INTERNATIONAL CONFERENCE ON COMBINATORICS, CRYPTOGRAPHY AND COMPUTATION

Iran University of Science &Technology

Proceedings of the 2nd International Conference on Combinatorics, Cryptography and Computation (I4C2017)

A Recursive Method to Construct the Optimal Exponent Matrices

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

ABSTRACT

Recently, an exhaustive search has been used to find all of the possible non-isomorphic 4-cycle free column-weight three QC-LDPC codes with the shortest length. The drawback of this approach, however, is the complexity which increases sharply by extending the exponent matrices. Moreover, the minimum lifting degrees of these codes are not the same with the lower-bounds, in general, i.e. QC-LDPC codes with the same exponent matrix may have cycles of length 4, for some lifting degrees greater than the given shortest length. Here, an explicit ordering on the positions of the desired exponent matrix is proposed to construct some column-weight three QC-LDPC codes with girth 6 having the shortest length. The constructed codes have two main benefits: The lower-bound is the same with the minimum-lifting degree and the overall complexity is polynomial, in terms of the length of the constructed codes.

KEYWORDS: QC-LDPC codes, Girth, Lower-bound, Lifting degree.

1 INTRODUCTION

Low-density parity-check (LDPC) codes are a class of linear block codes which come from the characteristic of their parity-check matrices containing only a few 1's in comparison to the number of 0's. Their main advantages are that they provide a performance which is very close to the Shannon capacity [7] for different channels and encoding and decoding algorithms with linear time complexities. They were first introduced by Gallager in his PhD thesis in 1960. But, they were mostly ignored about 30 years [3], due to the computational effort in implementing coder and encoder for such codes and the introduction of Reed-Solomon codes. In particular, the length of the shortest cycle in the graph, *girth*, is identified as one of the important factor to measure of the code's performance. Related to this, lower bounds have been derived on the block length of QC-LDPC codes as a function of girth [4]- [6]. There are however, very few cases, for which these bounds have been proved to be tight. One example is the array-based codes [2], which are cyclic liftings of some degree n of fully-connected base graphs of size $m \times n$, where n is a prime number.

2 PRELIMINARIES

Let N, s be two positive integers with $0 \le s < N$. By a circulant permutation matrix (CPM) of size N and exponent s, denoted by I_N^s , or I^s when N is known, we mean the matrix $I_N^s = \begin{pmatrix} 0 & I_s \\ I_{N-s} & 0 \end{pmatrix}$, in which $I_k, k \in \{s, N-s\},$ is the identity matrix of order k . Now, For the given positive integers $m, n, N, m < n$, a $(m,n)-$QC-LDPC code with CPM size N can be described by the following parity-check matrix:

$$H_{P,N} = \begin{pmatrix} I^{p_{0,0}} & I^{p_{0,1}} & \cdots & I^{p_{0,n-1}} \\ I^{p_{1,0}} & I^{p_{1,1}} & \cdots & I^{p_{1,n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ I^{p_{m-1,0}} & I^{p_{m-1,1}} & \cdots & I^{p_{m-1,n-1}} \end{pmatrix}$$

Where each exponent $p_{ij}, 0 \le i \le m-1, 0 \le j \le n-1,$ is a non-negative integer. We refer to the $m \times n$ matrix $P = (p_{i,j})$ as the exponent matrix with lifting-degree N . It is worth noted that some elements of P in $H_{P,N}$ may be greater than N which are reduced in modulus of N to construct the parity-check matrix $H_{P,N}$.

It is well-known [1] that the necessary and sufficient condition for the existence of a cycle of length $2r$ in the Tanner graph of C with parity-check matrix H is

$$\sum_{i=1}^{r-1} \left(p_{m_i,n_i} - p_{m_i,n_{i+1}} \right) = 0 \bmod N \qquad (1)$$

Now, to construct a QC LDPC code with girth at least $2g$, we should find an exponent matrix $P = (p_{i,j})$ such that (1) is not satisfied for each $r < g$. Corresponding to each QC-LDPC code with girth $2g$ and exponent matrix P, the lower-bound (LB) $N_{\mathrm{L,P}}$ is defined as the minimum positive integer such that $g\left(H_{P,N}\right) \ge 2g$, for each CPM-size $N \ge N_{\mathrm{L,P}}$. However, we may have $g(H_{P,N}) \ge 2g$ for some $N < N_{\mathrm{L,P}}$, while $g\left(H_{P,N'}\right) < 2g$, for some $N < N' < N_{\mathrm{L,P}}$. For this, we use $N_{\min,P}$ to denote the minimum lifting-degree (MLD) N with this property that $H_{P,N}$ has girth at least $2g$. Clearly, MLD is not greater than LB, i.e. $N_{\min,P} \le N_{L,P}$.

