A Subtraction Based Method for the Construction of Quasi-Cyclic LDPC Codes of Girth Eight

Ambar Bajpai,
Department of Electrical Engineering
Chulalongkorn University, Bangkok, Thailand
ambarbajpai@gmail.com

Abhishek Kalsi
Department of Electrical Engineering
Indian Institute of Technology, Ropar, India
abhishekkalsi@iitrpr.ac.in

Lunchakorn Wuttisittikulkij
Department of Electrical Engineering
Chulalongkorn University, Bangkok, Thailand
lunchakorn.w@chula.ac.th

Piya Kovintavewat,
Data Storage Technology Research Center
Nakhon Pathom Rajabhat University, Thailand
piya@npru.ac.th

***Abstract*— This article presents a simple, less computational complexity method for constructing exponent matrix $(3, K)$ having girth at least 8 of quasi-cyclic low-density parity-check (QC-LDPC) codes based on subtraction method. The construction of code deals with the generation of exponent matrix by three formulas. This method is flexible for any block-column length K. The simulations are shown in comparison with some existing appreciable work. The codes with girth 8 are constructed with circulant permutation matrix (CPM) size $P \geq max\{a_{2,r}, a_{2,r}, \ldots . a_{2,k}\} + 1$.**

Keywords*— Channel Coding; Circulant Permutation Matrix (CPM); Girth; Low-Density Parity-Check (LDPC) Codes; Quasi-Cyclic (QC) LDPC codes

I. INTRODUCTION

The introduction of LDPC codes was brought into existence in early 1962 [1] by Robert Gallager. Primarily LDPC codes were ignored for almost three decades because of its high computational complexity for hardware implementation at that time. In 1992, Berrou developed the Turbo code whose performance was very close to Shannon limit or channel capacity. Its success led to rediscovery of LDPC codes by Mackay and Neal [2]. The rediscovery of LDPC codes leads to its performance competent to turbo codes over an AWGN (additive white Gaussian noise) channel. Furthermore LDPC codes can also be represented in bipartite graph usually known as Tanner Graph [3]. By bipartite graph, we means set of nodes further categorized into two subsets such that each subset is independent and is connected to each other. The two subsets are known as variable nodes representing columns and check nodes representing rows of a parity-check matrix (PCM).

Since LDPC codes has high complexity in terms of hardware implementation and hence requires huge memory, so a new class of LDPC codes were introduced known as quasi-cyclic LDPC (QC-LDPC) codes. A (J, K) QC-LDPC codes are a special class of LDPC codes defined as null space of PCM, which can be represented as $J \times K$ array of circular permutation matrices (CPMs) having same size $P \times P$. QC-LDPC codes are known for high throughput, better hardware compatibility and good decoding performance that leads to standardized as channel codes in various practical implementation for wireless communication [4].

Recently, QC-LDPC codes have been attracted by many researchers since its QC structure of PCM allows for linear time encoding. These codes were also based on geometry and algebraic theories. In addition, QC-LDPC codes are a class of LDPC codes in which there are cyclic connections between rows or columns of a sub matrix [5]. By using shift registers QC-LDPC codes can be encoded efficiently by a simple mechanism of address generation, so as to have less memory requirement and localized memory access [6]-[8]. QC-LDPC code structure depends on the arrangement of sub matrices and the value's by which they are shifted, random shifting of a sub matrices may result in poor performance of the QC-LDPC codes.

In this paper, we present an effectively reduced complexity algorithm which not only reduces memory size of hardware employment but also takes the least time for its computation of parity-check matrix **H**. We construct **H** matrix by using a subtraction method which is based on firstly constructing a base matrix of size $(3, K)$ and further finding the remaining exponent indices by proposed mathematical formulas. Recently, in the field of QC-LDPC codes, the construction of **H** matrix by explicit method for $(3, K)$ of girth 8 is given in [9] is fairly appreciable. They showed three construction methods for generating exponent matrix. Moreover, array codes are a class of QC-LDPC codes based on CPMs of size $P \times P$ has been proven good decoding performance [10]. We compared our simulation results which are comparable to the work in [9] as well as shortened array codes as in [10].

