-check equation is satisfied if bit i is a 1. It is defined asB

$$P^{ext}_{j,i} = \frac{1}{2} - \frac{1}{2}\prod_{i \neq i'}(1 - 2P^{int}_{j,i'}) \tag{4.8}$$

where $P^{int}_{j,i'}$ is the current estimate, available to check j, of the probability that bit i is a 1.

$$E_{j,i} = log\left[\frac{\frac{1}{2} + \frac{1}{2}\prod_{i \neq i'}(1 - 2P^{int}_{j,i'})}{\frac{1}{2} - \frac{1}{2}\prod_{i \neq i'}(1 - 2P^{int}_{j,i'})}\right] \tag{4.9}$$

where,

$$\begin{aligned} 1 - 2P^{int}_{j,i'} &= \tanh\left[\frac{1}{2}log\left(\frac{P^{int}_{j,i'}}{1 - P^{int}_{j,i'}}\right)\right] \\ &= \tanh\left[\frac{1}{2}LLR(P^{int}_{j,i'})\right] \\ &= \tanh\left[\frac{1}{2}M_{j,i'}\right] \end{aligned}$$

$$E_{j,i} = log\left[\frac{1 + \prod_{i \neq i'}\tanh\left(\frac{M_{j,i'}}{2}\right)}{1 - \prod_{i \neq i'}\tanh\left(\frac{M_{j,i'}}{2}\right)}\right] \tag{4.10}$$

The total LLR of the i-th bit is the sum of these LLRs:

$$L_i = LLR(y_i) + \sum_{j \in C_i} E_{j,i} \tag{4.11}$$

4.3 Min-Sum Product Algorithm

The sum-product algorithm can be modified to reduce the implementation complexity of the decoder [19]. The Min-Sum (MS) algorithm is based on the sum-product algorithm with a simple approximation approach, and it is not necessary to estimate the noise power for an additive white Gaussian noise channel so it offers better solutions to reduce implementation complexity of the decoder in terms of hardware [20]. Messages from check node j to bit node i can be written as

$$E_{j,i} = log \left[\frac{1 + \prod_{i \neq i'} \tanh\left(\frac{M_{j,i'}}{2}\right)}{1 - \prod_{i \neq i'} \tanh\left(\frac{M_{j,i'}}{2}\right)} \right] \tag{4.12}$$

This equation can be written as

$$E_{j,i} = 2tanh^{-1} \left[\prod_{i \neq i'} tanh\left(\frac{M_{j,i'}}{2}\right) \right] \tag{4.13}$$

Firstly $M_{j,i'}$ can be factored as sign and magnitude separately

$$\begin{aligned} S_{j,i'} &= sign(M_{j,i'}) \\ \beta_{j,i} &= \mid M_{j,i'} \mid \end{aligned}$$

Then equation becomes

$$E_{j,i} = \left(\prod_{i \neq i'} S_{j,i'} \right) 2tanh^{-1} \left(\prod_{i \neq i'} tanh\left(\frac{\beta_{j,i'}}{2}\right) \right) \tag{4.14}$$

It can be re-arranged to replace the product by a sum

$$\begin{aligned} E_{j,i} &= \left(\prod_{i\neq i'} S_{j,i'}\right) 2tanh^{-1}log^{-1}log\left(\prod_{i\neq i'} tanh\left(\frac{\beta_{j,i'}}{2}\right)\right) \\ &= \left(\prod_{i\neq i'} S_{j,i'}\right) 2tanh^{-1}log^{-1}\left(\sum_{i\neq i'} logtanh\left(\frac{\beta_{j,i'}}{2}\right)\right) \end{aligned}$$

Note that the inverse hyperbolic tangent is

$$tanh^{-1}(x) = \frac{1}{2}log\frac{1+x}{1-x} \tag{4.15}$$

Define new function for $x > 0$, where the smaller x has larger value of $\phi(x)$

$$\phi(x) = \phi^{-1}(x) = log\frac{1+e^{-x}}{1-e^{-x}} = -log[tanh(x/2)] \tag{4.16}$$

Finally equation becomes

$$E_{j,i} = \left(\prod_{i\neq i'} S_{j,i'}\right) \phi\left(\sum_{i\neq i'} \phi(\beta_{j,i'})\right) \tag{4.17}$$

Now take minimum value of $\beta_{j,i'}$

$$E_{j,i} = \left(\prod_{i\neq i'} S_{j,i'}\right) min_{i\neq i'}\beta_{j,i'} \tag{4.18}$$

$$E_{j,i} = \left(\prod_{i\neq i'} sign(M_{j,i'})\right) min_{i\neq i'} \mid M_{j,i'} \mid \tag{4.19}$$

4.4 Modified Min-Sum Product Algorithm

The Min-Sum Product process is almost completely determined by the magnitude and sign of the minimum value. When the sub - minimum value among the extrinsic information is close to the minimum one, the MS algorithm sufferes great performance degradation, So we intend to take the sub - minimum value into consideration and

find a correction factor $\hat{\gamma}$ which is related to $E_{j,i}$ as shown in equation 4.20.

$$(E_{j,i})_{MMS} = \hat{\gamma}\ (E_{j,i})_{MS} \tag{4.20}$$

Let $m1$, $m2$ denote the minimum and sub - minimum value of $\mid M_{j,i'} \mid$. Using property of $\phi(x)$, we can make an approximation that

$$\phi\left(\sum_{i \neq i'} \phi(\mid M_{j,i'} \mid_{min_{i \neq i'}})\right) = \phi[\phi(m1) + \phi(m2)] \tag{4.21}$$

Assume

$$\phi[\phi(m1) + \phi(m2)] = \hat{\gamma}\ m1 \tag{4.22}$$

where, $\hat{\gamma}$ = correction factor, using the property $\phi(x), x > 0$ and applied on equation 4.22

$$\begin{aligned} \phi(\hat{\gamma}\ m1) &= \phi[\phi[\phi(m1) + \phi(m2)]] \\ &= \phi(m1) + \phi(m2) \end{aligned}$$

$$\phi(x) = \phi^{-1}(x) = log\frac{1 + e^{-x}}{1 - e^{-x}} = log\frac{e^{x} + 1}{e^{x} - 1} \tag{4.23}$$

Equation 4.22 and 4.23 can be rewritten as

$$\begin{aligned} log\left[\frac{e^{\hat{\gamma}\ m1} - 1}{e^{\hat{\gamma}\ m1} - 1}\right] &= log\left[\frac{e^{m1} + 1}{e^{m1} - 1}\right] + log\left[\frac{e^{m2} + 1}{e^{m2} - 1}\right] \\ &= log\left[\frac{e^{m1} + 1}{e^{m1} - 1}\ \frac{e^{m2} + 1}{e^{m2} - 1}\right] \\ \frac{e^{\hat{\gamma}\ m1} - 1}{e^{\hat{\gamma}\ m1} - 1} &= \frac{e^{m1} + 1}{e^{m1} - 1}\ \frac{e^{m2} + 1}{e^{m2} - 1} \\ &= \frac{e^{m1+m2} + e^{m1} + e^{m2} + 1}{e^{m1+m2} - e^{m1} - e^{m2} + 1} \end{aligned}$$

On solving, we get

$$e^{\hat{\gamma}\ m1+m1} + e^{\hat{\gamma}\ m1+m2} - e^{m1+m2} - 1 = 0$$

$$e^{\hat{\gamma}\ m1} = \frac{1 + e^{(m1+m2)}}{e^{m1} + e^{m2}}$$

Finally, we calculate correction factor $\hat{\gamma}$ in terms of $m1$ and $m2$

$$\hat{\gamma} = \frac{1}{m1} log \left[\frac{1 + e^{(m1+m2)}}{e^{m1} + e^{m2}} \right] \tag{4.24}$$

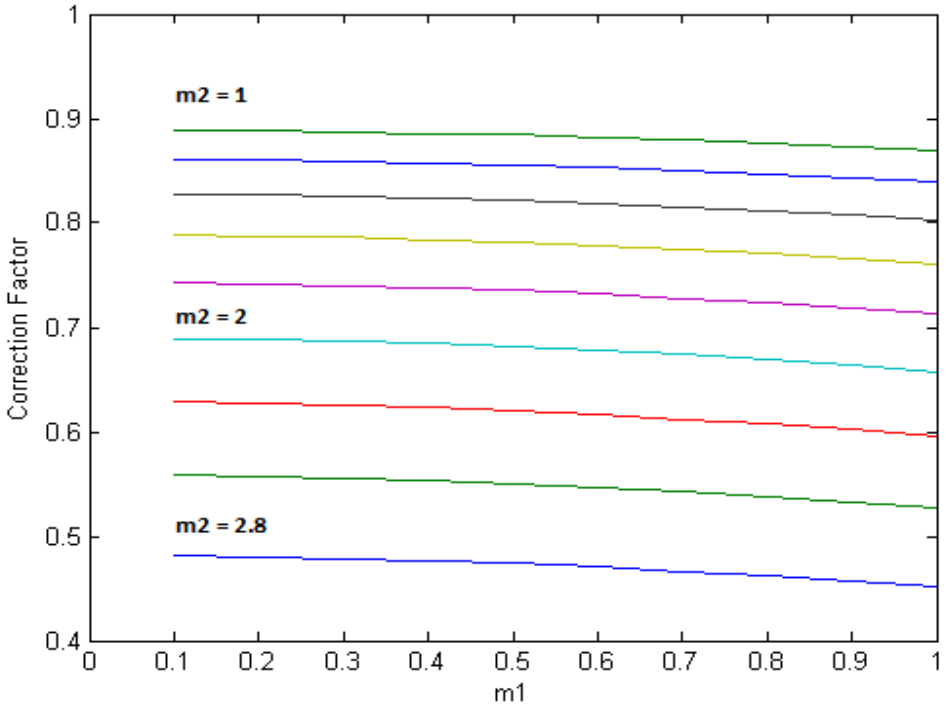


Figure 4.1: Relation between Correction factor ($\hat{\gamma}$) and m1

First we check the importance of the sub - minimum value. Figure 4.1 and figure 4.2 shows the relation between correction factor ($\hat{\gamma}$) and minimum value ($m1$), correction factor ($\hat{\gamma}$) and sub - minimum value ($m2$) respectively.

