Journal of Algebraic Systems
Vol. 7, No. 2, (2020), pp 271-280

A REDUCTION IN THE SEARCH SPACE OF QC-LDPC CODES WITH GIRTH 8

F. AMIRZADE, M. ALISHAHI AND M.-R. (RAFSANJANI) SADEGHI*

ABSTRACT. In this paper, we define a structure to obtain exponent matrices of girth-8 QC-LDPC codes with column weight 3. Using the difference matrices introduced by Amirzade et al., we investigate necessary and sufficient conditions which result in a Tanner graph with girth 8. Our proposed method contributes to reduce the search space in recognizing the elements of an exponent matrix. In fact, in this method we only search to obtain one row of an exponent matrix. The other rows are multiplications of that row.

1. INTRODUCTION

An LDPC code is a linear code (a vector space over a finite field) whose parity-check matrix is sparse. LDPC codes were introduced by Gallager in 1960 [6]. Tanner in 1981 [12] generalized LDPC codes and proposed a graphical representation of LDPC codes now called Tanner graph which is a bipartite graph whose incidence matrix is the parity-check matrix of the code. A parity-check matrix with column weight m and row weight n results in an (m,n)-regular LDPC code. An important parameter associated to LDPC codes is their *girth*, that is, the length of the shortest cycles of its corresponding Tanner graph. It is well-known that the girth as well as some graphical structures such as *trapping sets* [1] influence the code performance.

MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.
Keywords: QC-LDPC codes, protographs, girth, difference matrices, lifting degree.
Received: 16 February 2019, Accepted: 6 May 2019.
*Corresponding author.

Quasi-cyclic LDPC (QC-LDPC) codes form an essential category of LDPC codes that are known because of their practical implementations. Two matrices, a *base matrix* W and an *exponent matrix* B, as well as a lifting degree N are associated to a QC-LDPC code. If all elements of W are 0 and 1, then its corresponding parity-check matrix gives a single-edge QC-LDPC code. We replace 1-components and zero elements of W by some non-negative integers less than N and (∞), respectively, to obtain an exponent matrix. Non-negative integers in the exponent matrix are replaced by $N \times N$ circulant permutation matrices (CPMs), and (∞) is replaced by an $N \times N$ zero matrix (ZM). The resulting matrix gives the parity-check matrix whose null space provides us with a single-edge QC-LDPC code.

A necessary and sufficient condition for the exponent matrix of QC-LDPC codes to have a Tanner graph with a specific girth were presented in [5] by Fossorier. A large body of work has been devoted to obtain the smallest lifting degrees of (m, n)-regular QC-LDPC codes with different girths and different column weights [2–5], [7–11], [13], [14].

In this paper, we first propose a method to construct an exponent matrix which depends on one row of that matrix. The other rows are obtained by multiplying that row by an integer. Then by constructing its corresponding difference matrix, we consider a necessary and sufficient condition to have a girth-8 Tanner graph.

2. Preliminaries

Let N be an integer. Consider the following exponent matrix $B = [b_{ij}]$, where $b_{ij} \in \{0, 1, \cdots, N-1\}$ or $b_{ij} = (\infty)$,

$$B = \begin{bmatrix} b_{00} & b_{01} & \cdots & b_{0(n-1)} \\ b_{10} & b_{11} & \cdots & b_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(m-1)0} & b_{(m-1)1} & \cdots & b_{(m-1)(n-1)} \end{bmatrix}. \tag{2.1}$$

The ij-th element of the matrix B which is an integer is substituted by an $N \times N$ matrix $I^{b_{ij}}$. This matrix is a circulant permutation matrix (CPM) in which the unique 1-component of the top row is located at the b_{ij}-th position and other entries of the top row are zero. The r-th row of a CPM is formed by r right cyclic shifts of the first row and clearly the first row is a right cyclic shift of the last row. If $b_{ij} = (\infty)$, then it is replaced by an $N \times N$ zero matrix. The null space of the parity-check matrix gives a QC-LDPC code.

