Designs, Codes and Cryptography (2020) 88:41–49
https://doi.org/10.1007/s10623-019-00667-0

Construction of girth-8 *(3,L)*-QC-LDPC codes of smallest CPM size using column multipliers

Jasvinder Singh[1,2] · **Manish Gupta**[2] · **Jaskarn Singh Bhullar**[3]

Received: 26 October 2018 / Revised: 18 July 2019 / Accepted: 19 July 2019 / Published online: 2 August 2019

Abstract
In this paper, a new method for the construction of the exponent matrix of quasi-cyclic low-density parity-check (QC-LDPC) codes is proposed. The entries of the exponent matrix are based on the column multipliers. To find the column multipliers, a parameter S_{α} is defined which gives the value of column multiplier of the αth column. The proposed method reduced the complexity related to the formation of the exponent matrix and results in *(3,L)*-QC-LDPC codes with girth at least eight, for $L > 3$. Also, a lower bound on the size of the circulant permutation matrix (CPM) for a QC-LDPC code is derived, and the codes constructed by this method are optimal to the given bound. Further, most of the codes constructed using this method are of smaller CPM size. Specifically, for $L > 25$, our constructed QC-LDPC codes have the shortest CPM size compared to the existing ones in the literature.

Keywords Quasi-cyclic low-density parity-check codes · Girth · Circulant permutation matrix · Exponent matrix

Mathematics Subject Classification 94B60 · 94B65

1 Introduction

In the last 50 years, LDPC codes came to prominence, since they outperform in iterative decoding and show the capacity approaching performance. QC-LDPC codes, an important class of LDPC codes perform very well in encoding as well as in decoding because of its quasi-cyclic nature and so, have been adopted by many communication systems [2]. A regular-*(J,L)*-QC-LDPC code with CPM size q, is specified by a parity-check matrix (PCM)

Communicated by D. Panario.

✉ Manish Gupta
manishgupta.bti@gmail.com

[1] I.K.G Punjab Technical University, Jalandhar, Punjab, India

[2] Department of Applied Sciences, Baba Farid College of Engineering and Technology, Bathinda, Punjab, India

[3] Department of Applied Sciences, Malout Institute of Management and Information Technology, Malout, Punjab, India

H, which is a $J \times L$ array of $q \times q$ circulant permutation matrices (CPMs). The CPM $I(e_{ij})$, $1 \le i \le J, 1 \le j \le L$, is the $q \times q$ identity matrix in which ones in each row are cyclically shifted to the right by e_{ij} positions. The matrix $[e_{ij}]_{J \times L}$ is called the exponent matrix. The one can derive a PCM from an exponent matrix by replacing its elements with the corresponding circulant matrices. The iterative decoding performance of QC-LDPC codes depends upon the girth of the code. Girth is the length of the shortest cycle present in the Tanner graph representation of code [9]. QC-LDPC codes, free from short-cycles, i.e., with girth at least six have better decoding performance in comparison with codes having short-cycles. Therefore, to construct QC-LDPC codes with girth six or more and having the minimum CPM size is the core aim of current research [1, 3–7, 10, 12, 20]. QC-LDPC codes are also used as underlying codes for the construction of QC-LDPC lattices to achieve the sphere-bound [6].

Although QC-LDPC codes can be constructed by a variety of methods, the constructions based on exponent matrices or base matrices have attracted much attention [3, 5, 8, 11, 13, 14]; these constructions give ease to find the short-cycles even when the code has large block length. The construction of QC-LDPC codes with base matrices can further be categorised as the algebraic methods [8, 15–18] and the search based methods [1, 3, 13, 14]. The method based on difference matrices is also seemed useful to generate the QC-LDPC codes of more considerable girth and with less complexity [1].