From Figure 4.1, we can see at particular sum - minimum value ($m2$), correction

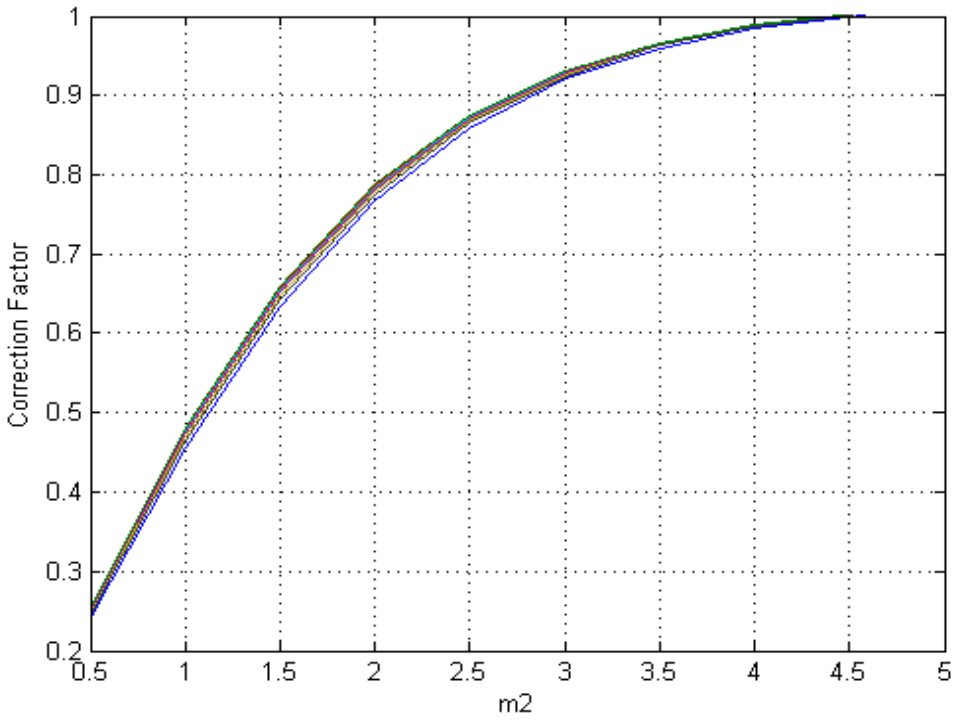


Figure 4.2: Relation between Correction factor ($\hat{\gamma}$) and m2

factor ($\hat{\gamma}$) changes slightly as minimum value ($m1$) changes. Figure 4.2 shows that with the increasing m2, correction factor ($\hat{\gamma}$) also increasing and converges from 0 to 1. As a result the curves with different m1 value are very close to each other. According to the above analysis, it seems that the sub - minimum value among the extrinsic messages from the variable nodes plays an important role in the valuation of the correction factor ($\hat{\gamma}$), so by allowing the factor to change at each iteration in view of the sub - minimum value, the MMS algorithm can improve the BER performance.

Table 4.2: Value of correction factor according to m2

m2	Correction factor	m2	Correction factor
0 to 0.5	0.25	1.6 to 2	0.75
0.5 to 0.7	0.35	2 to 2.5	0.85
0.7 to 1	0.45	2.5 to 3	0.90
1 to 1.3	0.55	3 to infinite	0.95
1.3 to 1.6	0.65		

According to figure 4.2, we choose different correction factor ($\hat{\gamma}$) which is shown in table 4.2.

4.5 Performance Evaluation and Numerical Result

In this section, we present the performance analysis of Sum product decoding scheme in terms of Bit Error Rate (BER) in additive white gaussian noise (AWGN) channel. For that we set 500 information bits, 500 parity bits, so codeword bits are 1000, weight of column W_c in H matrix is 3 and code rate is 1/2. It is seen from figure 4.3that BER at 3 dB is 6.034×10^{-3} and Signal to Noise Ratio (SNR) at 5.7 dB is 6.034×10^{-3}. It is observed that if any system requires BER of 10^{-3} then minimum value of E_b/N_0 should be 3 dB.

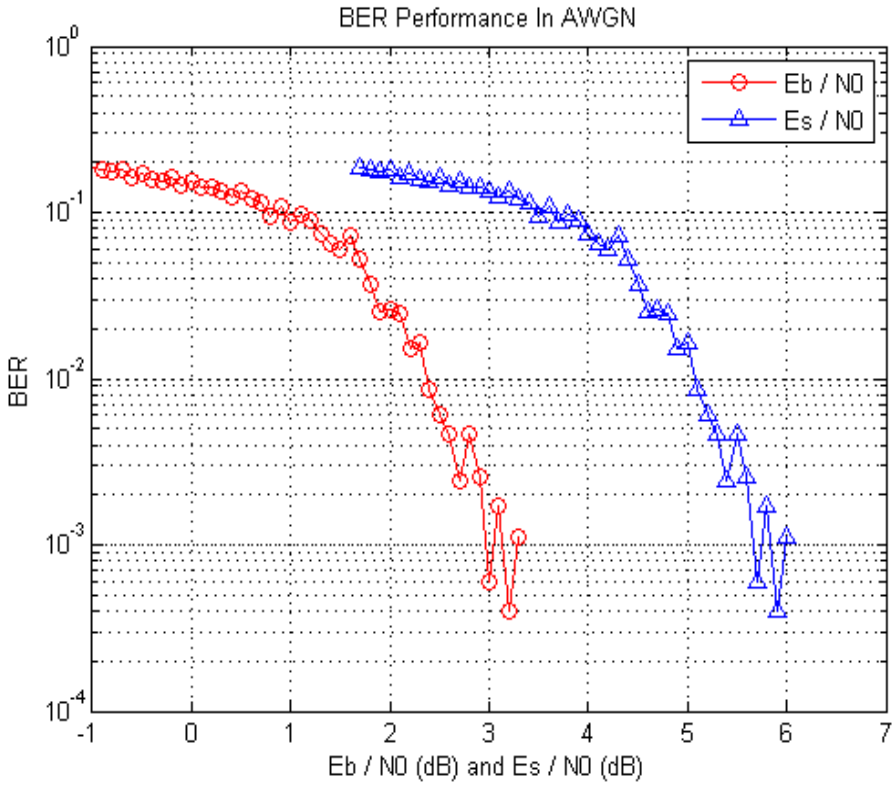


Figure 4.3: (1000,500,3) Sum Product decoding

We compare the performance analysis of Bit flipping and Sum product decoding

scheme in terms of Bit Error Rate (BER) in additive white gaussian noise (AWGN) channel as shown in figure 4.4. For that we set 1000 information bits, 1000 parity bits, so codeword bits are 2000, weight of column W_c in H matrix is 3 and code rate is 1/2. It is notated that bit flipping decoding gives 0.5 BER throughout the E_b/N_0 while sum product decoding gives 8.07×10^{-3} BER at 3 dB which is better than bit flipping because sum product decoding accepts soft decision as a input while bit flipping accepts hard decision.

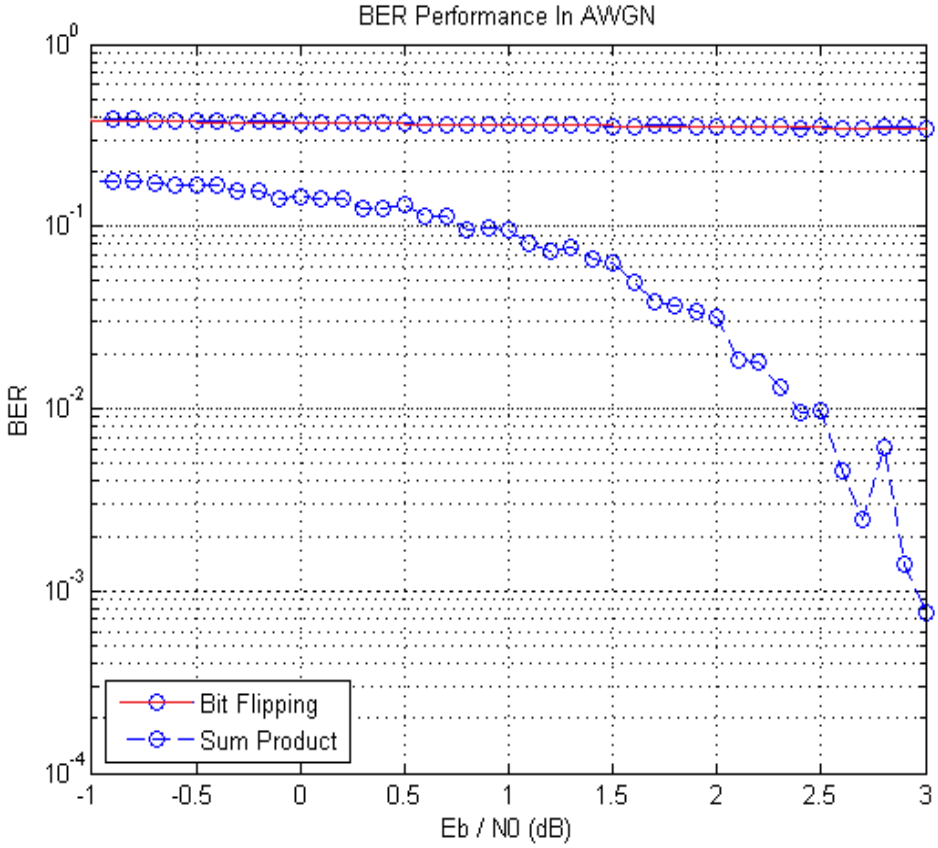


Figure 4.4: (2000,1000,3)code BER performance of bit flipping and Sum Product decoding

