An Explicit Construction of a Class of Type-III and Type-IV QC-LDPC Codes with Girth 6

Conference Paper · April 2021

CITATIONS
0

READ
1

2 authors:

Mohammad Gholami
Shahrekord University
31 PUBLICATIONS **156** CITATIONS
SEE PROFILE

Farzaneh Abedi
Shahrekord University
5 PUBLICATIONS **1** CITATION
SEE PROFILE

4th International Conference on
Combinatorics, Cryptography, Computer Science and Computing
November 20-21, 2019 - Iran University of Science & Technology

An Explicit Construction of a Class of Type-III and Type-IV QC-LDPC Codes with Girth 6

Mohammad Gholami
Shahrekord University
Department of Mathematics, Shrekord University, Shahrekord, Iran, and
School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran
gholami-m@sci.sku.ac.ir

Farzaneh Abedi
Department of Mathematics, Shrekord University, Shahrekord, Iran
abedi@stu.sku.ac.ir

ABSTRACT

Type-t, $t \geq 1$, quasi-cyclic (QC) low-density parity-check (LDPC) codes are a class of protograph codes whose parity-check matrices contain blocks each of which is a summation of at most t circulant permutation matrices (CPMs). In this paper, the parity-check matrices with a single row of circulants are used to generate a class of 4-cycle free type-III and type-IV QC-LDPC codes by an explicit method, such that the constructed codes have smaller length and better error performance than state-of-the-art constructions.

KEYWORDS: QC-LDPC codes, Girth, Explicit Constructions, Parity-check matrix

1 INTRODUCTION

QC-LDPC codes [1]-[8] have received much attention due to their implementation-friendly structure and similar decoding performance compared to computer-generated random LDPC codes. The parity-check matrices of QC-LDPC codes are comprised of blocks of circulant matrices, classified by the researchers as *type-I* [1]-[2], *type-II* [3, 6] and *type-III* [6] QC-LDPC codes, if each block is a combination of at most one, two and three circulant permutation matrices (CPMs), respectively.

Corresponding to each QC-LDPC code with parity-check matrix H we give *Tanner graph* $TG(H)$ as a bipartite graph whose incident matrix is the parity-check matrix H. A cycle is a closed path in the Tanner graph that begins and ends at the same vertex. The length of the shortest cycles in the Tanner graph is called *girth*. Also, a (J, L)-regular LDPC code with the parity-check matrix H is defined as a code in which column and row weight of H, i.e. the summation of elements of each column and row of H, are J and L, respectively.

The methods of construction of LDPC codes are classified in random-like and structured categories. Among the structural method, explicit approaches are practical because there is no need for a computer search to find the parity-check matrices. Lally [3] presented a class of type-II QC-LDPC codes with girth six whose parity-check matrices just contain blocks of weight 2. Moreover, *perfect cyclic difference sets* [5] and *Sidon sequences* [4], are used as two main combinatorial objects to construct some type-II QC-LDPC codes with girths at most 6. The authors in [6] have proposed a search algorithm to find a class of type-II, III QC-LDPC codes with girth at most 10. In [7], the authors have investigated all of the

patterns of the base graphs corresponding to multi-type QC-LDPC codes with a given maximum-achievable girth.

In this paper, we present an explicit construction for type-w, $w = 3,4$ QC-LDPC codes which are simpler and more flexible in terms of the length and rate than the codes recently constructed by algebraic and combinatorial approaches [8]. To achieve codes with a high rate, a single row of circulants is considered as the parity-check matrix of a class of QC-LDPC codes with column-weights w, $w = 3,4$. This construction of parity-check matrix is previously used in [8] to construct some type-III and type-IV QC-LDPC codes by *Cyclic Difference Families (CDF)*. Simulation results show that the constructed codes outperform the codes in [8] and the codes constructed from progressive edge growth (PEG).

