Journal of Algebraic Systems
Vol. 9, No. 2, (2022), pp 229-239

$(7, K)$ GIRTH-8 QC-LDPC CODES WITH AN EXPLICIT CONSTRUCTION

M. MAJDZADE, M. GHOLAMI* AND G. RAEISI

Abstract. Recently, for each row weight K and column-weight J, $3 \leq J < K$, several classes of (J, K) quasi-cyclic (QC) low-density parity-check (LDPC) codes with girth 8 have been constructed explicitly such that their corresponding lower-bounds on the size of circulant permutation matrices (CPMs) have been considered small as possible. In this paper, for $J = 7$, a class of $(7, K)$ QC-LDPC codes with girth 8 is generated by an explicit method such that the lower-bounds of the constructed codes remarkably are better than the state-of-the-art bound $(K-1)(K^2+K)+1$.

1. Introduction

Low-density parity-check (LDPC) codes [4] are a main class of capacity-approaching linear codes, adopted in many practical applications. Each LDPC code is defined by the null space of a sparse binary *parity-check matrix* (PCM). One of the well-known classes of structured LDPC codes is *protograph* LDPC codes which are constructed by lifting a smaller *Tanner graph*, called the *base graph*. In the case of using circulant permutations in the lifting process, the resultant code is called *quasi cyclic* (QC) [3] preferred to other types of LDPC codes because of simple implementations and practical usages.

By a (J, K) QC-LDPC code with CPM-size P, we mean a linear code whose PCM is a $J \times K$ array of *circulant permutation matrices*

DOI: 10.22044/jas.2021.8911.1434.
MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.
Keywords: QC-LDPC codes, explicit constructions, girth, exponent matrix.
Received: 16 September 2019, Accepted: 24 February 2021.
*Corresponding author.

(CPMs) of size P. In fact, a (J, K) QC-LDPC code can be described by a CPM size P and a $J \times K$ matrix, called *exponent matrix*, of some non-negative integers less than P. In this case, if $E = (e_{i,j})$ is the exponent matrix, the corresponding QC-LDPC code is described by its PCM constructed by replacing each entry $e_{i,j}$ of E by CPM $\mathcal{I}^{e_{i,j}}$, where $\mathcal{I}^e$, $0 \leq e \leq P-1$, is the $P \times P$ permutation matrix $(\xi_{i,j})_{1 \leq i,j \leq P}$ in which $\xi_{i,j} = 1$ if and only if $j - i = e \bmod P$, in the other words

$$\mathcal{I}^e = \left(\begin{array}{c|c} 0 & \mathcal{I}_{P-e} \\ \hline \mathcal{I}_e & 0 \end{array} \right)$$

in which $\mathcal{I}_q$, $q \in \{e, P-e\}$, is the identity matrix of size q.

The length of the shortest cycles of the Tanner graph [15], girth, has been known to influence the code performance and the error correction and detection are improved by enlarging the girth [12], so some efforts have been made to construct LDPC codes with large girth [12]-[10]. In addition to girth, another important factor to design the exponent matrix, is its *lower-bound* [2]. In fact, corresponding to the exponent matrix E of a QC-LDPC code with girth g, a lower-bound on CPM-size is associated which is defined as the minimum positive integer P', such that for each integer $P \geq P'$, the girth of the code with exponent matrix E and CPM-size P is at least g.

For $J = 3$, $J = 4$ and $J = 5, 6$, in [16], [17] and [7], the authors have used some explicit methods to construct girth-8 (J, K) QC-LDPC codes with lower-bounds $K(K + (K \bmod 2))/2$, $3K^2/4 + K - 1$, and $K^2(K-1)+1$, $(K^2+1)(K-1)+1$, respectively. Moreover, in [19], the authors have provided several constructions for girth-8 QC-LDPC codes with column-weights $J \geq 3$ such that for $J = 5, 6$, the obtained lower-bounds are smaller rather than the ones in [7]. In this paper, some $(7, K)$ QC-LDPC codes are constructed explicitly such that the corresponding lower-bounds are smaller than the bounds in [19]. In fact, the lower-bound of the proposed codes is reduced to $(K-1)(K(K-3)+2)+1$ for even K, and for odd K $(K > 11)$, it is reduced to $(K-1)(\frac{K(K+1)}{2}+2)+1$ or $(K-1)(\frac{K(K+1)}{2}+4)+1$ provided that $\frac{K-1}{2}$ is even or odd, respectively. Moreover, for $K = 9, 11$, the lower-bounds are $385, 681$, respectively, which are still better than the corresponding lower-bounds 721, 1321 in [19].

2. Preliminaries

Let J, K be some positive integers with $J < K$. Hereinafter, we consider regular (J, K) QC-LDPC codes whose exponent matrices are represented as follows.

Definition 2.1. [18] Let $a_0, a_1, \ldots, a_{J-1}, P$ be some non-negative integers satisfying $a_0 < a_1 < \cdots < a_{J-1}$. The following matrix can be considered as the exponent matrix of a (J, K) QC-LDPC code with CPM-size P, denoted breifly by $E(a_0, \ldots, a_{J-1})$.

$$E = \begin{pmatrix} a_0.0 & a_0.1 & \ldots & a_0.(K-1) \\ a_1.0 & a_1.1 & \ldots & a_1.(K-1) \\ \vdots & \vdots & \ddots & \vdots \\ a_{J-1}.0 & a_{J-1}.1 & \ldots & a_{J-1}.(K-1) \end{pmatrix}$$

where for each $0 \leq p \leq J-1$ and $0 \leq q \leq K-1$, the product of a_p and q in modulo of P is denoted by $a_p.q$.

