3TH INTERNATIONAL CONFERENCE ON COMBINATORICS, CRYPTOGRAPHY AND COMPUTATION
Iran University of Science &Technology
*Proceedings of the 3nd*International Conference on Combinatorics, Cryptography and Computation (I4C2018)

A New Explicit Construction for Girth-8 QC-LDPC Codes

Mohammad Gholami and Marjan Majdzade
Department of Mathematics
University of Shahrekord, Shahrekord, Iran
Gholami-m@sci.sku.ac.ir, marjanmajdzade@gmail.com

ABSTRACT

Recently, some explicit constructions for girth-8 (J, L) quasi-cyclic low-density parity-check (QC-LDPC) codes are proposed for any row weight L and column weight J, $J = 3,4,5$ such that their corresponding lengths have been considered small as possible. In this paper, a new construction to generate $(5, L)$ $(L \geq 6)$ QC-LDPC codes with girth 8 is proposed in which the constructed codes are shorter than perviously obtained codes by some explicit methods with the same girth and the row weight.

KEYWORDS QC-LDPC codes, explicit constructions, girth, exponent matrix.

1 INTRODUCTION

Quasi-cyclic low-density parity-check codes (QC-LDPC codes) are an essential category of LDPC codes that are preferred to other types of LDPC codes because of their favourably practical and simple implementations of Shannon noisy coding theorem [6]. One of the most important representation of codes is Tanner graph [3] which is a bipartite graph collecting variable and check nodes associated to the columns and rows of H, respectively, and a check node is connected to a variable node, if a nonzero entry exists in the intersection of the corresponding row and column. The length of the shortest cycles of Tanner graph, girth, has been known to influence the code performance [5].

Let P and s be some integers with $0 \leq s < P$. By a circulant permutation matrix (CPM) of size P and slope s, we mean a $P \times P$ binary matrix I_P^s , or Is when P is known, in which (i, j)-th element of I^s is nonzero if and only if $i - j = s \bmod P$. In fact, in the first row of I^s , the nonzero element is in $(s + 1)$'th position and each other row is obtained by cyclically shifting the previous row to the right by one position. Now, a (J, L) QC LDPC code can be described as a CPM size P and a $J \times L$ 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 parity check matrix (PCM) constructed by replacing each entry $e_{i,j}$ of E by CPM $I^{e_{i,j}}$.

In general, LDPC codes with large girth and small number of short cycles have good performances [7]. In addition to girth factor, another important factor to design the exponent matrix of a QC-LDPC code, is its CPM-size. In [5], the authors have used some explicit methods in order to construct girth-8 column-

weight $J = 3,4,5$ QC LDPC codes with CPM-sizes $L(L-1)+1$, $(L+1)(L-1)+1$, and $L^2(L-1)+1$ respectively. In this paper, an explicit method to construct $(5, L)$ QC-LDPC codes are proposed such that the corresponding CPM-size is smaller than the constructed codes in [5]. In fact, the CPM-size of the proposed codes are reduced to $(L-1)(3L-1)+1$ for even L, and for odd L, it reduced to $(L-1)(3L-1)+1$ and $(L-1)(3L+2)+1$ depending on $(L-1)/2$ is even or odd, respectively.

2 PRELIMINARIES

All QC-LDPC codes proposed in this paper are associated with the following type of exponent matrices.

Definition 2.1 *[8] Let $\{a_0, a_1, \cdots, a_{J-1}\}$ be J integers satisfying $0 \le a_0 < a_1 < \cdots < a_{J-1}$. Then, $E(a_0, \cdots, a_{J-1})$ is an $J \times L$ exponent matrix as follows:*

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

The following lemma provides a sufficient condition for QC-LDPC codes to have girth at least eight [8].

Lemma 2.2 (*GCD constraint) If $(a_k - a_i)/gcd(a_k - a_i, a_j - a_i) \ge L$ for all triples (a_i, a_j, a_k), $0 \le i < j < k \le J-1$, 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 $P \ge (a_{J-1} - a_0)(L-1)+1$.*

Now, in the following, for $J = 5$, an explicit method is proposed to construt the exponent matrix of QC LDPC codes with girth 8.

