AMSE JOURNALS –2014-Series: Advances D; Vol. 19; N° 1; pp 90-100

Submitted Feb. 2014; Revised May 17, 2014; Accepted June 15, 2014

Low Complexity Encoding of Quasi-Cyclic Low Density Parity Check Codes and their Performance Analysis

*V.Murugesh, **V.Agalya, ***V. Arthy

*Department of Computer Science, College of Computer Science, King Khalid University,
P.O.Box 394, Abha, Saudi Arabia
** Cognizant Technology Systems, Tambaram, Chennai - 600 119, T.N., India
*** Wipro Technologies, Sholinganallur, Chennai - 600 119, T.N., India
(murugesh72@gmail.com; agalyav@gmail.com; arthyagal88@gmail.com)

Abstract:

Demand for reliable and proficient digital data transmission and storage systems has greatly increased in our day to day life. High speed, large-scale networks for data exchange, processing and storing of digital information in government, military and commercial areas has increased this demand. So, for a system designer the major task is the control of errors for efficient reproduction of data by using various coding techniques. LDPC codes are the recently using codes, because it belongs to a specific class of Shannon's capacity approaching codes. Due to this advantage, LDPC codes are strong competitors of other codes used in communication system like turbo codes.Quasi-cyclic LDPC codes are the most promising class of structured LDPC codes due to their ease of implementation and excellent error performance when decoded with message passing algorithms.For a QC-LDPC codes to be effectively encodable and have better memory efficiency than other randomly constructed LDPC codes, the parity check matrix is obtained from a block circulant matrices. The performance of these codes over the additive white Gaussian noise(AWGN) channel for various block lengths and code rates are analyzed using MATLAB.

Key words: LDPC, MAP, Soft Decision Decoding, SPA, QC-LDPC codes.

1. Introduction

Low-density parity-check (LDPC) codes are forward error-correction codes, first proposed in the (Sarah J. Jonson, 1962) Ph.D thesis. At that time, their incredible potential remained undiscovered due to the computational demands of simulation in an era when vacuum tubes were only just being replaced by the first transistors.. In the mean time the field of forward error correction was dominated by highly structured algebraic block and convolutional codes. Despite the enormous practical success of these codes, their performance fell well short of the theoretically achievable limits set down by Shannon (D.J.C.Mackay and M.Davey, 1999) in his paper.

New generalizations of Gallager's (N.Miladinovic and M.Fossorier, 2004) LDPC codes by a number of researchers includes the cyclic and Quasi-cyclic codes. Today, design techniques for LDPC codes exist which enable the construction of codes which approach the Shannon's capacity to within hundredths of a decibel. In addition to the strong theoretical interest in LDPC codes, such codes have already been adopted in satellite based digital video broadcasting and long-haul optical communication standards, are highly likely to be adopted in the IEEE wireless local area network standard, and are under consideration for the long-term evolution of third generation mobile telephony.

Low density parity check codes have attracted considerable attention (Marcos B.S. Tavares and Gerhard P. Fettweis, 2004) in the coding community because they can achieve near-capacity performance with iterative message-passing decoding and sufficiently long block sizes. For many practical applications, however, the design of good codes with shorter block lengths (D.J.C. Mackay and R.M.Neal, 1996) is desired. Moreover, most methods for designing LDPC codes are based on random construction techniques; the lack of structure implied by this randomness presents serious disadvantages in terms of storing and accessing a large parity-check matrix, encoding data, and analyzing code performance. If the codes are designed with some (algebraic) structure, then some of these problems can be overcome.

2. Low Density Parity Check Codes

LDPC codes are block codes (Sarah J. Jonson, 1962) with parity-check matrices that contain only a very small number of non-zero entries. It is the sparseness of H which guarantees both a decoding complexity which increases only linearly with the code length and a minimum distance which also increases linearly with the code length. LDPC codes are designed by constructing a sparse parity-check matrix first and then determining a generator matrix for the code afterwards.

The biggest difference between LDPC codes and classical block codes is how they are decoded. Classical block codes are generally decoded with ML like decoding algorithms 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 are designed with the properties of H as a focus. An LDPC code parity-check matrix is called (w_c, w_r)-regular if each code bit is contained in a fixed number, w_c ,of parity checks and each parity-check equation contains a fixed number, w_r, of code bits.

