DOI: 10.21917/ijct.2011.0056

CONSTRUCTION OF REGULAR LDPC LIKE CODES BASED ON FULL RANK CODES AND THEIR ITERATIVE DECODING USING A PARITY CHECK TREE

H. Prashantha Kumar[1], U. Sripati[2] and K. Rajesh Shetty[3]
Department of Electronics and Communication Engineering, National Institute of Technology Karnataka, India
E-mail: [1]hprashanthakumar@gmail.com, [2]sripati_acharya@yahoo.co.in and [3]krshetty_nitte@yahoo.com

Abstract

Low density parity check (LDPC) codes are capacity-approaching codes, which means that practical constructions exist that allow the noise threshold to be set very close to the theoretical Shannon limit for a memory less channel. LDPC codes are finding increasing use in applications like LTE-Networks, digital television, high density data storage systems, deep space communication systems etc. Several algebraic and combinatorial methods are available for constructing LDPC codes. In this paper we discuss a novel low complexity algebraic method for constructing regular LDPC like codes derived from full rank codes. We demonstrate that by employing these codes over AWGN channels, coding gains in excess of 2dB over un-coded systems can be realized when soft iterative decoding using a parity check tree is employed.

Keywords:

LDPC Codes, Full Rank Codes, Conjugacy Class, Transform Domain Components Parity Check Tree, Soft Iterative Decoding

1. INTRODUCTION

Error control coding (ECC) is commonly used to achieve reliable transmission of information. Channel codes enable a decoder to recover from errors produced by noise in a communication channel. Codes ensure higher noise tolerance at the receiver by adding redundancy into the user data to achieve better separation of data sequences. ECC algorithms have constituted a significant enabler in the telecommunications revolution, the internet, digital recording and space exploration. The past decade has seen tremendous growth in availability and deployment of wireless services. This has been made possible by development of powerful signal processing algorithms to ensure efficient spectral usage/ error free communication as development of hardware platform on which these algorithms could be run. Thus developments in algorithm design and microelectronics have gone hand in hand to create the infrastructure for the information revolution that has transformed the way in which human beings live and work [1]. According to the manner in which redundancy is added to messages, error correcting codes can be divided into two classes: Block and Convolutional. Block codes implement a one-to-one mapping of a set of K information symbols on to a set of N code symbols. We call this code as a (N, K) linear block code. The $R = N - K$ symbols in a codeword are a function of the information symbols, and provide redundancy that can be used for error correction and/or detection purposes. The minimum distance d_{min} of a block code $\mathbf{C}$ is the smallest Hamming distance between any two codewords in the code.

However the Hamming metric is not always well suited to the characteristics of real channels. Consequently, metrics like the Lee metric [2] and the rank-metric [3, 4] have been introduced by different authors.

LDPC codes belong to the general class of linear block codes and can be described by parity check and generator matrices. Gallager first proposed LDPC codes and iterative decoding algorithm in 1962 [5]. Surprisingly, these codes were nearly forgotten for almost three decades. By the end of last century, with the extensive research on "turbo-like" codes and on iterative detection, LDPC codes re-emerged as another category of random codes approaching the Shannon capacity limit with practical decoding complexity. Unlike "structured" codes such as the Hamming code, the parity check matrix H for an LDPC code is sparse (a small portion of the entries being one, all others being zero) and the positions for the '1's are selected at random. The good performance of the LDPC codes results from the randomness in the parity check matrix. LDPC codes with uniform or nearly uniform column weights and row weights are referred to as the "regular" LDPC codes, while codes with non-uniform column weights and row weights are referred to as the "irregular" LDPC codes [6]. The decoding complexity of LDPC codes is proportional to the column weight of the parity check matrix, and is usually lower than that of a turbo code.

