Wireless Pers Commun (2016) 91:369–381
DOI 10.1007/s11277-016-3465-8

A New Construction Method for Large Girth Quasi-Cyclic LDPC Codes with Optimized Lower Bound using Chinese Remainder Theorem

Ambar Bajpai[1] · Gan Srirutchataboon[1] · Piya Kovintavewat[2] · Lunchakorn Wuttisittikulkij[1]

Published online: 29 June 2016

Abstract This paper presents a new construction algorithm of Quasi-cyclic low-density parity-check (QC-LDPC) codes of medium to large block-length by combining QC-LDPC codes of small block-length as their component codes, via Chinese remainder theorem. Such component codes were constructed by permuting each column block sequentially to attain the desire local girth. After combining all component codes to generate an expanded parity-check matrix, the resulting girth is greater than or at least equal to the highest girth of component codes. We investigate a lower bound for circulant permutation matrices in the proposed method, which provides efficient and fast encoding for a desired girth, and has very simple structure and more economical in terms of hardware implementation. As already proven, a high girth parameter of the parity-check matrix ensures a good error correcting performance. Thus, simulation results show that our proposed construction method of the parity-check matrix significantly outperforms the other well-known existing methods, has low error-floor, and can reduce encoding complexity for medium to large block-length QC-LDPC codes.

Keywords Chinese remainder theorem (CRT) · Girth · Low-density parity-check (LDPC) codes · Quasi cyclic (QC)-LDPC codes

✉ Ambar Bajpai
ambarbajpai@gmail.com

✉ Lunchakorn Wuttisittikulkij
wlunchak@chula.ac.th

Gan Srirutchataboon
srirutchataboon.research@gmail.com

Piya Kovintavewat
piya@npru.ac.th

[1] Department of Electrical Engineering, Faculty of Engineering, Chulalongkorn University, Bangkok, Thailand

[2] Data Storage Technology Research Center, Nakhon Pathom Rajabhat University, Nakhon Pathom, Thailand

1 Introduction

A low-density parity-check (LDPC) code is a class of linear block codes which can be categorized as a random or structured LDPC code, based on the construction method of a parity-check matrix, **H**. Practically, LDPC codes were first proposed in 1962 [1], since then it was ignored for almost three decades because of computation complexity at that time. Then, Tanner [2] investigated a bipartite graph, which can ease the encoding and decoding of LDPC codes. Later on in the late 1990s, many researchers focused on rediscovery of LDPC codes [3–5] and found that a carefully designed LDPC code can give an error performance close to the Shannon's limit over an additive white Gaussian noise (AWGN) channel. Currently, LDPC codes are considered as the most eligible channel codes for various practical applications in the field of wireless communications.

Although LDPC codes with large block-length usually provide a good performance but at the cost of huge memory requirement and computation complexity of the **H** matrix construction. To overcome this problem, Quasi-cyclic LDPC (QC-LDPC) codes were proposed by Fossorier [6], which is based on algebraic and geometric theories and combinatorial designs. However, the flexibility of code rate and code length is restricted by the matrix construction theories [6–10]. Nevertheless, good QC-LDPC codes are well suited for certain practical applications such as data storage systems, DVB-T2/S2, IEEE 802.16e, IEEE 802.11n, and 10 Gb Ethernet, because they can be easily encoded using shift-registers, thus requiring less memory and less computational complexity [7]. 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 data storage and communication systems. Note that the term "girth" implies the shortest cycle in a Tanner graph or in the **H** matrix.

In addition, remarkable efforts have been carried out to find various QC-LDPC constructions with explicit algebraic and combinatorial designs. For example, Fan [11] introduced an array code with no 4-cycle length that can be viewed as one of the properties of QC-LDPC codes. Another approaches to design large girth structured QC-LDPC codes based on CPM by deleting certain block-rows and block-columns of the **H** matrix were proposed in [12–16]. Recently, QC-LDPC codes up to the girth 8 were proposed by Sudarsan et al. [17], which based on complete protograph. Moreover, Eleftheriou et al. [13] presented a modified array code (MAC) by applying a cyclic shift to a Fan's array code so as to reduce the number of 1′s in a lower triangular **H** matrix, and its performance is superior to the Fan's array code. Additionally, Shu Lin et al. [9] had significant contribution for algebraic QC-LDPC codes, which have shown good performance with low error-floor and reduced-complexity.

A Chinese remainder theorem (CRT) based combining method was first introduced in [18]. It gives a unique reconstruction of a large positive integer K from its remainder modulo positive integers $\{L_1, L_2, \ldots, L_s\}$, where $K < \text{lcm}(L_1, L_2, \ldots, L_s)$ and lcm(**x**) stands for the least common multiplier of a vector **x**. In addition, CRT provides a simple reconstruction formula for an integer K, if all moduli are co-prime to one another. In a class of structured LDPC codes, a method based on CRT to extend the code length of the base matrix of QC-LDPC codes was proposed in [19], which offer significant less time consumption to construct the **H** matrix with high girth together with flexible code length and code rate.