Quasi-cyclic LDPC codes are the most promising class of structured LDPC codes due to their ease of implementation and excellent performance over noisy channels when decoded with message passing algorithm. A code is quasi-cyclic if for any cyclic shift of a codeword by c places the resulting word is also a codeword, and so a cyclic code is a quasi-cyclic code with c=1.

3. Construction of QC-LDPC Block Codes

A simple method to design a (j,k)regular QC-LDPC code is to construct the preliminary matrix Y by constructing the two sequences $\{a_0, a_1, \ldots . a_{j-1}\}$ and $\{b_0, b_1, .. . b_{k-1}\}$ with elements randomly selected from GF(p)(p is prime and p>2).The matrix Y is represented as

$$Y = \begin{bmatrix} y_{0,0} & y_{0,1} & \cdot & \cdot & y_{0,k-1} \\ y_{1,0} & y_{1,1} & \cdot & \cdot & y_{1,k-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ y_{j-1,0} & y_{j-1,1} & \cdot & \cdot & y_{j-1,k-1} \end{bmatrix} \qquad (1)$$

where the (*u*, *v*)-th element of **Y** can be calculated by the following quadratic congruential equation for fixed parameter *d*:

$$y_{u,v} = \left[d\,(a_u + b_v)^2 + e_u + e_v \right] \operatorname{mod}(p) \qquad (2)$$

where $d \in \{1, 2, \ldots . p-1\}$ and

$e_{u,} e_v \in \{0, 1, \ldots p-1\}$.

Then the proposed parity check matrix H can be constructed by using the following equation,

$$H = \begin{bmatrix} I(y_{0,0}) & I(y_{0,1}) & \cdot & \cdot & I(y_{0,k-1}) \\ I(y_{1,0}) & I(y_{1,1}) & \cdot & \cdot & I(y_{1,k-1}) \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ I(y_{j-1,0}) & I(y_{j-1,1}) & \cdot & \cdot & I(y_{j-i,k-1}) \end{bmatrix} \qquad (3)$$

where $I(x)$ is a $p \times p$ identity matrix with rows cyclically shifted to the right by x positions.

For example I(1) is represented as follows:

$$\mathrm{I}(1)=\begin{bmatrix} 0 & 1 & 0 & 0 & . & . & 0 \\ 0 & 0 & 1 & 0 & . & . & 0 \\ 0 & 0 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 1 & 0 & 0 & 0 & . & . & 0 \end{bmatrix} \qquad (4)$$

Hence, the resulting **H**, which has j ones in each column and k ones in each row, represents a (j, k)-regular LDPC code. This LDPC code is also an $[N,K]$ regular LDPC code, where $N = kp$ is the block length of the QC-LDPC code, and K is the number of message bits.

Since the cycles of short length may degrade the performance of LDPC codes, it is necessary to ensure that the Tanner graph of the LDPC codes is free of cycles of length 4 and hence has girth at least 6. It is easy to prove that the parity check **H** constructed by the proposed method can satisfy this. The proof is given in (Chun_Ming Huang *et al.*,2008)

Example: A [155, 64] QC-LDPC code (p= 31)

Let j=3and k=5.First construct sequences and then by assuming d=1ande_u, e_v=0the following parity check matrix can be formed by substituting the above parameters in equations (2) and (3).Therefore the matrix can be represented as

$$H = \begin{bmatrix} I(7) & I(4) & I(20) & I(28) & I(16) \\ I(5) & I(5) & I(2) & I(18) & I(0) \\ I(18) & I(25) & I(19) & I(2) & I(1) \end{bmatrix}$$

where $I(x)$ is a 31 ×31 identity matrix with rows shifted cyclically to the right by x positions.

4. Encoding and Decoding

A block code that has a parity-check matrix H composed of circulants will have a systematic generator matrix also composed of circulants if it can be written as

$$H=[\Lambda\ \Gamma] \qquad (5)$$

where H is an n-k×n matrix and Γ is an n-k×n-k invertible square matrix .