At the outset, in 2004, the girth-6 *(J,L)*-QC-LDPC codes for $J = 2, 3, 4, 5, 6$ have been constructed with a combination of algebraic method and the computer search, but the search was limited to only $L = 13$ [3]. The necessary and sufficient conditions for *(J,L)*-QC-LDPC codes for given girth were also derived in [3]. Later on, a significant part of the work has been devoted to the search of QC-LDPC codes with the minimum CPM size and higher girth [4, 5, 10, 12, 13, 20]. The work was extended in [18], which proposed the girth-8 *(3,L)*-QC-LDPC codes of smaller CPM size. In continuity, *(5,L)* and *(6,L)*-QC-LDPC codes with girth at least eight were deterministically constructed by [19] and proved that *(5,L)* and *(6,L)*-QC-LDPC codes always exist for CPM size $q \ge (2L + 3)(L - 1) + 1$ and $q \ge 2(L + 5)(L - 1) + 1$ respectively, which were the improvements over two existing bounds $L^2(L - 1) + 1$ and $(L^2 + 1)(L - 1) + 1$, respectively. Similar work was done by [14], which searched the *((3,4,5,6),L)*-QC-LDPC codes with girth at least eight for $L \le 25$, out of which most of the codes are of smaller size in comparison with existing codes. In literature, it is observed that the most of the algebraic constructions of *(J,L)*-QC-LDPC codes are based on row multipliers, as in [5], girth-8 *(J,L)*-QC-LDPC codes for $J = 3, 4, 5, 6$, were constructed by row multipliers $(0, 1, L, L + 1, L^2, L^2 + 1)$. In [17], row multipliers, to construct a girth-8 QC-LDPC code were derived using the greatest common divisor (GCD) method. In [19], (J, L)-QC-LDPC codes with girth at least eight were constructed by taking the row multipliers $(0, 1, L, L + 1, L^2, L^2 + 1, L^2 + L, L^2 + L + 1)$, for $J = 3$ to 8. Therefore, we can see that most of the existing methods concentrated only on row multipliers to construct the exponent matrices of QC-LDPC codes and also the codes constructed by row multipliers have larger CPM size for larger values of L.

In this paper, a new way to construct the exponent matrix E of a QC-LDPC code is proposed, which is based on the column multipliers. The idea gives an algebraic structure of *(3,L)*-QC-LDPC codes with girth at least eight, and having smaller CPM size as compared to the respective codes constructed by row multipliers. The structure of the exponent matrix based on column multipliers is defined as follow:

Definition 1.1 Let $E = [e_{ij}]$ be an exponent matrix of order $3 \times L$, such that $e_{ij} = (i - 1)(S_j - 1)$ for all $1 \le i \le 3, 1 \le j \le L\,(L > 3)$. i.e.

$$E = \begin{bmatrix} (S_1-1).0 & (S_2-1).0 & (S_3-1).0 & \dots\dots & (S_L-1).0 \\ (S_1-1).1 & (S_2-1).1 & (S_3-1).1 & \dots\dots & (S_L-1).1 \\ (S_1-1).2 & (S_2-1).2 & (S_3-1).2 & \dots\dots & (S_L-1).2 \end{bmatrix}_{3\times L}$$

Here, S_α gives us the value of column multiplier for the αth column. The exponent matrix is derived with the help of generator column $[0, 1, 2]^T$ by multiplying it with different column multipliers. To find the adequate values of column multipliers, S_α is defined as follow:

Definition 1.2 $S_\alpha = 1 + \sum_{m=0}^{k} \alpha_m \zeta_m$, where, $\alpha_m = \left\lfloor \frac{\alpha + 2^m - 1}{2^{m+1}} \right\rfloor$ and $\zeta_m = \frac{3^m+1}{2}$ such that $2^k \le \alpha < 2^{k+1}$, $\alpha \in \mathbb{N}$ and $k \in \mathbb{Z}^*$.

Example If $L = 7$, then the column multipliers S_α for $1 \le \alpha \le 7$ are 1, 2, 4, 5, 10, 11, 13 respectively, and the corresponding exponent matrix E is given by:

$$E = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 4 & 9 & 10 & 12 \\ 0 & 2 & 6 & 8 & 18 & 20 & 24 \end{bmatrix}$$

This exponent matrix has corresponded to a *(3,7)*-QC-LDPC code with girth at least eight.

Also, a lower bound $q \ge 2S_L - 1$ for the minimum CPM size q of *(3,L)*-QC-LDPC codes with girth at least eight, has been proposed, which is the tightest bound among the literature. The main advantage of this method is that it is an algebraic based method due to which it reduces the complexity and gives ease to derive the exponent matrix for any value of $L > 3$. Moreover, all the codes constructed from this method are optimal to the given lower bound on the minimum CPM size and for $L > 25$ are of shortest CPM size as compared to existing QC-LDPC codes of girth at least eight.

The rest of the paper is ordered as follow: In Sect. 2, the construction and the bound on the minimum CPM size for *(3,L)*-QC-LDPC codes with girth at least eight are presented. The conclusion of the paper is given in Sect. 3.