Values of BER have been computed for Bit flipping and Sum product decoding scheme with different code rate, which is shown in table 4.3. It is observed that at low code rate of 1/9, bit flipping gives 0.3756 BER and sum product gives 0.0811 BER. At high code rate of 4/5 bit flipping gives 0.3360 BER and sum product gives

0.0834 BER and for standard code rate at 1/2, bit flipping gives 0.3550 BER and sum product gives 0.1550 BER. So it can be stated that LDPC code work better at high code rates as well as low code rates.

Table 4.3: Code comparison with different Code Rate

Code Rate	**Weight of column (W_c)**	**Bit Flipping**	**Sum Product**
1/9	3	0.3756	0.0811
1/5	3	0.3860	0.090
1/4	3	0.3975	0.1250
1/3	3	0.3933	0.1367
2/5	4	0.4320	0.160
1/2	3	0.3550	0.1550
3/5	3	0.4500	0.1240
2/3	4	0.3800	0.1167
3/4	3	0.3600	0.0980
4/5	4	0.3360	0.0834

For, LDPC codes increasing block length results in increasing BER performance. This is because the bit nodes and check nodes receive some extrinsic information from the nodes that are far from them in a given block length. This increases the error correction capability of the code. For simulation purpose we set different block length N = 96, 408, 1008, 4000 with code rate = 1/2, using sum product algorithm. Moreover, modulations by BPSK and transmission over an AWGN channel are assumed, and the maximum number of iterations is set to 50. The BER performance is shown in figure 4.5.

For N=96, M=48 BER value can be computed using different value of E_b/N_0 which is shown in table 4.4. At 4 E_b/N_0 BER value is 0.001297. For N=408, M=204 and N=1008, M=504 and N=4000, M=2000 BER value are computed using different value of E_b/N_0 and are shown in table 4.5, 4.6, 4.7 respectively. From table 4.5, 4.6 and 4.7 at 4 E_b/N_0, BER value is 0.00035 and 0.00010 and 0.00005 respectively. As the block length is increasing from N=96 to N=4000, BER performance also increasing from 0.001297 to 0.00005.

Table 4.4: For N = 96, M = 48, Max iteration = 50

E_b/N_0 (dB)	Block	Total bit	Uncoded error	Error after decoding	BER
0	250	24000	3861	7102	0.295917
1	250	24000	3188	3998	0.166583
2	250	24000	2576	1634	0.068083
3	615	59040	4617	504	0.008537
4	4457	427872	24228	555	0.001297

Table 4.5: For N = 408, M = 204, Max iteration = 50

E_b/N_0 (dB)	Block	Total bit	Uncoded error	Error after decoding	BER
0	250	102000	16242	31894	0.312686
1	250	102000	13302	14375	0.140931
2	250	102000	10795	2152	0.021098
3	8156	3327648	261648	2152	0.001762
4	20000	8160000	460821	2856	0.000350

Table 4.6: For N = 1008, M = 504, Max iteration = 50

E_b/N_0 (dB)	Block	Total bit	Uncoded error	Error after decoding	BER
0	250	252000	39924	78932	0.313222
1	250	252000	32971	36670	0.145516
2	1266	1276128	132799	4842	0.003794
3	14576	14692608	1159184	25200	0.000515
4	20000	20160000	1138510	2016	0.000100

Table 4.7: For N = 4000, M = 2000, Max iteration = 50

E_b/N_0 (dB)	Block	Total bit	Uncoded error	Error after decoding	BER
0	250	1000000	158172	308053	0.308053
1	250	1000000	130749	132001	0.132001
2	20000	80000000	8323674	92398	0.001155
3	20000	80000000	6313316	8000	0.000100
4	20000	80000000	4521418	4000	0.000050

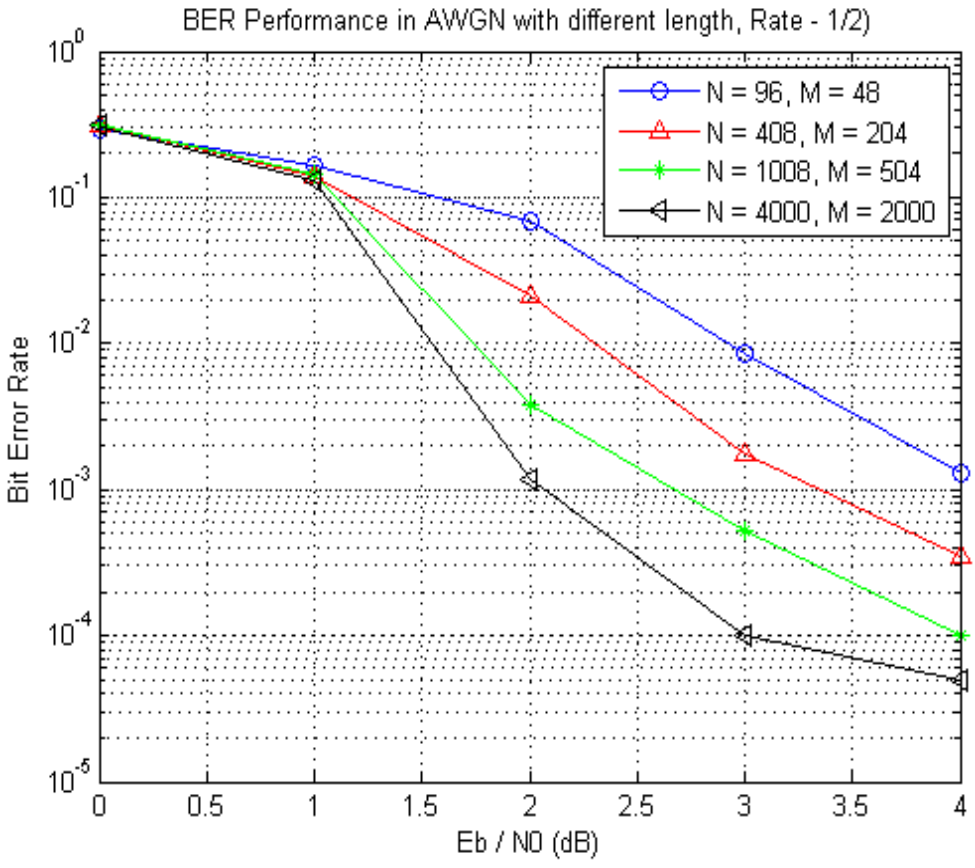


Figure 4.5: BER performance In AWGN with different block length

Figure 4.6 shows the BER performances of (500, 250) LDPC codes with (W_c, W_r) = (3, 6) and compare sum product, min sum product, modified MS algorithm (correction factor = 0.95). The maximum number of iterations is set to 50 using AWGN channel, BPSK modulation scheme is considered. Results shows that modified MS algorithm ($\hat{\gamma} = 0.95$). offers $3.457 * 10^{-5}$ BER at 3 dB which is better compare to sum product gives $9.345 * 10^{-4}$ BER at 3 dB and MS algorithm gives $8.32 * 10^{-5}$ BER at 3 dB. Thus it is evident that modified MS algorithm can efficiently reduce the computational complexity and achieve good BER performance.