Generally, a researcher's most challenging problem is to find out optimized memory requirement for hardware deployment of QC-LDPC codes and to select meaningful lower

bound on the circulant permutation matrices (CPMs). Recently, the necessary conditions for QC-LDPC codes to have girth up to 12 was proposed in [20, 21]. In this paper, we optimize the lower bound for our proposed QC-LDPC codes for various girths, which are necessary conditions to obtain the desired girth of proposed QC-LDPC codes. The lower bound obtained using a greedy computer based search algorithm for a given girth is more realistic than that obtained from the recent work in [10]. Furthermore, our results can be applied to any general class of regular QC-LDPC codes.

For large block-length codes, LDPC codes require a large computation time for encoding the **H** matrix. For instance, the most popular LDPC code constructed from a progressive-edge growth (PEG) algorithm normally has the computational complexity scaled as $O(mn)$ [22], where n is the number of symbol/variable nodes and m is the number of check nodes. Recently, in [23], proposed QC-LDPC codes based on constraint selection of shifting matrix, with reduced encoding complexity mainly an area reduction of 40–55 % is stated.

This paper aims to reduce the complexity of encoding for regular QC-LDPC codes with large block-length. To do so, we propose a novel algorithm to construct the **H** matrix with a large girth and then apply the CRT algorithm to expand the component QC-LDPC code without reducing its local girth. To illustrate the contribution of this paper, we compare the bit-error rate (BER) performance with the PEG based QC-LDPC codes and the other array codes with CRT. We found that the proposed method outperforms the others in terms of BER performance and computation complexity of the **H** matrix.

The rest of the paper is organized as follows. Section 2 summarizes the preliminaries of QC-LDPC codes and CRT. Section 3 explains a method to generate the **H** matrix based on our proposed algorithm to construct the component QC-LDPC codes combined with CRT. Section 4 presents simulation details and results with an example. Some important properties of the proposed method are discussed in Sect. 5 followed by conclusion in Sect. 6.

2 Preliminaries

2.1 Quasi-Cyclic LDPC Codes

The **H** matrix of a (j, k) QC-LDPC code with column weight j and row weight k, is called regular if the **H** matrix has uniform column weight and row weight [6]. It is based on $L \times L$ CPMs, defined as a mother matrix, $\mathbf{M}(\mathbf{H})$, of size $mL \times nL$, which can be uniquely constructed by shifting the order of an identity matrix, **I**, based on its corresponding CPM, as given by

$$\mathbf{M}(\mathbf{H}) = \begin{bmatrix} \mathbf{I}_{a_{11}} & \mathbf{I}_{a_{12}} & \cdots & \mathbf{I}_{a_{1n}} \\ \mathbf{I}_{a_{21}} & \mathbf{I}_{a_{22}} & \cdots & \mathbf{I}_{a_{2n}} \\ \vdots & \vdots & \ddots & \\ \mathbf{I}_{a_{m1}} & \mathbf{I}_{a_{m2}} & \cdots & \mathbf{I}_{a_{mn}} \end{bmatrix}, \tag{1}$$

where $a_{ij} \in \{0, 1 \ldots, L-1, \infty\}$ and $\mathbf{I}_{a_{ij}}$ is defined as the **I** matrix of size $L \times L$ for $1 \leq i \leq m$ and $1 \leq j \leq n$, which is obtained by cyclically right shifting the rows of the **I** matrix by a_{ij} times. The zero matrix of size $L \times L$ is represented when $a_{ij} = \infty$. The **H** matrix consists of m block-rows indexed from 0 to $m-1$, and n block-columns indexed from 0 to $n-1$. It is noted in ([6], Theorem 2.5) that the girth of an ultra-sparse QC-LDPC code, where $j \geq 3$ cannot be greater than 12.

In addition, the matrix $\mathbf{E}(\mathbf{H})$ is called the exponent or shifting matrix and it can be obtained by replacing each element $\mathbf{I}_{a_{ij}}$ in $\mathbf{M}(\mathbf{H})$ by a_{ij} as follows:

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

By combining the exponent matrix $\mathbf{E}(\mathbf{H})$ and the CPM $\mathbf{I}_{a_{ij}}$, it will give the $\mathbf{H}$ matrix. For example, the $\mathbf{M}(\mathbf{H})$ matrix in (1) can be constructed using an exponent coupling procedure according to

$$\mathbf{M}(\mathbf{H}) = \mathbf{E}(\mathbf{H}) \cdot \mathbf{I}_{a_{ij}}, \tag{3}$$

where $\circ$ is a coupling operator.