978-1-4673-8383-7/16/$31.00 ©2016 IEEE

The rest of this paper is organized as follows. Preliminaries of QC-LDPC are described in Section II. Section III describes a proposed method based on subtraction and process to generate **H** matrix, so as to construct QC-LDPC codes and related proofs. In Section IV, we examine the performance by presenting the simulation details and results of constructed codes and finally, Section V concludes the paper.

II. PRELIMINARIES

A. QC-LDPC Codes

Consider a regular QC-LDPC code whose parity-check matrix **H** of column weight J and row weight K is said to be uniform, if **H** matrix has constant row and column weight. The structure of QC-LDPC codes are generalize as $J \times K$ array of $P \times P$ circulant permutation matrix (CPM) as

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}_{a_{11}} & \mathbf{I}_{a_{12}} & \cdots & \mathbf{I}_{a_{1K}} \\ \mathbf{I}_{a_{21}} & \mathbf{I}_{a_{22}} & \cdots & \mathbf{I}_{a_{2K}} \\ \vdots & \vdots & \ddots & \\ \mathbf{I}_{a_{J1}} & \mathbf{I}_{a_{J2}} & \cdots & \mathbf{I}_{a_{JK}} \end{bmatrix}, \tag{1}$$

where $a_{JK} \in \{0,1\ldots,P-1,\infty\}$ and $\mathbf{I}_{a_{JK}}$ is basically a CPM of size $P \times P$ obtained by cyclic shifting of rows of an identity matrix **I** by a_{JK} times. In case of $a_{JK} = \infty$, we will be having a zero matrix of size $P \times P$.

The shortest cycle in **H** matrix is called girth. The girth of a QC-LDPC codes will always be less than or equal to 12 for $J \geq 3$ [5]. Finally **H** matrix is having a combination of $m = J \times P$ rows and $n = K \times P$ columns. Moreover, the shifting or exponent matrix of **H** is defined as

$$\mathbf{E(H)} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1K} \\ a_{21} & a_{22} & \cdots & a_{2K} \\ \vdots & \vdots & \ddots & \vdots \\ a_{J1} & a_{J2} & \cdots & a_{JK} \end{bmatrix} \tag{2}$$

and **H** matrix can be evaluated from $\mathbf{E(H)}$ by replacing each entry of a_{JK} with $\mathbf{I}_{a_{JK}}$. The presence of short cycles decreases the decoding performance of LDPC codes, so in order to avoid short cycles of length $2z$ a necessary condition as given in [4] is

$$\sum_{q=1}^{z} (a_{J_q,K_q} - a_{J_{q+1},K_q}) \equiv 0 \bmod P \tag{3}$$

where $J_q \neq J_{q+1,} K_q \neq K_{q+1}$ and $J_{z+1=} J_z$.

III. SUBTRACTION METHOD FOR GIRTH 8 QC-LDPC CODES

This section deals with the construction of exponent or shifting matrix of QC-LDPC codes by subtraction based method. By using this method we are able to reduce time complexity for generating **H** matrix by a good amount.

A. Essential conditions:

There are three easy rules for the generation of base matrix as follow:

1) The first row and the first column of an exponent matrix both are fixed to be a zero vector.

2) It is mandatory that the 2nd row will always be in the ascending order.

3) Repetitions of indices are not allowed, i.e. at different indices we will have different values.

For simplicity, we demonstrate $3 \times K$ exponent matrix of non-negative integers is expressed as

$$\mathbf{E(H)} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & a_{1,1} & \cdots & a_{1,K-1} \\ 0 & a_{2,1} & \cdots & a_{2.K-1} \end{bmatrix} \tag{4}$$

To obtain high girth, we should take care of indices in (4) in order to avoid presence of small cycle. Before exploring more towards proposed construction, we start with following lemma.

Lemma 1: For any $l(1 \leq l \leq K-1)$ and $k(0 \leq k \leq l-1)$ $a_{2,l} - a_{2,k} \geq a_{1,l} - a_{1,k}$.