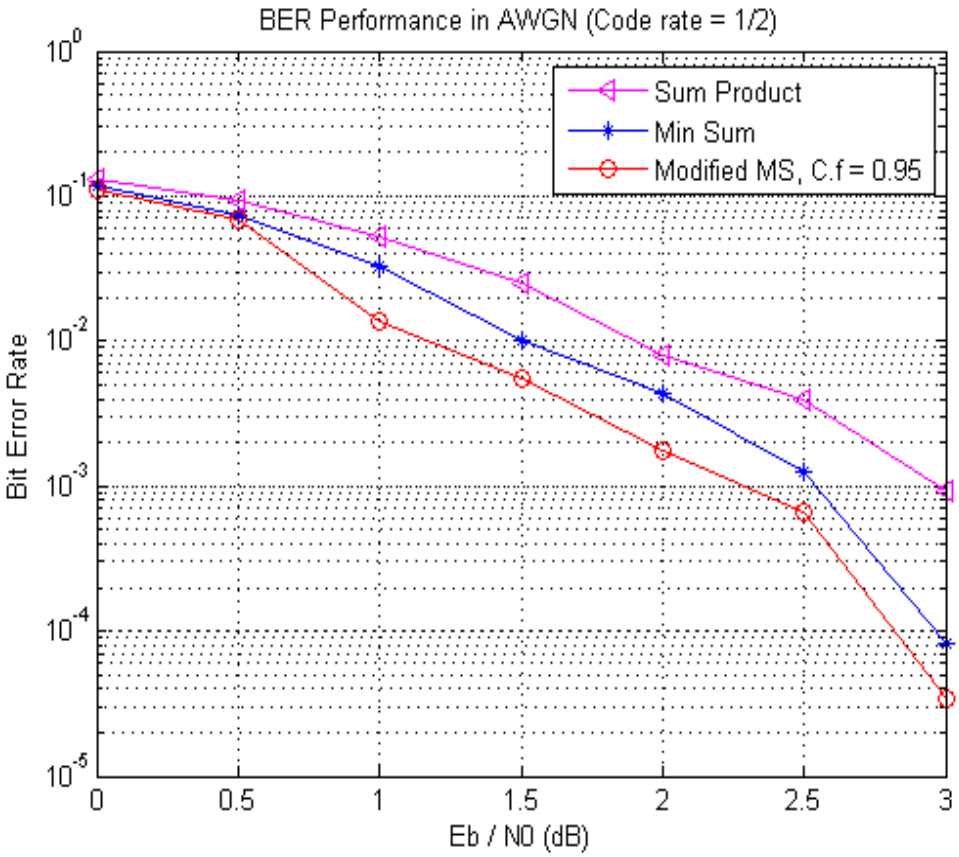


Figure 4.6: Comparison of SP, Min Sum, Modified MS algorithm

4.6 Summary

In this chapter the decoding logic using bit flipping and sum product decoding algorithm is explained. The simulation results shows that soft decoding (which accepts input bit probabilities) is better than hard decoding (which accepts binary bit as a input). In the case of LDPC code with large-code length for a sufficient number of iterations, the BER performance of LDPC codes is close to the shannon limits. Min sum algorithm has the advantage of improvement in decoding performance and the reduction in complexity. Our proposed modification in MS algorithm shows that sum - minimum value plays important role in determining a correction factor which relates to $E_{j,i}$ and is used to update check nodes. It results in decoding improvements.

Chapter 5

Application of LDPC Code in DVB-S2

LDPC codes have been applied to applications in satellite communication and storage systems. Satellite downlinks are generally characterized as power limited channels. On board batteries and solar cell are heavy and contribute significantly to launch costs. Communication channel with bit error rate 10^{-6} is desired for many applications. Storage system require very high data rate ($\frac{9}{10}$) and higher, low SNR(3 to 7 dB) with expected BER value 10^{-8} to 10^{-10}. So, LDPC codes are one of the most suitable codes of these recursive channels [21]. Communication standard such as digital video broadcasting standard 2 uses LDPC code with a variety of rate, $\frac{1}{4}$ to $\frac{9}{10}$, and long block length 32400 to 64800. LDPC code are also recommended for other communication environments such as gigabyte ethernet, wireless broadband and optical communication [22].

5.1 Digital Video Broadcasting

Digital satellite transmission system was the first area addressed by the digital video broadcasting (DVB) Project in 1993 by the European Telecommunications Standards Institute (ETSI). Its initial standard for satellite delivery of digital television and data

services (DVB - S) and digital satellite news gathering (DVB - DSNG), used a serial concatenation of an outer reed Solomon code and an inner variable rate convolution code. There are increased demands for larger capacity and innovative services by satellite broadcast service since first system established. So the new specification DVB - S2 is enacted. The existing standards of DVB - S and DVB - DSNG offered QPSK (DVB - S and DVB - DSNG), 8PSK and 16QAM (for DVB - DSNG) modulation scheme.

It provides only downlink but an uplink is also needed to enable interactive applications such as web browsing. The uplink and downlink need not be symmetric because many Internet services require a faster downlink. A more attractive alternative is for the subscriber equipment to transmit an uplink signal back to the satellite over the same antenna used for receiving the downlink signal. However, given the small antenna aperture and requirement for a low-cost, low-power amplifier, there is very little margin on the uplink. This was a limitation of DVB-S. Therefore, strong FEC coding is desired. For this reason it makes use of the latest modulation schemes and coding techniques to deliver performance that approaches the theoretical limit for such systems.

5.2 Function block diagram of DVB-S2

The DVB - S2 System is composed of a sequence of functional blocks as described in figure 5.1. The block identified as "Baseband Interface" is suitable for operation with single and multiple input streams of transport streams, generic streams (packetized or continuous) [22]. Second block "Mode Adaptation" is application dependent like satellite broadband applications, including point-to-point applications like IP unicasting or DSNG with the adoption of Variable Coding and Modulation (VCM) and Adaptive Coding and Modulation (ACM), allowing different modulation formats and error protection levels (coding rates) to be used and changed on a frame-by-frame

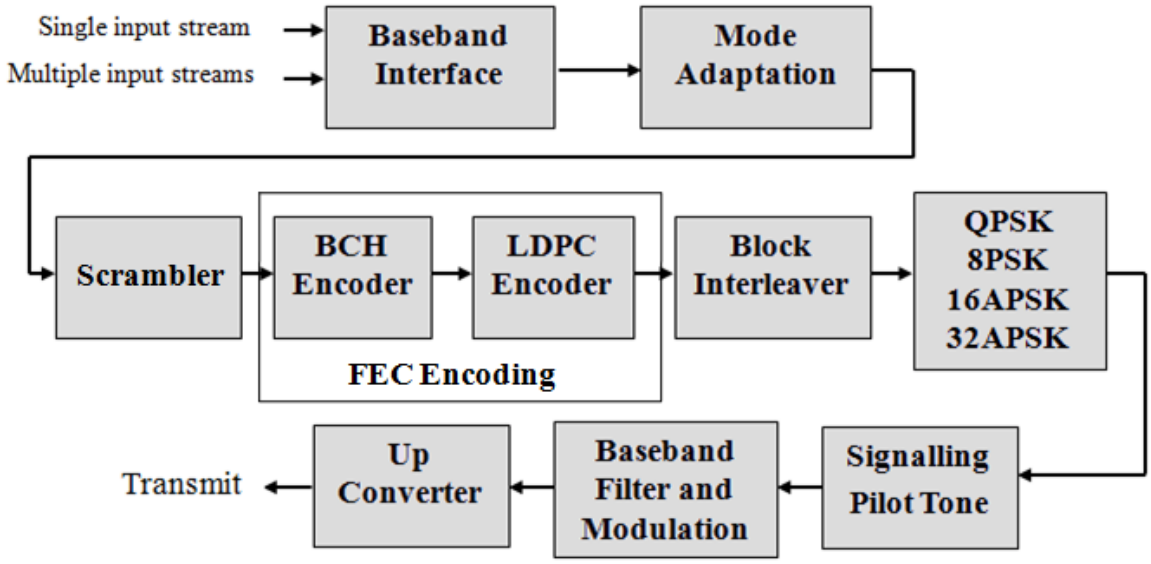


Figure 5.1: Functional block diagram of the DVB-S2 system

basis within the transmitted data stream so ACM has been considered as a powerful tool to further increase system capacity. Scrambler is used for synchronization, clock recovery and security purpose by removing long string of 1's and 0's.

The DVB - S2 specification is the world's first standard using a serial concatenation of LDPC codes for the FEC together with an outer Bose-Chaudhuri-Hoquenghem (BCH) code, it allows for outstanding communications performance with reasonable complexity [23]. Data is first encoded using a BCH code which capable of up to t = 12 error correction and its Blocklength varies from n_{BCH} = 3,240 to n_{BCH} = 58,320. After encoded BCH data further encoded using LDPC code with variable rate R_{LDPC} = 1/4 to R_{LDPC} = 9/10. Depending on the application area, the FEC coded blocks (FEC frames) can have length 64,800 (normal frame) or 16,200 (short frame) bits.

After encoded data passing through interleaver which is a tool that can be used in digital communications systems to enhance the random error (bit errors are independent of each other. Additive noise typically causes random errors) correcting

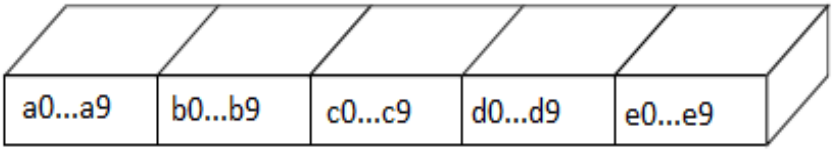


Figure 5.2: Data Bits Output from the Encoder for N = 10, K = 5

capabilities of block codes such as RS codes, turbo code and LDPC code. Block interleaving is more commonly invoked because it is more easily accomplished in hardware which accept symbols in blocks as shown in figure 5.2 and perform identical permutations over each block of data. One way this is accomplished involves taking the input data and writing the symbols by rows into a matrix with i rows and n columns and then reading the data out of the matrix by columns as shown in figure 5.3. Output of block interleaver which is shown in figure 5.4.