A necessary and sufficient condition for the existence of cycles of length $2k$ (or simply $2k$-cycles) in the Tanner graph of QC-LDPC codes was provided in [5]. If

$$\sum_{i=0}^{k-1}(b_{m_in_i} - b_{m_in_{i+1}}) = 0 \pmod{N}, \tag{2.2}$$

where $n_k = n_0$, $m_i \neq m_{i+1}$, $n_i \neq n_{i+1}$ and $b_{m_in_i}$ is the (m_i, n_i)-th entry of B, then the Tanner graph of the parity-check matrix has cycles of length $2k$.

To avoid 4-cycles, using Equation (2.2), one has to check every 2×2 submatrix of the exponent matrix. Submatrices of size 3×3 must be checked to avoid 6-cycles and to check 8-cycles we must consider all submatrices of sizes 2×2, 2×3, 2×4, 3×2, 3×3, 3×4, 4×2, 4×3 and 4×4. In [2], difference matrices are introduced to simplify checking even cycles of lengths 4 to 12. In the following, we present these difference matrices which are our main tools in the next results.

Definition 2.1. Let B be an $m \times n$ exponent matrix with elements b_{ij}, $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$. The difference matrix D is defined as follows:

$$D = \begin{bmatrix} b_{00} - b_{10} & \dots & b_{0(n-1)} - b_{1(n-1)} \\ \vdots & \ddots & \vdots \\ b_{00} - b_{(m-1)0} & \dots & b_{0(n-1)} - b_{(m-1)(n-1)} \\ b_{10} - b_{20} & \dots & b_{1(n-1)-b_{2(n-1)}} \\ \vdots & \ddots & \vdots \\ b_{10} - b_{(m-1)0} & \dots & b_{1(n-1)} - b_{(m-1)(n-1)} \\ \vdots & \ddots & \vdots \\ b_{(m-2)0} - b_{(m-1)0} & \dots & b_{(m-2)(n-1)} - b_{(m-1)(n-1)} \end{bmatrix}. \tag{2.3}$$

If $b_{ij} = (\infty)$ or $b_{i'j} = (\infty)$, then we set $b_{ij} - b_{i'j} = (\infty)$.

Example 2.2. Let $B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 7 & 10 & 4 \\ 0 & 4 & 7 & 9 \end{bmatrix}$ be a 3×4 exponent matrix with the lifting degree $N = 13$. Its associated difference matrix D is defined as follows,

$$D = \begin{bmatrix} 0 & -7 & -10 & -4 \\ 0 & -4 & -7 & -2 \\ 0 & 3 & 3 & -5 \end{bmatrix}. \tag{2.4}$$

A necessary and sufficient condition for the difference matrix to avoid 4-cycles is provided in the next proposition.

Proposition 2.3. [2] *A Tanner graph is 4-cycle free if and only if each row of the difference matrix D is free of repeated elements in modulo N.*

In the above example, we compute all elements of D in modulo $N = 13$. Since the third row of D in modulo N has repeated elements, Proposition 2.3 indicates that the exponent matrix B with the lifting degree 13 yields a QC-LDPC code with girth 4.

Using the difference matrix D, we can also simplify Equation 2.2 to deal with 6-cycles. This simplification is presented in the following Lemma.

Lemma 2.4. *Let D be a difference matrix corresponding to a $3 \times n$ exponent matrix B. The Tanner graph is 6-cycle free if and only if $-D_{0j_0} + D_{1j_1} - D_{2j_2} \not\equiv 0 \pmod N$ for all $j_0 \neq j_1, j_0 \neq j_2, j_1 \neq j_2$ where j_0, j_1, j_2 are chosen from $\{0, 1, \ldots, (n-1)\}$.*

In Example 2.2, the equality $-D_{01} + D_{12} - D_{20} = -(-7) + (-7) - 0 = 0$ results in the existence of 6-cycles.

