FFT based sum product decoding algorithm of LDPC coder for GF(q)

Conference Paper · February 2015

DOI: 10.1109/ET2ECN.2014.7044980

3 authors, including:

Prof Neeta Chapatwala
Sarvajanik College of Engineering and Technology
3 PUBLICATIONS **1** CITATION
SEE PROFILE

Mrugesh r Patel
Sarvajanik College of Engineering and Technology
4 PUBLICATIONS **1** CITATION
SEE PROFILE

FFT based Sum Product Decoding Algorithm of LDPC coder for GF(q)

[1]Jigisha Patel
Teaching Assistant, E & C Department,
Sardar Vallabhai National Institute of Technology,
Surat, Gujarat, India.
jigisha.ptel@gmail.com

[2]Neeta Chapatwala
Associate Professor, E & C Department,
Sarvajanik College of Engineering & Technology,
Surat, Gujarat, India.
neeta.chapatwala@scet.ac.in

[3]Mrugesh Patel
Lecturer, E & C Department,
Sarvajanik College of Engineering & Technology,
Surat, Gujarat, India.
mrugesh11@gmail.com

Abstract- **Low Density Parity Check (LDPC) codes have excellent error correcting performance. LDPC codes are one of the block coding techniques and it performs near Shannon limit and recommended for many practical applications. Non-binary LDPC codes extension of binary LDPC in error correcting property especially for short and moderate block length. In many digital communication systems these codes have strong competitors of turbo codes for error control. Low Density Parity Check as it name is suggests that in a parity check matrix (H) consists of very small number of non-zero elements comparing with zero elements. The strength of the LDPC code defines Parity Check Matrix (PCM). LDPC code contains two types of decoding algorithms hard and soft decision algorithm. By comparing with other traditional decoding algorithm FFT based sum product algorithm reduced computation complexity with better decoding performance. In this paper, LDPC codes for FFT based sum product decoding algorithm performances are analysed for various order of Galois Field GF(q) using AWGN channel. Decoding performance measured in terms of symbol error rate which improve with increasing order of Galois field.**

Keywords - **NB-LDPC, Bit Flipping, FFT based Sum Product Algorithm, AWGN Channel.**

I. INTRODUCTION

Low Density Parity Check (LDPC) codes are excellent error correcting codes that are nearer to Shannon limit with high decoding performance [1]. LDPC codes were first introduced by R.G.Gallager and rediscovered by MacKay in 1996. Davey and Mackay rediscovered that by extending the order of Galois Field GF (q) [2]. This class of codes is known as non-binary LDPC codes. Comparison of binary and non-binary LDPC codes shows that non-binary LDPC codes outperforms binary in terms of decoding performance [2]. But computation complexity increases in non-binary LDPC codes in the design of NB-LDPC architecture comparatively. Hence there is always a trade-off between the decoding performance and computation complexity. LDPC code contains two types of decoding algorithms hard and soft decision algorithm. The hard decision algorithm contains Bit flipping algorithm [11]. Among the decoding algorithm sum product algorithm (SPA) has the better decoding performance [6]. In penalty of the increased multiplication, the computation strength of the decoder is high. To reduce the complexity, Fast Fourier Transform (FFT) based SPA is proposed with nominal decoding performance [7]. The degradation in the decoding performance with the FFT-SPA can be compensated with the PCM structures.

Performance of binary LDPC code is degraded when the code word length is small or moderate. LDPC codes designed over Galois Field GF (q>2) (also known as non-binary LDPC codes) have shown great performance for these cases. But decoding complexity increases with q which makes the use of non-binary LDPC (NB-LDPC) codes [10].

Organization of this paper is as follows: Section I contains the introduction of LDPC coder. Section II contains representation of LDPC coder. Section III contains Decoding algorithm of LDPC coder. Section IV contains results and analysis of LDPC coder for different order of Galois field. Section V contains Conclusion.

II. REPRESENTATION OF LDPC CODER

NB-LDPC codes are a class of linear block codes whose parity check matrix H contains a small fixed number of non-zero elements in its columns and rows.