A cycle of length $2l$ in the Tanner graph of $\mathbf{M}(\mathbf{H})$ is called a $2l$-block cycle, which can be represented by an exponent chain in the $\mathbf{M}(\mathbf{H})$ matrix according to

$$(\mathbf{I}_{a_{i_1 j_1}} \rightarrow \mathbf{I}_{a_{i_1 j_2}} \rightarrow \mathbf{I}_{a_{i_2 j_2}}, \ldots, \mathbf{I}_{a_{i_l j_l}} \rightarrow \mathbf{I}_{a_{i_l j_1}} \rightarrow \mathbf{I}_{a_{i_1 j_1}}) \tag{4}$$

or in the $\mathbf{E}(\mathbf{H})$ matrix according to

$$(a_{i_1 j_1} \rightarrow a_{i_1 j_2} \rightarrow a_{i_2 j_2}, \ldots, \rightarrow a_{i_l j_l} \rightarrow a_{i_l j_1} \rightarrow a_{i_1 j_1}). \tag{5}$$

Due to the presence of short length cycle in the $\mathbf{H}$ matrix, the performance of LDPC codes will degrade. It is very important to understand the structure of the $\mathbf{H}$ matrix. The theorem mentioned below was first proposed by Fossorier in [6], which stated that in QC-LDPC codes, the necessary and sufficient condition for the existence of length $2l$-block cycle is given by

$$\sum_{k=1}^{2l} (a_{m_k, n_k} - a_{m_{k+1}, n_k}) \equiv 0 \bmod L, \tag{6}$$

where $i_k \neq i_{k+1}, j_k \neq j_{k+1}$, and $i_{l+1=} i_l$.

2.2 Chinese Remainder Theorem

Let I be a positive integer, $L_1, L_2, \ldots, L_s$ be s moduli, and $r_1, r_2, \ldots, r_s$ be s remainders of I, i.e.,

$$r_b \equiv I|L_b|, \tag{7}$$

where $0 \leq r_b \leq L_b$ for $1 \leq b \leq s$. If all the moduli L_b's are co-prime and $0 \leq I < \prod_{b=1}^{s} L_b$, then I can be uniquely reconstructed from its s remainders via a simple CRT theorem according to [19], i.e.,

$$I = \sum_{b=1}^{s} r_b A_b \overline{L_b} |L|, \tag{8}$$

where $L = \prod_{b=1}^{s} L_b$, $\overline{L_b} = L/L_b$, and $A_b \overline{L_b} \equiv 1|L_b|$.

2.3 Generalized Combination of QC-LDPC Codes via CRT

Let C_b be a QC-LDPC codeword, where $b = 1, 2, \ldots, s$, whose $\mathbf{H}_b$ is an $m \times n$ array of $L_b \times L_b$ CPMs and/or zero matrices. Let $\mathbf{E}(\mathbf{H}_b) = (a_{ij}^{(b)})$ be the exponent matrix and $L = \prod_{b=1}^{s} L_b$. A QC-LDPC code C with the $\mathbf{H}$ matrix of size $mL \times nL$ can be constructed by using the generalized combining method, which gives us the exponent matrix $\mathbf{E}(\mathbf{H}) = (a_{ij})$ according to (2). In the case, where $a_{ij}^{(b)} \neq \infty$ in $\mathbf{E}(\mathbf{H})$ for all $b = 1, 2, \ldots, s$, we can obtain a_{ij} according to

$$a_{ij} = \sum_{b=1}^{s} a_{ij}^{b} A_b \overline{L_b} |L|. \tag{9}$$

Proposition 1 [24]. For $b = 1, 2, \ldots, s$, let g_b denote the girth of C_b and g denote the girth of C then

$$g \geq \max\{g_1, g_2, \ldots, g_s\}. \tag{10}$$

In the next section, we propose a novel method to obtain a large block-length $\mathbf{H}$ matrix, that has the properties, such as high girth and less complex encoding, by constructing the component QC-LDPC codes. Thereafter, these component codes will be combined with CRT without reducing their local girth.

3 Proposed Method

This section introduces a novel method for constructing the $\mathbf{H}$ matrix that is suitable for medium to large block-length, and has high girth and less complex in terms of computation.