In [18], a sufficient condition is provided for QC-LDPC codes to have girth at least 8.

Lemma 2.2. *If* $(a_k - a_i)/\gcd(a_k - a_i, a_j - a_i) \geq K$ *for all triples* (a_i, a_j, a_k), $0 \leq i < j < k \leq J-1$, *called GCD constraint, then the QC-LDPC code with exponent matrix* $E(a_0, a_1, \cdots, a_{J-1})$ *has girth at least eight for each CPM-size* $P \geq (a_{J-1} - a_0)(K-1) + 1$.

Moreover, an algorithm, called GCDg8 is provided in [18] to generate the finite sequence $(a_0, \ldots, a_{J-1})$ satisfying in Lemma 2.2 by a recursive method.

For each integer X, if k is the integer satisfying in $2^k \leq X < 2^k + 1$, define the function $f_K(X)$ as $f_K(X) = x_k K^k + x_{k-1} K^{k-1} + \cdots + x_0 K^0$, where $(x_k, x_{k-1}, \ldots, x_0)$ is the binary representation of X. In [19], the authors have shown that for $\mathbf{a} = (a_0, \ldots, a_{J-1}) = (f_K(0), f_K(1), \ldots, f_K(J-1))$, the QC-LDPC code with exponent matrix $E(\mathbf{a})$ has girth at least 8, for each CPM-size $P \geq f_K(J-1)(K-1) + 1$. Especially, for $J = 7$, the exponent matrix is $E(0, 1, K, K+1, K^2, K^2+1, K^2+K)$ with the corresponding lower-bound $(K-1)(K^2+K) + 1$.

By the polynomial PCM of a QC-LDPC code, we mean a $J \times K$ matrix $H(x) = (h_{i,j}(x))$, where $h_{i,j}(x) = \sum_{l=0}^{P-1} h_{i,j,l} x^l \in \mathbb{F}_2[x]/ < x^P + 1 >$ and $wt(h_{i,j}(x))$ is defined as the number of non-zero terms in $h_{i,j}(x)$. Now, in [13], the following upper-bound is given on the minimum-distance based on the permanent of some submatrices of $H(x)$.

$$d_{\min}(C) \leq \min_{\substack{S \subseteq \{0, 1, \ldots, K-1\} \\ |S| = J+1}}^{*} \sum_{i \in S} wt(\mathrm{perm}(H_{S \setminus \{i\}}(x))) \qquad (2.1)$$

where the operator $\min^{*}$ gives back the minimum value of all nonzero entries in a list of values and $H_{S \setminus \{i\}}$ denotes a $J \times J$ submatrix of H with column indices in S except i.