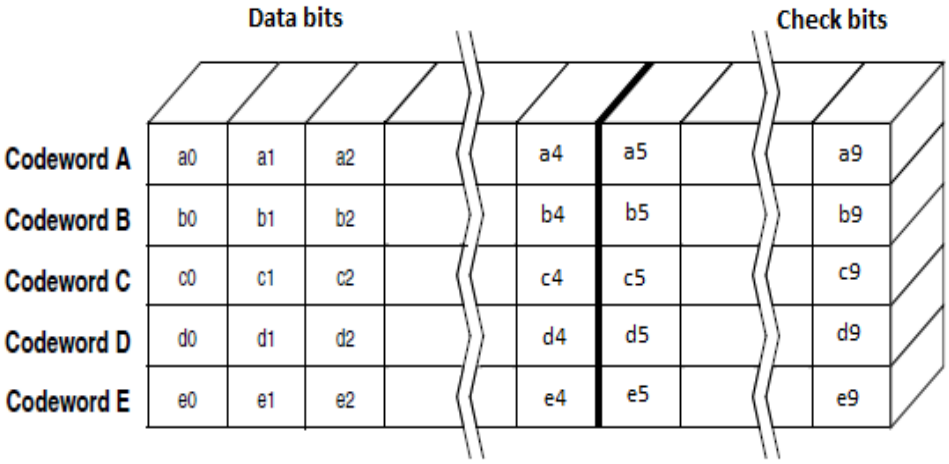


Figure 5.3: Data Bits are Input Row by Row and Output Column by Column

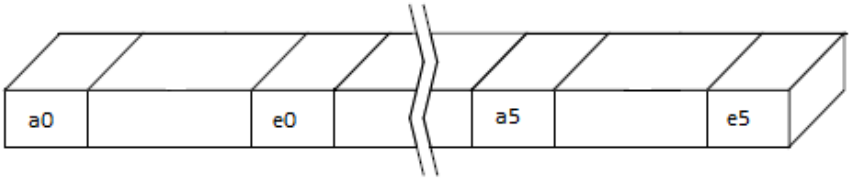


Figure 5.4: Data Bits Output from the Block Interleaver

After encoded data mapped in to different modulation modes to get a complex XFECFRAME. The new DVB - S2 standard allows four modulation modes like QPSK, 8PSK, 16APSK and 32APSK and its constellations point are shown in figure 5.5. Generally QPSK and 8PSK are typically proposed for broadcast applications and 16APSK, 32APSK are mainly targeted to professional applications.

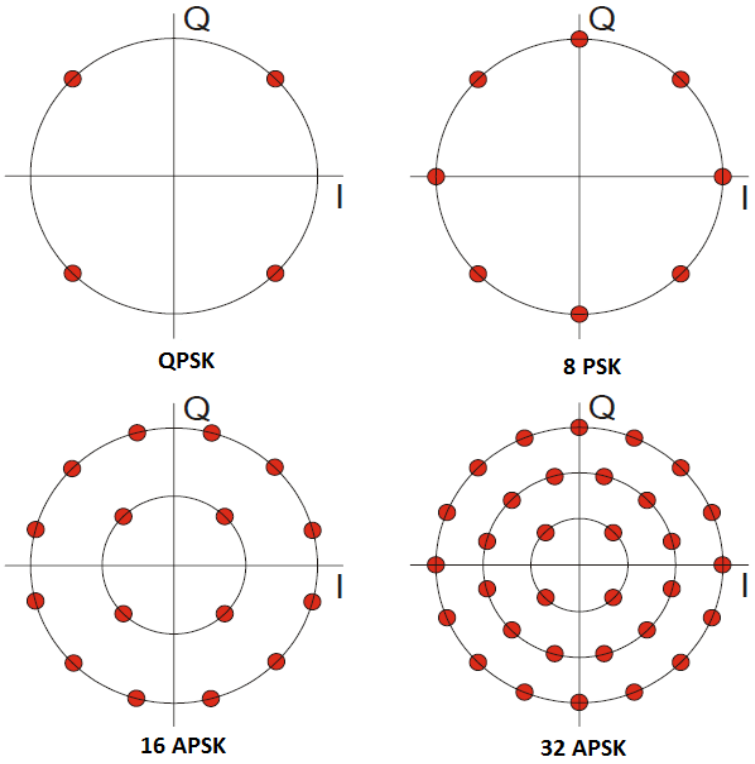


Figure 5.5: DVB - S2 Constellations

Adding pilot signalling information from which the receiver is informed about the coding and modulation parameters of the following payload after decoding. Finally, "Modulation" applies Base-Band Filtering and Quadrature Modulation, to shape the signal spectrum to remove aliasing effect and the up converter will generate the RF signal for transmission to satellite.

5.3 Performance Evaluation of LDPC in DVB-S2

In this section, simulation results are presented that illustrate the BER performance of the DVB - S2 LDPC code. For simulation purpose we set different code rate varies from 1/4 to 9/10 as shown in table 5.1, with QPSK modulation scheme, Normal frame size = 64800, AWGN channel and maximum iteration are limited to 50. Figure 5.6 shows BER performance of normal frame size. At low code rate 1/4, it gives 6.12×10^{-6} BER at 3 dB and at high code rate 9/10, it gives 8.097×10^{-5} BER at 7 dB. At standard code rate 1/2, it gives 2.11×10^{-6} BER at 4 dB which is suitable for broadcasting application.

Table 5.1: Coding parameter for $N_{ldpc} = 64800$

LDPC code rate	BCH uncoded Block K_{bch}	BCH coded Block N_{bch}	BCH t-error correction	LDPC coded Block N_{ldpc}
1/4	16008	16200	12	64800
1/3	21408	21600	12	64800
2/5	25728	25920	12	64800
1/2	32208	32400	12	64800
3/5	38688	38880	12	64800
2/3	43040	43200	10	64800
3/4	48408	48600	12	64800
4/5	51648	51840	12	64800
5/6	53840	54000	10	64800
8/9	57472	57600	8	64800
9/10	58192	58320	8	64800

Figure 5.7 shows BER performance of QPSK and BPSK modulation scheme with a code rate 1/2, and maximum iteration are limited to 50. Both are gives same BER performance at 1 and 0.8 E_b/N_0 respectively. So we analyze that LDPC inner coding performance is within 1dB of the theoretical maximum performance of Shannon's limit, resulting in 2dB to 3dB improvement over the DVB - S standard for given information rate. Figure 5.7 shows that it is impossible for the DVB-S2 codes (without BCH code) to reach the specifications of BER = 10^{-7} of DVB-S2 for given code rate

= 1/2 and E_b/N_0 (dB) = 1dB even for the code length is 64800 bits. If we increase the code length, the BER performance still can not be improved. To overcome this problem MMS algorithm can be used with a shorter block length which is called advanced broadcasting system - satellite.

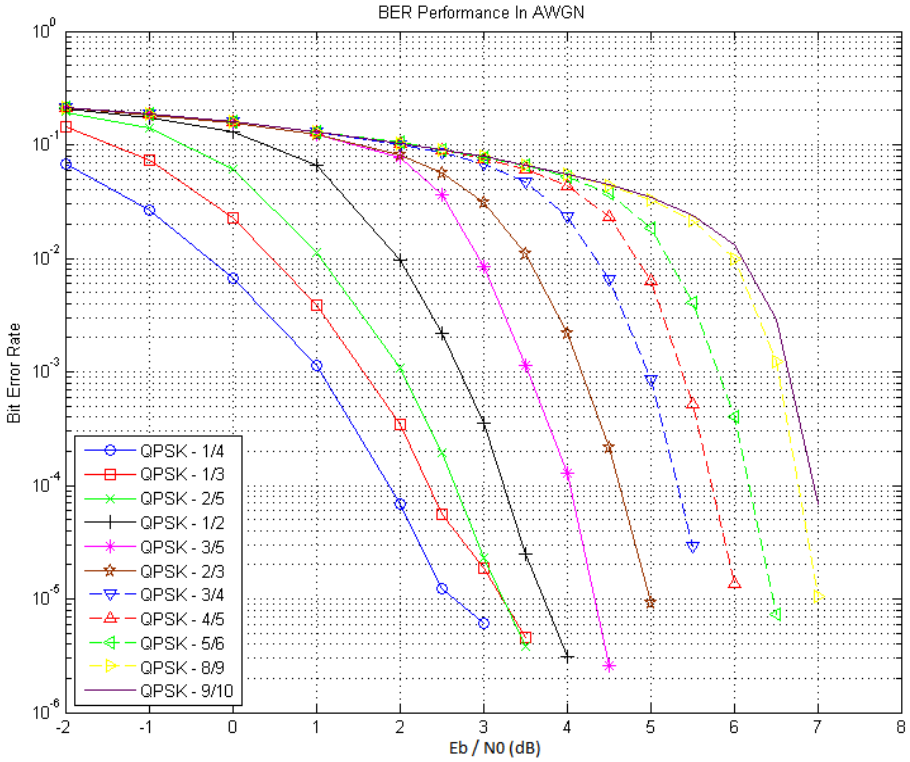


Figure 5.6: BER performance of all code rates using QPSK modulation

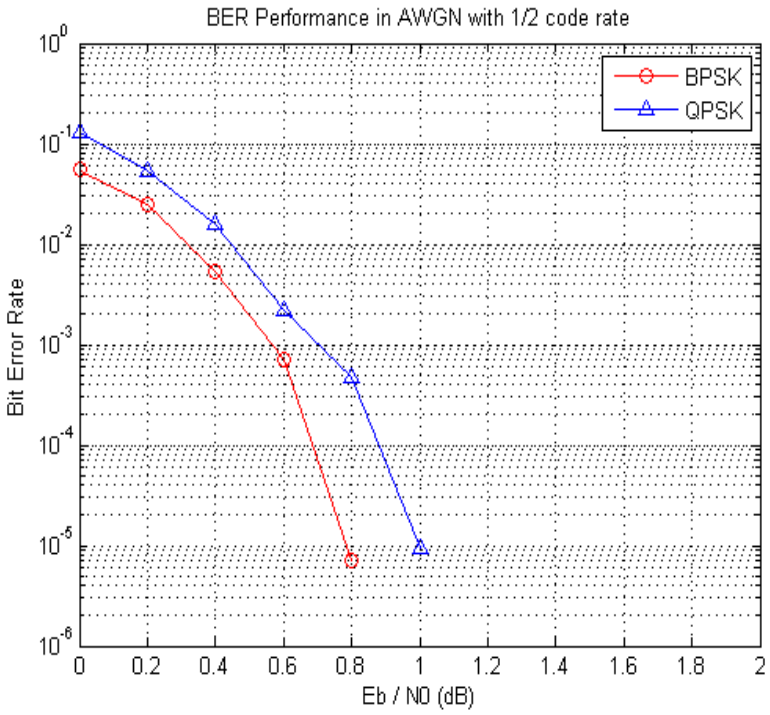


Figure 5.7: Performance of LDPC codes over AWGN channel, N = 64 800 bits

5.4 Advanced Broadcasting System - Satellite

The next generation satellite TV broadcasting system (ABS - S) have better BER performance and lower complexity compared with DVB-S2 system. Under this initiative, we have designed a single LDPC based Advanced Broadcasting System by Satellite [24]. The main purpose of ECC design is to construct LDPC codes with a reduction in transmission power consumption and to lower the error floor to provide satisfactory services [25]. It is capable to support interactive services to consumer IRD, personal computers and other professional service that provides two-way satellite communication devices. The high level function blocks for the ABS - S transmission system are shown in figure 5.8.