The conventional method for constructing the generator matrix G is to find an n-k×n-k matrix Φ such that $\Phi\Gamma = I_{(n-k)}$,where $I_{(n-k)}$ is an n-k×n-k identity matrix.

Then the generator matrix will have the following form

$$G=[I_k\ (\Phi\Lambda)^T] \qquad (6)$$

As it might be conjectured, not all circulant matrices H will have Γ in an invertible form. In that case we have to cyclically right shift the particular columns of H in the left most side to the right side until we obtain Γ that has full rank.

LDPC code decoding tries to reconstruct the transmitted codeword c, from the possibly corrupted received word, y. It is achieved by using the parity-check matrix, H. The condition that $cH^T = 0$ defines the set of parity-check constraints or equations that must be satisfied for the received codeword to be the same as the transmitted code word. LDPC code decoding is achieved through iterative processing based on the Tanner graph, to satisfy the parity check conditions.

The sum-product algorithm is a soft decision message passing decoding algorithm (Sarah J. Jonson, 1962) (Y.Kou *et al.*, 2001) The input bit probabilities are called the a priori probabilities for the received bits because they were known in advance before running the LDPC decoder. The bit probabilities returned by the decoder are called the a posteriori probabilities. In the case of sum-product decoding these probabilities are expressed as log-likelihood ratios (LLRs).

The sum-product algorithm iteratively computes an approximation of the MAP value for each code bit. However, the a posteriori probabilities returned by the sum-product decoder are only exact MAP probabilities if the Tannergraph is cycle free.

The steps of the message passing algorithm are given below:

Step 1: Initialization of LLR value [5]

$$r_i = \left(2/\sigma^2\right) r \qquad (7)$$

Step 2: Check-node update [2]

$$E_{j,i=}\, 2\tanh^{-1}(\prod\nolimits_{i^{'}\in B_{j},i^{'}\neq i} \tanh\left(M_{j,i^{'}}/2\right)) \tag{8}$$

Step 3: Variable-node update [2]

$$L_{i}=r_{i}+\sum_{j\in A_{i}} E_{j,i} \tag{9}$$

Step 4: Decision

Tentative decision must be done for reconstructing the transmitted codeword.

4. Simulation Results

The simulation results of QC-LDPC codes with different block lengths and code rates are shown here. In all cases, the iterative sum product algorithm (SPA) was used for decoding, and the maximum number of decoding iterations is 50. The SPA decoder stops when either a valid codeword is found or the maximum number of decoding iterations is reached.

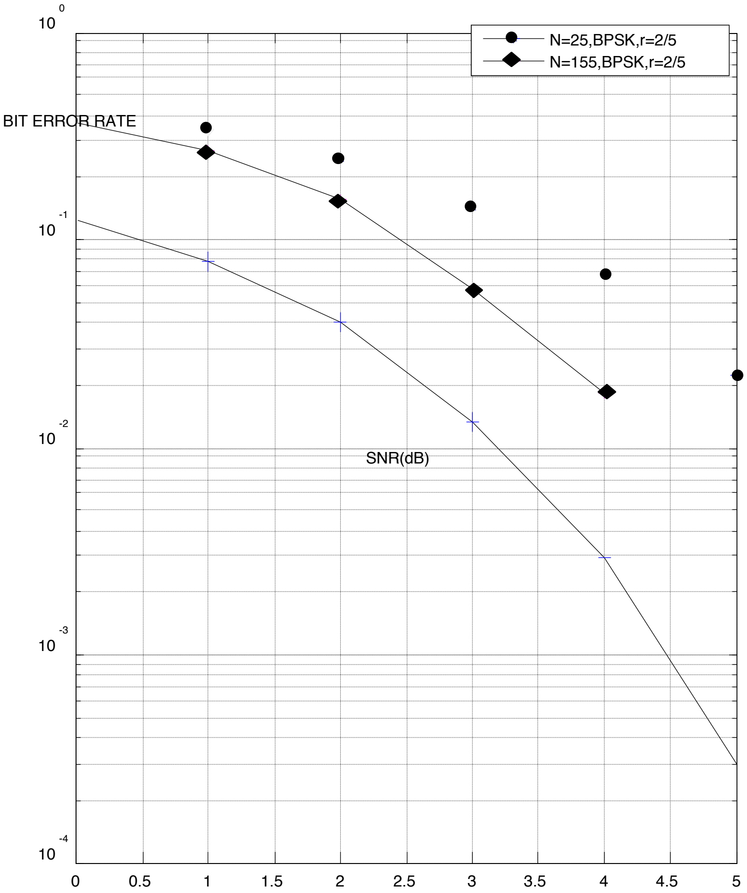

Fig 1: Performance analysis of QC-LDPC codes for different code lengths for r=2/5.