TABLE 1. All possible triples (i, j, k) in the proof of Theorem 3.1

(i,j,k)	(a_i, a_j, a_k)	type of K	g_c	G	$K_{\min}$
$(0,1,2)$	$(0,1,K)$	–	1	K	0
$(0,1,3)$	$(0,1,K+1)$	–	1	$K+1$	0
$(0,1,4)$	$(0,1,3K-1)$	–	1	$3K-1$	0.5
$(0,1,5)$	$(0,1,5K-1)$	–	1	$5K-1$	0.25
$(0,1,6)$	$(0,1,K(K-3)+2)$	–	1	$K(K-3)+2$	3.414
$(0,2,3)$	$(0,K,K+1)$	–	1	$K+1$	0
$(0,2,4)$	$(0,K,3K-1)$	–	1	$3K-1$	0.5
$(0,2,5)$	$(0,K,5K-1)$	–	1	$5K-1$	0.25
$(0,2,6)$	$(0,K,K(K-3)+2)$	–	2	$(K(K-3)+2)/2$	4.561
$(0,3,4)$	$(0,K+1,3K-1)$	–	1	$3K-1$	0.5
$(0,3,5)$	$(0,K+1,5K-1)$	$K=6k+2,\ k\in\mathbb{Z}^+$	3	$(5K-1)/3$	0.5
		otherwise	1	$5K-1$	0.25
$(0,3,6)$	$(0,K+1,K(K-3)+2)$	$K=6k+2,\ k\in\mathbb{Z}^+$	3	$(K(K-3)+2)/3$	5.645
		otherwise	1	$K(K-3)+2$	3.414
$(0,4,5)$	$(0,3K-1,5K-1)$	–	1	$5K-1$	0.25
$(0,4,6)$	$(0,3K-1,K(K-3)+2)$	$K=10k+2,\ k\in\mathbb{Z}^+$	5	$(K(K-3)+2)/5$	7.741
		otherwise	1	$K(K-3)+2$	3.414
$(0,5,6)$	$(0,5K-1,K(K-3)+2)$	$K=18k+2,\ k\in\mathbb{Z}^+$	9	$(K(K-3)+2)/9$	11.830
		$K=6k+2, K\neq 18k+2,\ k\in\mathbb{Z}^+$	3	$(K(K-3)+2)/3$	5.645
		otherwise	1	$K(K-3)+2$	3.414
$(1,2,3)$	$(1,K,K+1)$	–	1	K	0
$(1,2,4)$	$(1,K,3K-1)$	–	1	$3K-2$	1
$(1,2,5)$	$(1,K,5K-1)$	$K=6k+4,\ k\in\mathbb{Z}^+$	3	$(5K-2)/3$	1
		otherwise	1	$5K-2$	0.5
$(1,2,6)$	$(1,K,K(K-3)+2)$	–	1	$K(K-3)+1$	3.732
$(1,3,4)$	$(1,K+1,3K-1)$	–	2	$(3K-2)/2$	2
$(1,3,5)$	$(1,K+1,5K-1)$	–	2	$(5K-2)/2$	0.666
$(1,3,6)$	$(1,K+1,K(K-3)+2)$	–	1	$K(K-3)+1$	3.732
$(1,4,5)$	$(1,3K-1,5K-1)$	$K=4k+6,\ k\in\mathbb{Z}^+$	4	$(5K-2)/4$	2
		$K=4k+4,\ k\in\mathbb{Z}^+$	2	$(5K-2)/2$	0.666
$(1,4,6)$	$(1,3K-1,K(K-3)+2)$	$K=10k+4,\ k\in\mathbb{Z}^+$	5	$(K(K-3)+1)/5$	7.872
		otherwise	1	$K(K-3)+1$	3.732
$(1,5,6)$	$(1,5K-1,K(K-3)+2)$	–	1	$K(K-3)+1$	3.732
$(2,3,4)$	$(K,K+1,3K-1)$	–	1	$2K-1$	1
$(2,3,5)$	$(K,K+1,5K-1)$	–	1	$4K-1$	0.333
$(2,3,6)$	$(K,K+1,K(K-3)+2)$	–	1	$K(K-3)+2-K$	4.561
$(2,4,5)$	$(K,3K-1,5K-1)$	–	1	$4K-1$	0.333
$(2,4,6)$	$(K,3K-1,K(K-3)+2)$	–	1	$K(K-3)+2-K$	4.561
$(2,5,6)$	$(K,5K-1,K(K-3)+2)$	$K=34k-4,\ k\in\mathbb{Z}^+$	17	$(K(K-3)+2-K)/17$	20.904
		otherwise	1	$K(K-3)+2-K$	4.561
$(3,4,5)$	$(K+1,3K-1,5K-1)$	–	2	$(4K-2)/2$	1
$(3,4,6)$	$(K+1,3K-1,K(K-3)+2)$	–	1	$K(K-3)+1-K$	4.791
$(3,5,6)$	$(K+1,5K-1,K(K-3)+2)$	$K=6k+2,\ k\in\mathbb{Z}^+$	3	$(K(K-3)+1-K)/3$	6.854
		otherwise	1	$K(K-3)+1-K$	4.791
$(4,5,6)$	$(3K-1,5K-1,K(K-3)+2)$	$K=6k+6,\ k\in\mathbb{Z}^+$	3	$(K(K-3)+3-3K)/3$	8.653
		otherwise	1	$K(K-3)+3-3K$	6.541

3. $(7, K)$ QC-LDPC codes with girth 8

In continue, for $J = 7$, some exponent matrices are generated by an explicit method such that the corresponding QC-LDPC codes have girth at least 8.

Theorem 3.1. *For $J = 7$ and even K, the finite sequence $(a_0, a_1, \ldots, a_6) = (0, 1, K, K+1, 3K-1, 5K-1, K(K-3)+2)$ satisfies the GCD constraint. Therefore, $E(0, 1, K, K+1, 3K-1, 5K-1, K(K-3)+2)$ corresponds to a $(7, K)$ QC-LDPC code with girth 8 for each $P \geq (K-1)(K(K-3)+2)+1$.*

Proof. Based on Lemma 2.2, it is sufficient to check the GCD condition $G = (a_k - a_i)/\gcd(a_k - a_i, a_j - a_i) \geq K$ for each triple of indices $0 \leq i < j < k \leq 6$ which is enumerated in $\binom{7}{3} = 35$ cases. All such cases are provided in Table 1. In the table, by g_c, we mean $\gcd(a_k - a_i, a_j - a_i)$. Moreover, for each case (i, j, k), the GCD condition holds for each $K > K_{\min}$. In some cases, g_c is computed for several states. To clarify the cases more clear to find $K_{\min}$, we refer the reader to Example 3.2 and Example 3.3. □

Example 3.2. For the case $(i, j, k) = (0, 5, 6)$ in Table 1, we have $(a_i, a_j, a_k) = (0, 5K-1, K(K-3)+2)$. Hence, for the subcase $K = 18k+2$, $k \geq 1$, we have $g_c = 9$, because $g_c = \gcd(90k+9, 324k^2+18k) = 9\gcd(10k+1, 2k(18k+1))$. On the other hand, $\gcd(10k+1, 2k(18k+1)) = \gcd(10k+1, 18k+1)$, because $\gcd(10k+1, 2k) = 1$. Moreover, $\gcd(10k+1, 18k+1) = \gcd(10k+1, (18k+1)-(10k+1)) = \gcd(10k+1, 8k) = 1$. In this case, from the equation $G = (K(K-3)+2)/9 \geq K$, we have $K \geq 6 + \sqrt{34} \sim 11.830$.