The transmission system is defined as a series of functional blocks that take the transport stream or generic packet data as a input, format the signal into FEC blocks, encode each block into coded blocks named codeword with an LDPC encoder, insert synchronization words and other necessary overhead, pulse-shape the packed signal

with an filter and up-convert the signal in to a radio frequency.

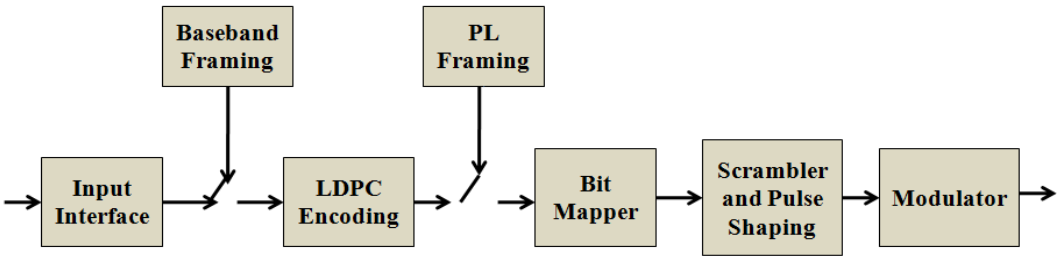


Figure 5.8: Functional block diagram of the ABS - S transmission system

In comparison to the LDPC codes in the DVB - S2 standard, the family of LDPC codes in ABS - S has two advantages [26]. First, the codeword length of the LDPC codes in ABS - S system is much shorter than 64800, and 16200, which are the codeword lengths of the normal and the short LDPC codes in the standard DVB - S2, respectively [27]. It is well known in the ECC area that, the longer the codeword length of an LDPC code, the better the asymptotic performance the LDPC code can offer. Nevertheless the LDPC codes in ABS - S system can provide similar performance as the longer LDPC codes in the DVB - S2 standard. It is also known that, from the application perspective, hardware implementation favors shorter LDPC codes which cause less design trouble and less hardware cost. The second advantage is, the LDPC codes in ABS - S can offer BER lower than 10^{-7}, which is required by video broadcasting application. By contrast, the LDPC codes in the DVB - S2 standard cannot provide BER lower than 10^{-7} by themselves therefore outer BCH codes are concatenated to LDPC code.

In comparison to the existing DVB - S2, ABS - S offers the following advantages:

- No BCH code which reduces the complexity dramatically.
- Low cost implementation due to shorter frame
- Powerful FEC that employs LDPC
- Variable code rates with QPSK/8PSK/16APSK/32APSK modulation for different application
- Support different mode adaptation like ACM, VCM, CCM

5.5 The Proposed MMS Algorithm for ABS - S

The MS algorithm will suffers from performance degradation in terms of bit error rate due to this minimum value. Proposed algorithm based on sub - minimum value which is affected by decoding performance. At each iteration of the proposed algorithm also consists of two phases : (1) updating sub - minimum value, find correction factor (2) update bit node. Instead of using the notation r_i, $E_{j,i}$, $M_{j,i}$ and L_i in min sum algorithm, the proposed modified Min-Sum algorithm use the corresponding notations of λ_n, $\alpha_{m,n}$, $C_{m,n}$, and $L(q)$.

In the proposed algorithm, the likelihood ratio λ_n is first computed for bit nodes, $n = 1, 2, .., N$. The message $C_{m,n} = \lambda_n$ was initialized for each (m, n) satisfying $H_{m,n} = 2$. Based on the message $C_{m,n}$, the minimum values including min_{1st}, min_{2nd} and stored in memory. Based on min_{2nd}, find correction factor $\hat{\gamma}$ according to equation 4.24, and multiplied with $\alpha_{m,n}$. Update the bit node and take the decision. At each iteration update min_{2nd}, according to this correction factor $\hat{\gamma}$ is also updated. The proposed algorithm is summarized in below. Before presenting the algorithm lets introduce this notations:

λ_n	=	LLR of priori message probabilities.
$C_{m,n}$	=	Messages sent from the bit node n to the check node m.
$\alpha_{m,n}$	=	Messages sent from check node m to bit node n.
$\hat{\gamma}$	=	Correction factor.

Initialization: Compute the log likelihood ratio λ_n for each bit nodes *(n=1,2,...,N)* using received data by channel.

Set $C_{m,n} = \lambda_n$ for each *(m,n)* with satisfying $H_{m,n} = 2$.

Phase 1: Check message

Calculate LLR message form connected check node m to bit node n using equation

$$(\alpha_{m,n})_{MS} = \left(\prod_{n \neq n'} sign(C_{m,n'}) \right) min_{n \neq n'} \mid C_{m,n'} \mid \tag{5.1}$$

$$(\alpha_{m,n})_{MMS} = \hat{\gamma}\,(\alpha_{m,n})_{MS} \tag{5.2}$$

Phase 2: Bit message

Updated bit node can be calculated using

$$L(q) = \lambda_n + \sum_{m \in C_n} (\alpha_{m,n})_{MMS} \tag{5.3}$$

Decision: Compute tentative LDPC codeword $y_n \simeq$ sign [L(q)]

$$y_n = \begin{cases} 0 & \text{if sign [L(q)] = 1;} \\ 1 & \text{if sign [L(q)] = -1.} \end{cases}$$

Termination: Repeat this procedure until $H \cdot (y_1, y_2 .... y_n)^T = 0$ or maximum number of iteration otherwise go to Phase 1 and continue with iteration.

5.6 Results and Analysis

For simulation purpose, we set codeword length 64800 for DVB - S2, 15360 for ABS - S with code rate 1/2 and both case we set base matrix which is an identity matrix whose size is 32×32. From figure 5.9 it can be analyze that DVB - S2 gives $4.45 * 10^{-7}$ BER, ABS-S gives $2.32 * 10^{-7}$ BER at 1.4 dB. Results shows that the ABS - S system has shown almost the same BER performance as that of commercial DVB - S2 system, meanwhile, the complexity of the ABS - S system is much lower than that of the DVB - S2 system. Figure 5.9 shows that the proposed method not only offers a better performance but also achieves a lower error floor in the high E_b/N_0 region with a modest increase in computation complexity.

5.7 Computational Complexity

The computational complexity depends on the number of operations involved in decoding a single information bit. It obviously is a function of the average number of

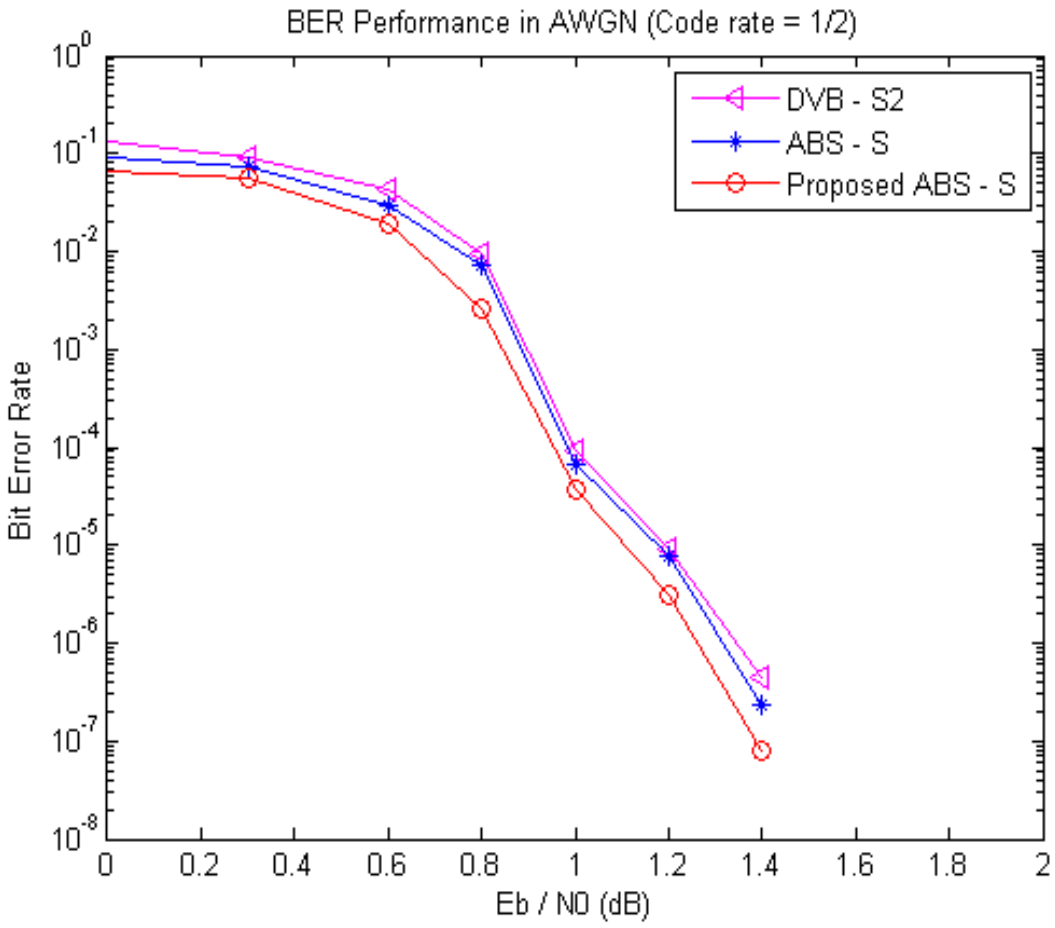


Figure 5.9: Comparison of DVB - S2 and ABS - S and Proposed system

iterations. The average complexity of the decoding process is hence the product of two factors:

- The number of operations per node,
- The average number of iterations

SP algorithm require multiplications and divisions to update the check nodes. In contrast, min sum and proposed min sum algorithm requires additions and subtractions instead of multiplications and divisions for the check node updates. In general, in terms of hardware complexity and delay, both multiplication and division are much more complicated and longer than addition and subtraction [7]. Table 5.2 shows

comparison complexity of different decoding algorithm. Therefore, the proposed algorithm can reduce the computational complexity compared with the existing SP algorithms.

Table 5.2: Comparison of Computational Complexity

Factor	SP algorithm	Min Sum	Proposed Min Sum
tanh and $tanh^{-1}$	2 quantization Table	1 quantization Table	1 quantization Table, 1 correction factor table
Multiplication	α-1	0	0
Division	α	0	0
Addition	0	α-1	α-1
Subtraction	0	α	α

Where α = Represents the number of bit nodes connected to the single check node

5.8 Summary

In this chapter, I have explained application of LDPC code in DVB - S2 standard and presented the performance evaluation of DVB-S2 with employing LDPC codes. Simulation results shows that LDPC code delivers excellent BER performance, which are close to the Shannon limit. It also shows that without BCH code requirement of digital broadcasting system can't be satisfied and with long block length complexity of the decoding algorithm increases.

I have explained transmission system for direct broadcast satellite applications which is called Advanced Broadcasting System for Satellite (ABS-S). It uses only LDPC code with shorter block length and give same BER performance. I have applied MMS algorithm on ABS-S system and the simulation results shows that proposed algorithm gives slightly better performance with reasonable complexity.

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

In this dissertation, I presented a detailed analysis of the LDPC decoding methods like bit flipping and sum product algorithm and showed that sum product (soft) algorithm is more suitable than bit flipping (hard) algorithm. I have also studied 4 cycle remove algorithm which removes 4 cycle from parity check matrix, and improves the decoding performance in terms of BER. LDPC codes are extremely good in terms of the BER performance. If the code length is large $N = 10,000$, for instance, have a BER performance curve is very close to the Shannon limit. But these long block lengths lead to significant decoding delay, and considerable encoding and decoding complexity. Encoding complexity can be reduced by using *LU decomposition* method and decoding complexity can be reduced by using min sum algorithm.

The MS algorithm suffers from performance degradation in terms of bit error rate due to this minimum value. The proposed modification in MS algorithm based on sub - minimum value, calculate a correction factor $\hat{\gamma}$ which includes minimum and sub - minimum value of extrinsic information. For applying correction factor to $E_{j,i}$, the BER performance with short block length LDPC code has improved as compared to

MS algorithm. Simulation results show that the modified min sum algorithm outperforms compare to the SP algorithm and MS algorithm with a reasonable complexity.

I have applied the proposed modified min sum algorithm to ABS-S system and simulation results showed that it achieves better BER performance with a lower error floor in the high E_b/N_0 region. Our proposed modified min sum algorithm have two advantages. First is shorter block length, which cause less design trouble and less hardware cost. Second is without BCH code, LDPC codes in ABS - S can offer BER lower than 10^{-7}, which is required by video broadcasting application.

6.2 Future Scope

There are several areas in LDPC that have the potential for new projects. With some research, it would be possible to write software to create custom size of generic G and H matrices for any application. A comparison of other channel codes with LDPC codes, using different matrices, code rates, and perhaps puncturing, would be an interesting exercise. Obtained codes in this thesis were tested using a single channel model and modulation (AWGN and BPSK). These codes could be applied to other channels and higher modulation for other technologies. Future work is needed, for better BER performance with lower SNR without significantly increasing the computational complexity of proposed algorithm.

Appendix A

Shannon's Limit

An ideal communication system characterized by a given signal to noise ratio $\frac{S}{N}$ and a given bandwidth B is able to perform error free transmission at a rate $R = Blog_2(1 + \frac{S}{N})$. The ideal system as defined by Shannon is shown in below

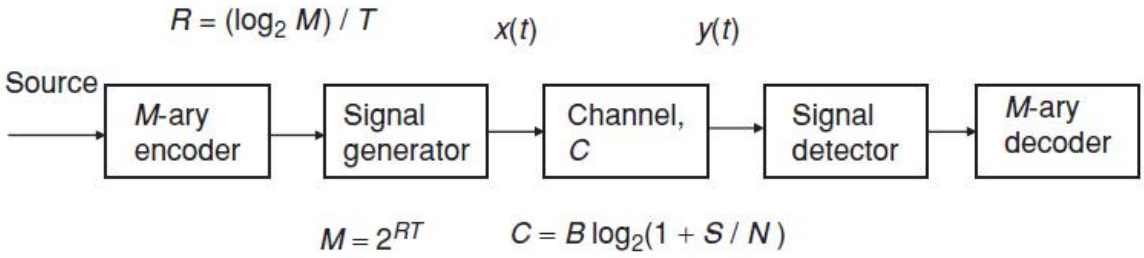


Figure A.1: An ideal Communication System

The source information is provided in blocks of duration T and encoded as one of the M possible signals such that $R = log_2(M/T)$. So $M = 2^{RT}$ signals are possible. The signal y(t) = x(t) + n(t) is the noisy version of the transmitted signal x(t), which is obtained after passing through the band-limited AWGN channel. The Shannon theorem states that

$$\lim_{T\to\infty} \frac{log_2 M}{T} = Blog_2(1 + \frac{S}{N})$$

The transmission rate of the communication system tends to the channel capacity, $R \to C$ the decoding delay, tends to infinity, $T \to \infty$ than expression like that

$C = Blog_2(1 + \frac{S}{N})$ leads to the conclusion that both the bandwidth and the signal - to - noise ratio contribute to the performance of the system, as their increase provides a higher capacity, and their product is constant for a given capacity, and so they can be interchanged to improve the system performance.

For a band - limited communication system of bandwidth B and in the presence of white noise (white noise means PSD of the noise in a channel are constant at all frequencies.), the noise power is equal to N = N0B, where N0 is the power spectral density of the noise in that channel. Then

$$\frac{C}{B} = log_2\left(1 + \frac{S}{N_0 B}\right) \tag{A.1}$$

equivalent expression for the signal - to - noise ratio described in terms of the average bit energy E_b and the transmission rate R, time duration for each bit T.

$$\frac{E_b}{N_0} = \frac{ST}{\frac{N}{B}} = \frac{S}{N}\frac{B}{R}$$

$$\frac{S}{N} = \frac{E_b}{N_0}\frac{R}{B}$$

$$\frac{C}{B} = log_2\left(1 + \frac{E_b}{N_0}\frac{R}{B}\right)$$

If R = C then,

$$\frac{R}{B} = log_2\left(1 + \frac{E_b}{N_0}\frac{R}{B}\right) \tag{A.2}$$

Now take $x = \frac{E_b}{N_0}\ \frac{R}{B}$

$$\frac{R}{B} = log_2\left(1 + x\right)$$

$$\frac{R}{B} = x\left[log_2\left(1 + x\right)^{\frac{1}{x}}\right]$$

If B $\rightarrow \infty$, $\frac{R}{B} \rightarrow 0$

$$\frac{R}{B} = xlog_2 e$$

$$\frac{R}{B} = \frac{E_b}{N_0}\frac{R}{B} log_2 e$$

$$\frac{E_b}{N_0} = \frac{1}{log_2 e}$$

$$\frac{E_b}{N_0} = 0.693$$

$$\frac{E_b}{N_0} = -1.6db \tag{A.3}$$

This value is usually called the Shannon limit. This means that if the ratio E_b/N_0 is kept slightly higher than this value, and use of such a sophisticated coding technique than error-free transmission is possible. from equation A.2

$$\frac{R}{B} = log_2\left(1 + \frac{E_b}{N_0}\frac{R}{B}\right)$$

$$2^{\frac{R}{B}} \leqslant 1 + \frac{E_b}{N_0}\frac{R}{B}$$

$$\frac{E_b}{N_0} \geqslant \frac{B}{R}\left(2^{R/B} - 1\right) \tag{A.4}$$

This Expression shows that R/B (Spectral Efficiency)as a function of the ratio E_b/N_0. Figure A.2 shows that two operating regions, one of practical use and another one of impractical use. For each value of R/B, there exists a different bound, which can be obtained by using this curve.