2 TYPE-w QC-LDPC CODES

Let m, s be some positive integers such that $0 \leq s \leq m-1$. By the *circulant permutation matrix* (CPM) I^s of *slope* s, we mean the $m \times m$ permutation matrix $(p_{i,j})_{1 \leq i,j \leq m}$, in which $p_{i,j} = 1$ if and only if $i - j = s \bmod m$. Note that when $s = 0$, the circulant I^s is the $m \times m$ identity matrix I. Now, for the positive integers w, l, let $H = (H_j)_{1 \leq j \leq l}$ in which each H_j is the sum of w CPM's of size m as $H_j = I^{s_{1,j}} + \cdots + I^{s_{w,j}}$ for some slopes $0 \leq s_{i,j} \leq m-1$, $1 \leq i \leq w$. The $1 \times ml$ matrix H can be considered as the parity-check matrix of a type-w QC-LDPC code of length ml which contains a cycle of length 4 if and only if the following condition is hold [3].

$$s_{i_0,j_0} - s_{i_1,j_0} + s_{i_2,j_1} - s_{i_3,j_1} = 0 (\bmod m), \tag{1}$$

for some $1 \leq j_0 \leq j_1 \leq l$, $1 \leq i_0 \neq i_1 \leq w$ and $1 \leq i_2 \neq i_3 \leq w$, such that $i_1 \neq i_2$ and $i_0 \neq i_3$ if $j_0 = j_1$.

In continue, we give some *explicit constructions* for the *slope matrix* $S = (s_{i,j})_{1 \leq i \leq w, 1 \leq j \leq l}$, such that the corresponding type-w, $w = 3,4$, QC-LDPC code with parity-check matrix H is 4-cycle free.

2.1 Type-III QC-LDPC Codes

Theorem 2.1. For $1 \leq j \leq l$, let $(s_{1,j}, s_{2,j}, s_{3,j}) = (ja_0, ja_1, ja_2)$, where $a_0 = 1, a_1 = 2$ and $a_2 = l + 3$, then the slope matrix $S = (s_{i,j})_{1 \leq i \leq 3, 1 \leq j \leq l}$ corresponds to a type-III QC-LDPC code with girth 6 for enough large CPM size m.

Proof. To show that the code is 4-cycle free, it is sufficient to prove that left-hand side (LHS) of Eq. 1 is not zero. Thus, we consider the following two cases.

Case 1 • If 4-cycle occurs in one block $j_0 = j_1$, then for each $0 \leq t_1 \neq t_2 \neq t_3 \leq 2$, we have following cases.

(a) $(s_{i_0,j_0}, s_{i_1,j_0}, s_{i_2,j_0}, s_{i_3,j_0}) = (j_0 a_{t_1}, j_0 a_{t_2}, j_0 a_{t_1}, j_0 a_{t_2})$, then the LHS is $2j_0(a_{t_2} - a_{t_1})$ which is obviously non-zero.

(b) $(s_{i_0,j_0}, s_{i_1,j_0}, s_{i_2,j_0}, s_{i_3,j_0}) = (j_0 a_{t_1}, j_0 a_{t_2}, j_0 a_{t_1}, j_0 a_{t_3})$, $(j_0 a_{t_2}, j_0 a_{t_1}, j_0 a_{t_3}, j_0 a_{t_1})$, then LHS is $j_0(a_{t_2} + a_{t_3} - 2a_{t_1})$ which is non-zero, because of $a_{t_2} + a_{t_3} \neq 2a_{t_1}$.

Case 2 • If 4-cycle occurs in two blocks j_0, j_1, $1 \leq j_0 < j_1 \leq l$ in which $(s_{i_0,j_0}, s_{i_1,j_0}) = (j_0 a_{t_1}, j_0 a_{t_2})$ and $(s_{i_2,j_1}, s_{i_3,j_1}) = (j_1 a_{k_1}, j_1 a_{k_2})$, for some $0 \leq t_1 \neq t_2 \leq 2$ and $0 \leq k_1 \neq k_2 \leq 2$, then LHS of Eq.1 is equal to $j_0(a_{t_1} - a_{t_2}) + j_1(a_{k_1} - a_{k_2})$ which is zero if and only if

$$\frac{j_1}{j_0} = \frac{a_{k_2} - a_{k_1}}{a_{t_2} - a_{t_1}} \tag{2}$$

Or, equivalently $\frac{j_1}{j_0} \in \{\frac{a_2-a_1}{a_1-a_0}, \frac{a_2-a_0}{a_2-a_1}, \frac{a_2-a_0}{a_1-a_0}\}$. By setting $a_0 = 1$ and $a_1 = 2$, we must have $\frac{j_1}{j_0} \in \{a_2 - 2, a_2 - 1, \frac{a_2-1}{a_2-2}\}$ which is not hold for $a_2 \geq l + 3$, so the constructed code is 4-cycle free. ■