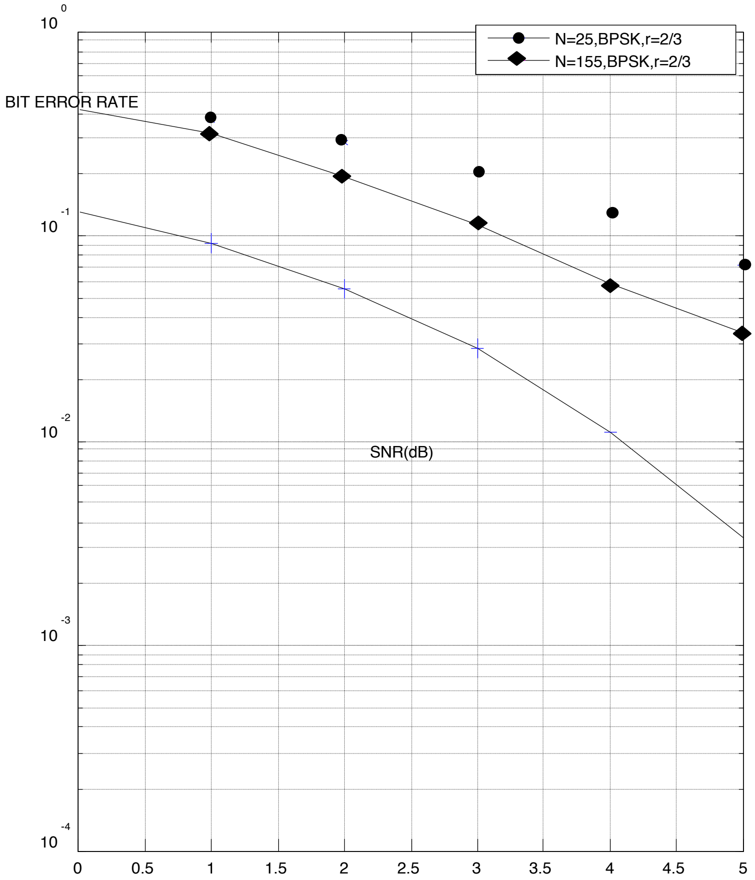

Fig 2: Performance analysis of QC-LDPC codes for different code lengths for r=2/3.

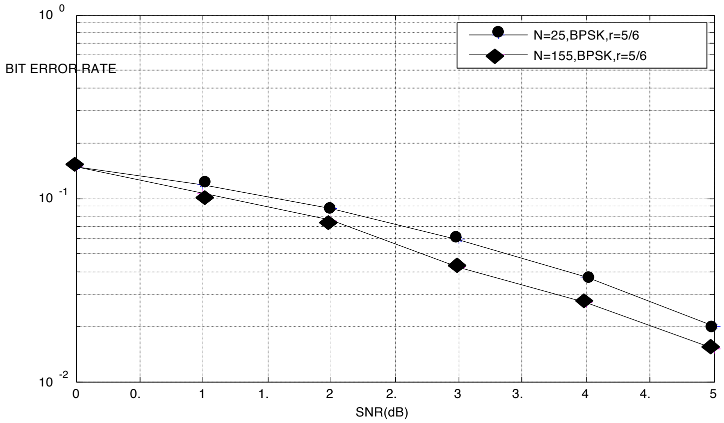

Fig 3: Performance analysis of QC-LDPC codes for different code lengths for r=5/6.