A) Matrix Representation

A low-density parity-check code is a linear block code given by the null space of an M×N parity-check matrix H. The number of non-zero elements in its column and row referred to as column weight (W_c) and row weight (W_r) respectively. A regular LDPC code is a linear block code whose parity-check matrix H has column weight W_c and row weight W_r , where $r = W_c (n/m)$ and $W_c << m$. If H is low density, but its row and column weight are not both constant, then the code is an irregular LDPC code [4]. Almost all LDPC code constructions impose the following additional structural property on H no two rows (or two columns) have more than one position in common that contains a nonzero element. This property is called the row and column constraint, or simply, the RC constraint.

978-1-4799-6986-9/14/$31.00©2014 IEEE

The construction of LDPC codes usually involves the construction of H, which need not be full rank. In this case, the code rate R [3] for a regular LDPC code is bounded as

$$R \geq 1 - \frac{m}{n} = 1 - \frac{\mathrm{Wc}}{\mathrm{Wr}} \qquad (1)$$

B) Graphical Representation

The Tanner graph of an LDPC code is analogous to the trellis of a convolution code in that it provides a complete representation of the code and it aids in the description of decoding algorithms. A Tanner graph is a bipartite graph whose nodes may be separated into two types are the variable nodes (or code-bit nodes) and the check nodes (or constraint nodes), which is denote by VNs and CNs respectively [2]. If the block length is N then H characterizes an (N, W_c, W_r) code. If the message vector m is a Kx1 vector and codeword C is an Nx1 vector so the generator matrix G is NxK and the parity check matrix H is (N-K)xN. The equation $H^TC = 0$ is said to be a linear parity check constraint on the codeword C. Elements in H-matrix is defined by order of Galois Field GF (q)[6]. For example a non-binary LDPC code over GF(4) consists of elements of the set {0, 1, 2, 3} in its H-matrix. The graphical representation of the H-matrix is shown in Figure 1, which is called as bipartite graph or tanner graph.

$$\mathrm{H} = \begin{bmatrix} 2 & 0 & 1 & 2 & 0 & 1 \\ 3 & 2 & 0 & 1 & 1 & 0 \\ 0 & 2 & 3 & 0 & 3 & 1 \end{bmatrix} \qquad (2)$$

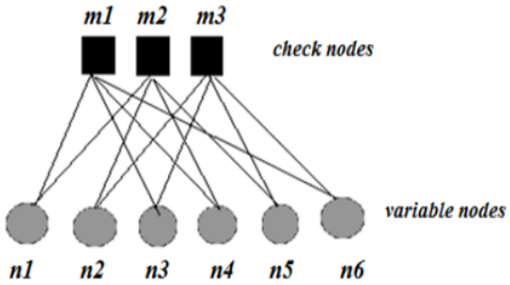

Figure II. An Example of parity check matrix H over GF(4) and its corresponding Tanner Graph [2]

The first set N nodes are called as variable nodes. The second set M nodes called check nodes, representing the parity constraints. The graph has an edge between the n^{th} variable node and the m^{th} check node if and only if n^{th} variable is involved in the m^{th} check, i.e. $H_{mn} = 1$. This representation of the code gives an underlying structure that facilitates the application of the sum product decoding algorithm (SPA).

III. DECODING ALGORITHM OF LDPC CODER

LDPC contains hard decision (Bit Flipping) [11] and soft decision (FFT based SPA) algorithm. FFT based Sum product algorithm which is basically soft decoding algorithm is explain for different order of GF(q).

The generator matrix G^T is developed from the parity check matrix H such that $H\ G^T = 0$. The generator matrix G helps in encoding the information to be transmitted (x). This encoding process produces the codeword y .i.e. $y = G^Tx$. The codeword y is modulated using different modulation technique resulting in t vector. This t vector is sent out over an AWGN channel which adds white noise (η), yielding a received vector r given by Equation (3).

$$r = t + \eta \qquad (3)$$

The channel reliabilities are calculated with this received vector r. The decoding of the codeword is done with these channel reliabilities and parity check matrix.