The study of LDPC codes is very important as they are fast becoming one of the most popular coding schemes for a number of future applications in wireless communications and magnetic storage. The approaching fourth-generation (4G) wireless systems are promising to support very high data rates from 100Mbps to 1Gbps. High performance LDPC codes are employed in many 4G wireless standards such as IEEE 802.16e WiMax, IEEE 802.20, IEEE 802.3an (10 GBase-T Ethernet), DVB-S2 (satellite transmission of digital television) and 3GPP Long Term Evolution (LTE) networks. Several potential advantages can be listed for LDPC codes over their strong competitor turbo codes. In a very natural way, the decoder declares a decoding failure when it is unable to correctly decode, where as turbo decoders must perform extra computations for a stopping criterion. Also, LDPC codes of almost any rate and block length can be created simply by specifying the shape of the parity check matrix, while the rate of turbo codes is governed largely by a puncturing scheme, so flexibility in rate is obtained only through considerable design effort. As an additional boon on the commercial side, LDPC codes are not patent protected [7].

In this paper, we discuss the design of full rank codes using the transform domain characterization of cyclic codes and then derive regular LDPC like codes from this construction. The soft iterative decoding of these codes is performed by using a parity check tree obtained from the Tanner graph. Coding gain of more than 2dB is observed for these codes over AWGN channel compared to un-coded systems. These codes can achieve

reasonable coding gain at very low SNR for big block size and large minimum distance.

2. CONSTRUCTION OF REGULAR LDPC LIKE CODES

Linear codes comprising of m x n matrices over the finite field F_q were studied by Roth [8] to facilitate correction of criss-cross type of errors, i.e. errors in which a certain number of rows or columns have been erroneously received. Let C be a (N, K) linear code over F_{q^m}. For any pair of codewords, c,c'∈C, the Rank-distance between them is defined to be the rank over F_q of the m x n matrix corresponding to **c** – **c'** as an m-tuple along a basis of F_{q^m} over F_q. This is denoted by $Rank_q$(c – c'). The rank weight of a code vector **c** over F_{q^m} is defined to be the rank of the corresponding m x n matrix over F_q obtained by expanding each entry of **c** as an m-tuple along a basis of F_{q^m} over F_q [9].

Example 1: As an example, let us consider the following 7-tuple over F_{2^3}, **c** = [1, α^6, α^3, α^2, α^5, α, α^4] where α is a primitive element of F_{2^3} generated by primitive polynomial $x^3 + x + 1$. The rank of **c** is the F_2 rank of the 3 x 7 matrix,

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

with entries from F_2 obtained by expanding each entry of **c** as a 3-tuple along a basis of F_{2^3} over F_2.

A linear code over F_q, (q is a power of a prime p) is closed under addition and multiplication with elements of F_q. Further, the code is said to be cyclic if a cyclic shift of every codeword yields another codeword of the code. Let **a** = (a_0, a_1, a_2,…..,a_{n-1})∈ $F_{q^m}^n$ and gcd(n, q) = 1. Let n be the positive integer such that $n|q^m - 1$, and $\alpha \in F_{q^m}$ be an element of order n The Discrete Fourier Transform (DFT) of **a** is defined to be the vector, A = (A_0, A_1, A_2,…..,A_{n-1})∈ $F_{q^m}^n$ given by,

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i,\ j = 0,1,2,....,n-1 \qquad (1)$$

The inverse Discrete Fourier Transform (IDFT) is defined by,

$$a_i = \frac{1}{n \bmod p} \sum_{j=0}^{n-1} \alpha^{-ij} A_j, i = 0,1,2,.....,n-1. \qquad (2)$$

The vectors a and A will be referred to as the time domain and corresponding transform domain vector respectively. Let I_n={0,1,….,n – 1}. For any $j \in I_n$, and for any divisor d of m, the q^d -cyclotomic coset of j mod n is defined to be the set,

$$[j]^d = \{i \in I_n \mid j = iq^{dt} \bmod n \text{ for some } t \geq 0\}. \qquad (3)$$

The cardinality of this set is denoted by $e_j^{(d)}$, where d = 1, we will denote the q-cyclotomic coset of j mod n by [j] and it's cardinality by e_j. By the term "cyclotomic coset", we mean q-cyclotomic coset j mod n. If $J \subseteq$ [0, n – 1], we write $[J]^d = \cup_{j \in J}[j]^d$.

Example 2: Suppose n = 15 and q = 2. I_{15}={0,1,2,….,14}. Then the q-cyclotomic coset of $j$mod15 where j∈[0,14] are listed below.