At SNR=4dB		
	Bit Error Rate	
Rate	N=25	N=155
0.4	10^{-3}	10^{-4}
0.6	10^{-2}	$\leq 10^{-3}$
0.8	$\geq 10^{-1}$	$\leq 10^{-2}$

Figure 4: Analysis of Bit error rate for different block lengths and code rates

5. Conclusion

In this paper, QC-LDPC codes constructed with different block lengths and codes rates are compared and their performance was analyzed. The above simulation results shows that at SNR=4dB,BER $\approx 10^{-4}$ for (155,64) code and BER $\approx 10^{-3}$ for (25,11) code at rate=2/5.But at rate=2/3 and 5/6, the performance of both the (155,64) and (25,11) codes are reduced at SNR=4dB.Since the future wireless standards are designed for a wide band of application in a single hardware platform, it needs to be adapted to different code rates, and different block lengths according to the available computational capability. The QC-LDPC can be effectively used for the multi rate wireless applications. The analyses and the simulation results will give an insight to the design of QC- LDPC codes for the future wireless standards.

REFERENCES

1. Chun-Ming Huang, Jen-Fa Huang and Chao-Chin Yang (2008)“Construction of Quasi-Cyclic LDPC Codes from Quadratic Congruences”, *IEEE Communication Letters*, Vol. 12-4.

2. Sarah J.Johnson, *Introducing Low-Density Parity-Check Codes*, School of Electrical Engineering and Computer science, The University of Newcastle, Ph.D thesis, Australia.

3. Marcos B. S. Tavares and Gerhard P. Fettweis, *LDPC Convolutional Codes Based on Permutation Polynomials over Integer Rings*, Vodafone Chair Mobile Communications Systems, Dresden University of Technology, 01062 Dresden, Germany.

4. Y. Kou, S. Lin, and M. Fossorier (2001)Low-density parity check codes based on finite geometries: a rediscovery and new results, *IEEE Transactions on Information Theory*, vol. 47-7, pp. 2711-2736.

5. M. P. C. Fossorier (2004) Quasi-cyclic low density parity check codes from circulant permutation matrices,*IEEE Transactions on Information Theory*, vol. 50-8, pp. 1788-1794.

6. D. J. C. MacKay and R. M. Neal (1996) Near Shannon limit performance of low-density parity-check codes,*Electronics Letters*, vol. 32, pp.1645-1646.

7. D.J.C.Mackay and M.Davey (2000) Evaluation of Gallager codes for short block length and high rate applications, IMA Volumes in Mathematics and its Applications, Springer-Verlag, Vol. 123, pp. 113-130.

8. N.Miladinovic and M.Fossorier (2004)systematic recursive construction of LDPCCcodes, *IEEE Communication Letters*, Vol. 8-5,pp.302-304.

9. Z. Li, L. Chen, L. Zeng, S. Lin and W. Fong (2006) Efficient encoding of quasi-cyclic low-density parity-check codes, *IEEE Transactions on Communications*, Vol. 54, no.1 , pp. 71-81, 2006.

10. Q. Huang, Q. Diao, S. Lin, and K. Abdel-Ghaffar (2012)Cyclic and quasicyclic LDPC codes on constrained parity-check matrices and their trapping sets, *IEEE Transaction on Information Theory*, vol. 58, no. 5, pp. 2648–2671, 2012.

11. Y. Y. Tai, L. Lan, L. Zheng, S. Lin and K. Abdel-Ghaffar (2006) Algebraic construction of quasi-cyclic LDPC codes for the AWGN and erasure channels, *IEEE Transactions on Communications*, vol 54, no. 7, pp. 1765–1774, 2006.

12. K. Lally and P. Fitzpatrick (2001) Algebraic structure of quasicyclic codes, *Discrete Applied Mathmatics*, vol. 111, pp. 157–175, 2001.

13. V.Murugesh and Devarajan Gopal (2009) Modelling and Synthesis of Self-Similar Network Traffic, AMSE journals; Advances in Modeling – Series D : Computer Science and Statistics, Vol. 14, N°. 1-2, 2009.

14. V.Murugesh and K.Murugesan (2013) RK-Butcher Algorithm for Non-linear Singular Systems from fluid dynamics, AMSE journals, Modelling, Measurement and Control-Serie B, Vol. 82, N°. 2, 2013.