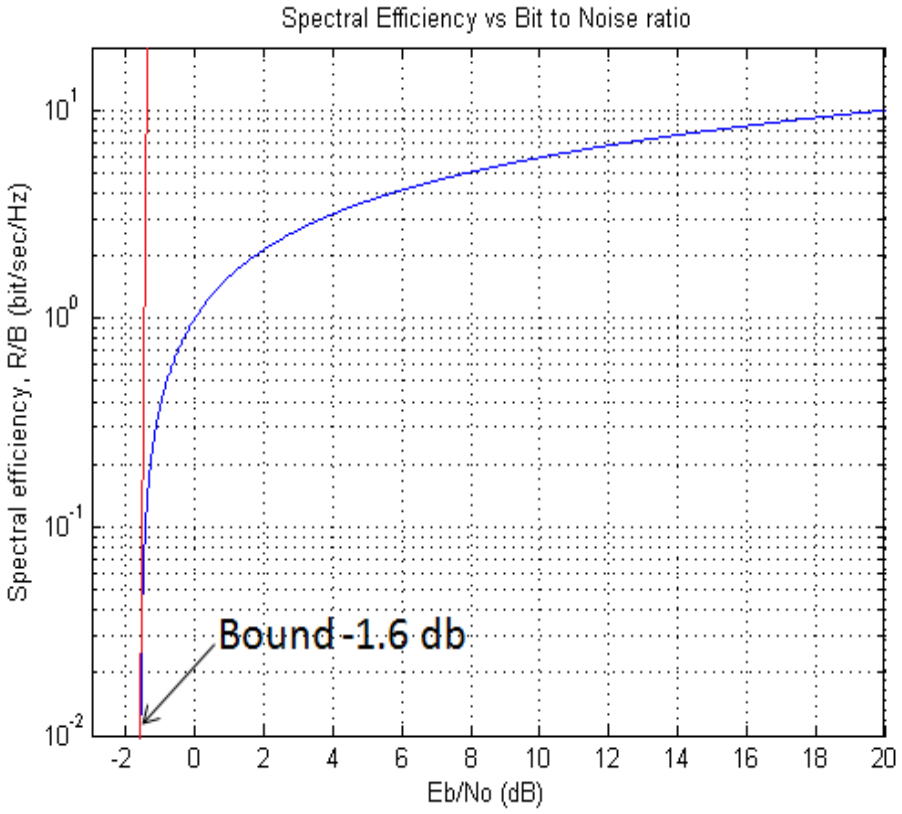


Figure A.2: Practical and non-practical operation regions. The Shannon limit

Appendix B

A Posterior Probability for C_i

Consider a sequence of n independent bits A=$\{a_1, a_2...a_n\}$ with $P_r[a_1 = 1] = P_r$. The probability that a contains an even number of 1_s is

$$\frac{1}{2} + \frac{1}{2}\prod_{r=1}^{n}(1 - 2P_r) \tag{B.1}$$

Proof:

[9] We prove this by induction. If a sequence of n independent bits A=$\{a_1, a_2...a_n\}$ contains an even number of 1_s, the modulo-2 sum of all bits in A, designated as a_n, is 0.

For n = 2, we can have

$$\begin{aligned} P_r\left[A_2 = 0\right] &= P_r\left[a_1 + a_2 = 0\right] \\ &= P_1P_2 + (1 - P_1)(1 - P_2) \\ &= \frac{1}{2} + \frac{1}{2}(1 - 2P_1)(1 - 2P_2) \\ &= \frac{1}{2} + \frac{1}{2}\prod_{r=1}^{2}(1 - 2P_1) \end{aligned} \tag{B.2}$$

Assume that the equation holds for n =L - 1,

$$P_r\left[A_{L-1}=0\right]=\frac{1}{2}+\frac{1}{2}\prod_{r=1}^{L-1}(1-2P_1) \tag{B.3}$$

Then, for n = L , we get

$$\begin{aligned} P_r\left[A_L=0\right] &= P_r\left[A_{L-1}+a_L=0\right] \\ &= \frac{1}{2}+\frac{1}{2}(1-2P_r[A_{L-1}=1])(1-2P_L) \\ &= \frac{1}{2}+\frac{1}{2}(1-2(1-P_r[A_{L-1}=0]))(1-2P_L) \\ &= \frac{1}{2}+\frac{1}{2}\prod_{r=1}^{L}(1-2P_L) \end{aligned} \tag{B.4}$$

Appendix C

$\phi(x)^{-1} = \phi(x)$

Proof :

$$\phi(x) = log\left[\frac{1+e^{-x}}{1-e^{-x}}\right] \tag{C.1}$$

$$\begin{aligned}
\phi(\phi(x)) &= log\left[\frac{1+e^{-\phi(x)}}{1-e^{-\phi(x)}}\right] \qquad \text{(C.2)}\\
&= log\left[\frac{1+e^{loge\frac{1+e^{-x}}{1-e^{-x}}}}{1-e^{loge\frac{1+e^{-x}}{1-e^{-x}}}}\right]\\
&= log\left[\frac{-2e^{-x}}{2}\right]\\
&= log_e^{(-e^{-x})}\\
&= xlog_e^e\\
&= x \qquad \text{(C.3)}
\end{aligned}$$

References

[1] J. C. Moreira and P. G. Farrell, *Essentials Of Error-control Coding*. John Wiley & Sons Ltd, 2006.

[2] R. H. Morelos-Zaragoza, *The Art of Error Correcting Coding*. San Jose State University, USA: A John Willey & Sons, Inc., Publication,2^{nd} edition, 2006.

[3] R. G. Gallager, "Low-density parity-check codes," in *IEEE Transactions on Information Theory*, 1963.

[4] T. K. Moon, *Error Correction Coding*. New Jersey.: A John Willey & Sons, Inc., Publication, 2005.

[5] S. Zhang and Z. Tu, "Overview of ldpc codes," *IEEE* 7^{th} *International Conference on Computer and Information Technology*, 2007.

[6] S. Chung and G. Forney, "On the design of low-density parity-check codes within 0.0045 db of the shannon limit," *IEEE Communication Letter*, Feb 2001.

[7] J. H. Han and M. H. Sunwoo, "Simplified sum-product algorithm using piecewise linear function approximation for low complexity ldpc decoding," *IEEE Transactions On Circuits, Communication And Systems*, 2009.

[8] E. Zimmermann and G. F. Wolfgang Rave, "Forced convergence decoding of ldpc codes exit chart analysis and combination with node complexity reduction techniques," *Vodafone Chair Mobile Communications Systems*, 2007.

[9] D. A. Ramamoorthy, J. Kim, and D. Kline, "Development of rate-compatible structured ldpc code," tech. rep., Georgia Institute of Technology, 2006.

[10] A. E. Maleh, B. Arkasosy, and A. A. Andalusi, "Interconnect - efficient ldpc code design," 2005.

[11] B. W. Chung, "Efficient design of structured ldpc codes," tech. rep., Yonsei University, 2005.

[12] S. K. Bae, "Efficient design of ldpc code using circulant matrix and eira code," tech. rep., Yonsei University, 2004.

[13] O. O. Khalifa and M. Z. Sheroz khan, "Performance evaluation of low density parity check codes," *International Journal of Computer Science and Engineering*, 2008.

[14] R. M. Neal, "Sparse matrix methods and probabilitic inference algorithms," 1999.

[15] D. J. MacKay, *Information Theory, Inference, and Learning Algorithms*. New Jersey.: Cambridge University Press, 2003.

[16] F. Guilloud, "Generic architecture for ldpc decoding," 2004.

[17] S. J. Johnson, "Introducing low-density parity-check codes," (Australia), 2006.

[18] G. A. Malema, "Ldpc code: Construction and implememtation," *IEEE* 7^{th} *International Conference on Computer and Information Technology*, 2007.

[19] J. Zhao and F. Zarkeshvari, "On implementation of min-sum algorithm and its modifications for decoding low-density parity-check (ldpc) codes," *IEEE Transactions On Communications*, April 2005.

[20] H. Jeong and J. T. Kim, "Implementation of ldpc decoder in dvb-s2 using min-sum algorithm," *IEEE Conference on Convergence and Hybrid Information Technology*, 2008.

[21] F. wen, L. Nan, and M. Eroz, "Dvb-s2 low density parity check codes with near shannon limit performance," *International Journal of Satellite Communications and Networking*, 2004.

[22] "Digital video broadcasting (dvb)," tech. rep., European Telecommunications Standards Institute (ETSI), 2005.

[23] Y. Xiao and K. Kim, "Alternative good ldpc codes for dvb-s2," *IEEE International Conference on Signal Processing*, 2008.

[24] S. Yuhai, Liu, and Chunjiang, "A fast encoding method of qc-ldpc code used in abs-s system," *IEEE Pacific-Asia Conference on Circuits,Communications and System*, 2009.

[25] S. Yuhai, L. Chunjiang, and Y. Ming, "The application of ldpc code in abs-s system," *IEEE International Forum on Information Technology and Applications*, 2009.

[26] D. Oh and K. K. Parhi, "Min-sum decoder architectures with reduced word length for ldpc codes," *IEEE Transactions On Circuits And Systems*, Jan, 2010.

[27] J. Ma and R. Lv, "A new generation satellite broadcasting system in china," *IEEE Transactions On Information Theory*, 2008.