[0]={0}	[1]={1,2,4,8}	[3]={3,6,12,9}	[7]={7,14,13,11}	[5]={5,10}

We consider cyclic codes of length n over F_{q^m}, $n|q^m - 1$, $m \leq n$ as m x n matrices over F_q. Given a description of the code in the transform domain, (i.e. a listing of the free transform components and all other transform components constrained to zero), we can determine the exact rank or an upper bound on the rank of the corresponding code. Now consider the case where the cyclic code is characterized by a single free transform component. The following theorem gives the rank of such codes [10].

Theorem 1: Let C be a cyclic code of length $n|q^m - 1$ over F_{q^m} such that the transform domain component $A_{jq^s} \in A[j]$, ($|[j]| = e_j$, $0 \leq s \leq e_j - 1$) is free and all other transform components are constrained to zero. Then $Rank_q$(C) = e_j. In other words, for a length $n|q^m - 1$ cyclic code over F_{q^m}, with a single non zero transform component in only one q^m cyclotomic coset, the rank of the code is equal to the size of the q-cyclotomic coset to which the free transform component belongs. The proof is given in [11].

The following example illustrates Theorem 1.

Example 3: Consider the (7, 1) code over F_{2^3} characterized by free transform component A_1. The remaining transform components are constrained to zero. We list in Table.1, 7 codewords have F_2 rank equal to 3.

Table.1. Codewords corresponding to Example 3

A_1	a_0	a_1	a_2	a_3	a_4	a_5	a_6	Matrix Form	F_2-Rank
1	100	101	111	011	110	001	010	$\begin{pmatrix}1&1&1&0&1&0&0\\0&0&1&1&1&0&1\\0&1&1&1&0&1&0\end{pmatrix}$	3
α	010	100	101	111	011	110	001	$\begin{pmatrix}0&1&1&1&0&1&0\\1&0&0&1&1&1&0\\0&0&1&1&1&0&1\end{pmatrix}$	3
α^2	001	010	100	101	111	011	110	$\begin{pmatrix}0&0&1&1&1&0&1\\0&1&0&0&1&1&1\\1&0&0&1&1&1&0\end{pmatrix}$	3
α^3	110	001	010	100	101	111	011	$\begin{pmatrix}1&0&0&1&1&1&0\\1&0&1&0&0&1&1\\0&1&0&0&1&1&1\end{pmatrix}$	3
α^4	011	110	001	010	100	101	111	$\begin{pmatrix}0&1&0&0&1&1&1\\1&1&0&1&0&0&1\\1&0&1&0&0&1&1\end{pmatrix}$	3
α^5	111	011	110	001	010	100	101	$\begin{pmatrix}1&0&1&0&0&1&1\\1&1&1&0&1&0&0\\1&1&0&1&0&0&1\end{pmatrix}$	3
α^6	101	111	011	110	001	010	100	$\begin{pmatrix}1&1&0&1&0&0&1\\0&1&1&1&0&1&0\\1&1&1&0&1&0&0\end{pmatrix}$	3

Let us stack individual full rank matrix shown above to obtain a Gallager parity check matrix H_{GA}.

$$H_{GA} = \begin{bmatrix}1&1&1&0&1&0&0\\0&0&1&1&1&0&1\\0&1&1&1&0&1&0\\0&1&1&1&0&1&0\\1&0&0&1&1&1&0\\0&0&1&1&1&0&1\\0&0&1&1&1&0&1\\0&1&0&0&1&1&1\\1&0&0&1&1&1&0\\1&0&0&1&1&1&0\\1&0&1&0&0&1&1\\0&1&0&0&1&1&1\\0&1&0&0&1&1&1\\1&1&0&1&0&0&1\\1&0&1&0&0&1&1\\1&0&1&0&0&1&1\\1&1&1&0&1&0&0\\1&1&0&1&0&0&1\\1&1&0&1&0&0&1\\0&1&1&1&0&1&0\\1&1&1&0&1&0&0\end{bmatrix}^T \quad (4)$$

It is observed that the row weight and column weight of this matrix are uniform. Further, Gallager parity check matrices H_{GA} computed for the (15, 1) and (31, 1) cyclic codes over F_{2^4} and F_{2^5} by taking one free transform domain component from a full size conjugacy class respectively possess uniform row weight and column weight.

We list in Table 2, row weight and column weight of parity check matrix H_{GA} for these codes.

Table.2. Comparison of code parameters

H_{GA} obtained from (7,1) full rank code over F_{2^3}	Column Weight =4	Row Weight = 12
H_{GA} obtained from (15,1) full rank code over F_{2^4}	Column Weight =8	Row Weight = 32
H_{GA} obtained from (31,1) full rank code over F_{2^5}	Column Weight =16	Row Weight = 80

By checking the linear independency, we can derive parity check matrix H from H_{GA}. Once a parity check matrix H is constructed, Gaussian elimination and re-ordering of columns turn the original H into a systematic form, from which the generator matrix G can be easily constructed.

3. DECODING USING A PARITY CHECK TREE

We have observed that H_{GA} exhibits regular LDPC like structure. Associated with a parity check matrix H is a graph called the Tanner graph containing two set of nodes. The first set consists of *N* nodes which represent the *N* bits of a codeword; nodes in this set are called bit nodes. The second set consists of *M* nodes, called check nodes, representing the parity constraints. The graph has an edge between j^{th} bit node and the i^{th} check node if and only if j^{th} bit is involved in the i^{th} check, that is, if H_{ij} = 1. Thus the Tanner graph is a graphical depiction of the parity check matrix [12]. Fig.1 illustrates the Tanner graph for parity check matrix H, derived from H_{GA} given in Eq.(4). The leitmotiv here is soft decoding of regular LDPC like codes described through graphical structures. A graph such as this, consisting of two distinct sets of nodes and having edges only between the nodes in different sets, is called a bipartite graph (or Tanner graph). The Tanner graph is used to develop insight into the decoding algorithm. The iterative soft decoding algorithm to decode LDPC like codes using a parity check tree associated with the Tanner graph is explained below.

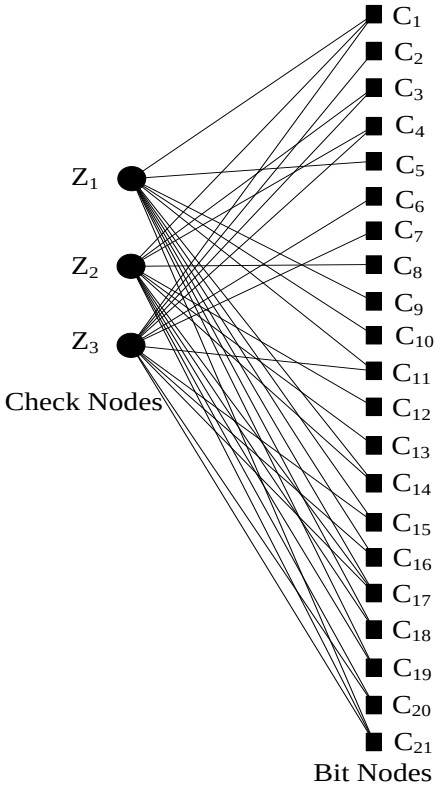

Fig.1. Tanner graph for parity check matrix H

For each code bit c_n, compute the checks for those checks that are influenced by c_n. To do this, we propagate probabilities through the Tanner graph, there by accumulating the evidence that the checks provide about the bits. Suppose that c_n is in error and that other bits influencing its checks are also in error. Let arrange the Tanner graph with c_n as a root shown in Fig.2. This arrangement of Tanner graph is called a parity check tree. The situation is particularly simple if the graph is a tree, i.e. it is connected, but if any one edge is removed, the graph is no longer connected, in particular a tree has no circuits (A closed path containing at least one edge is called a circuit).

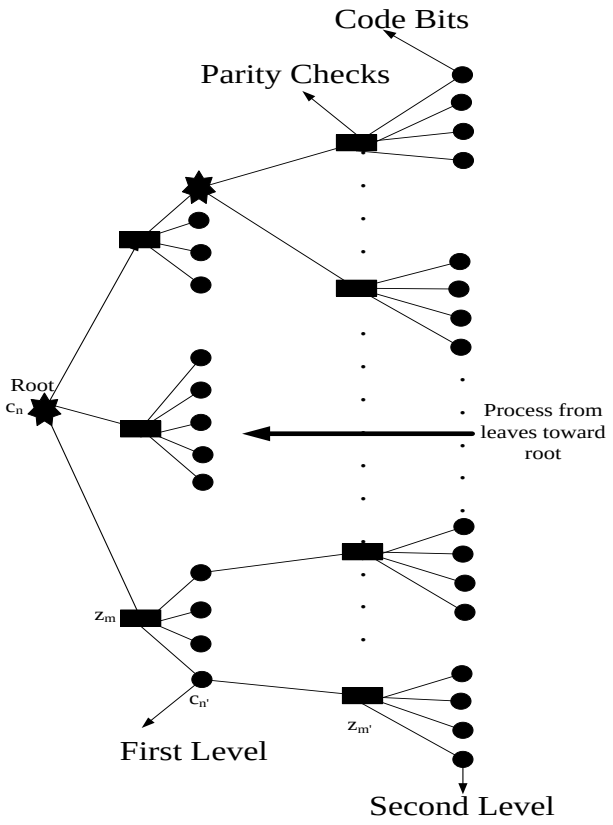

Fig.2. Two level parity check tree associated with the Tanner graph

Thus for each edge we can talk about the sub graph on either side of it. Assume the bits in the star mark are in error. The bits that connect to the checks that connected to the root node are said to be in level 1. The bits that connect to the checks from the first level are said to be in level 2. We can establish many such levels. Then, decode by proceeding from the leaves of the tree (right most part of the Fig.). By the time decoding on c_n is reached, other erroneous bits may have been corrected. Thus bits and checks which are not directly connected to c_n still influence c_n[7].

4. MATHEMATICAL DESCRIPTION OF DECODING ALGORITHM

In this section, mathematical description of iterative decoding algorithm for near LDPC like codes by traversing parity check tree is presented. The following notation is convenient in describing the algorithm [13, 14, 15]. Let $h_{i,j}$ denote the entry of H in the i^{th} row and j^{th} column. Then,

$$L(M) = \{l : h_{m,l} = 1\}, \quad (5)$$

denote the set of code positions that participate in the m^{th} parity check equation and let,

$$M(l) = \{m : h_{m,l} = 1\}, \quad (6)$$

denote the set of check positions in which code position l participates. The algorithm iteratively computes two types of conditional probabilities:

$q_{m,l}^{x}$, the probability that the l^{th} bit of codeword **c** has the value x, given the information obtained via the check nodes other than check node m.

$r_{m,l}^{x}$, the probability that a check node m is satisfied when bit l is fixed to a value x and the other bits are independent with probabilities $q_{ml'}^{x}, l' \in L(m) \setminus l$.

In the following, BPSK transmission over AWGN channel is assumed. Modulated symbols $m(c_i) = (-1)^{c_i}\sqrt{E_s}$ are transmitted over an AWGN channel and received as $r_i=m(c_i)+w_i$, where w_i is a Gaussian distributed random variable with zero mean and variance $N_0/2$, $1 \le i \le N$.

Initialization:

For $l \in \{1, 2, 3, \ldots, N\}$, initialize the a priori probabilities of the code nodes,

$$p_l^1 = \frac{1}{1+\exp(r_l \frac{4}{N_0})} \tag{7}$$

and $p_l^0 = 1 - p_l^1$. For every (l, m) such that $h_{m,l} = 1$,

$$q_{m,l}^0 = p_l^0; \quad q_{m,l}^1 = p_l^1 \tag{8}$$

Horizontal Step: Updating r_{ml}^{x}

For each l, m compute

$$\delta r_{m,l} = \prod_{l' \in L(m)\setminus l} (q_{m,l'}^0 - q_{m,l'}^1) \tag{9}$$

and

$$r_{m,l}^0 = (1+\delta r_{m,l})/2; \quad r_{m,l}^1 = (1-\delta r_{m,l})/2 \tag{10}$$