For the subcase $K = 6k+2$, $K \neq 18k+2$, $k \geq 1$, we have $g_c = \gcd((6k+2)(6k-1)+2, 30k+9) = \gcd(6k(6k+1), 3(10k+3)) = 3\gcd(2k(6k+1), 10k+3)$. On the other hand, $\gcd(2k(6k+1), 10k+3) = \gcd(2k, 10k+3)$, because $\gcd(6k+1, 10k+3) = \gcd(6k+1, (10k+3)-(6k+1)) = \gcd(6k+1, 4k+2) = \gcd(6k+1, 2k+1) = \gcd(4k, 2k+1) = 1$. Now, $\gcd(2k, 10k+3) = \gcd(2k, 3) = \gcd(k, 3) = 1$ if and only if $3 \nmid k$, or equivalently $18 \nmid K-2$. Then, $g_3 = 3$ and so $K \geq 3 + \sqrt{7} \sim 5.645$ by the equation $G = (K(K-3)+2)/3 \geq K$.

For the other subcases, we have $g_c = 1$, because $g_c = \gcd(K^2-3K+2, 5K-1) = \gcd(5K^2-15K+10, 5K-1) = \gcd(5K^2-15K+10, 5K-1) = \gcd(-14K+10, 5K-1) = \gcd(K+7, 5K-1) = \gcd(K+7, 36)$. On the other hand, $\gcd(K+7, 6) = \gcd(K+1, 6) = 1$, because K is even and $K \neq 2 \bmod 6$, so $\gcd(K+7, 36) = 1$. Then, from the equation $G = (K(K-3)+2) \geq K$, we have $K \geq 2 + \sqrt{2} \sim 3.414$.

Example 3.3. For the case $(i,j,k) = (2,5,6)$ in Table 1, we have $(a_i, a_j, a_k) = (K, 5K-1, K(K-3)+2)$. Hence, $\gcd(K(K-3)+2-K, 4K-1) = \gcd(K^2-4K+2, 4K-1) = \gcd(K^2-4K+2+(4K-1), 4K-1) = \gcd(K^2+1, 4K-1)$. On the other hand, $\gcd(K^2+1, 4K-1) = \gcd(K^2+1, K(4K-1)) = \gcd(K^2+1, K(4K-1)-(K^2+1)) = \gcd(K^2+1, 3K^2-K-1) = \gcd(K^2+1, 3K^2-K-1-3(K^2+1)) = \gcd(K^2+1, K+4) = \gcd((K^2+1-K(K+4), K+4) = \gcd(4K-1, K+4) = \gcd(4K-1-4(K-4), K+4) = \gcd(17, K+4)$. In this case, if $17 \mid K+4$, i.e. $K = 17k'-4$ for an even $k' = 2k$ (K is even), then $g_c = 17$ and from the equation $G = (K(K-3)+2-K)/17 \geq K$, we have $K \geq 21/2 + 1/2\sqrt{433} \sim 20.904$. Otherwise, $g_c = 1$ and $K \geq 5/2+1/2\sqrt{17} \sim 4.561$ by the relation $G = (K(K-3)+2-K) \geq K$.

Theorem 3.4. *For $J = 7$ and odd $K \neq 9$, where $(K-1)/2$ is even, let $(a_0, a_1, \ldots, a_6) = (0, 1, K, K+1, 3K-1, \frac{K(K+1)}{2}-1, \frac{K(K+1)}{2}+2)$ and for $K = 9$, just modify a_6 to $\frac{K(K+1)}{2}+3 = 48$. Then, the finite sequence $(a_0, a_1, \ldots, a_6)$ satisfies the GCD constraint. Therefore, $E(a_0, \ldots, a_6)$ corresponds to a $(7, K)$ QC-LDPC code with girth 8 for each $P \geq (K-1)(a_6-a_0)+1$.*

Proof. Similar to the proof of Theorem 3.1, it is sufficient to check the GCD condition for each distinct triples (a_i, a_j, a_k). All of such cases are investigated briefly in Table 2. It is noticed that for the case $(i,j,k) = (4,5,6)$, the state $K = 9$ is not included in the case of "otherwise", because $K_{min} = 10.424$. In this case, i.e. $K = 9$, we have $a_6 = \frac{K(K+1)}{2}+3 = 48$ which satisfies GCD condition. □

Theorem 3.5. *For $J = 7$, and odd $K \neq 11$, where $(K-1)/2$ is odd, let $(a_0, a_1, \ldots, a_6) = (0, 1, K, K+1, 3K+2, \frac{K(K+1)}{2}+2, \frac{K(K+1)}{2}+4)$ and for $K = 11$, modify $a_5 = \frac{K(K+1)}{2}-2$ and $a_6 = \frac{K(K+1)}{2}+2$. Then, the finite sequence $(a_0, a_1, \ldots, a_6)$ satisfies the GCD constraint. Therefore, $E(a_0, \ldots, a_6)$ corresponds to a $(7, K)$ QC-LDPC code with girth 8 for each $P \geq (K-1)(a_6-a_0)+1$.*

Proof. Referring to Table 6, the proof is the same as Theorem 3.4 with this exception that for the case $(i,j,k) = (0,4,6)$, the state $K = 11$ is not included in the case of $K = 140k-129$, because $K_{min} = 68.883$. In this case, i.e. $K = 11$, $(a_0, \ldots, a_6) = (0, 1, 11, 12, 35, 64, 68)$ which obviously satisfies GCD condition. □