2 Construction of *(3,L)*-QC-LDPC codes with girth at least 8

In this section, explicit construction of the exponent matrix of a girth-8 QC-LDPC code is given. To define the essential properties and characteristics of S_α, some of the lemmas are proved. With the help of these lemmas and theorems, it is proved that the exponent matrix E corresponds a *(3,L)*-QC-LDPC codes of girth at least eight.

Lemma 2.1 *If $\alpha < \beta$ then $\alpha_m < \beta_m$, for at least one of the value of m such that $0 \le m \le k$, $m \in \mathbb{Z}^*$ and $2^k \le \alpha < \beta < 2^{k+1}$.*

Proof

Case 1 *If $\beta = \alpha + 1$*

Sub-case 1.1 *When α is odd,*
Since $\beta = \alpha + 1$ and α is odd $\Rightarrow \beta$ is even

$\Rightarrow$ there exists a number $t \in \mathbb{N}$ such that $\frac{\beta}{2} = t$ and $\frac{\alpha}{2} = t - \frac{1}{2}$

$\therefore \beta_0 = \left\lfloor \frac{\beta+2^0-1}{2^{0+1}} \right\rfloor = \left\lfloor \frac{\beta}{2} \right\rfloor = t$ and $\alpha_0 = \left\lfloor \frac{\alpha+2^0-1}{2^{0+1}} \right\rfloor = \left\lfloor \frac{\alpha}{2} \right\rfloor = \left\lfloor t - \frac{1}{2} \right\rfloor = t - 1 \Rightarrow \alpha_0 < \beta_0$

Sub-case 1.2 *When α is even*
We, further divide it into two cases

Sub-case 1.2.a *When* $\alpha = 2^k$
Then, $\beta_k = \left\lfloor \frac{2^k+1+2^k-1}{2^{k+1}} \right\rfloor = 1$ and $\alpha_k = \left\lfloor \frac{2^k+2^k-1}{2^{k+1}} \right\rfloor = 0 \Rightarrow \alpha_k < \beta_k$

Sub-case 1.2.b *When* $\alpha \neq 2^k$
Since α is even, therefore, there exists at least one i $(0 < i < k)$ such that $2^i | \alpha$ but $2^{i+1} \nmid \alpha$
therefore, $\alpha_i = \left\lfloor \frac{\alpha+2^i-1}{2^{i+1}} \right\rfloor$ and $\beta_i = \left\lfloor \frac{\beta+2^i-1}{2^{i+1}} \right\rfloor = \left\lfloor \frac{\alpha+2^i}{2^{i+1}} \right\rfloor$
as, $2^i | \alpha$ then there exists a number $t \in \mathbb{N}$ such that $\frac{\alpha}{2^i} = t$
but $2^{i+1} \nmid \alpha \Rightarrow 2^{i+1} \nmid 2^i.t \Rightarrow 2 \nmid t \Rightarrow t$ is odd and so, let $\frac{t+1}{2} = n \in \mathbb{N}$
now, $\alpha_i = \left\lfloor \frac{\alpha+2^i-1}{2^{i+1}} \right\rfloor$ and $\beta_i = \left\lfloor \frac{\alpha+2^i}{2^{i+1}} \right\rfloor \Rightarrow \alpha_i = \left\lfloor \frac{2^i.t+2^i-1}{2^{i+1}} \right\rfloor = n - 1$ and $\beta_i = \left\lfloor \frac{2^i.t+2^i}{2^{i+1}} \right\rfloor = n \Rightarrow \alpha_i < \beta_i$.

Case 2 *When* $\beta > \alpha + 1$
Let, $\beta = \alpha + n$ where $n \geq 2$
then $\beta_0 = \left\lfloor \frac{\beta+2^0-1}{2^{0+1}} \right\rfloor = \left\lfloor \frac{\beta}{2} \right\rfloor = \left\lfloor \frac{\alpha+n}{2} \right\rfloor \geq \left\lfloor \frac{\alpha}{2} + 1 \right\rfloor > \left\lfloor \frac{\alpha}{2} \right\rfloor = \left\lfloor \frac{\alpha+2^0-1}{2^{0+1}} \right\rfloor = \alpha_0$
$\Rightarrow \alpha_0 < \beta_0$.
Hence, the proof is complete. □

Lemma 2.2 *If $\alpha < \beta$ then $S_\alpha < S_\beta$ for all $\alpha, \beta \in \mathbb{N}$.*