Definition 2.5. A $\binom{m}{2} \times \binom{n}{2}$ difference matrix DD is constructed by subtracting every two columns of D. Suppose D_{ij} and $D_{ij'}$ are two elements in the ith row of the difference matrix D and distinct columns j and j' respectively, where $j < j'$. If we subtract j'-th column from j-th column, then

$$DD_{i(j,j')} = (D_{ij} - D_{ij'}, D_{ij'} - D_{ij}) \pmod N$$

is defined as an element of the i-th row and (j, j')-th column of DD.

Example 2.6. Let B and N be the exponent matrix and the lifting degree in Example 2.2. According to Definition 2.5,

$$DD = \begin{bmatrix} (7,6) & (10,3) & (4,9) & (3,10) & (10,3) & (7,6) \\ (4,9) & (7,6) & (2,11) & (3,10) & (11,2) & (8,5) \\ (10,3) & (10,3) & (5,8) & (0,0) & (8,5) & (8,5) \end{bmatrix}. \quad (2.5)$$

A necessary and sufficient condition for difference matrix DD to avoid 6-cycles is provided in the following Lemma.

Lemma 2.7. [2] *Let DD be a difference matrix corresponding to an $m \times n$ exponent matrix B. Take $DD_{i(j,j')}$ and $N - DD_{i(j,j')}$ as the first and the second components, respectively, of an element of DD occurring in the i-th row and the (j, j')-th column. If the Tanner graph is 6-cycle free, then any submatrix of DD corresponding to a 3×3 submatrix of*

B whose first row is all-zero fulfills the following inequalities:

$$\begin{array}{ll} 1)\ DD_{i(j_0,j_1)} \neq DD_{i'(j_0,j_2)} & 2)\ DD_{i(j_0,j_1)} \neq N - DD_{i'(j_1,j_2)} \\ 3)\ DD_{i(j_0,j_2)} \neq DD_{i'(j_1,j_2)} & 4)\ DD_{i(j_0,j_2)} \neq DD_{i'(j_0,j_1)} \\ 5)\ DD_{i(j_1,j_2)} \neq N - DD_{i'(j_0,j_1)} & 6)\ DD_{i(j_1,j_2)} \neq DD_{i'(j_0,j_2)}, \end{array} \tag{2.6}$$

where $i, i' \in \{0, \ldots, m-2\}$ and $i \neq i'$ and also, distinct column indices j_0, j_1 and j_2 of DD correspond to the three columns of B.

Since the difference matrix DD in Example 2.6 contains two pairs $DD_{0(0,1)} = DD_{1(0,2)} = (7, 6)$ which do not hold in the condition (1) of Lemma 2.7, the Tanner graph has 6-cycles.

3. New Construction of QC-LDPC codes with girth 8

In this section, we propose a structure for an exponent matrix to construct a QC-LDPC code with girth 8 and column weight 3. This structure helps to reduce the size of the search space to obtain elements of an exponent matrix. Using Proposition 2.3 and Lemmas 2.4 and 2.7 we provide the requirements to construct a girth-8 Tanner graph.

Suppose that for each $1 \leq i \leq n-1$ we have $B_i \in \{1, \ldots, N-1\}$ and also, for $2 \leq d \leq \frac{N}{2}$ put $C_i = d.B_i \pmod N$. The following matrix can be an exponent matrix with the lifting degree N where all computations are in modulo N.

$$B = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 \\ 0 & B_1 & B_2 & \ldots & B_{n-1} \\ 0 & C_1 & C_2 & \ldots & C_{n-1} \end{bmatrix}. \tag{3.1}$$

We apply Proposition 2.3 as well as Lemmas 2.4 and 2.7 to the above matrix B to obtain a QC-LDPC code with girth 8. In the following, we mention the most contribution of this method. In general, if a $3 \times n$ exponent matrix is desired, then, by assuming that the first row and the first column are all-zero, $2(n-1)$ elements have to be searched which belong to $\{1, 2, \ldots, N-1\}$. In other words, the number of choices for all of these elements are $(N-1)^{2(n-1)} = O(M)$, which makes constructing an exponent matrix difficult for large column weights. Whereas, in our method, this search will be reduced to $O(\sqrt{M})$. In fact, by recognizing the elements of the second row, we can construct the whole matrix and the number of our choices is $(N-1)^{(n-1)}$.