Example 2.2. For $l = 3$, the slope matrix S which is given by Theorem 2.1 and the corresponding parity-check matrix $\mathcal{H}$ of type-III QC-LDPC code with girth 6 for CPM-size $m = 21$ are as follows.

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 6 & 12 & 18 \end{pmatrix}, \quad \mathcal{H} = (I^1 + I^2 + I^6 \quad I^2 + I^4 + I^{12} \quad I^3 + I^6 + I^{18}).$$

2.2 Type-IV QC-LDPC codes

Theorem 2.3. For $1 \leq j \leq l$, let $(s_{1,j}, s_{2,j}, s_{3,j}, s_{4,j}) = (ja_0, ja_1, ja_2, ja_3)$, where $(a_0, a_1, a_2, a_3) = (1,3,2l + 4,4l + 6)$, then the slope matrix $S = (s_{i,j})_{1 \leq i \leq 4, 1 \leq j \leq l}$ corresponds to a type-IV QC-LDPC code with girth 6 for enough large CPM size m.

Proof. To show that the code is 4-cycle free, it is sufficient to prove that LHS of Eq.1 is not zero. Thus, we consider the following two cases.

Case 1. If 4-cycle occurs in one block $j_0 = j_1$, then for each $0 \leq t_1 \neq t_2 \neq t_3 \neq t_4 \leq 3$, we have the following cases.

1. $(s_{i_0,j_0}, s_{i_1,j_0}, s_{i_2,j_0}, s_{i_3,j_0}) = (j_0 a_{t_1}, j_0 a_{t_2}, j_0 a_{t_1}, j_0 a_{t_2})$, then LHS is $2j_0(a_{t_2} - a_{t_1})$ which is nonzero.
2. $(s_{i_0,j_0}, s_{i_1,j_0}, s_{i_2,j_0}, s_{i_3,j_0}) = (j_0 a_{t_1}, j_0 a_{t_2}, j_0 a_{t_1}, j_0 a_{t_3})$, $(j_0 a_{t_2}, j_0 a_{t_1}, j_0 a_{t_3}, j_0 a_{t_1})$, then LHS is $j_0(a_{t_2} + a_{t_3} - 2a_{t_1})$ which is nonzero, because of $a_{t_2} + a_{t_3} \neq 2a_{t_1}$.
3. $(s_{i_0,j_0}, s_{i_1,j_0}, s_{i_2,j_0}, s_{i_3,j_0}) = (j_0 a_{t_1}, j_0 a_{t_2}, j_0 a_{t_3}, j_0 a_{t_4})$, then LHS is $j_0(a_{t_1} - a_{t_2} + a_{t_3} - a_{t_4})$, which is nonzero because $a_{t_1} - a_{t_2} \neq a_{t_4} - a_{t_3}$.

Case 2. If 4-cycle occurs in two blocks j_0, j_1, $0 \leq j_0 < j_1 \leq l$, where $(s_{i_0,j_0}, s_{i_1,j_0}) = (j_0 a_{t_1}, j_0 a_{t_2})$ and $(s_{i_2,j_1}, s_{i_3,j_1}) = (j_1 a_{k_1}, j_1 a_{k_2})$, for some $t_1 \neq t_2$ and $k_1 \neq k_2$ in $\{0,1,2,3\}$, then LHS is equal to $j_0(a_{t_1} - a_{t_2}) + j_1(a_{k_1} - a_{k_2})$ which is zero if and only if

$$\frac{j_1}{j_0} = \frac{a_{k_1} - a_{k_2}}{a_{t_1} - a_{t_2}} \tag{3}$$

Or, equivalently

$$\frac{j_1}{j_0} \in \{\frac{a_2-a_1}{a_1-a_0}, \frac{a_2-a_0}{a_3-a_2}, \frac{a_3-a_1}{a_2-a_0}, \frac{a_3-a_2}{a_2-a_1}, \frac{a_2-a_0}{a_2-a_1}, \frac{a_3-a_1}{a_3-a_2}, \frac{a_3-a_2}{a_1-a_0}, \frac{a_2-a_0}{a_1-a_0}, \frac{a_3-a_1}{a_2-a_1},$$
$$\frac{a_3-a_1}{a_1-a_0}, \frac{a_3-a_0}{a_3-a_1}, \frac{a_3-a_0}{a_2-a_0}, \frac{a_3-a_0}{a_3-a_2}, \frac{a_3-a_0}{a_2-a_1}, \frac{a_3-a_0}{a_1-a_0}\} \tag{4}$$

Without less of generality, we consider $a_0 < a_1 < a_2 < a_3$, then from $j_0 < j_1$, we have $a_1 - a_0 < a_2 - a_1 < a_3 - a_2 < a_2 - a_0 < a_3 - a_1 < a_3 - a_0$. By setting $a_0 = 1$ and $a_1 = 3$, from LHS of Eq. 1 to be nonzero, we must have $\frac{a_{k_1} - a_{k_2}}{a_{t_1} - a_{t_2}} \notin \{\frac{j_1}{j_0},\ 1 \leq j_0 < j_1 \leq l\}$, therefore according to $\frac{j_1}{j_0} \neq \frac{a_2-a_1}{a_1-a_0}$, we must have $\frac{a_2-3}{2} > l$, i.e. $a_2 \geq 2l + 4$. Let $a_2 = 2l + 4$, then from $\frac{j_1}{j_0} \neq \frac{a_3-a_2}{a_2-a_1}$, we have $\frac{a_3-a_2}{a_2-3} > l$, or $a_3 \geq a_2(l + 1) - 3l + 1$. Then, $a_3 = 2l^2 + 3l + 5$ is a proper choice for a_3. In each way, Eq. 4 is not satisfied for $(a_0, a_1, a_2, a_3) = (1,3,2l + 4,2l^2 + 3l + 5)$, then the constructed code is 4-cycle free. ■

Example 2.4. For $l = 3$, the slope matrix S which is given by Theorem 2.2 and the corresponding parity-check matrix $\mathcal{H}$ of type-IV QC-LDPC code with girth 6 for CPM-size $m = 63$, are as follows.

$$S = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 6 & 9 \\ 10 & 20 & 30 \\ 32 & 64 & 96 \end{pmatrix},$$

$$\mathcal{H} = (I^1 + I^3 + I^{10} + I^{32} \quad I^2 + I^6 + I^{20} + I^{64} \quad I^3 + I^9 + I^{30} + I^{96}).$$

2.3 Some Comparisons with other Constructions

Using Theorem 2.1 and Theorem 2.2, Table 1 presents some constructed type-IV QC-LDPC codes with girth 6 against the Type-II QC-LDPC codes in [3, 4, 5] having the same column/row weights. As the table shows, the constructed codes are smaller than the codes in [3, 4, 5].

Table 1: The length of type-IV QC-LDPC codes against the codes in [3, 4, 5]

l	R	n_1	n_2 [3]	n_3 [4]	n_4 [5]
2	0.5	70	144	92	1092
3	0.66	189	468	210	-
4	0.75	496	1088	568	7944
5	0.8	750	2100	1110	-
6	0.83	1170	3600	2052	-

Finally, Table 2 provides a 6,8-cycle multiplicities comparison between some constructed type-III QC-LDPC codes lifted from $1 \times l$ base matrices, $4 \leq l \leq 8$, denoted by prop and the QC-LDPC codes of the same length and regularity in [8]. As the table shows, the constructed codes have better 6,8-cycle multiplicities than the codes in [8].