Assume that L_1 and L_2 are the prime numbers, which indicate the CPM size of the two component matrices, $\bar{\mathbf{H}}_1$ and $\bar{\mathbf{H}}_2$ having girth g_1 and g_2, respectively. The procedure explained here is for constructing the proposed $\mathbf{H}$ matrix of size $jL \times kL$ such that $L = L_1 \times L_2$ by using CRT as in (9) without losing its local girth. Later in this work, it can be extended to combine the $\bar{\mathbf{H}}_1, \bar{\mathbf{H}}_2, \ldots, \bar{\mathbf{H}}_s$ component matrices having the CPM size of $L_1, L_2, \ldots, L_s$, respectively, to obtain the $\mathbf{H}$ matrix such that $L = L_1 \times L_2 \times \cdots \times L_s$. Below are the steps of the proposed method.

Table 1 A proposed generalized component matrix

Block-row index	Block-column index				
$\bar{\mathbf{H}}_1$	**1**	**2**	$\cdots$	***k* – 1**	***k***
1	0	1	$\cdots$	$k-2$	$k-1$
2	Z	Z	$\cdots$	Z	Z
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
***j* – 1**	Z	Z	Z	Z	Z
j	Z	Z	Z	Z	Z

Step 1 To construct a component $\bar{\mathbf{H}}_1(j,k)$ matrix, where j and k are the number of block-rows and block-columns, respectively. The method for constructing this $\bar{\mathbf{H}}_1(j,k)$ matrix is given in Table 1, where the indexed number 0 represents the $\mathbf{I}$ matrix of size $L_1 \times L_1$, and 1 denotes cyclically one right shifted order of the $\mathbf{I}$ matrix, and so on. The indexed number Z is the designed cyclically right shifted order of the $L_1 \times L_1$ CPM. It should be noted that the size of $\bar{\mathbf{H}}_1$ matrix is $jL_1 \times kL_1$.

Step 2 For each column-block (starting from the leftmost column to the right), replace each Z from the 2nd to jth row using a number between 0 to $L_1 - 1$. To do so, we find all possible data patterns of each column-block. The maximum number of data patterns is denoted as P_{fc}. For instance, if $L_1 = 3$, we will take the 2nd and the 3rd block-row from Table 1. In this case, there will be 9 different data patterns available for the 1st column. In general, the maximum number of possible data patterns in P_{fc} can be calculated according to

$$P_{fc} = \binom{p}{1}^{j-1}, \tag{11}$$

where p is the size of the chosen CPM's. We replace the remaining block-rows indexed by Z as shown in Table 1 with the data pattern, through column by column succession order and computing its local girth g by considering up to the correspondent column. To find a local girth for each data pattern, we will assume that all sub-matrices other than the existed numbered data patterns labeled as Z are zero matrices of size $L_1 \times L_1$. If we cannot find the local girth (i.e., no cycle), we will assume that the girth is infinite.

Step 3 The data pattern that yields the largest local girth with minimum indexed value in all possible data patterns will be selected for the 1st column. Then, we proceed the same procedure as explained in Step 2 in a column by column manner until all block-columns are filled with the chosen number of data patterns. Table 2 shows an example of the component matrix $\bar{\mathbf{H}}_1$ after obtaining all Z's for $L_1 = 29$ and $g_1 = 8$. This process ensures the minimum size of CPM's in the QC-LDPC codes, which will be useful for constructing a good $\mathbf{H}$ matrix with high girth and low memory requirement for hardware implementation. Table 3 illustrates the minimum lower bound of the CPM size for various block lengths of the component matrix based on extensive simulation search for regular (3, k) LDPC codes. The obtained CPM size will be the optimized lower bound for constructing the QC-LDPC parity-check matrix with high girth and variable code rates.

Step 4 The other component matrix $\bar{\mathbf{H}}_2$ can be obtained by choosing a suitable size of a prime number L_2 based on Table 4, such that it maintains the optimum lower bound for the desired girth g_2. For instance, we choose a lower bound of the CPM size from Table 3, i.e., $L_2 \geq 7$ for $g = 6$. The construction procedure for $\bar{\mathbf{H}}_2$ is similar to that for

Table 2 A designed $\bar{\mathbf{H}}_1$ index matrix

Block-row index	Block-column index						
$\bar{\mathbf{H}}_1$	1	2	3	4	5	6	7
1	0	1	2	3	4	5	6
2	0	3	8	0	0	10	24
3	0	0	13	1	8	0	15

Table 3 Estimation of minimum CPM size L with corresponding girth

k (Block-length)	$g = 6$	$g = 8$	$g = 10$	$g = 12$
5	7	17	83	223
7	7	29	239	709
9	11	47	499	1399
11	11	61	743	3271

$\bar{\mathbf{H}}_1$. Table 4 shows an example of the component matrix $\bar{\mathbf{H}}_2$ after obtaining all Z's for $L_2 = 7$ and $g_2 = 6$.