To reach our goal we have to construct difference matrices. The difference matrix D which is used to check 4-cycles is

$$D = \begin{bmatrix} 0 & -B_1 & -B_2 & \dots & -B_{n-1} \\ 0 & -C_1 & -C_2 & \dots & -C_{n-1} \\ 0 & B_1 - C_1 & B_2 - C_2 & \dots & B_{n-1} - C_{n-1} \end{bmatrix}. \tag{3.2}$$

Theorem 3.1. *The exponent matrix B is 4-cycle free if and only if*

(1) $B_i \not\equiv B_j$ *(mod N)*
(2) *for $l \in \{d, d-1\}$ and $i \neq j \in \{1, \dots, n-1\}$ we have $l.B_i \not\equiv l.B_j$ (mod N) and $l.B_i \not\equiv 0$ (mod N).*

Proof. According to Proposition 2.3, a necessary and sufficient condition to have no 4-cycle is to avoid repeated elements in every row of the difference matrix D. Therefore, the first item (1) is trivial. In the second row of the difference matrix D we have $C_i \not\equiv C_j$ and $C_i \not\equiv 0$. Hence, $d.B_i \not\equiv d.B_j$ (mod N) and $d.B_i \not\equiv 0$ (mod N). In the third row, $B_i - C_i = B_i - d.B_i = (1-d).B_i$ (mod N). So, the second item for $l = d-1$ is trivial. □

Theorem 3.2. *A necessary and sufficient condition to obtain a girth-8 QC-LDPC code from the exponent matrix B is as follows:*

(1) $|\{B_1, B_2 \dots, B_{n-1}\} \cup \{d.B_1, d.B_2 \dots, d.B_{n-1}\}| = 2(n-1)$ *in modulo N,*
(2) $B_i + d.B_j \not\equiv 0$ *(mod N) and* $B_j + d.B_i \not\equiv 0$ *(mod N), where* $|j - i| \geq 2$,
(3) $B_i - d.B_j + (d-1).B_k \not\equiv 0$ *(mod N).*

Proof. Since the first row and the first column of the exponent matrix B are all-zero, we can use Lemma 2.7. In order to show the first item we must check 6-cycles in 3×3 submatrices of the exponent matrix B whose first column is all-zero. Therefore, it is sufficient to apply the six conditions in Lemma 2.7 to the first two rows and the first $n-1$ columns of DD. From the conditions (1), (3), (4), and (6) we conclude that $B_i \not\equiv d.B_j$ (mod N), where $i \neq j \in \{1, \dots n-1\}$. Consequently, $\{B_1, B_2 \dots, B_{n-1}\} \cap \{d.B_1, d.B_2 \dots, d.B_{n-1}\} = \emptyset$. Tanner graph is supposed to be 4-cycle free. So, according to the second condition of Theorem 3.1, we have $|\{B_1, B_2 \dots, B_{n-1}\}| = n-1$ and $|\{d.B_1, d.B_2 \dots, d.B_{n-1}\}| = n-1$. Since these two sets do not intersect, their union contains $2(n-1)$ elements.

To prove the second item of Theorem, we use the conditions (2) and (5) of Lemma 2.7. These two conditions imply that for each two column indices i, j, where $|i-j| \geq 2$, we have $B_i \not\equiv N - d.B_j$ (mod N) and $B_j \not\equiv N - d.B_i$ (mod N). Therefore, if $|i-j| \geq 2$, then $B_i + d.B_j \not\equiv 0$ (mod N) and $B_j + d.B_i \not\equiv 0$ (mod N).