TABLE 2. All possible triples (i, j, k) in the proof of Theorem 3.4

(i,j,k)	(a_i, a_j, a_k)	type of K	g_c	G	$K_{\min}$
$(0,1,2)$	$(0,1,K)$	–	1	K	0
$(0,1,3)$	$(0,1,K+1)$	–	1	$K+1$	0
$(0,1,4)$	$(0,1,3K-1)$	–	1	$3K-1$	0.5
$(0,1,5)$	$(0,1,K(K+1)/2-1)$	–	1	$K(K+1)/2-1$	2
$(0,1,6)$	$(0,1,K(K+1)/2+2)$	–	1	$K(K+1)/2+2$	0
$(0,2,3)$	$(0,K,K+1)$	–	1	$K+1$	0
$(0,2,4)$	$(0,K,3K-1)$	–	1	$3K-1$	0.5
$(0,2,5)$	$(0,K,K(K+1)/2-1)$	–	1	$K(K+1)/2-1$	2
$(0,2,6)$	$(0,K,K(K+1)/2+2)$	–	1	$K(K+1)/2+2$	0
$(0,3,4)$	$(0,K+1,3K-1)$	–	2	$(3K-1)/2$	1
$(0,3,5)$	$(0,K+1,K(K+1)/2-1)$	–	2	$(K(K+1)/2-1)/2$	3.561
$(0,3,6)$	$(0,K+1,K(K+1)/2+2)$	–	1	$K(K+1)/2+2$	0
$(0,4,5)$	$(0,3K-1,K(K+1)/2-1)$	$K=28k+5,\ k\in\mathbb{Z}^+$	14	$(K(K+1)/2-1)/14$	27.073
		otherwise	2	$(K(K+1)/2-1)/2$	3.561
$(0,4,6)$	$(0,3K-1,K(K+1)/2+2)$	$K=20k-3,\ k\in\mathbb{Z}^+$	5	$(K(K+1)/2+2)/5$	8.531
		otherwise	1	$K(K+1)/2+2$	0
$(0,5,6)$	$(0,K(K+1)/2)-1,K(K+1)/2+2)$	$K=12k+1,\ k\in\mathbb{Z}^+$	3	$(K(K+1)/2+2)/3$	4
		otherwise	1	$K(K+1)/2+2$	0
$(1,2,3)$	$(1,K,K+1)$	–	1	K	0
$(1,2,4)$	$(1,K,3K-1)$	–	1	$3K-2$	1
$(1,2,5)$	$(1,K,K(K+1)/2-1)$	–	1	$K(K+1)/2-2$	2.561
$(1,2,6)$	$(1,K,K(K+1)/2+2)$	$K=8k+5,\ k\in\mathbb{Z}^+$	4	$(K(K+1)/2+1)/4$	6.701
		otherwise	2	$(K(K+1)/2+1)/2$	2
$(1,3,4)$	$(1,K+1,3K-1)$	–	1	$3K-2$	1
$(1,3,5)$	$(1,K+1,K(K+1)/2-1)$	–	1	$K(K+1)/2-2$	2.561
$(1,3,6)$	$(1,K+1,K(K+1)/2+2)$	–	1	$K(K+1)/2+1$	0
$(1,4,5)$	$(1,3K-1,K(K+1)/2-1)$	$K=52k+5,\ k\in\mathbb{Z}^+$	13	$(K(K+1)/2-2)/13$	25.158
		otherwise	1	$K(K+1)/2-2$	2.561
$(1,4,6)$	$(1,3K-1,K(K+1)/2+2)$	$K=28k-11,\ k\in\mathbb{Z}^+$	7	$(K(K+1)/2+1)/7$	12.844
		otherwise	1	$K(K+1)/2+1$	0
$(1,5,6)$	$(1,K(K+1)/2)-1,K(K+1)/2+2)$	–	1	$K(K+1)/2+1$	0
$(2,3,4)$	$(K,K+1,3K-1)$	–	1	$2K-1$	1
$(2,3,5)$	$(K,K+1,K(K+1)/2-1)$	–	1	$K(K+1)/2-1-K$	3.561
$(2,3,6)$	$(K,K+1,K(K+1)/2+2)$	–	1	$K(K+1)/2+2-K$	0
$(2,4,5)$	$(K,3K-1,K(K+1)/2-1)$	$K=36k+5,\ k\in\mathbb{Z}^+$	9	$(K(K+1)/2-1-K)/9$	19.104
		$K=12k+5, K\neq 36k+5,\ k\in\mathbb{Z}^+$	3	$(K(K+1)/2-1-K)/3$	7.274
		otherwise	1	$K(K+1)/2-1-K$	3.561
$(2,4,6)$	$(K,3K-1,K(K+1)/2+2)$	$K=60k-7,\ k\in\mathbb{Z}^+$	15	$(K(K+1)/2+2-K)/15$	30.870
		$K=20k-7, K\neq 60k-7,\ k\in\mathbb{Z}^+$	5	$(K(K+1)/2+2-K)/5$	10.623
		$K=12k+5, K\neq 20k-7, K\neq 60k-7,\ k\in\mathbb{Z}^+$	3	$(K(K+1)/2+2-K)/3$	6.372
		otherwise	1	$K(K+1)/2+2-K$	0
$(2,5,6)$	$(K,K(K+1)/2-1,K(K+1)/2+2)$	$K=12k+5,\ k\in\mathbb{Z}^+$	3	$(K(K+1)/2+2-K)/3$	6.372
		otherwise	1	$K(K+1)/2+2-K$	0
$(3,4,5)$	$(K+1,3K-1,K(K+1)/2-1)$	$K=16k+5,\ k\in\mathbb{Z}^+$	8	$(K(K+1)/2-2-K)/8$	17.232
		$K=16k-3,\ k\in\mathbb{Z}^+$	4	$(K(K+1)/2-2-K)/4$	9.424
		otherwise	2	$(K(K+1)/2-2-K)/2$	5.701
$(3,4,6)$	$(K+1,3K-1,K(K+1)/2+2$	–	1	$K(K+1)/2+1-K$	2
$(3,5,6)$	$(K+1,K(K+1)/2-1,K(K+1)/2+2)$	–	1	$K(K+1)/2+1-K$	2
$(4,5,6)$	$(3K-1,K(K+1)/2-1,K(K+1)/2+2)$	$K=12k+1,\ k\in\mathbb{Z}^+$	1	$K(K+1)/2+3-3K$	6
		otherwise	3	$(K(K+1)/2+3-3K)/3$	10.424