3 A NEW METHOD TO CONSTRUCT COLUMN-WEIGHT-5 QC LDPC CODES

By definition 2.1 and lemma 2.2, our method can be described for different types of L, as follows.

Construction 1 *For $J = 5$ and even L, the finite sequence $(a_0, a_1, \cdots, a_4) = (0,1, L, L+1, 3L-1)$ satisfies the GCD constraint. Therefore, in this case $E(0,1, L, L+1, 3L-1)$ corresponds to a $(5, L)$ QC-LDPC code with girth 8 for each $P \ge (L-1)(3L-1)+1$.*

Proof. Based on Lemma 2.2, it is sufficient to check the GCD condition for each triple of indices $0 \le i < j < k \le 4$. All of such cases are presented in Table 3. Moreover, the GCD condition is hold for each integer $L > L_{\min}$.

Construction 2 *For $J = 5$ and odd L, where $(L-1)/2$ is even, let $(a_0, a_1, \cdots, a_4) = (0,1, L, L+1, 3L-1)$. Then, this finite sequence is satisfied in the GCD constraint. Therefore, in*

this case $E(0,1,L,L+1,3L-1)$ *corresponds to a* $(5,L)$ *QC-LDPC code with girth 8 for each* $P \geq (L-1)(3L-1)+1$.

Proof. Similar to the proof of Construction 1, it is sufficient to check the GCD condition for each distinct triples (a_i, a_j, a_k). All of such cases are provided in Table 3.

Construction 3 *For* $J = 5$ *and odd* L*, where* $(L-1)/2$ *is odd, let* $(a_0, a_1, \cdots, a_4) = (0,1,L,L+1,3L+2)$. *Then, this finite sequence is satisfied in the GCD constraint. Therefore, in this case* $E(0,1,L,L+1,3L+2)$ *corresponds to a* $(5,L)$ *QC-LDPC code with girth 8 for each* $P \geq (L-1)(3L+2)+1$.

Proof. Refereing to Table 3, the proof is simillar to the proofs of Constructions 1 and 2 .

(i,j,k)	(a_i, a_j, a_k)	$\gcd(a_k - a_i, a_j - a_i)$	GCD condition	$L_{\min}$
(0,1,2)	$(0,1,L)$	1	L	0
(0,1,3)	$(0,1,L+1)$	1	$L+1$	0
(0,1,4)	$(0,1,3L-1)$	1	$3L-1$	1
(0,2,3)	$(0,L,L+1)$	1	$L+1$	0
(0,2,4)	$(0,L,3L-1)$	1	$3L-1$	1
(0,3,4)	$(0,L+1,3L-1)$	1	$3L-1$	1
(1,2,3)	$(1,L,L+1)$	1	L	0
(1,2,4)	$(1,L,3L-1)$	1	$3L-2$	1
(1,3,4)	$(1,L+1,3L-1)$	2	$(3L-2)/2$	2
(2,3,4)	$(L,L+1,3L-1)$	1	$2L-1$	1

Table 1. All possible triples (i,j,k) in the proof of Construction 1

(i,j,k)	(a_i,a_j,a_k)	$\gcd(a_k-a_i,a_j-a_i)$	GCD condition	$L_{\min}$
(0,1,2)	$(0,1,L)$	1	L	0
(0,1,3)	$(0,1,L+1)$	1	$L+1$	0
(0,1,4)	$(0,1,3L-1)$	1	$3L-1$	1
(0,2,3)	$(0,L,L+1)$	1	$L+1$	0
(0,2,4)	$(0,L,3L-1)$	1	$3L-1$	1
(0,3,4)	$(0,L+1,3L-1)$	2	$(3L-1)/2$	1
(1,2,3)	$(1,L,L+1)$	1	L	0
(1,2,4)	$(1,L,3L-1)$	1	$3L-2$	1
(1,3,4)	$(1,L+1,3L-1)$	1	$3L-2$	1
(2,3,4)	$(L,L+1,3L-1)$	1	$2L-1$	1

Table 2. All possible triples (i,j,k) in the proof of Construction 2

(i,j,k)	(a_i,a_j,a_k)	$\gcd(a_k-a_i,a_j-a_i)$	GCDcondition	$L_{\min}$
(0,1,2)	$(0,1,L)$	1	L	0
(0,1,3)	$(0,1,L+1)$	1	$L+1$	0
(0,1,4)	$(0,1,3L+2)$	1	$3L+2$	0
(0,2,3)	$(0,L,L+1)$	1	$L+1$	0
(0,2,4)	$(0,L,3L+2)$	1	$3L+2$	0
(0,3,4)	$(0,L+1,3L+2)$	1	$3L+2$	0
(1,2,3)	$(1,L,L+1)$	1	L	0
(1,2,4)	$(1,L,3L+2)$	2	$(3L+1)/2$	0
(1,3,4)	$(1,L+1,3L+2)$	1	$3L+1$	0
(2,3,4)	$(L,L+1,3L+2)$	1	$2L+2$	0

Table 3. All possible triples (i,j,k) in the proof of Construction 3

4 NUMERICAL RESULTS AND CONCLUSION

Based on *GCD constraint* and Constructions 1-3, $(5,L)$-QC LDPC codes with different types of L are constructed explicitly such that the corresponding CPM -size is smaller than the CPM-size of constructed codes in [5]. In fact, the CPM size of the new codes are reduced to $(L-1)(3L-1)+1$ for even L, and for odd L, it reduced to $(L-1)(3L-1)+1$ and $(L-1)(3L+2)+1$ depending on $\frac{L-1}{2}$ is even or odd, respectively, which are smaller than the obtained CPM size in [5], i.e, $L^2(L-1)+1$.

Due to constructions 1-3, some $(5,L)$-QC LDPC codes with different row-weights L, $6 \leq L < 15$, are provided in Table 4. In this table, P_{new} is the obtained CPM size in the constructions 1-3. Moreover, to have a comparison with the reported results for $(5,L)$ QC-LDPC codes, the obtained conclusions are compared with the CPM size of codes in [5], denoted by $P_{[5]}$. Clearly, the proposed CPM-sizes are remarkably better than the CPM-sizes of explicitly constructed $(5,L)$ QC-LDPC codes in [5].

L	P_{new}	$P_{[5]}$
6	86	181
7	139	295
8	162	449
9	209	649
10	262	901
11	351	1211
12	386	1585
13	457	2029
14	534	2549
15	659	3151

Table 4. CPM sizes of new $(5, L)$-QC LDPC codes compared to obtained CPM sizes in [5].

5 REFERENCES

[1] R. G. Gallager, “Low-density parity-check codes", IEEE Trans. Inf. Theory, vol. IT-8,(1), pp. 21-28, Jan. 1962.

[2] M. P. C. Fossorier, “Quasi-cyclic low-density parity-check codes from circulant permutation matrices", IEEE Trans. Inf. Theory, vol. 50, no. 8, pp. 1788–1793, 2004.

[3] R. M. Tanner, “Arecursive approach to low complexity codes", IEEE Trans. Inf. Theory, Vol. IT-27, pp. 533–542, Sept 1981.

[4] 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, vol. 53, pp. 2885-2891, Aug 2007.

[5] M. Karimi, and A. H. Banihashemi, “On the girth of quasi-cyclic protograph LDPC codes", IEEE Trans. Inf. Theory, vol. 59, pp. 4542–4552, July 2013.

[6] Shannon, “A Mathematical Theory Of Communication, ACM SIGMOBILE mobile computing and communications review“, vol. 5, no. 1. 3-55, 2001.

[7] 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., vol. 62, no. 8, pp. 2626Â–-2637, Aug. 2014.

[8] G. Zhang, R. Sun, X. Wang, “Construction of girth-eight QC-LDPC codes from greatest common divisor", IEEE Commun. Lett., vol. 17, no. 2, pp. 369-72, 2013.