Factor graph is almost same as tanner graph has two different nodes which are the variable nodes (v-node) and the check nodes (c-node). Each row of a parity check matrix H is to match each check node of factor graph and each column of a parity check matrix H is to match each variable node of Factor graph. Check node i is connected to neighbour variable node j when h_{ij} in H is assigned to 1. Otherwise, it is not connected; the value of this element is 0. Therefore, n variable nodes and m = n-k check nodes are existed in a parity check matrix H and are matched to Factor graph[9] which shown in Figure 2.

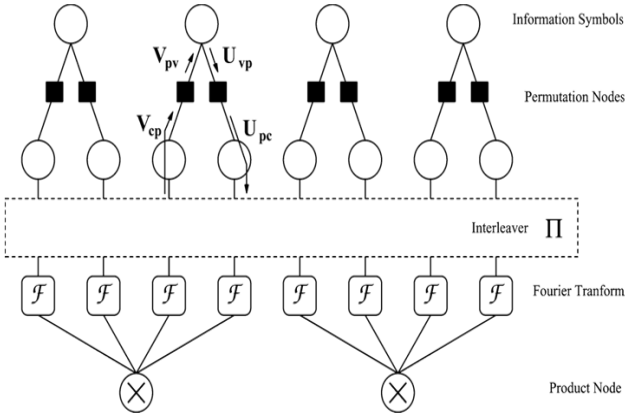

Figure 2. Factor graph of an LDPC code over GF(q)[9]

The decoding process of FFT based SPA and its notations are given below:

1) Initialization

Variable nodes are initially assigned with the channel reliabilities which are calculated using the received vector [8].

2) Permutation Step

Each coded symbol has q likelihoods associated with it. When the coded symbol is multiplied by a non-binary parity check element one can compensate for this by cyclically shifting downwards this column vector of likelihoods, with the exception of the first likelihood, corresponding to the probability of the coded symbol being zero. The number of cyclic shifts is equal to the power of the primitive element that is multiplied with the coded symbol. This cyclic shift of the likelihoods is known as a permutation.

3) Horizontal Step

This step is also known as horizontal update [8]. Each check node m is updated using the channel reliability messages from adjacent variable nodes except this check node m.

$$r_{mn}(x) = F^{-1}\left(\prod_{n\in\frac{Nm}{n}} F(q_{mn'}(x))\right) \quad (4)$$

Where F is the Fourier transform and F^{-1} is the inverse Fourier transform.

3) Depermutation Step

The inverse of a permutation is a depermutation, where the likelihoods are cyclically shifted upwards, again with the exception of the first likelihood.

4) Vertical step

This step is also known as vertical update [8]. A variable node receives messages from check node. Adjacent check node's messages are utilized for updating a variable node n. By using below equation one can find message transfer from the check node to variable node.

$$q_{mn}(x) = \beta_{mn} f_n^x \prod_{Mn/m} r_{m'n}(x) \quad (5)$$

Where β_{mn} is a normalizing constant such that $\sum q_{mn}(x) = 1$, that is

$$\beta_{mn} = \frac{1}{\sum_x f_n^x \prod_{Mn\setminus m} r_{m'n}(x)} \quad (6)$$

The $q_{mn}(x)$ are placed in the matrix Q Where each element in the parity check matrix has a corresponding 1× 4 column vector containing the probabilities $q_{mn}(0)$, $q_{mn}(1)$,$q_{mn}(2)$ and $q_{mn}(3)$. In this step, the pseudo posterior probabilities $q_n(x)$ are also determined by

$$q_n(x) = \beta_{mn} f_n^x \prod_{m\in Mn} r_{mn}(x) \quad (7)$$

Where again β_n is a normalizing constant such that $\sum q_n(x) = 1$. The pseudo posterior Probabilities are place in a matrix Q

$$C_n = \arg max\, \beta_{mn} f_n^x \prod_{m\in Nm} r_{mn}(x) \quad (8)$$

From these pseudo posterior probabilities estimates of the transmitted code word can be found by above equation.

4) Tentative decoding

The most likely value of code word is computed with the initial channel reliabilities and variable nodes messages. The decoded codeword is valid only if it satisfies $HC^T=0$. When it is satisfied, the decoding algorithm is halted.

IV. RESULTS AND ANALYSIS

LDPC code contains Hard decision (Bit flipping) and Soft decision (FFT based Sum Product) algorithms. Simulation for Hard and Soft decision algorithm carried out for both binary and non binary data with different order of galois field as an input. Block diagram of simulation process is shown in Figure 3.

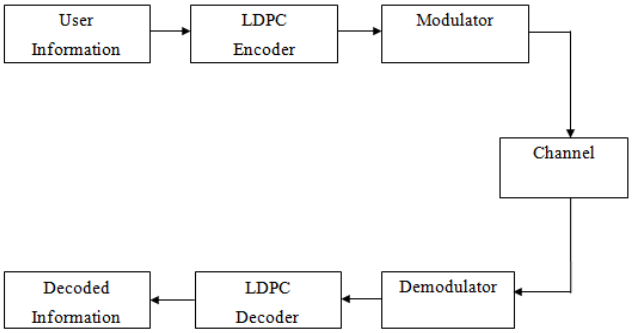

Figure 3 Block diagram of simulation process

The encoder for a LDPC divides the information sequence into message blocks of k information bits each. A message block is represented by the binary or non binary k-tuple u = $(u_0,u_1,\ldots,u_{k-1})$ called a message. There are a total of 2^k different possible messages. The encoder transforms each message u independently into an n-tuple v = $(v_0,v_1,\ldots,v_{n-1})$ of discrete symbols called a codeword. Encoder may encodes the user information and generate codeword. This codeword is transmitted over AWGN channel using different modulation technique. Due to AWGN channel noise is introduce with information carrying signals which pass on demodulator. At receiver decoding process is done using FFT based SPA decoding algorithm. LDPC decoder used to correct or detect errors in received vector.

Simulation of Bit Flipping and FFT based sum product algorithm with irregular (508, 1016) LDPC codes with codeword length is 1016 and code rate is 0.5 are implemented. The simulations are performed over an additive white Gaussian noise (AWGN) with BPSK modulation.

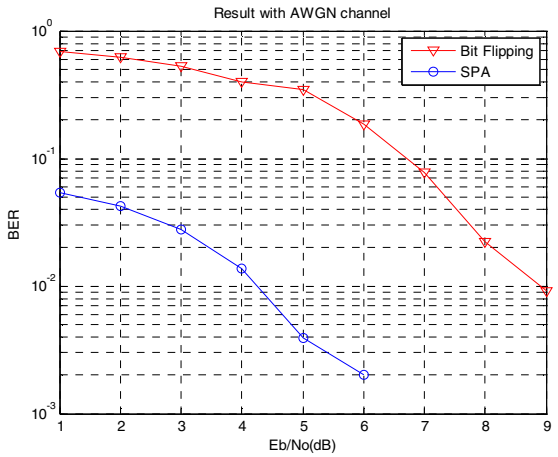

Figure 4 Simulation result for BF and SPA algorithm for AWGN channel

BER Performance for FFT based Sum Product Algorithm and Bit Flipping Algorithm is implemented for GF(2) using AWGN channel environment. It is observed that BER performance of the FFT based Sum Product Algorithm is better in comparison with Bit Flipping Algorithm.

Detail of simulation parameters used for simulate FFT based SPA algorithm of NB-LDPC are shown in Table 1.

Table 1 Simulation Parameters

Size of Parity Check matrix(n,k)	(648, 324)
Order of Galois Field	GF(4),GF(8) and GF(16)
Channel	AWGN
Software used	MATLAB R2009a

Decoding results for FFT based SPA (Probability Domain) are carried out at different E_s/N_o (e.g. 5dB and 6dB) for GF (4), GF(8) and GF(16) with additive white Gaussian noise (AWGN) channel. The results for the same are shown in Figure 5.

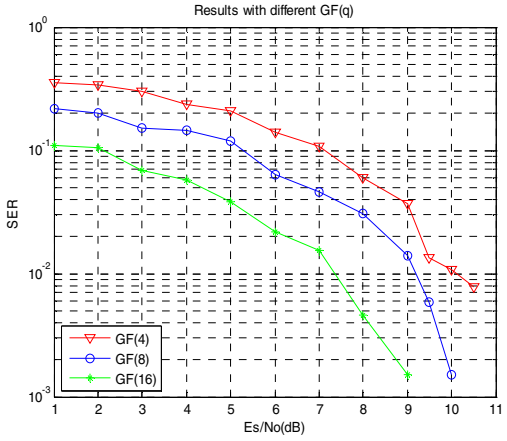

Figure 5 SER Vs SNR for Different order of Galois Field for FFT-SPA decoding algorithm

FFT-SPA decoding algorithm is evaluated for the different Galois field. From the result we can say that if the order of the Galois field is increases SER performances of LDPC is improve. Non Binary Low Density Parity Check code gives high performance compare with binary LDPC.

V. CONCLUSION

FFT Sum Product Algorithm gives better BER performance in comparison with Bit flipping Algorithm. Performance of Non Binary Low Density Parity Check code gives high-quality in terms of symbol Error Rate (SER) at low SNR values. Decoding process is carried out with Probability Domain Sum Product Algorithm (Soft Decision based). It can be seen from SER curves that FFT based Sum Product Algorithm works better in lower SNR region. By increases the order of the Galois field of non binary LDPC coder SER performances is improve but decoding complexity increases with GF(q).

ACKNOWLEDGMENT

I am really thankful to my guide without which the accomplishment of the task would have never been possible. I am also thankful to all other helpful people for providing me relevant information and necessary clarifications.

REFERENCES

[1] M. C. Davey, "Error correction using low density parity check codes." Cambridge, U. K. Univ. Cambridge, 1999.

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

[3] M.C. Davey, D.J.C. Mackay, "Low density parity check codes GF (q)," IEEE Communication Letters, vol. 2, no. 6, pp.165-167, June 1998.

[4] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message passing decoding," IEEE Trans. Inform. Theory, vol. 47, pp. 599 – 618, 2001.

[5] Sanae El Hassani, Marie-Helene Hamon and Pierre P´enard "A Comparison Study of Binary and Non-Binary LDPC Codes Decoding", IEEE Trans. International Conference,pp.355 – 359, 2010.

[6] Adrian Voicila, David Declercq, François Verdier, Marc Fossorier, and Pascal Urard. "Low-Complexity Decoding for Non-Binary LDPC Codes in High Order Fields" IEEE transactions on communications, vol.58, no. 5,pp.1365,1375,may 2010.

[7] Safarnejad, L, Sadeghi, M.-R., "FFT Based Sum-Product Algorithm for Decoding LDPC Lattices," IEEE Communications Letters, vol. 16, no.9, pp.1504,1507, September 2012.

[8] Haili Hong, Zhuo Sun, "An Improved Decoding Algorithm of Non binary LDPC Code", IEEE Trans. International Conference, vol.3, pp.104 - 107, 2011.

[9] David declercq, marc fossorier, fellow, "Decoding algorithms for non binary ldpc codes over gf(q)," IEEE transactions on communications, vol. 55, no. 4,pp.633,643, april 2007.

[10] Gabi Sarkis, Student Member, IEEE, Saied Hemati, Senior Member, IEEE, Shie Mannor, Senior Member,IEEE,and Warren J. Gross, Senior Member, IEEE, "Stochastic Decoding of LDPC Codes over GF(q)" IEEE transactions on communications, vol. 61, no. 3, march 2013.

[11] D. Burshtein, "On the error correction of regular LDPC codes using the Bit flipping algorithm," IEEE Trans. Inf. Theory, vol. 54, no. 2, pp.517–530, Feb. 2008.