TABLE 3. The proposed lower-bounds given by Theorems 3.1, 3.4 and 3.5

type of K	Q
9	$(K-1)(\frac{K(K+1)}{2}+3)+1=385$
11	$(K-1)(\frac{K(K+1)}{2}+2)+1=681$
$K \bmod 2 = 0$	$(K-1)(K(K-3)+2)+1$
$K \bmod 2 = 1$, $\frac{K-1}{2} \bmod 2 = 0$	$(K-1)(\frac{K(K+1)}{2}+2)+1$
$K \bmod 2 = 1$, $\frac{K-1}{2} \bmod 2 = 1$	$(K-1)(\frac{K(K+1)}{2}+4)+1$

TABLE 4. Some lower-bounds of the constructed $(7, K)$-codes for an even K

K	Q	Q [19]	Q [18]	K	Q	Q [19]	Q [18]
8	295	505	295	24	11639	13801	2439
10	649	991	514	26	15001	17551	2326
12	1211	1717	782	28	18955	21925	3457
14	2029	2731	703	30	23549	26971	3423
16	3151	4081	1006	32	28831	32737	3535
18	4625	5815	1276	34	34849	39271	3895
20	6499	7981	1559	36	41651	46621	4971
22	8821	10627	1702	38	49285	54835	4663

TABLE 5. Some lower-bounds of the constructed $(7, K)$-codes for an odd K

K	Q	Q [19]	Q [18]	K	Q	Q [19]	Q [18]
9	385	721	385	25	7849	15601	2089
11	681	1321	631	27	9933	19657	2445
13	1117	2185	685	29	12237	24361	3333
15	1737	3361	757	31	15001	29761	3541
17	2481	4897	1137	33	18017	35905	3585
19	3493	6841	1567	35	21557	42841	4183
21	4661	9241	1581	37	25381	50617	4465
23	6161	12145	1805	39	29793	59281	5397

4. NUMERICAL RESULTS

Based on theorems 3.1, 3.4 and 3.5, some $(7, K)$-QC-LDPC codes with different row-weights K, $8 \leq K < 40$, are provided in Table 4 and Table 5 for even and odd K, respectively. In the tables, Q is the lower-bound $(a_6 - a_0)(K-1)+1$ given by Theorem 3.1–Theorem 3.5. These lower-bounds are reported briefly in Table 3. Moreover, to have a comparison with the state-of-the-art results, the lower-bounds of the constructed codes are compared with the ones in [19] and [18]. As it can be seen in Table 4 and Table 5, lower-bounds of our codes are better than those of explicitly constructed $(7, K)$ QC-LDPC codes in [19].