Vertical Step: Updating q_{ml}^{x}

For each l, m compute

$$q_{m,l}^0 = p_l^0 \prod_{m' \in M(l)\setminus m} r_{m',l}^0; \quad q_{m,l}^1 = p_l^1 \prod_{m' \in M(l)\setminus m} r_{m',l}^1 \tag{11}$$

and normalize, with $\alpha = \frac{1}{q_{m,l}^0 + q_{m,l}^1}$,

$$q_{m,l}^0 = \alpha q_{m,l}^0; \quad q_{m,l}^1 = \alpha q_{m,l}^1 \tag{12}$$

For each l, compute the a posteriori probabilities

$$q_l^0 = p_l^0 \prod_{m \in M(l)} r_{m,l}^0; \quad q_l^1 = p_l^1 \prod_{m \in M(l)} r_{m,l}^1 \tag{13}$$

and normalize, with $\alpha = \frac{1}{(q_l^0 + q_l^1)}$,

$$q_l^0 = \alpha q_l^0; \quad q_l^1 = \alpha q_l^1 \tag{14}$$

Final Step:

Make a tentative decision: Set, $\hat{c}_n = 1$, if $q_l^0 > 0.5$, else set $\hat{c}_n = 0$. If $\mathbf{H}\hat{\mathbf{c}} = 0$, Stop.

We have done simulation for regular LDPC like codes derived from full rank codes over F_{2^3}, F_{2^4} and F_{2^5}. From below shown simulation results we notice that for the AWGN channel, gains in excess of 2dB at reasonable bit error rates with respect to uncoded systems is attained.

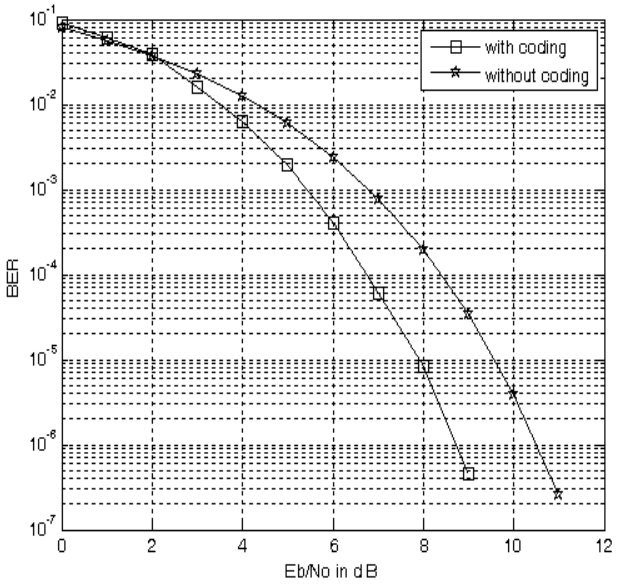

Fig.3. Performance for the regular LDPC like codes derived from full rank codes over F_{2^3}

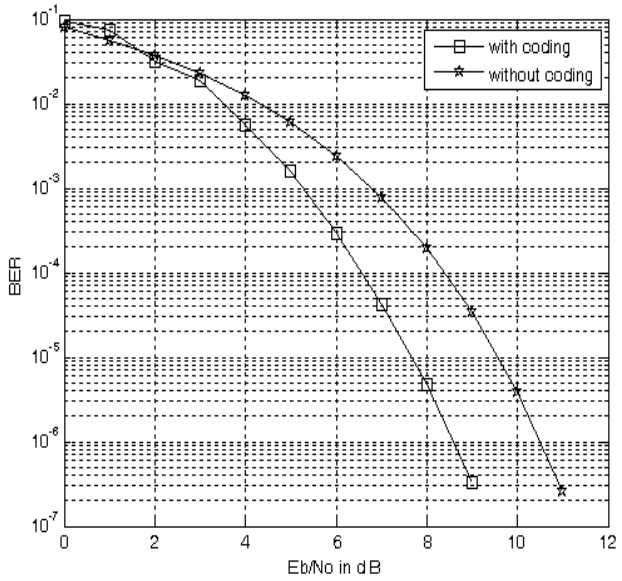

Fig.4. Performance for the regular LDPC like codes derived from full rank codes over F_{2^4}