Proof Since, $\alpha < \beta \Rightarrow \frac{\alpha+2^m-1}{2^{m+1}} < \frac{\beta+2^m-1}{2^{m+1}} \quad \forall m \in \mathbb{Z}^* \Rightarrow \left\lfloor \frac{\alpha+2^m-1}{2^{m+1}} \right\rfloor \leq \left\lfloor \frac{\beta+2^m-1}{2^{m+1}} \right\rfloor \quad \forall m \in \mathbb{Z}^*$ $\Rightarrow \alpha_m \leq \beta_m \; \forall m \in \mathbb{Z}^* \Rightarrow \alpha_m \zeta_m \leq \beta_m \zeta_m \; \forall m \in \mathbb{Z}^*$ from Lemma 2.1, we have $\alpha_m < \beta_m$ for at least one value of $m \Rightarrow \sum_{m=0}^{k} \alpha_m \zeta_m < \sum_{m=0}^{k} \beta_m \zeta_m$ where $\alpha < \beta < 2^{k+1} \Rightarrow S_\alpha < S_\beta$.

Lemma 2.3 *If $\alpha = 2^k$ then $S_\alpha = \zeta_k \; \forall \, k \geq 0$.*

Proof Since,

$$\alpha_m = \left\lfloor \frac{\alpha + 2^m - 1}{2^{m+1}} \right\rfloor \text{ and } 0 \leq m \leq k$$

$$\Rightarrow \alpha_m = \left\lfloor \frac{2^k + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m-1} + \frac{1}{2} - \frac{1}{2^{m+1}} \right\rfloor = \begin{cases} 2^{k-1-m} & when \; 0 \leq m < k \\ 0 & m \geq k \end{cases}$$

$$\Rightarrow S_\alpha = 1 + \sum_{m=0}^{k} \alpha_m \zeta_m = 1 + \alpha_0 \zeta_0 + \alpha_1 \zeta_1 + \ldots + \alpha_{k-1} \zeta_{k-1} + \alpha_k \zeta_k$$

$$\Rightarrow S_\alpha = 1 + 2^{k-1}\left(\frac{3^0+1}{2}\right) + 2^{k-2}\left(\frac{3^1+1}{2}\right) + \ldots + 2^{k-1-k-1}\left(\frac{3^{k-1}+1}{2}\right) + 0.\left(\frac{3^k+1}{2}\right) = \zeta_k$$

Hence, the proof is complete. □

Theorem 2.4 *If* $0 < \alpha < \beta < \gamma$ *then* $2S_\beta \neq S_\alpha + S_\gamma$ *for all* $\alpha, \beta, \gamma \in \mathbb{N}$.

Proof Since, $0 < \alpha < \beta < \gamma$, and let k is any positive integer, then the following cases arise:

Case 1 When $\beta = 2^k$, α and γ may have any value.
Since $\beta = 2^k$, we have from Lemma 2.3, $S_\beta = \zeta_k \, \forall \, k \geq 0$, and also $\beta < \gamma \Rightarrow \gamma \geq 2^k + 1$

$$\Rightarrow \gamma_m \geq \left\lfloor \frac{2^k + 1 + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m-1} + \frac{1}{2} \right\rfloor = \begin{cases} 2^{k-1-m} & when\ 0 \leq m < k \\ 1 & m = k \\ 0 & otherwise \end{cases}$$

$$\text{and } \beta_m = \left\lfloor \frac{2^k + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m-1} + \frac{1}{2} - \frac{1}{2^{m+1}} \right\rfloor = \begin{cases} 2^{k-1-m} & when\ 0 \leq m < k \\ 0 & m = k \end{cases}$$

$$\Rightarrow S_\gamma = 1 + \sum_{m=0}^{k} \gamma_m \zeta_m \geq 1 + \sum_{m=0}^{k-1} 2^{k-1-m} \zeta_m + \zeta_k \geq 1 + \sum_{m=0}^{k} \beta_m \zeta_m + \zeta_k = 2S_\beta$$

$$\Rightarrow S_\gamma + S_\alpha > 2S_\beta \text{ and so } 2S_\beta \neq S_\alpha + S_\gamma$$