To show the third item, we have to check 6-cycles in 3×3 submatrices of the exponent matrix B which do not contain the first column of B. This inequality is a straightforward consequence of Lemma 2.4. $\square$

Corollary 3.3. *A lower bound for the lifting degree of a girth-8 QC-LDPC code whose exponent matrix is the exponent matrix B is $N = 2n-1$.*

Proof. Since the necessary condition to avoid 6-cycles in the exponent matrix B is the nonexistence of repeated elements in the set $\{B_1, B_2 \dots, B_{n-1}\} \cup \{d.B_1, d.B_2 \dots, d.B_{n-1}\}$, and all computations are in modulo N, the lifting degree has to be more than the cardinality of this set. Hence, $N \geq 2(n-1)+1 = 2n-1$. $\square$

The minimum lifting degrees for the exponent matrix B with column weights $4 \leq n \leq 10$ are shown in Tables 1-4 in Appendix. These tables contain the second row of B as well as the multiple d for any column weight n.

Corollary 3.4. *There exists a girth-8 QC-LDPC code from the exponent matrix B for any lifting degree $N \geq 2\binom{n}{2}+1$.*

Proof. If we restrict ourselves to search for an exponent matrix whose difference matrix DD contains distinct elements in the first two rows, then DD holds in the conditions of Theorem 3.2. So, in this case the mentioned rows contain $2\binom{n}{2}$ distinct elements. Similar to the proof of Corollary 3.3, it can be shown that the lifting degree must be at least $2\binom{n}{2}+1$. $\square$

4. Conclusion

In this paper, we presented a technique to reduce the size of the search space in obtaining the elements of an exponent matrix with column weight 3. Our method is used to construct a QC-LDPC code with girth 8. We showed that by recognizing the elements of one row in the exponent matrix we obtain the whole matrix. In fact, the computational complexity is reduced from $O(M)$ to $O(\sqrt{M})$.

References

1. F. Amirzade and M. R Sadeghi, Analytical lower bounds on the size of elementary trapping sets of variable-regular LDPC codes with any girth and irregular ones with girth 8, *IEEE Trans. Commun.*, **66**(6) (2018), 2313–2321.

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. F. Amirzade and M. R Sadeghi, Analytical lower bound on the lifting degree of multiple-edge QC-LDPC codes with girth 6, *IEEE Comm. Letters*, **22**(8) (2018), 1528–1531.
4. I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov and R. V. Satyukov, Searching for voltage graph-based LDPC tailbiting codes with large girth, *IEEE Trans. Inf. Theory*, **58**(4) (2012), 2265–2279.
5. M. P. C. Fossorier, Quasi-cyclic low-density parity-check codes from circulant permutation matrices, *IEEE Trans. Inf. Theory*, **50**(8) (2004), 1788–1793.
6. R. G. Gallager, *Low-Density Parity-Check Codes*, Cambridge, MA, MIT Press, 1963.
7. M. Hagiwara, M. P. C. Fossorier, T. Kitagawa and H. Imai, Smallest size of circulant matrix for $(3, L)$ and $(4, L)$ quasi-cyclic LDPC codes with girth 6, *IEICE Trans. Fundam. Electronics, Commun. Comput. Sci.*, **92**(11) (2009), 2891–2894.
8. M. Karimi and A. H. Banihashemi, On the girth of quasi-cyclic protograph LDPC codes, *IEEE Trans. Inf. Theory*, **59**(7) (2013), 4542–4552.
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**(8) (2007), 2885–2891.
10. M. E. O'Sullivan, Algebraic construction of sparse matrices with large girth, *IEEE Trans. Inf. Theory*, **52**(2) (2006), 718–727.
11. S. V. S. Ranganathan, D. Divsalar and R. D. Wesel, On the girth of $(3, L)$ quasi-cyclic LDPC codes based on complete protographs, *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, (2015), 731–735.
12. R. M. Tanner, A Recursive approach to low complexity codes, *IEEE Trans. Inf. Theory*, **27**(9) (1981), 533–547.
13. Y. Wang, J. S. Yedidia and S. C. Draper, