Performance and analysis of high girth Non-Binary Quasi-Cyclic LDPC Codes based on subtraction method

Ambar Bajpai[1], Piya Kovintavewat[2], and Lunchakorn Wuttisittikulkij[3]
[1]*School of Engineering, Avantika University, India*
[2]*Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand*
[3]*Data Storage Technology Research Center, Nakhon Pathom Rajabhat University, Thailand*

ambar.bajpai@avantika.edu.in, piya@npru.ac.th, and Lunchakorn.W@chula.ac.th

Abstract

Since the revolutionary introduction of Turbo codes and rediscovery of LDPC codes and its non-binary variant in 90's, the world of forward error correcting codes (FEC) in channel coding has undergone a major transformation. Quasi-Cyclic low-density parity-check (QC-LDPC) codes is an on-going research area in the field of channel coding to construct a parity-check matrix, **H**. *It comprises of realistic, hardware-friendly architecture and reasonable error-correction performance. This article presents a simple, less computational complexity method for constructing non-binary QC-LDPC codes, having girth of at least 8 using the subtraction method. The code construction deals with the generation of an exponent matrix by three formulas. The simulation illustrates that the proposed non-binary QC-LDPC codes perform better than its binary counterpart.*

Keywords: Channel coding; Circulant Permutation Matrix (CPM); Girth; Non-Binary (NB)-LDPC codes; Quasi-Cyclic (QC) LDPC codes

1. Introduction

LDPC channel codes, proposed by Gallager are one of the best choice for FEC in communication systems [1]. They were further reinvented in 1996 by Mackay and Neal [2] and, since then, many researchers have contributed remarkable literature for practical wireless communication standards. As the name depicts, these codes are lies in the category of block codes defined in the form of parity-check matrix with low density of number of 1's. These codes have iterative decoding scheme which has increased complexity as block-length increases. These codes beat all other existing FEC codes for half rate and large block-length in terms of BER performance and decoding complexity. It is the world's best performing code falls only 0.0045 dB short of Shannon limit [3].

LDPC codes with large block-length usually provide a good performance at the cost of huge memory requirement and computation complexity of the **H** matrix [4]. To overcome this problem, Quasi-cyclic LDPC (QC-LDPC) codes were proposed by Fossorier [5], which is based on algebraic, geometric theories along with combinatorial designs, that are mostly accepted form of structured LDPC codes. However, the flexibility of code rate and code length is restricted by the matrix construction theories [6-9].

These features motivate us to take an intensive interest in the construction of large block-length QC-LDPC codes with high girth for future applications in the data storage and communication system. Note that the term "girth" implies the shortest cycle in a Tanner graph or in the **H** matrix. Application of good QC-LDPC codes includes in standards such as enhanced Mobile Broadband (eMBB) service category in 5G, IEEE 802.11n/ac, 802.16e, 802.20, ETSI DVB S2/T2, 10 Gb Ethernet etc. QC-LDPC codes can be easily encoded using shift-registers, thus demanding less memory and less computational complexity [10].

Furthermore, Non-Binary LDPC (NB-LDPC) codes were first investigated by Davey and Mackay in 1998 [11], During the last two decades, NB-LDPC codes were investigated rigorously by researchers, basically evolving from a binary LDPC code over a Galois field, GF(q), where $q = 2^p$, p is an integer number. An NB-LDPC code generally offers enhanced performance, compared to its binary counterpart [11-14] for a trivial to modest block length. Although many researchers are working on the topic of NB-LDPC codes, there is still the possibility for extensive research in the field of NB-LDPC codes. Moreover, NB-LDPC code can be pooled with a greater order of modulation in a quite straightforward manner. A commonly used belief propagation (BP) algorithm in binary LDPC codes causes NB-LDPC codes to increase computational analysis, almost infeasible in the higher order of q. It is shown that decoding complexity can be reduced to $O(q\log_2 q)$ if we extend a BP algorithm for GF(q) using frequency domain computation [13].

In this paper, we present an effectively reduced complexity algorithm for high girth QC-NB-LDPC codes based on subtraction method, which not only reduces memory requirement of shift registers but also takes the least time for computing the girth of **H** matrix. In our proposed method, we construct **H** matrix by using a subtraction method which is based on initially constructing a base matrix of size $(3, K)$ and further finding the remaining exponent indices by mathematical formulas. Recently, in the domain of QC-LDPC codes, the construction of **H** matrix by explicit method for $(3, K)$ of girth 8 is appreciable [15]. 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 [16]. We analyzed method for constructing NB-QC-LDPC codes is further extension of our work as in [17] has an advantage of reducing the time complexity for generating large-block length NB-QC-LDPC codes along with less CPM size a good amount. This method can be useful to generate column weight 3 class of LDPC codes which has good error performance and less hardware memory size requirement.

This correspondence is organized as follows. Preliminaries of QC-LDPC and NB-LDPC codes are described in Section 2. Section 3 deals with the algorithm to generate **H** matrix so as to construct NB-QC-LDPC codes. Section 4 investigates the performance by presenting the simulation details and finally, Section 5 concludes this paper.

2. Quasi-Cyclic LDPC Codes

2.1 Construction of NB-QC-LDPC codes

In general, for QC-LDPC codes having a quasi-cyclic construction of the parity-check matrix (PCM), binary or NB-QC-LDPC codes can be divided into either the structure-based method or the random-like method. In the latter method, the shift offset values for component circulant permutation sub-matrices are determined through random methods [7], [14]. However, in structure-based methods, a special algebraic and structural method [7], [14] is used for computing circulant permutation sub-matrices. Using these methods can achieve high girth, but code block length is not always fixed, because it limits the performance of this constructed PCM, as different multimedia applications have a different quality of service, and wireless channels are persistently time-varying.

Consider an $m \times n$ matrix named **B**(**H**), called a base matrix. After smearing cyclic expansion, which is actually the substitution of entries "0" and "1" in **B**(**H**) with zero sub-matrices of size $L\times L$ and circulant permutation sub-matrices of size $L\times L$, respectively, one can construct a PCM **H** matrix of dimensions $mL \times nL$, which describes a binary QC-LDPC matrix. Precisely, let **P** be an $L \times L$ permutation matrix, as follows:

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \tag{1}$$

For a finite PCM, $0 \le a < L$, $\mathbf{P}^a$ denotes a circulant permutation sub-matrix of size $L \times L$, which is obtained by cyclically shifting identity matrix $\mathbf{I}_L$ to the right by a times. For simple notation, $\mathbf{P}^\infty$ denotes a zero matrix of size $L \times L$. By applying cyclic expansion to the mother matrix, **B**(**H**), a PCM of size $mL \times nL$ for a binary QC-LDPC code can be obtained [7] :

$$\mathbf{H} = \begin{bmatrix} \mathbf{P}^{a_{11}} & \mathbf{P}^{a_{12}} & \cdots & \mathbf{P}^{a_{1n}} \\ \mathbf{P}^{a_{21}} & \mathbf{P}^{a_{22}} & \cdots & \mathbf{P}^{a_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}^{a_{m1}} & \mathbf{P}^{a_{m2}} & \cdots & \mathbf{P}^{a_{mn}} \end{bmatrix} \tag{2}$$

where the shift offset value $a_{ij} \in \{0, 1, \ldots, L-1, \infty\}$ for $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, and $a_{ij} = \infty$, when the corresponding entry in **B**(**H**) is "0".

In a given binary PCM, as in (2), a non-binary PCM **H** matrix can be obtained by replacing each non-zero entity in **H** with a non-zero element from GF(q). Below is a summary of a design algorithm of non-binary QC-LDPC matrix.

- Step 1: Construct base matrix **B**(**H**).
- Step 2: Specify the shift offset value, a_{ij}, in (7) for each nonzero entry of **B**(**H**). After cyclic expansion, obtain a binary PCM **H**.
- Step 3: Specify the non-zero elements of **H** over GF(q) by replacing each "1" entry in **H** by an element from GF(q), excluding "0" entries.

3. Parity-check matrix generation algorithm and its generalized form for girth 8

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

3.1 Necessary 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.

3.2 Base matrix generation

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

$$\mathbf{E(H)} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & a_{1,1} & \cdots & a_{1,K-1} \\ 0 & a_{2,1} & \cdots & a_{2,K-1} \end{bmatrix} \quad (3)$$

3.3 Algorithm for generating $(3, K)$ exponent matrix of girth 8

Since we have fixed our first row and first column to be a zero vector as in (3), 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 $a_{1,\,1} = 1$, $a_{1,\,2} = 2$ and so on. For realizing the 3rd row, we have to apply the below three formulas so as to get the desired row

$$\begin{aligned} a_{2,1} &= a_{2,0} + a_{1,1} + \left(max\left\{a_{1,1},\, a_{1,2},\ldots,a_{1,K-1}\right\} - a_{1,0}\right) \\ a_{2,K-1} &= a_{2,K-2} + a_{1,K-1} + \left(max\left\{a_{1,1},\, a_{1,2},\ldots,a_{1,K-1}\right\} - a_{1,1}\right) \end{aligned} \quad (4)$$

The above two formulas will generate the first non-zero element and the last non-zero element of the 3rd row in $\mathbf{E(H)}$. In between, the $\mathbf{E(H)}$ matrix indices can be intended by the equation as follows for $t\ (2 \le t \le K-2)$

$$a_{2,t} = \mathrm{a}_{2,t-1} + \mathrm{a}_{1,t} + \left(max\left\{ \mathrm{a}_{1,1},\, \mathrm{a}_{1,2}\ldots\ldots a_{1,K-1}\right\} - \mathrm{a}_{1,t}\right) \quad (5)$$

By using the subtraction method, we can 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 formula as in (4) and (5).

4. Simulation and results

In this Section we simulated the proposed GF(2) LDPC codes in addition with random allocation of non-binary number based on GF(q) at each indices of constructed **E(H)** and also find the bit-error rate (BER) performance of our algorithm with comparison of some well-known existing methods. For computing the BER performance we have considered a $m\times n$ size **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 $\sigma^2 = N_0/2$, and zero mean. A NB-LDPC decoder is used at the receiver end to decode received sequence y_k with 50 iterations by using FFT based decoding algorithm. The parity-check matrix has 3 non-zero elements in each column.

A minimum of 50000 data packets are used to compute each BER point. Signal to noise ratio (SNR) is defined in decibel as dB. The mathematical formula for SNR is defined as

$$\mathrm{SNR} = 10\log_{10}\left(\frac{1}{R\sigma^2}\right) \quad (6)$$

Figure 1 compares the performance of different QC-LDPC codes as in [15], [16] and [17] over GF (q) at the 50th iteration in terms of bit-error rate (BER), where $\boldsymbol{q} = 2, 4, 8,$ and 16. Note that $\boldsymbol{q} = 2$ represents a binary LDPC code. In addition, we also plot the BER performance of a conventional binary phase shift keying (BPSK) system for the sake of comparison. As expected a NB-LDPC code with large q performs better than that with small q.

Example 2: By using our algorithm, the exponent matrix **E(H)** for the case of $K = 6$ having girth 8 can be generated as per algorithm given in Sec. 3 as

$$\mathbf{E(H)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 6 & 11 & 16 & 21 & 30 \end{bmatrix} \quad (7)$$

The comparison of CPM's size of our method with Zhang [15] as shown in Table 2, where construction I refer to method II of Zhang [13] and construction II refers to our proposed method.

Table 1: CPM's size compares for girth 8

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

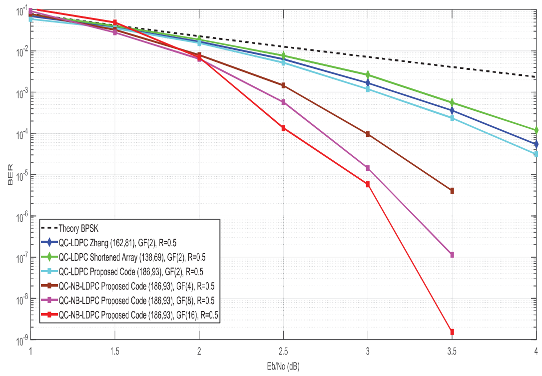

Figure 1. BER performance comparison

We also compare the performance of different schemes by plotting the number of iterations needed to decode all codeword of finite GF(q) LDPC codes as a function of BER with fixed SNR as shown in Figure 2.

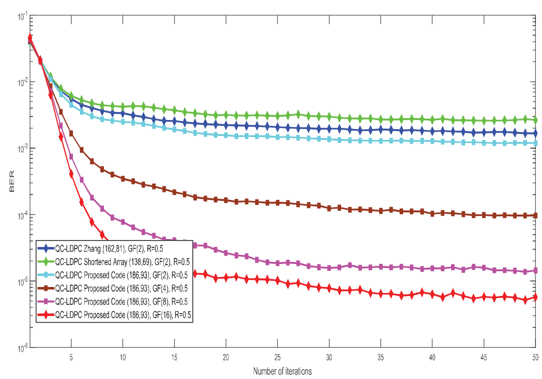

Figure 2. BER performance as a function of the number of iterations for different **H** matrices at $\mathrm{SNR} = 3\,\mathrm{dB}$

5. Conclusion

In this paper, we presented a simple less time consuming construction method for **H** matrix that can be useful to construct NB-QC-LDPC codes. We obtained a class of NB-QC-LPDC codes as explained in Section 3. The performance of proposed NB-QC-LDPC codes is simulated in terms of BER and number of iterations with considerations of higher order of GF(q), which is comparable to the existing work. The results are helpful in construction of regular NB-QC-LDPC codes. In a broader prospective, the field of LDPC code is huge and well-studied but several areas especially NB-LDPC codes still offer challenging problems in terms of decoding complexity and throughput optimization. There would be some features that will be of great interest in specific when applied to our class of QC-LDPC codes.

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. MacKay and R. Neal, "Near Shannon-limit performance of low-density parity-check codes," *Electronics letters*, vol. 32, pp. 645–1646, 1996.

[3] S.-Y. Chung, G. F. Jr., T. Richardson, and R. Urbanke," On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," IEEE Communications letters, vol. 5(2), pp. 58–60, Feb. 2001.

[4] Z. Li and B. V. K. V. Kumar, "A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph", *In Proc. 2004 Asilomar Conf. Signals, Syst. Comput*., pp. 1990-1994.

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

[6] G. Malema and M. Nkwebi, "Construction of flexible type II and III QC-LDPC codes", *Signal Process*., vol. 3, pp. 31-34, May 2014.

[7] S. Lin and D. J. Costello, "Error control coding: Fundamentals and Applications", *2nd ed. Prentice Hall*, 2004.

[8] A. Bajpai, G. Srirutchataboon, P. Kovintavewat, and L. Wuttisittikulkij, "A New Construction Method for Large Girth Quasi-Cyclic LDPC Codes with Optimized Lower Bound using Chinese Remainder Theorem", *Wireless Personal Communications*, vol. 91(1), pp.369-381, 2016.

[9] M. Saadi, A. Bajpai, Y. Zhao, P. Sangwongngam, and L. Wuttisittikulkij, "Design and Implementation of Secure and Reliable Communication using Optical Wireless Communication," *Frequenz 68*, no. 11-12, pp. 501-509, 2014.

[10] B. Li, J. Huang, S. Zhou, K. Ball, M. Stojanovic, L. Freitag, and P. Willett, "MIMO-OFDM for high rate underwater acoustic communications," *IEEE J. Ocean. Engr.,* vol. 34, no. 4, pp. 634–644, Oct. 2009.

[11] M. C. Davey and D. Mackay, "Low-density parity-check codes over GF(q)," *IEEE Comm. Letters,* vol. 2, pp. 165-167, June 1998.

[12] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices", *IEEE Trans. Inform. Theory*, vol. 45, pp. 399-431, Feb. 1999.

[13] M. C. Matthew and D. J. C. MacKay. "Low density parity check codes over GF (q)", *Information Theory Workshop*, IEEE, 1998.

[14] L. Dolecek, D. Divsalar, S. Yizeng, and A. Behzad, "Non-binary protograph-based LDPC codes: Enumerators, analysis, and designs," *IEEE Transactions on Information Theory,* vol. 60, no. 7, pp. 3913-3941, 2014.

[15] 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.

[16] 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.

[17] A. Bajpai, L. Wuttisittikulkij, A. Kalsi, and P. Kovintavewat, "A subtraction based method for the construction of quasi-cyclic LDPC codes of girth eight," *in proc. of International Siberian Conference on Control and Communications (SIBCON),* Moscow, May, 2016.