Table 2: 6,8-cycle multiplicities of the constructed type-III QC-LDPC codes of length n against the codes in [8]

Cycle Length		6		8	
l	n	prop	[8]	prop	[8]
4	124	2077	2139	31248	30969
5	215	4085	4128	80625	80625
6	342	7182	8341	173052	180519
7	511	11680	14746	328719	364343
8	728	17927	19474	572208	593957

Figure 1 has provided a bit-error-rate comparison between the type-III QC-LDPC code lifted from a 1×8 base matrix with lifting degree $m = 91$ and girth 6, on one hand, and a 4-cycle free QC-LDPC code from cyclic difference sets in [8] and an LDPC code from progressive

edge growth (PEG) [9], on the other hand. As the figure shows, the constructed code, denoted by $C(1 \times 8; m = 91; g = 6)$, outperforms the code in [8] and PEG LDPC code.

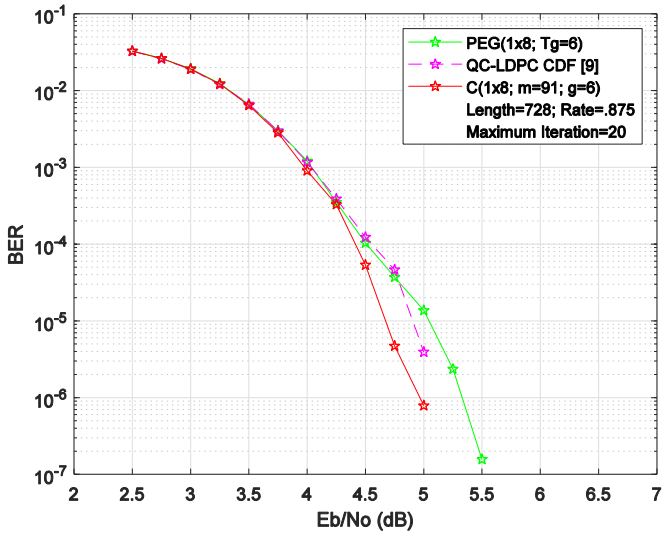

Figure 1: The constructed type-III QC-LDPC code with girth 6 against QC-LDPC code in [8] and PEG LDPC code [9]

3 ACKNOWLEDGEMENTS

This work was supported in part by the research council of Shahrekord University. Moreover, the first author was in part supported by a grant from IPM (No. CS1398-4-279)

REFERENCES

[1] M. P. C. Fossorier, "*Quasi-cyclic low density parity-check codes from circulant permutation matrices*," IEEE Transactions on Information Theory., vol. 50, 2004, pp. 1788–1793.

[2] M. Gholami, M. Samadieh, and G. Raeisi, "*Column-weight three QC LDPC codes with girth 20*," IEEE Communications Letters., vol. 17, 2013, pp. 1439-1442.

[3] K. Lally, "*Explicit construction of type-II QC-LDPC codes with girth at least 6*," In 2007 IEEE International Symposium on Inform. Theory., 2007, pp. 2371-2375.

[4] G. Zhang, "Type-II quasi-cyclic low-density parity-check codes from Sidon sequences," Electronics Lett., vol. 52, 2016, pp. 367–369.

[5] L. Zhang, B. Li and L. Cheng, "*Construction of type-II QC-LDPC codes based on perfect cyclic difference set*," Chinese Journal of Electronics, vol. 24, 2015, pp. 146-151.

[6] G. Malema, and M. Nkwebi, "*Construction of flexible type II and III QC-LDPC codes ,"* Science Journal of Circuits, Systems and Signal Processing, vol. 3, 2014, pp. 31–34.

[7] H. Park, S. Hong, JS. No, DJ. Shin, "*Design of multiple-edge protographs for QC-LDPC codes avoiding short inevitable cycles*," IEEE Trans. Inform. Theory., vol. 59, 2013, pp. 4598–4614.

[8] H. Park, S. Hong, J.S. No and D. J. Shin, "*Construction of high-rate regular quasi-cyclic LDPC codes based on cyclic difference families*," IEEE Trans. Commun., vol. 61, 2013, pp. 3108–3113.

[9] X. Jiang, M.H. Lee, and J. Qi., "*Improved progressive edge-growth algorithm for fast encodable LDPC codes*," EURASIP Journal on Wireless Communications and Networking, 2012. Vol.1, 2012, p. 178.