Step 5 Finally, we construct the exponent matrix $\mathbf{E}(\mathbf{H})$ by combining all the component matrices via CRT and replacing each entry a_{ij} of $\mathbf{E}(\mathbf{H})$ with $\mathbf{I}_{a_{ij}}$ so as to obtain the $\mathbf{H}$ matrix of size $mL \times nL$ with girth g, which still satisfies the condition in (10), i.e., $g \geq \max\{g_1, g_2\}$ as shown in Table 5.

It should be pointed out that with carefully selecting the CPM size and block length, we can construct any large block-length $\mathbf{H}$ matrix up to the girth of 12 for QC-LDPC codes.

4 Simulation and Results

To compare the BER performance of the proposed method with some existing methods, we consider the $\mathbf{H}$ matrix of size $M \times N$, where M is the number of parity bits, N is the code length with code rate R, and R is equal to $1 - M/N$. To evaluate its performance, we simulate the system based on an additive white Gaussian noise (AWGN) channel, where a binary input sequence $a_k \in \{0, 1\}$ of length $N - M$ bits is encoded by an LDPC encoder and is mapped to an N-bit coded sequence $b_k \in \{\pm 1\}$. Hence, the received sequence is given by $y_k = b_k + n_k$, where n_k is AWGN with zero mean and variance σ^2. At the receiver, the received sequence y_k is decoded by LDPC decoder based on a message passing algorithm [1] with 10 iterations. The signal-to-noise ratio (SNR) is defined as $\text{SNR} = 10\log_{10}(1/2R\sigma^2)$ in decibel (dB). Each BER point is computed based on a minimum number of 10,000 data packets.

Example 1 In this example, we study the proposed method based on the component matrices combined with CRT to construct a large block-length $\mathbf{H}$ matrix. The obtained matrix has a uniform degree of 3 for each symbol node. By using our proposed algorithm, we construct a code C_1 for girth $g_1 = 8$, whose exponent matrix $\bar{\mathbf{H}}_1$ is of size 3×7 as shown in Table 2. To expand $\bar{\mathbf{H}}_1$, we first select $s = 2$. For $g_1 = 8$ and assume that $g_2 = 6$, Table 3 gives $L_1 \geq 29$ and $L_2 \geq 7$, respectively. Then, we choose $L_1 = 29$ and $L_2 = 7$ so as to maintain the lower bound on CPMs. After combining, the CPM size of $\mathbf{E}(\mathbf{H})$ matrix will be $L = L_1 \times L_2 = 203$. Similarly, we construct the 3×7 exponent matrix, $\bar{\mathbf{H}}_2$, using our

Table 4 A designed $\bar{\mathbf{H}}_2$ index matrix

Block-row index	Block-column index						
$\bar{\mathbf{H}}_2$	1	2	3	4	5	6	7
1	0	1	2	3	4	5	6
2	0	4	1	1	5	2	1
3	0	2	4	2	2	1	3

Table 5 A combined exponent matrix, $\mathbf{E}(\mathbf{H})$ via CRT

Block-row index	Block-column index						
$\mathbf{E}(\mathbf{H})$	1	2	3	4	5	6	7
1	0	1	2	3	4	5	6
2	0	32	8	29	145	184	169
3	0	58	158	30	37	29	73

proposed algorithm for $g_1 = 6$ as shown in Table 4. Then, we obtain $\mathbf{E}(\mathbf{H})$ by combining $\bar{\mathbf{H}}_1$ and $\bar{\mathbf{H}}_2$ via CRT as given in Table 5. Finally, we replace each entities a_{ij} of $\mathbf{E}(\mathbf{H})$ with $\mathbf{I}_{a_{ij}}$. The obtained $\mathbf{H}$ matrix will provide the QC-LDPC code with girth $g_1 = 8$.

Figure 1 illustrates the BER performance of the proposed (609, 1421) QC-LDPC code, which is compared with some well-known existing LDPC codes, where FAN-CRT is the code from the shortened array code based on CRT [17], IMAC QC-LDPC is the code from Singhaudom et al. [14], and QC-LDPC-PEG is the PEG based QC-LDPC code as described in [7]. Clearly, the proposed algorithm performs better than other algorithms, especially when the SNR is high.

We also compare the BER performance of different schemes as a function of the number of iterations at SNR = 4 dB in Fig. 2. It is apparent that the proposed algorithm converges faster than other algorithms. Furthermore, we also investigate the local girth of each algorithm as given in Fig. 3. Clearly, the proposed algorithm offers the girth of 8 similar to other algorithms except IMAC QC-LDPC. Note that the proposed CRT-based $\mathbf{H}$ matrix can have a higher girth by carefully choosing the value of CPMs and block-length size as depicted in Table 3.

5 Properties of the Proposed Codes

The component QC-LDPC codes, which are constructed by using the proposed method when combined with CRT to construct a large block-length $\mathbf{H}$ matrix, have good attributes, such as large girth, less complexity, good storage, flexible code rates, and flexible code

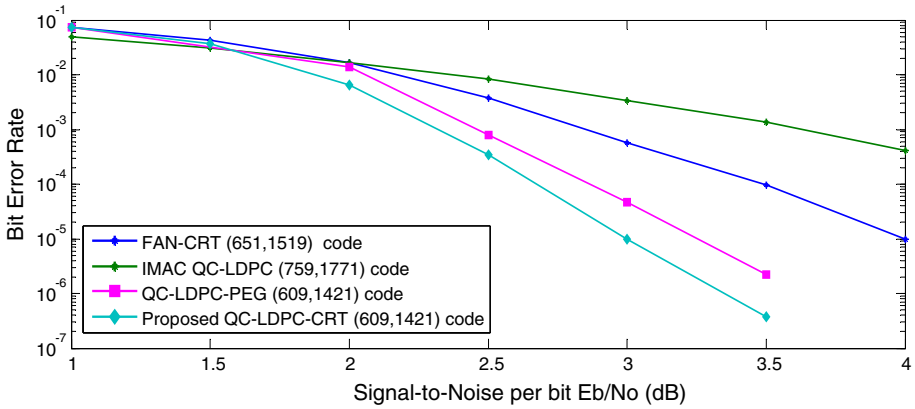

Fig. 1 Performance comparison of various QC-LDPC codes

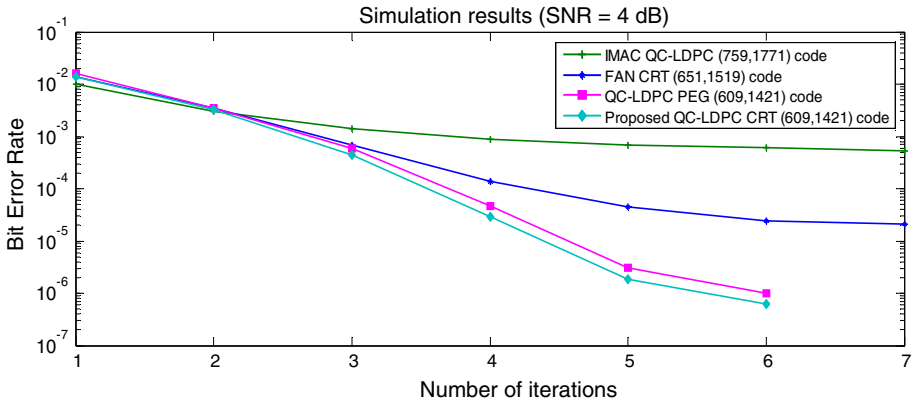

Fig. 2 BER performance as a function of the number of iterations for different **H** matrices at SNR = 4 dB

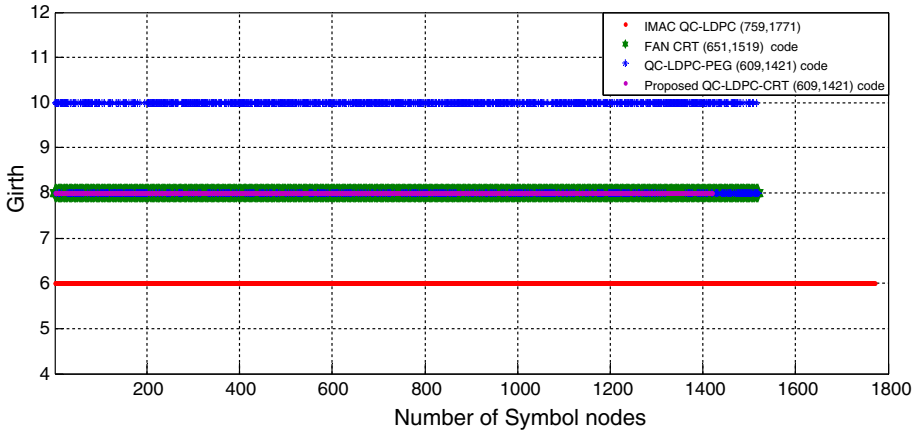

Fig. 3 Girth comparison of proposed-CRT codes

lengths. Details of some properties are discussed below. Furthermore, our proposed QC-LDPC code has lower computational complexity and is much more practical as compared to that obtained from the PEG algorithm.

5.1 Girth

It is one of the well-known parameters to determine the performance of decoding. In iterative belief propagation decoding, the algorithm converges to the most optimal solution, if the **H** matrix is free of short-cycle length. Cycle lengths of 4 and 6 lead to undesirable decoded data. When short-cycle lengths exist in the **H** matrix, the algorithm breaks down very soon. Therefore, the **H** matrix with large girth should always be taken into account. Our algorithm still satisfies (10), i.e., the girth $g \geq \max\{g_1, g_2\}$ as shown in Fig. 3.

5.2 Complexity

Let us analyze the computational complexity and the storage usage of the proposed algorithm.

5.2.1 Computational Complexity

Computational complexity of the proposed algorithm primarily depends on the algorithm's exploration time to obtain the exponent matrix indices. Exploration time depends on a row weight and a column weight of the desired exponent matrix. In the **H** matrix, the row and column weights are small numbers irrespective of code length. So we can divide computational complexity into two categories, the one for calculating the exponent matrix and the other for applying the CRT algorithm for large size block-length LDPC codes. However, both categories depend on codeword length, but the combining algorithm does not grow with the size of **H** matrix. From CRT formulas in Sect. 2.2, we can see that, each CRT computation needs only $(s-1)$ additions, $2(s-1)$ multiplications, and 1 modulo operation. Some of the values like L, $\overline{L_b}$, and A_b can be computed prior to initialize our CRT based combining method, and $L_1, L_2, \ldots, L_s$ should be selected optimally. Hence, the complexity of each CRT computation is negligible, if compared to the complexity of the design of parity-check component codes.

5.2.2 Storage Usage

In the **H** matrix, the row and column indices of '1' entries will be pre-defined and stored in the shift registers for practical applications. Therefore, our proposed method has a significant advantage of storing smaller index values, as shown in $\bar{\mathbf{H}}_1$ and $\bar{\mathbf{H}}_2$ in our example, discussed in Sect. 3, which has a minimum number of CPM size with large girth. This may reduce the storage requirement of a decoder of the proposed code. Furthermore, the scope of this method can be expanded in hardware implementation as well [25].

6 Conclusion

In this paper, we propose a new method for constructing the **H** matrix of QC-LDPC codes that aims for selecting the indices of the exponent matrix with a maximized local girth for column weight 3, by sequentially assigning proper sub-matrix for each column of $\mathbf{E}(\mathbf{H})$ matrix. A class of structured regular QC-LDPC codes has been constructed by using a CRT algorithm. This method can also be generalized to any number of column weights. As shown in simulation results, the proposed code outperforms the well-known algorithms in certain cases. Any general case of large block-length LDPC codes with good performance can be constructed using our proposed method. It fulfills almost all the parameters required for good LDPC codes and suitable for practical applications in terms of cost efficiency. Nevertheless, we found that the proposed algorithm might require higher computational search than some existing algorithms. Consequently, one should trade-off between performance and complexity when designing the QC-LDPC codes.

Acknowledgments This work is part of research fund allocated to Ambar Bajpai implemented within the framework from 90th year Chulalongkorn University scholarship.