Proof: Since

$$a_{2,l} - a_{2,l-1} > a_{1,K-1} - a_{1,l-1} \tag{5}$$

and also

$$a_{1,K-1} - a_{1,l-1} \geq a_{1,l} - a_{1,l-1} \tag{6}$$

Therefore from (5) and (6) we have

$$a_{2,l} - a_{2,k} \geq a_{1,l} - a_{1,k}.$$

B. Formula for constructing matrix of girth 8

Since we have fixed our first row and first column to be a zero vector as in (4), so we have to work basically for only the 2nd row and 3rd row indices. To obtain the 2nd row of our exponent matrix, we replace $a_{1,\,l} = l$, which means $a_{1,\,1} = 1$, $a_{2,\,2} = 2$ and so on. For attaining the 3rd row, we have to apply the below three formulas so as to get the desired row

$$\begin{aligned} a_{2,1} &= a_{2,0} + a_{1,1} + \left(\max\{a_{1,1}, a_{1,2},\ldots,a_{1,K-1}\} - a_{1,0}\right) \\ a_{2,K-1} &= a_{2,K-2} + a_{1,K-1} + \left(\max\{a_{1,1}, a_{1,2},\ldots,a_{1,K-1}\} - a_{1,1}\right) \end{aligned} \tag{7}$$

The above two formulas will generate the first non-zero element and the last non-zero element of the 3rd row. In between, the indices can be calculated by the formula as follows for t $(2 \leq t \leq K-2)$

$$a_{2,t} = a_{2,t-1} + a_{1,t} + \left(\max\{a_{1,1}, a_{1,2}.....a_{1,K-1}\} - a_{1,t}\right) \tag{8}$$

By using the subtraction method we are able to reduce the computational complexity by a very good amount, since we have already fixed our 1st row and 1st column, so the other entries in 2nd row are sequence wise indices from 1 onwards. In the 3rd row the elements can be generated by a simple mathematical formulas as in (7) and (8), which takes less than a second to execute, hence our computational complexity is reduced by a very good amount.

Theorem 1: Let $\mathbf{E}(\mathbf{H})$ be a base matrix. For $\mathbf{E}(\mathbf{H})$ to be of girth 8 it's CPM size $P \geq max\{a_{2,r}, a_{2,r},\ldots,a_{2,k}\} + 1$ for any $k(0 \leq k \leq l-1)$

Proof: For simplicity we will write $\mathbf{E}(\mathbf{H})$ to be $\mathbf{B}$. We will use induction method to justify our proof and the absence of 4 and 6 cycles. To prove it, suppose $P = +\infty$ then 4 cycles cannot exist according to definition of $\mathbf{E}(\mathbf{H})$ (by using theorem 2.1 [4] mod equation will become a normal equation). Now to prove that cycle 6 is also absent we will assume that $\mathbf{B}(l-1)$ be the current setting of exponent matrix having 0th and 1st row and the first $(l-1)$ elements of the 2nd row. The new setting is assumed to be $\mathbf{B}(l)$ which is obtained by adding a new entry $(a_{2,k})$ of 2nd row to be $\mathbf{B}(l-1)$. We will prove that no 6 cycle exist in $\mathbf{B}(l-1)$. The proof is by induction method so we will assume that there exists a 6 cycle in $\mathbf{B}(l)$, so if this exist then there are only two patterns of cycle 6 as in [8]. Let us denotes u, v and w be the three columns $(0 \leq u \leq P-1, 0 \leq v \leq u-1, u \neq v, v \neq w)$ respectively which form a 6-cycle, as per in *Theorem 1*[10], it is impossible to have 6-cycle if $P \geq max\{a_{2,r}, a_{2,r},\ldots,a_{2,k}\} + 1$.