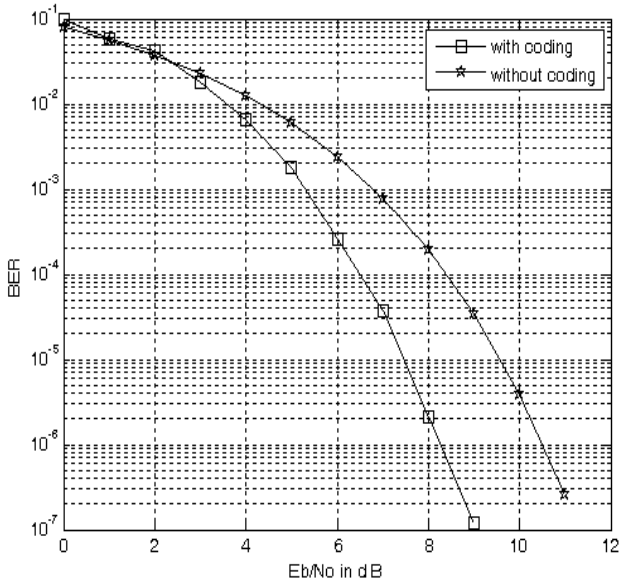

Fig.5. Performance for the regular LDPC like codes derived from full rank codes over F_{2^5}

5. CONCLUSION

A new method which enables construction of regular LDPC like codes from full rank codes defined over finite fields is proposed. The proposed method of construction is simple. The proposed decoding algorithm requires less transmitter/receiver power and provides a coding gain of the order of 2dB with respect to un-coded systems. In wireless applications, 3dB coding gain over un-coded transmission means that data throughput can be increased by a factor of 2 for a fixed SNR. Equivalently, transmitter power can be reduced by a factor of 2 if increase in throughput is not desired. This translates into smaller transmit antennas or, alternatively, smaller receive antennas for the same transmission power. Hence, these regular LDPC like codes derived from full rank cyclic codes over finite fields can find applications in LTE-Networks, WiMax and other high speed data transmission systems.

REFERENCES

[1] Daniel Costello, David Forney, "Channel coding: The road to channel capacity", *Proceedings of the IEEE*, Vol. 95, No. 6, pp. 1150-1177, 2007.

[2] Martin Bossert, "*Channel Coding for Telecommunications*", First Edition, Wiley International, 1999.

[3] E. M. Gabidulin,, "Theory of Codes with Maximum Rank Distance", *Problems of Information Transmission*, Vol. 21, No.1, pp. 3-14, 1985.

[4] R.M. Roth," *Introduction to Coding Theory*", First Edition, Cambridge University Press, 2006.

[5] R.G. Galleger, Jan, "Low Density Parity-Check Codes", *IRE Transactions on Information Theory*, Vol. 8, No. 1, pp. 21-28, 1962.

[6] William Ryan and Shu Lin, "*Channel Codes: Classical and Modern*", First Edition, Cambridge University Press, 2009.

[7] Todd K. Moon, "*Error Correction Coding: Mathematical Methods and Algorithms*", First Edition, Wiley Interscience, 2005.

[8] R.M. Roth, March 1991, "Maximum-rank array codes and their application to criss-cross error correction", *IEEE Transactions on Information Theory*, Vol. 37, No. 2, pp. 328-336, 2006.

[9] U. Sripati and B. Sundar Rajan, "On the rank-distance of cyclic codes", *Proceedings. IEEE International Symposium on Information Theory*, pp. 72, Yokohoma, Japan, 2003,.

[10] U. Sripati, B. Sundar Rajan and V. Shashidhar,, "Full diversity STBCs for block-fading channels from cyclic codes", *IEEE Global Telecommunications Conference*, Vol. 1, pp. 566-570,, Dallas, Texas, 2004.

[11] U. Sripati and B. Sundar Rajan, "On the rank-distance of cyclic codes", Technical Report No. TR-PME-2003-2004, Dept. of ECE, IISC Bangalore. Available for download at www.ece.iisc.ernet.in/~bsrajan/Technical_Reports.html, 2003.

[12] R.M. Tanner, "A recursive approach to low complexity codes", *IEEE Transactions on Information Theory*, Vol. 27, No. 9, pp. 533-547, 1981.

[13] Robert H. Morelos-Zaragoza, "*The Art of Error Correcting Coding*", Second Edition, John Wiley and Sons, Ltd, 2006.

[14] Kschischang and Fray, "Iterative decoding of compound codes by probability propagation in graphical models", *IEEE Journal on Selected Areas in Communications*, Vol. 16, No.1, 1998.

[15] Kschischang, Frey and Loeliger,"Factor graphs and the sum product algorithm", *IEEE Transactions on Information Theory*, Vol. 47, No. 2, pp. 498-519, 2001.