Case 2 When $\beta = 2^k + 1$ and

Sub-case 2.1 $\gamma \leq 2^{k+1}$ and α may have any value
Since $\beta = 2^k + 1$, $\gamma \leq 2^{k+1}$ and α may have any value

$$\Rightarrow \beta_m = \left\lfloor \frac{2^k + 1 + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m-1} + \frac{1}{2} \right\rfloor = \begin{cases} 2^{k-1-m} & when\ 0 \leq m < k \\ 1 & m = k \end{cases}$$

$$\text{and } \gamma_m \leq \left\lfloor \frac{2^{k+1} + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m} + \frac{1}{2} - \frac{1}{2^{m+1}} \right\rfloor = \begin{cases} 2^{k-m} & when\ 0 \leq m \leq k \\ 0 & m = k+1 \end{cases}$$

$$\text{we have, } S_\gamma = 1 + \sum_{m=0}^{k+1} \gamma_m \zeta_m \leq 1 + \sum_{m=0}^{k} 2^{k-m} \zeta_m = 1 + 2 \sum_{m=0}^{k} 2^{k-1-m} \zeta_m$$

$$\Rightarrow S_\gamma \leq 1 + 2 \sum_{m=0}^{k-1} 2^{k-1-m} \zeta_m + \zeta_k$$

$$\Rightarrow S_\gamma \leq 1 + 2 \sum_{m=0}^{k} \beta_m \zeta_m - 2\beta_k \zeta_k + \zeta_k = 2S_\beta - 1 - \zeta_k$$

$$\Rightarrow S_\gamma + 1 + \zeta_k \leq 2S_\beta \tag{2.1}$$

since $\alpha < \beta = 2^k + 1 \Rightarrow \alpha \leq 2^k \Rightarrow S_\alpha \leq \zeta_k$ [$\because$ of Lemma 2.3]
we have from (2.1), $S_\gamma + 1 + S_\alpha \leq S_\gamma + 1 + \zeta_k \leq 2S_\beta \Rightarrow S_\gamma + S_\alpha < 2S_\beta \Rightarrow 2S_\beta \neq S_\alpha + S_\gamma$.

Sub-case 2.2 $\gamma > 2^{k+1}$ and α may have any value
Since $\gamma > 2^{k+1} \Rightarrow \gamma \geq 2^{k+1} + 1$

$$\Rightarrow \gamma_m > \left\lfloor \frac{2^{k+1} + 1 + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m} + \frac{1}{2} \right\rfloor = \begin{cases} 2^{k-m} & when\ 0 \leq m \leq k \\ 1 & m = k+1 \\ 0 & otherwise \end{cases}$$

$$\text{and } \beta_m = \begin{cases} 2^{k-1-m} & when\ 0 \leq m < k \\ 1 & m = k \end{cases}$$

$$\text{now, } S_\gamma = 1 + \sum_{m=0}^{k+1} \gamma_m \zeta_m > 1 + \sum_{m=0}^{k} 2^{k-m} \zeta_m + \zeta_{k+1}$$

$$\Rightarrow S_\gamma > 1 + 2 \sum_{m=0}^{k} 2^{k-1-m} \zeta_m + \zeta_{k+1} = 1 + 2 \sum_{m=0}^{k-1} 2^{k-1-m} \zeta_m + 2.2^{k-1-k} \zeta_k + \zeta_{k+1}$$

$$\Rightarrow S_\gamma > 1 + 2 \sum_{m=0}^{k-1} \beta_m \zeta_m + \zeta_k + \zeta_{k+1} = 1 + 2 \sum_{m=0}^{k} \beta_m \zeta_m - 2\beta_k \zeta_k + \zeta_k + \zeta_{k+1}$$

$$\Rightarrow S_\gamma > 2S_\beta - 1 - \zeta_k + \zeta_{k+1} = 2S_\beta - 1 - \frac{3^k + 1}{2} + \frac{3^{k+1} + 1}{2} = 2S_\beta - 1 + 3^k > 2S_\beta$$

$$\Rightarrow S_\gamma > 2S_\beta \Rightarrow S_\gamma + S_\alpha > 2S_\beta \Rightarrow 2S_\beta \neq S_\alpha + S_\gamma$$

Case 3. When $2^k + 1 < \beta < 2^{k+1}$

Sub-case 3.1 $\gamma > 2^{k+1}$ and α may have any value
since $2^k + 1 < \beta < 2^{k+1}$, $2^{k+1} < \gamma$ and $\alpha < \beta \Rightarrow \gamma \geq 2^{k+1} + 1$

$$\Rightarrow \gamma_m \geq \left\lfloor \frac{2^{k+1} + 1 + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m} + \frac{1}{2} \right\rfloor = \begin{cases} 2^{k-m} & when\ 0 \leq m \leq k \\ 1 & m = k+1 \\ 0 & otherwise \end{cases}$$

$$\text{and, } \beta_m < \left\lfloor \frac{2^{k+1} + 2^m - 1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m} + \frac{1}{2} - \frac{1}{2^{m+1}} \right\rfloor = \begin{cases} 2^{k-m} & when\ 0 \leq m \leq k \\ 0 & m = k+1 \end{cases}$$

$$\text{we have, } S_\gamma = 1 + \sum_{m=0}^{k+1} \gamma_m \zeta_m = 1 + \sum_{m=0}^{k} \gamma_m \zeta_m + \gamma_{k+1} \zeta_{k+1} > 1 + \sum_{m=0}^{k} 2^{k-m} \zeta_m + \zeta_{k+1}$$

$$\Rightarrow S_\gamma > 1 + \sum_{m=0}^{k} 2^{k-m} \zeta_m + S_{2^{k+1}} [\because \text{of Lemma 2.3, } \zeta_{k+1} = S_{2^{k+1}}]$$

$$\Rightarrow S_\gamma > 1 + \sum_{m=0}^{k} \beta_m \zeta_m + S_{2^{k+1}} > S_\beta + S_\beta [\because \text{of Lemma 2.2}]$$

$$\Rightarrow S_\gamma > 2S_\beta \Rightarrow S_\gamma + S_\alpha > 2S_\beta \Rightarrow 2S_\beta \neq S_\alpha + S_\gamma$$

Sub-case 3.2 $\gamma \leq 2^{k+1}$ and α may have any value
since $2^k + 1 < \beta < 2^{k+1}, \gamma \leq 2^{k+1}$ and $\alpha < \beta$

$$\Rightarrow \gamma_m \le \left\lfloor \frac{2^{k+1}+2^m-1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m} + \frac{1}{2} - \frac{1}{2^{m+1}} \right\rfloor = \begin{cases} 2^{k-m} & when\ 0 \le m \le k \\ 0 & m = k+1 \end{cases}$$

$$\text{and } \beta_m \ge 2^k + 2 = \left\lfloor \frac{2^k+2+2^m-1}{2^{m+1}} \right\rfloor = \left\lfloor 2^{k-m-1} + \frac{1}{2} + \frac{1}{2^{m+1}} \right\rfloor = \begin{cases} 2^{k-1}+1 & when\ m = 0 \\ 2^{k-1-\mathrm{m}} & 0 < m \le k-1 \\ 1 & when\ m = k \end{cases}$$

now,

$$S_\gamma = 1 + \sum_{m=0}^{k+1} \gamma_m \zeta_m = 1 + \gamma_0\zeta_0 + \sum_{m=1}^{k-1} \gamma_m\zeta_m + \gamma_k\zeta_\mathrm{k} + \gamma_{k+1}\zeta_{k+1} < 1 + \sum_{m=0}^{k-1} 2^{k-m}\zeta_m + \zeta_k$$

$$\Rightarrow S_\gamma < 1 + 2\sum_{m=0}^{k-1} 2^{k-1-m}\zeta_m + \zeta_k < 1 + 2\sum_{m=0}^{k} \beta_m\zeta_m - 2\beta_k\zeta_k + \zeta_k$$

$$\Rightarrow S_\gamma + S_\alpha < 2S_\beta$$

Therefore, for all the cases $S_\gamma + S_\alpha \ne 2S_\beta$. Hence, the proof is complete. □

Theorem 2.5 *The exponent matrix E is corresponded to a QC-LDPC code with girth at least 8 and with CPM size* $q \ge 2S_L - 1$.

Proof To prove that the corresponding codes are of girth at least 8, firstly we have to prove that there is no 4-cycle. For this, if possible, let us suppose there is a 4-cycle present in *a*th and *b*th rows and *c*th and *d*th columns. So by Theorem 2.1 of [3], we have

$$\begin{aligned}
&\left(e_{ac} - e_{bc}\right) + \left(e_{bd} - e_{ad}\right) \equiv 0(modq) \\
&\Rightarrow \left((a-1)\left(S_c - 1\right) - (b-1)\left(S_c - 1\right)\right) + \left((b-1)\left(S_d - 1\right) - (a-1)\left(S_d - 1\right)\right) \equiv 0(modq) \\
&\Rightarrow \left(S_c - 1\right)(a-b) - \left(S_d - 1\right)(a-b) \equiv 0(modq) \Rightarrow (a-b)\left(S_c - S_d\right) \equiv 0(modq) \\
&\text{since, } q \ge 2S_L - 1,\ 1 \le a < b \le 3 \text{ and } 1 \le c < d \le L \\
&\Rightarrow 1 \le S_c < S_d \le S_L [\because \text{of Lemma 2.2}]
\end{aligned}$$

also $0 < (\mathrm{a}-\mathrm{b})\left(\mathrm{S_c} - \mathrm{S_d}\right) = (\mathrm{b}-\mathrm{a})\left(\mathrm{S_d} - \mathrm{S_c}\right) < 2\left(\mathrm{S_L} - 1\right) < q$ therefore, $(a-b)\left(S_c - S_d\right) \equiv 0(modq)$ becomes a simple equation i.e. $(a-b)\left(S_c - S_d\right) = 0$ and so, we have $a = b$ or $S_c = S_d$, which is not possible. Therefore, there is no 4-cycle present in QC-LDPC codes corresponding to exponent matrix E. □

Now, we will prove that there is no 6-cycle present in the corresponding QC-LDPC codes. If possible, suppose there is a 6-cycle present in 1st, 2nd and 3rd rows and *d*th, *e*th and *f*th columns. So again, by Theorem 2.1 of [3], we have

Table 1 Comparison on the minimum CPM size $\boldsymbol{q}$ of the proposed *(3,L)*-QC-LDPC codes with the codes given by [18] for girth at least 8 and for $26 \leq \boldsymbol{L} \leq 40$

L	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Proposed	219	223	225	235	237	241	243	487	489	493	495	505	507	511	513
[18]	339	379	393	436	451	497	513	562	579	631	649	704	723	781	801

$$
\begin{aligned}
(e_{1d} - e_{3d}) + (e_{3e} - e_{2e}) + (e_{2f} - e_{1f}) &\equiv 0(modq)\\
(e_{1d} - e_{3d}) + (e_{3f} - e_{2f}) + (e_{2e} - e_{1e}) &\equiv 0(modq)\\
(e_{2d} - e_{3d}) + (e_{3f} - e_{1f}) + (e_{1e} - e_{2e}) &\equiv 0(modq)\\
(e_{1d} - e_{2d}) + (e_{2e} - e_{3e}) + (e_{3f} - e_{1f}) &\equiv 0(modq)\\
(e_{2d} - e_{3d}) + (e_{3e} - e_{1e}) + (e_{1f} - e_{2f}) &\equiv 0(modq)\\
(e_{1d} - e_{2d}) + (e_{2f} - e_{3f}) + (e_{3e} - e_{1e}) &\equiv 0(modq)
\end{aligned}
$$

substitute the values of e_{ij} for different values of i and j, and after some simple calculations, we get

$$S_e + S_f \equiv 2S_d(modq) \tag{2.2}$$

$$S_f + S_e \equiv 2S_d(modq) \tag{2.3}$$

$$2S_f \equiv (S_d + S_e)(modq) \tag{2.4}$$

$$2S_f \equiv (S_d + S_e)(modq) \tag{2.5}$$

$$2S_e \equiv (S_d + S_f)(modq) \tag{2.6}$$

$$2S_e \equiv (S_d + S_f)(modq) \tag{2.7}$$

From Eqs. (2.2) and (2.3), we have

$$S_e + S_f \equiv 2S_d(modq)$$

since $\mathrm{d} < e < f \leq L \Rightarrow \mathrm{S_d} < \mathrm{S_e} < \mathrm{S_f} \leq \mathrm{S_L} \Rightarrow S_e + S_f \leq S_L - 1 + S_L \leq q$ and also $2S_d < q$ hence, both the sides of Eqs. (2.2) and (2.3), are less than q so that the equations can be written as a simple equation, i.e., $S_e + S_f = 2S_d < S_e + S_d \Rightarrow S_f < S_d$, which contradicts the Lemma 2.2. Similarly, the remaining four equations also become simple equations. Now, from Eqs. (2.4) and (2.5), we have $2S_f = S_d + S_e < S_e + S_e \Rightarrow 2S_f < 2S_e \Rightarrow S_f < S_e$ which is not possible, because $S_d < S_e < S_f$. Similarly, from Eqs. (2.6) and (2.7), we have $2S_e = S_d + S_f$ where, $\mathrm{d} < e < f$, which contradicts the Theorem 2.4 and so, $2S_e \neq S_d + S_f$. Hence, all the six equations are not satisfied, which contradicts our supposition that there exists a 6-cycle.

Therefore, QC-LDPC codes corresponded by exponent matrix E are free from 4-cycles, and 6-cycles. Moreover, it is also make cleared from the above theorem that the proposed codes satisfy the tightest lower bound $q \geq 2S_L - 1$ on the minimum CPM size q, and hence are of the smallest size in literature. To validate our claim, we compare the minimum CPM size of our proposed girth-8 QC-LDPC codes with the ones in [18] (see Table 1).

3 Conclusion

A new and simple method to construct the exponent matrix for a QC-LDPC code is given in this paper. The method is capable of constructing the exponent matrix of order $3 \times L$, for any value of $L > 3$, by using the column multipliers. For the proposed method, a lower bound on the minimum CPM size q is given, which is the tightest lower bound in literature. Moreover, all the constructed QC-LDPC codes by the proposed method are optimal to the given bound. Most of the constructed codes are of the smallest CPM size in comparison with existing codes based on algebraic constructions.

References

1. Amirzade F., Sadeghi M.R.: Lower bounds on the lifting degree of QC-LDPC codes by difference matrices. IEEE Access. **6**, 23688–23700 (2018).
2. Draft DVB-S2 Standard: ETSI EN 302 307-1 V1.4.1. https://www.dvb.org/standards/dvb-s2 (2014). Accessed 23 January 2018.
3. Fossorier M.P.C.: Quasi-cyclic low-density parity-check codes from circulant permutation matrices. IEEE Trans. Inf. Theory **50**(8), 1788–1793 (2004).
4. Gholami M., Gholami Z.: An explicit method to generate some QC-LDPC codes with girth 8. Iran. J. Sci. Technol. Trans. A Sci. **40**(2), 145–149 (2016).
5. Karimi M., Banihashemi A.H.: On the girth of quasi-cyclic protograph LDPC codes. IEEE Trans. Inf. Theory **59**(7), 4542–4552 (2013).
6. Khodaiemehr H., Sadeghi M.R., Sakzad A.: Practical encoder and decoder for power constrained QC LDPC-lattice codes. IEEE Trans. Commun. **65**(2), 486–500 (2017).
7. Kim K.J., Chung J.H., Yang K.: Bounds on the size of parity-check matrices for quasi-cyclic low-density parity-check codes. IEEE Trans. Inf. Theory **59**(11), 7288–7298 (2013).
8. Li L., Li H., Li J., Jiang H.: Construction of type-II QC-LDPC codes with fast encoding based on perfect cyclic difference sets. Optoelectron. Lett. **13**(5), 358–362 (2017).
9. Mao Y., Banihashemi A.H.: A heuristic search for good low-density parity-check codes at short block lengths. Proc. IEEE ICC. **1**, 41–44 (2001).
10. Mellinger K.E.: LDPC codes from triangle-free line sets. Des. Codes Cryptogr. **32**(1–3), 341–350 (2004).
11. Sadeghi M., Amirzade F.: Analytical lower bound on the lifting degree of multiple-edge QC-LDPC codes with girth 6. IEEE Commun. Lett. **22**(8), 1528–1531 (2018).
12. Sakzad A., Sadeghi M., Panario D.: Codes with girth 8 tanner graph representation. Des. Codes Cryptogr. **57**(1), 71–81 (2010).
13. Tasdighi A., Banihashemi A.H., Sadeghi M.R.: Efficient search of girth-optimal QC-LDPC codes. IEEE Trans. Inf. Theory **62**(4), 1552–1564 (2016).
14. Tasdighi A., Banihashemi A.H., Sadeghi M.R.: Symmetrical constructions for regular girth-8 QC-LDPC codes. IEEE Trans. Commun. **65**(1), 14–22 (2017).
15. Vandendriessche P.: Some low-density parity-check codes derived from finite geometries. Des. Codes Cryptogr. **54**(3), 287–297 (2010).
16. Yuan J., Liang M., Wang Y., Lin J., Pang Y.: A novel construction method of QC-LDPC codes based on CRT for optical communications. Optoelectron. Lett. **12**(3), 208–211 (2016).
17. Zhang G., Sun R., Wang X.: Construction of girth-eight QC-LDPC codes from greatest common divisor. IEEE Commun. Lett. **17**(2), 369–372 (2013).
18. Zhang G., Sun R., Wang X.: Several explicit constructions for (3, L)-QC-LDPC codes with girth at least eight. IEEE Commun. Lett. **17**(9), 1822–1825 (2013).
19. Zhang J., Zhang G.: Deterministic girth-eight QC-LDPC codes with large column weight. IEEE Commun. Lett. **18**(4), 656–659 (2014).
20. Zhang L., Li B., Cheng L.: Constructions of QC-LDPC codes based on integer sequences. Sci. China Inf. Sci. **57**(6), 1–14 (2014).