IV. Simulation and Results

In this section, we deals with the above mentioned procedure and also deals with the bit error rate (BER) performance of our algorithm with some well known existing methods. For computing the BER performance we have considered a $m \times n$ size $\mathbf{H}$ matrix, where n is the length of a codeword, and m is the number of parity bits. The code rate R will be $(1-m/n)$. The BER plot based on AWGN channel model, in which a binary input sequence $a_k \in \{0,1\}$ of length $n-m$ bits is encoded and is mapped to a n bit coded sequence $b_k \in \{\pm 1\}$. After mapping the received sequence is y_k which is given by $y_k = b_k + n_k$, where n_k stands for AWGN with variance σ^2 and zero mean. A LDPC decoder is used at the receiver end to decode received sequence y_k with 50 iterations by using message passing algorithm.

A minimum of 10000 data packets are used to compute each BER point. Signal to noise ratio (SNR) is defined in decibel as dB. The mathematical formula for computing SNR is defined as

$$\text{SNR} = 10\log_{10}\left(\frac{1}{R\sigma^2}\right)$$

Example 1: By using the subtraction method proposed in Section III, the exponent matrix **B** for block-column length of $K = 9$ having girth 8 is expressed as

$$\mathbf{B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 9 & 17 & 25 & 34 & 42 & 50 & 58 & 73 \end{bmatrix}$$

The 1st row and 1st column of **B** matrix filled as per our defined necessary conditions in Section III-A. To obtain remaining indices of 2nd row we follow Section III-B. After obtaining indices of 2nd row we move for the indices of the 3rd row, in order to get first non-zero element of the 3rd row which is $9(0+1+(8-0))$ and the last non-zero element of 3rd row is $73(58+8+(8-1))$ according to (7), in between indices can be obtained by third formula as in (8), for example $a_{2,3} = 25$ is basically $(17+3+(8-3)) = 25$ according to (8) and so on. Therefore we can obtain the rest of the indices of the 3rd row. Since the maximum index of the 3rd row is 73 so according to the *Theorem 1,* the size of CPM should be $P = 73 + 1 = 74$ for girth 8. In this way, we get our desired exponent matrix, hence **H** matrix, which is having reduced computational time complexity by a good amount.

The Table 1 compares the CPM size of Construction **I** (refer to the method I of Zhang [9]) and Construction **II** based on our proposed algorithm. We can obtain better BER performance while losing lower bound as compared to construction **I**, still, there exists a trade-off between performance and complexity.

Table 1 CPM size comparison of proposed algorithm

K	5	6	7	8	9	10	11	12
I	19	27	37	48	61	75	91	108
II	21	31	43	57	74	91	111	133

We also compares BER performance as illustrates in Fig. 1 of the proposed code for different code rates of one third and half code rate respectively, which is compared with some well-known existing QC-LDPC codes such as shortened array codes as in [10] and QC-LDPC codes as described in [9].

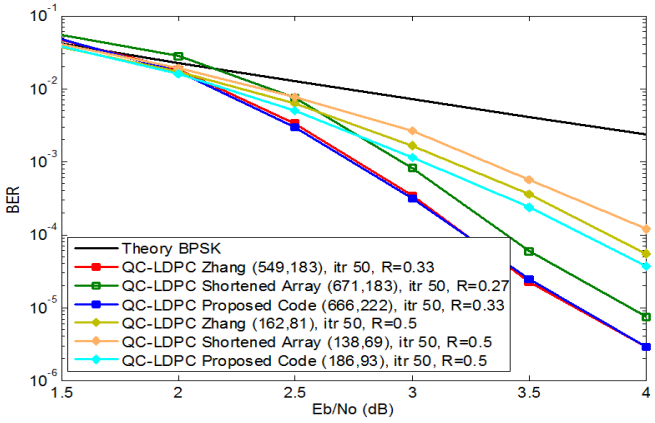

Fig. 1. BER performance comparison

Clearly, the proposed algorithm performs better than other algorithms when the SNR is high with reduced construction complexity.

Furthermore, we also compare the BER performance of different schemes as a function of the number of iterations at SNR=3 dB as shown in Fig. 2. It is apparent that the proposed algorithm converges faster than other compared algorithms at around 20 iterations. Our simulation results can be useful to construct good QC-LDPC codes in less computation time with comparable performance to other applicable existing work in the domain of QC-LDPC codes.