Example 2.1. The following matrix can be considered as the exponent matrix of a $(3,4)-$QC LDPC code with girth 6, for each lifting-degree $N \ge N_{L,P} = 7$, so LB is 7.

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 4 & 6 \end{pmatrix}$$

Moreover, it is easy to see that the MLD corresponding to the exponent matrix P is 5, i.e we have $g(H_{P,5})=6$. (It is noted that for $N=6$, we have $g(H_{P,6})=4$, so 5 is not a lower-bound).

3 ORDERING MATRIX

In this section, an *ordering matrix* is used to generate the elements of the exponent matrix P recursively such that the QC-LDPC code with parity-check matrix $H_{P,N}$ has girth 6 for enough large N such that the corresponding LB and MLD are small as possible.

Definition 3.1. Let $n>3$ be a positive integer. By an $n-$ ordering, we mean a $3\times n$ matrix $O=\left(o_{i,j}\right)_{3\times n}, o_{i,j}\in\{1,2,\ldots,3n\}$ such that each element $k\in\{1,2,\ldots,3n\}$ appears exactly once in the matrix O, i.e. for each $(i_1,j_1)\neq(i_2,j_2)$, we have $o_{i_1,j_1}\neq o_{i_2,j_2}$.

For a given $n-$ ordering matrix $O=\left(o_{i,j}\right)_{3\times n}$, we propose an algorithm which generates the elements of the exponent matrix $P=(p_{i,j})_{3\times n}$ recursively as follows.

Algorithm 1.

1- Let
$o_{i_1,j_1}=1<o_{i_2,j_2}=2<\ldots<o_{i_{3n},j_{3n}}=3n$

2- Set $p_{i_1,j_1}=0$.

3- For each $1\le k\le 3n-1$, the element $p_{i_{k+1},j_{k+1}}$ is defined recursively from $p_{i_1,j_1}, p_{i_2,j_2},..., p_{i_k,j_k}$, as follow:

$p_{i_{k+1},j_{k+1}}:=\min\{N\in Z^{\ge 0}$: if $p_{i_{k+1},j_{k+1}}=N$, then $H\left((i_1,j_1);(i_2,j_2);\ldots;(i_k,j_k),(i_{k+1},j_{k+1})\right)$ is free of 4-cycle$\}$

in which, $H\left((i_1,j_1);(i_2,j_2);\ldots;(i_{k+1},j_{k+1})\right)$ in the algorithm is the parity-check matrix induced by the elements of the exponent matrix which are appeared in the positions $(i_1,j_1);(i_2,j_2);\ldots;(i_{k+1},j_{k+1})$. Moreover, after constructing $p_{i_1,j_1}, p_{i_2,j_2},..., p_{i_k,j_k}$, the element $p_{i_{k+1},j_{k+1}}$ is selected as the minimal non-negative integer with this property that the $H\left((i_1,j_1);(i_2,j_2);\ldots;(i_{k+1},j_{k+1})\right)$ has no 4-cycle. In fact, if A_{k+1} is the set of all $p_{i'_k,j_{k+1}}-p_{i_{k+1},j'_k}+p_{i'_k,j'_k}$ with

$$\{(i'_k,j_{k+1}),(i_{k+1},j'_k),(i'_k,j'_k)\}\subseteq\{(i_1,j_1),(i_2,j_2),\ldots,(i_k,j_k)\},$$

then A_{k+1} contains the values which lead to 4-cycles in the induced Tanner graph, so

$$p_{i_{k+1},j_{k+1}}=\min\{N\in\mathbb{Z}^{\ge 0}: N\notin A_{k+1}\}.$$

4 AN EXPILICIT CONSTRUCTION FOR QC-LDPC CODES WITH GIRTH 6.

For $n>3$, let $O=(o_{i,j})$ be the following $n-$ ordering matrix. For even n, define

$$o_{i,j}=\begin{cases} n/2-j+1, & i=1, 1\le j\le n/2 \\ j, & i=1, n/2<j\le n \\ n+j, & i=2, 1\le j\le n/2 \\ 5n/2-j+1, & i=2, n/2<j\le n \\ 5n/2-j+1, & i=3, 1\le j\le n/2 \\ 2n+j, & i=3, n/2<j\le n \end{cases} \quad (2)$$

And for odd n,

$$o_{i,j}=\begin{cases} \lfloor n/2\rfloor-j+1, & i=1, 1\le j\le \lfloor n/2\rfloor \\ j, & i=1, \lceil n/2\rceil\le j\le n \\ n+j, & i=2, 1\le j\le \lfloor n/2\rfloor \\ \lfloor 5n/2\rfloor-j+1, & i=2, \lceil n/2\rceil\le j\le n \\ \lfloor 5n/2\rfloor-j+1, & i=3, 1\le j\le \lfloor n/2\rfloor \\ 2n+j, & i=3, \lceil n/2\rceil\le j\le n \end{cases} \quad (3)$$

It can be seen easily that O is an $n-$ordering matrix, since $o_{i,j}, 1\le i\le 3, 1\le j\le 3n$ are distinct elements belong to the set $\{1,...,3n\}$. Now, applying Algorithm 1 on the ordering O, let $P=P(O)$ be the corresponding exponent matrix.