TABLE 6. All possible triples (i, j, k) in the proof of Theorem 3.5

(i,j,k)	(a_i, a_j, a_k)	type of K	g_c	G	$K_{\min}$
$(0,1,2)$	$(0,1,K)$	–	1	K	0
$(0,1,3)$	$(0,1,K+1)$	–	1	$K+1$	0
$(0,1,4)$	$(0,1,3K+2)$	–	1	$3K+2$	0
$(0,1,5)$	$(0,1,K(K+1)/2+2)$	–	1	$K(K+1)/2+2$	0
$(0,1,6)$	$(0,1,K(K+1)/2+4)$	–	1	$K(K+1)/2+4$	0
$(0,2,3)$	$(0,K,K+1)$	–	1	$K+1$	0
$(0,2,4)$	$(0,K,3K+2)$	–	1	$3K+2$	0
$(0,2,5)$	$(0,K,K(K+1)/2+2)$	–	1	$K(K+1)/2+2$	2
$(0,2,6)$	$(0,K,K(K+1)/2+4)$	–	1	$K(K+1)/2+4$	0
$(0,3,4)$	$(0,K+1,3K+2)$	–	1	$3K+2$	0
$(0,3,5)$	$(0,K+1,K(K+1)/2+2)$	$K=8k+3,\ k\in\mathbb{Z}^+$	4	$(K(K+1)/2+2)/4$	6.372
		otherwise	2	$(K(K+1)/2+2)/2$	0
$(0,3,6)$	$(0,K+1,K(K+1)/2+4)$	$K=16k+7,\ k\in\mathbb{Z}^+$	8	$(K(K+1)/2+4)/8$	14.446
		$K=16k-1,\ k\in\mathbb{Z}^+$	4	$(K(K+1)/2+4)/4$	5.561
		otherwise	2	$(K(K+1)/2+4)/2$	0
$(0,4,5)$	$(0,3K+2,K(K+1)/2+2)$	$K=68k-29,\ k\in\mathbb{Z}^+$	17	$(K(K+1)/2+2)/17$	32.878
		otherwise	1	$K(K+1)/2+2$	0
$(0,4,6)$	$(0,3K+2,K(K+1)/2+4)$	$K=140k-129,\ k\in\mathbb{Z}^+$	35	$(K(K+1)/2+4)/35$	68.883
		$K=28k+11$	7	$(K(K+1)/2+4)/7$	12.352
		$K=20k+11$	5	$(K(K+1)/2+4)/5$	8
		otherwise	1	$K(K+1)/2+4$	0
$(0,5,6)$	$(0,K(K+1)/2)+2, K(K+1)/2+4)$	–	2	$(K(K+1)/2+4)/2$	0
$(1,2,3)$	$(1,K,K+1)$	–	1	K	0
$(1,2,4)$	$(1,K,3K+2)$	–	2	$(3K+1)/2$	0
$(1,2,5)$	$(1,K,K(K+1)/2+2)$	–	1	$K(K+1)/2+1$	0
$(1,2,6)$	$(1,K,K(K+1)/2+4)$	–	1	$K(K+1)/2+3$	0
$(1,3,4)$	$(1,K+1,3K+2)$	–	1	$3K+1$	0
$(1,3,5)$	$(1,K+1,K(K+1)/2+2)$	–	1	$K(K+1)/2+1$	0
$(1,3,6)$	$(1,K+1,K(K+1)/2+4)$	$K=12k+3,\ k\in\mathbb{Z}^+$	3	$(K(K+1)/2+3)/3$	3
		otherwise	1	$K(K+1)/2+3$	0
$(1,4,5)$	$(1,3K+2,K(K+1)/2+2)$	–	1	$(K(K+1)/2+1)/2$	2
$(1,4,6)$	$(1,3K+2,K(K+1)/2+4)$	$K=52k-9,\ k\in\mathbb{Z}^+$	13	$(K(K+1)/2+3)/13$	24.757
		otherwise	1	$K(K+1)/2+3$	0
$(1,5,6)$	$(1,K(K+1)/2+2,K(K+1)/2+4)$	–	1	$K(K+1)/2+3$	0
$(2,3,4)$	$(K,K+1,3K+2)$	–	1	$2K+2$	0
$(2,3,5)$	$(K,K+1,K(K+1)/2+2)$	–	1	$K(K+1)/2+2-K$	0
$(2,3,6)$	$(K,K+1,K(K+1)/2+4)$	–	1	$K(K+1)/2+4-K$	0
$(2,4,5)$	$(K,3K+2,K(K+1)/2+2)$	$K=12k-1,\ k\in\mathbb{Z}^+$	3	$(K(K+1)/2+2-K)/3$	6.372
		otherwise	1	$K(K+1)/2+2-K$	0
$(2,4,6)$	$(K,3K+2,K(K+1)/2+4))$	$K=20k-1,\ k\in\mathbb{Z}^+$	5	$(K(K+1)/2+4-K)/5$	10.216
		otherwise	1	$K(K+1)/2+4-K$	0
$(2,5,6)$	$(K,K(K+1)/2)+2, K(K+1)/2+4)$	–	1	$K(K+1)/2+4-K$	0
$(3,4,5)$	$(K+1,3K+2, K(K+1)/2+2)$	$K=44k-17,\ k\in\mathbb{Z}^+$	11	$(K(K+1)/2+1-K)/11$	22.912
		otherwise	1	$K(K+1)/2+1-K$	2
$(3,4,6)$	$(K+1,3K+2,$ $K(K+1)/2+4)$	$K=108k-41$	27	$(K(K+1)/2+3-K)/27$	54.890
		$K=72k-41, K\neq 108k-41\ ,k\in\mathbb{Z}^+$	9	$(K(K+1)/2+3-K)/9$	18.678
		$K=12k+7, K\neq 108k-41, K\neq 72k-41,\ k\in\mathbb{Z}^+$	3	$(K(K+1)/2+3-K)/3$	6
		otherwise	1	$K(K+1)/2+3-K$	0
$(3,5,6)$	$(K+1,K(K+1)/2+2,K(K+1)/2+4)$	–	2	$(K(K+1)/2+3-K)/2$	3
$(4,5,6)$	$(3K+2,K(K+1)/2+2,K(K+1)/2+4)$	–	1	$K(K+1)/2+2-3K$	6.372

J/K	4	5	6	7	8	9	10	11	12
5 [19]	-	-	308	336	332	376	368	396	400
6 [19]	-	-	-	396	452	452	516	516	516
7 [18]	-	-	-	-	1740	1860	2084	2256	2736
7	-	-	-	-	2016	2232	2956	3208	3964

TABLE 7. Some upper-bounds on the minimum-distance of the constructed codes with those of girth-8 (J, K) QC-LDPC codes in [18],[19]

Although, the lower-bound given by GCDg8 algorithm in [18] seems better than ours, the construction method in [18] is not explicit, i.e. it finds the finite sequence $(a_0, \ldots, a_6)$ by a recursive algorithm. Moreover, as Table 7 shows, the constructed codes have better minimum-distance bounds (given by Eq. 2.1) rather than the codes in [19] and [18].

Acknowledgments

This work was supported by the research council of Shahrekord University.