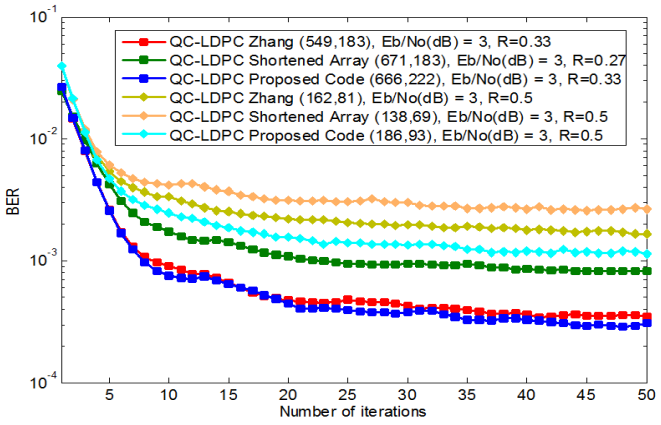

Fig. 2. BER performance as a function of the number of iterations for different **H** matrices

V. CONCLUSION

In this paper, we presented a simple less time consuming construction method for **H** matrix, the construction of QC-LDPC codes having girth 8. The choice of the block-column length *K* is kept flexible and the method was able to reduce the computational complexity of the **H** matrix by a decent amount. The CPM size *P* can be obtained by adding one to maximum indices of the 2nd row of **E(H)** matrix. We obtained a class of QC-LPDC code having girth 8 as explained in our example in section IV. The performances of the proposed QC-LDPC codes are simulated in terms of BER which is comparable to the existing recent work. The results are helpful in the construction of binary and non- binary QC-LDPC codes.

ACKNOWLEDGEMENT

This work is part of research fund allocated to Ambar Bajpai, implemented within the framework from prestigious 90th year Chulalongkorn University scholarship. (Ratchadaphisek Somphot Endowment Fund).

REFERENCES

[1] R. G. Gallagar, "Low-density parity-check codes," IRE Trans. Inform. Theory, vol. IT-8, pp. 21-28, Jan. 1962.

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," Electron. Lett., vol. 33, pp. 457-458, June 1997.

[3] R. M. Tanner, "A recursive approach to low complexity codes," IEEE Trans. Inform. Theory, vol. 27, pp. 533-547, May 1981.

[4] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," IEEE Trans. Inform. Theory, vol. 50, pp. 1788-1793, Aug. 2004.

[5] G. Malema, "Low density Parity-Check Codes: Construction and Implementation," Ph.D. dissertation, Faculty of Eng. Comp. and Math. Sci., Univ. of Adelaide, Australia, 2007.

[6] H. Fujita and K. Sakaniwa, "Some Classes of Quasi-Cyclic LDPC Codes: Properties and Efficient Encoding Methods," IEICE Trans. Fundam. Electr. Commun. Comp. sci., vol. 88, pp. 3627-3635, 2005.

[7] Y. Chen and K. Parhi, "Overlapped Message Passing For Quasi-Cyclic Low Density Parity Check Codes," IEEE Trans. Circuits syst., vol. 51, pp. 1106-1113, June 2004.

[8] M. Saadi, A. Bajpai, Y. Zhao, P. Sangwongngam, and L. Wuttisittikulkij, "Design and Implementation of Secure and Reliable Communication using Optical Wireless Communication," Frequenz, vol. 68, pp. 501-509, Nov.-Dec. 2014.

[9] G. Zhang and R. Sun, "Several Explicit Constructions for (3, L) QC-LDPC Codes with Girth at Least Eight," IEEE Communication Letters, vol. 17, Sept. 2013.

[10] O. Milenkovic, N. Kashyap, and D. Leyba, "Shortened array codes of large girth," IEEE Transactions on Information Theory, vol. 52, pp. 3707-3722, Aug. 2006.