Example 4.1: For $n=6,$ let O be the following $6-$ordering defined by Eq. 2.

$$O=\begin{pmatrix} 3 & 2 & 1 & 4 & 5 & 6 \\ 7 & 8 & 9 & 12 & 11 & 10 \\ 15 & 14 & 13 & 16 & 17 & 18 \end{pmatrix}$$

Then, applying Algorithm 1, the corresponding exponent matrix $P=P(O)$ is as follows.

$$P=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 5 & 4 & 3 \\ 2 & 1 & 0 & 4 & 5 & 6 \end{pmatrix}$$

Moreover, it can be seen easily that $N_{L,P}=N_{\min,P}=7$

5 THE ALGORITHM OUTPUTS.

In [8], the authors have introduced an exhaustive search to find all of possible non-isomorphic 4-cycle free column-weight three QC-LDPC codes with the shortest lengths. For $4\le n\le 8$, Table 1 provides all of non-isomorphic $3\times n$ exponent matrices of girth-6 QC-LDPC codes along with dimension, minimum distance, LB and MLD. The first row of the exponent matrices is zero, so for simplicity, the second and

third rows of the exponent matrix are given, such that the upper and lower indices of the given matrices correspond to the minimum distance and dimension of the constructed QC-LDPC codes.

Table1

All of non-isomorphic $3\times n$ exponent matrices of some girth-6 QC-LDPC codes in [8] along with dimension, minimum distance, LB and MLD

Size of base matrix	3×4	3×5	3×6	3×7	3×8
$N_{\min,P}$	5	5	7	7	9
Second and Third Rows of the Exponent Matrix	$\begin{pmatrix}0,2,3,4\\0,3,2,1\end{pmatrix}^{6}_{7}$ $N_{L,P}=5$	$\begin{pmatrix}0,1,2,3,4\\0,3,1,4,2\end{pmatrix}^{6}_{12}$ $N_{L,P}=5$	$\begin{pmatrix}0,1,3,4,5,6\\0,5,1,6,4,2\end{pmatrix}^{6}_{23}$ $N_{L,P}=9$ $\begin{pmatrix}0,1,3,4,5,6\\0,4,5,2,6,3\end{pmatrix}^{6}_{23}$ $N_{L,P}=9$ $\begin{pmatrix}0,1,3,4,5,6\\0,3,6,5,2,4\end{pmatrix}^{4}_{23}$ $N_{L,P}=7$ $\begin{pmatrix}0,1,3,4,5,6\\0,5,6,2,4,1\end{pmatrix}^{4}_{26}$ $N_{L,P}=10$	$\begin{pmatrix}0,1,2,3,4,5,6\\0,2,4,6,1,3,5\end{pmatrix}^{6}_{30}$ $N_{L,P}=7$ $\begin{pmatrix}0,1,2,3,4,5,6\\0,3,6,4,2,1,5\end{pmatrix}^{4}_{30}$ $N_{L,P}=9$	$\begin{pmatrix}0,1,2,3,4,5,6,8\\0,2,5,1,8,7,3,4\end{pmatrix}^{6}_{47}$ $N_{L,P}=9$ $\begin{pmatrix}0,1,2,3,4,5,6,8\\0,3,8,7,5,1,4,2\end{pmatrix}^{6}_{47}$ $N_{L,P}=13$ $\begin{pmatrix}0,1,2,3,4,5,6,8\\0,7,4,8,5,3,1,2\end{pmatrix}^{6}_{47}$ $N_{L,P}=13$ $\begin{pmatrix}0,1,2,3,4,5,6,8\\0,5,4,6,2,1,3,7\end{pmatrix}^{6}_{47}$ $N_{L,P}=9$ $\begin{pmatrix}0,1,2,3,4,5,6,8\\0,7,5,4,8,3,2,1\end{pmatrix}^{4}_{47}$ $N_{L,P}=14$ $\begin{pmatrix}0,1,2,3,4,5,6,8\\0,5,7,4,1,3,8,2\end{pmatrix}^{4}_{47}$ $N_{L,P}=12$ $\begin{pmatrix}0,1,2,3,4,5,6,8\\0,5,3,8,1,7,4,2\end{pmatrix}^{4}_{47}$ $N_{L,P}=12$ $\begin{pmatrix}0,1,2,3,4,5,6,8\\0,4,8,5,2,1,7,3\end{pmatrix}^{4}_{47}$ $N_{L,P}=12$