References

1. Gallager, R. G. (1962). Low-density parity-check codes. *IRE Transactions on Information Theory, 8*(1), 21–28.
2. Tanner, R. M. (1981). A recursive approach to low complexity codes. *IEEE Transactions on Information Theory, 27*(5), 533–547.
3. MacKay, D. J. C., & Neal, R. M. (1997). Near Shannon limit performance of low density parity check codes. *Electronics Letters, 33*(6), 457–458.
4. Davey, M. C., & MacKay, D. J. (1998). Low density parity check codes over GF (q). In *Proceedings of IEEE information theory workshop*. (pp. 70–71). USA, June 1998.
5. MacKay, D. J. (1999). Good error-correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory, 45*(2), 399–431.
6. Fossorier, M. P. (2004). Quasicyclic low-density parity-check codes from circulant permutation matrices. *IEEE Transactions on Information Theory, 50*(8), 1788–1793.
7. Li, Z., & Kumar, B. V. (2004). A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph. In *Proceedings of 38th Asilomar Conference on Signals, Systems and Computers*, (Vol. 2, pp. 1190–1994). Pacific Grove, CA, USA, November 2004.
8. Vasic, B., Pedagani, K., & Ivkovic, M. (2004). High-rate girth-eight low-density parity-check codes on rectangular integer lattices. *IEEE Transactions on Communications, 52*(8), 1248–1252.
9. Lin, S., & Costello, D. J. (2004). *Error control coding: fundamentals and applications,* chapter 17, vol. 114, Englewood Cliffs: Pearson Prentice Hall.
10. Zhang, J., & Zhang, G. (2014). Deterministic girth-eight QC-LDPC codes with large column weight. *IEEE Communications Letters, 18*(4), 656–659.
11. Fan, J. L. (2001). Array codes as LDPC codes. In *Constrained Coding and Soft Iterative Decoding,* (pp. 195–203). Springer USA.
12. Milenkovic, O., Kashyap, N., & Leyba, D. (2006). Shortened array codes of large girth. *IEEE Transactions on Information Theory, 52*(8), 3707–3722.
13. Eleftheriou, E., & Olcer, S. (2002). Low-density parity-check codes for digital subscriber lines. In *Proceedings of IEEE international conference on communications*, (Vol. 3, pp. 1752–1757). New York, USA, 2002.
14. Singhaudom, W., Noppankeepong, S., & Suphithi, P. (2007). May. Design of high-rate modified array codes for magnetic recording system. In *Proceedings of 4th international conference on electrical engineering/electronics, computer, telecommunications and information technology,* (pp. 553–556). ECTI, Chiangrai, Thailand, 2007.
15. Saadi, M., Bajpai, A., Zhao, Y., Sangwongngam, P., & Wuttisittikulkij, L. (2014). Design and Implementation of Secure and Reliable communication using optical wireless communication. *Frequenz, 68*(11–12), 501–509.
16. Zhang, Y., & Da, X. (2015). Construction of girth-eight QC-LDPC codes from arithmetic progression sequence with large column weight. *Electronics Letters, 51*(16), 1257–1259.
17. Ranganathan, S. V., Divsalar, D., & Wesel, R. D. (2015). On the Girth of (3, L) Quasi-cyclic LDPC codes based on complete protographs. doi: 10.1109/ISIT.2015.7282491.
18. Myung, S., & Yang, K. (2005). A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem. *IEEE Communications Letters, 9*(9), 823–825.
19. Jiang, X., & Lee, M. H. (2009). Large girth quasi-cyclic LDPC codes based on the Chinese remainder theorem. *IEEE Communications Letters, 13*(5), 342–344.
20. Karimi, M., & Banihashemi, A. H. (2013). On the girth of quasi-cyclic protograph LDPC codes. *IEEE Transactions on Information Theory, 59*(7), 4542–4552.
21. Kim, K. J., Chung, J. H., & Yang, K. (2013). Bounds on the size of parity-check matrices for quasi-cyclic low-density parity-check codes. *IEEE Transactions on Information Theory, 59*(11), 7288–7298.
22. Hu, X. Y., Eleftheriou, E., & Arnold, D. M. (2005). Regular and irregular progressive edge-growth tanner graphs. *IEEE Transactions on Information Theory, 51*(1), 386–398.
23. Mahdi, A., & Paliouras, V. (2015). On the encoding complexity of quasi-cyclic LDPC codes. *IEEE Transactions on Signal Processing, 63*(22), 6096–6108.
24. Liu, Y., Wang, X., Chen, R., & He, Y. (2008). Generalized combining method for design of quasi-cyclic LDPC codes. *IEEE Communications Letters, 12*(5), 392–394.
25. Oh, D., & Parhi, K. K. (2010). Low-complexity switch network for reconfigurable LDPC decoders. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 18*(1), 85–94.

Ambar Bajpai He has done his M.E. (Communication Systems) from BITS Pilani, India in 2007. Presently he is pursuing Ph.D in Chulalongkorn University, Bangkok Thailand. In addition, he worked as an assistant professor in ITM University, Gurgaon India for 3.5 years. He also worked in industry as project engineer with ST Microelectronics Pvt. Ltd., Bangalore India. His areas of interests are channel coding, visible light communication and Bluetooth. Currently he is working as visiting faculty in KMUTNB Bangkok, Thailand.

Gan Srirutchataboon He received a B.Eng. from Bangkok University, Thailand. He has done M. Eng. in Electrical Engineering from Chulalongkorn University. He received Chulalongkorn 90th Year's research scholarship and associated as an intern in Hanyang University, Seoul, South Korea.

Dr. Piya Kovintavewat received the B.Eng. summa cum laude from Thammasat University, Thailand (1994), the M.S. degree from Chalmers University of Technology, Sweden (1998), and the Ph.D. degree from Georgia Institute of Technology (2004), all in Electrical Engineering. Dr. Piya is currently an associate professor in Telecommunication Program, Faculty of Science and Technology, Nakhon Pathom Rajabhat University, Nakhon Pathom, Thailand. His main research interests include coding and signal processing as applied to digital data storage systems.

Dr. Lunchakorn Wuttisittikulkij received the B.Eng. degree in Electrical Engineering from Chulalongkorn University in 1990, the M.Sc. in Telecommunications and Information Systems and PhD in 1992 and 1997 respectively from the University of Essex. Dr. Lunchakorn is an associate professor in the department of Electrical Engineering and associated with the telecommunication system research laboratory, Chulalongkorn University. His main research interests are channel coding techniques and medium access control protocols for wireless networks. Specific current research topics include LPDC codes, multi-wavelength optical networks and design and analysis of collision resolution algorithms.