References

1. F. Abedi and M. Gholami, Some explicit constructions of type-II, III, IV, V QCLDPC codes with girth 6, *China Communications*, **17** (2020), 89–109.
2. F. Amirzade and M. R. Sadeghi, lower-bounds on the lifting degree of QC-LDPC codes by difference matrices, *IEEE Access*, **6** (2018), 23688–23700.
3. M. P. C. Fossorier, Quasi-cyclic low-density parity-check codes from circulant permutation matrices, *IEEE Trans. Inf. Theory*, **50** (2004), 1788–1793.
4. R. G. Gallager, Low-density parity-check codes, *IRE Trans. Inf. Theory*, **8** (1962), 21–28.
5. Z. Gholami and M. Gholami, 4-cycle free APM LDPC codes with an explicit construction, *Journal of Algebraic System*, **8** (2021), 283–289.
6. Z. Gholami and M. Gholami, Anti quasi-cyclic LDPC codes, *IEEE Commun. Lett.*, **22** (2018), 1116–1119.
7. M. Karimi and A. H. Banihashemi, On the girth of quasi-cyclic protograph LDPC codes, *IEEE Trans. Inf. Theory,* **59** (2013), 4542–4552.
8. K. J. Kim, J. H. Chung, and K. Yang, Bounds on the size of parity-check matrices for quasi-cyclic low-density parity-check codes, *IEEE Trans. Inf. Theory*, **59** (2013), 7288–7298.
9. S. Kim, J-S. No, H. Chung, and D-J. Shin, Quasi-cyclic low-density parity-check codes with girth larger than 12, *IEEE Trans. Inf. Theory,* **53** (2007), 2885–2891.

10. J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, Algebraic quasi-cyclic LDPC codes: Construction, low error-floor, large girth and a reduced-complexity decoding scheme, *IEEE Trans. Commun.*, **62** (2014), 2626–2637.
11. M. Majdzade and M. Gholami, *On the class of high-rate QC-LDPC codes with girth 8 from sequences satisfied in GCD condition, IEEE Commun. Lett.*, **24** (2020), 1391–1394.
12. M. E. O'Sullivan, J. Brevik, and R. Wolski, The performance of LDPC codes with large girth, *In Proc. 43rd Allerton Conf. on Commun., Control, and Computing*, 2005.
13. R. Smarandache and P. O. Vontobel, Quasi-cyclic LDPC codes: Influence of proto-and Tanner-graph structure on minimum Hamming distance upper bounds, *IEEE Trans. Inf. Theory*, **58** (2012), 585–607.
14. H. Song, J. Liu, and B. V. K. V. Kumar, Large girth cycle codes for partial response channels, *IEEE Trans. Magn.*, **40** (2004), 3084–3086.
15. R. M. Tanner, A recursive approach to low complexity codes, *IEEE Trans. Inf. Theory,* **27** (1981), 533–547.
16. G. Zhang, R. Sun, X. Wang, *Several explicit constructions for* $(3, L)$ *QC-LDPC codes with girth at least eight, IEEE Commun. Lett.*, **17** (2013), 1822–1825.
17. G. Zhang, R. Sun, X. M. Wang, Explicit construction of girth-eight QC-LDPC codes and its application in CRT method, *Journal of China Institute of Commun.*, **33** (2012), 171.
18. G. Zhang, R. Sun, X. Wang, Construction of girth-eight QC-LDPC codes from greatest common divisor , *IEEE Commun. Lett.*, **17** (2013), 369–372.
19. J. Zhang J, G. Zhang, Deterministic girth-eight QC-LDPC codes with large column-weight, *IEEE Commun. Lett.*, **18** (2014), 656–659.

Marjan Majdzade
Department of Mathematics, Shahrekord University, Shahrekord, Iran.
Email: marjanmajdzade@gmail.com

Mohammad Gholami
Department of Mathematics, Shahrekord University, Shahrekord, Iran.
Email: gholami-m@sku.ac.ir

Ghaffar Raeisi
Department of Mathematics, Shahrekord University, Shahrekord, Iran.
Email: ghaffar.raisy@gmail.com

Journal of Algebraic Systems

(7, K) GIRTH-8 QC-LDPC CODES WITH AN EXPLICIT CONSTRUCTION

M. MAJDZADE AND M. GHOLAMI AND G. RAEISI

ساخت کدهای خلوت شبه دوری با کمر ۸ و وزن ستونی ۷ با استفاده از یک روش صریح

مرجان مجدزاده[۱] ، محمد غلامی[۲] و غفار رئیسی[۳]

[۱،۲،۳]دانشکده ریاضی، دانشگاه شهرکرد، شهرکرد، ایران

اخیراً چندین کلاس از (J, K) کدهای خلوت شبه دوری با کمر ۸ به ازای وزن ستونی J ($۳ \leq J < K$) و وزن سطری دلخواه K به طور صریح ساخته شده‌اند به گونه ای که کران‌های پایین روی اندازه ی ماتریس‌های جایگشتی دوری، تا حد ممکن کوچک باشد. در این مقاله به ازای $J = ۷$ دسته ای از $(۷, K)$ کدهای خلوت شبه دوری با کمر ۸ با استفاده از یک روش صریح تولید می شود به طوری‌که کران پایین کدهای ساخته شده به طور قابل توجهی نسبت به جدیدترین کران موجود، یعنی $(K - ۱)(K^۲ + K) + ۱$، بهتر می باشد.

کلمات کلیدی: کدهای خلوت شبه دوری، ساختارهای صریح، کمر، ماتریس توانی.