Table2

Some $3\times n$ exponent matrices of girth-6 QC-LDPC codes constructed by Algorithm1 along with dimension, minimum distance, LB and MLD

Size of base matrix	3×4	3×5	3×6	3×7	3×8
$N_{\min,P}$	5	5	7	7	9
Second and Third Rows of the Exponent Matrix	$\begin{pmatrix}0,1,3,2\\1,0,3,4\end{pmatrix}_7^6$ $N_{L,P}=5$	$\begin{pmatrix}0,1,4,3,2\\1,0,2,3,4\end{pmatrix}_{12}^6$ $N_{L,P}=5$	$\begin{pmatrix}0,1,2,5,4,3\\2,1,0,4,5,6\end{pmatrix}_{23}^6$ $N_{L,P}=7$	$\begin{pmatrix}0,1,2,6,5,4,3\\2,1,0,3,4,5,6\end{pmatrix}_{30}^6$ $N_{L,P}=7$	$\begin{pmatrix}0,1,2,3,7,6,5,4\\3,2,1,0,5,6,7,8\end{pmatrix}_{47}^6$ $N_{L,P}=9$

For example, by $\begin{pmatrix}0,1,3,4,5,6\\0,5,1,6,4,2\end{pmatrix}_{23}^6$, we mean the code with the exponent matrix $P=\begin{pmatrix}0,0,0,0,0,0\\0,1,3,4,5,6\\0,5,1,6,4,2\end{pmatrix}$ having minimum-distance 6, dimension 23, LB $N_{L,P}=9$ and MLD $N_{\min,P}=7$.

Against, for $4\le n\le 8$, some of the constructed exponent matrices $P=P(O)$ (obtained by Algorithm 1) are provided in Table 2. Based on the ordering O reported in Eq.1, the first row of the constructed exponent matrix $P=P(O)$ is zero, so the second and third rows of P are just reported. As Table II shows, the constructed exponent matrices have better LB rather than the exponent matrices reported in Table I, while they have the same MLD, minimum distance and dimension. In addition, the constructed exponent matrices in Table II have another benefit rather than the exponent matrices given in Table I in terms of the complexity. In fact, the exponent matrices in Table II have constructed explicitly and no computer search is needed to generate such exponent matrices. Against, the complexity to generate the exponent matrices in Table I increases exponentially by enlarging n.

6 COCLUSIONS.

In this paper, an $n-$ordering matrix is defined which is helpful to construct some $3\times n$ exponent matrices recursively, such that the corresponding QC-LDPC codes are free of 4-cycles. Interestingly, the constructed codes have better LB and complexity rather than the previously reported codes, while the MLD, minimum-distance and dimension are the same.

REFERENCES

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

[2] J. L. Fan, "Array codes as low-density parity-check codes," in Proc. *2nd Int. Symp. Turbo Codes and Related Topics*, Brest, France, Sept. 2000, pp. 543-546.

[3] R. G. Gallagar, "Low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 21-28, Jan. 1962.

[4] M. Gholami, M. Alinia and Z. Rahimi, “An explicit method for construction of CTBC codes with girth 6,” AEU *Int. J. Elect. And Commun.* vol. 74, pp. 183-191, April. 2017.

[5] K. Kyung-Joong, C. Jin-Ho, and Y. Kyeongcheol, “Bounds on the size of parity-check matrices for quasi cyclic low-density parity-check codes,” *IEEE Trans. on Inform. Theory*, vol. 59, pp. 7288-7298, 2013.

[6] M. Karimi and A. H. Banihashemi, “On the girth of quasi cyclic protograph LDPC codes,” *IEEE Trans. Inform. Theory*, vol. 59, no. 7, pp. 4542-4552, July 2013.

[7] D. J. C. Mackay and R.M Neal, “Near Shannon limit performance of low density parity check codes,” *IEEE Elect. Lett.*, vol. 32, no. 18, pp. 1645–1646, Aug. 1996.

[8] A. Tasdighi, A. H. Banihashemi, and M. R. Sadeghi, “Efficient Search of Girth-Optimal QC-LDPC Codes,” *IEEE Trans. Inform. Theory*, vol. 62, no. 4, pp. 1552–1564, April 2016.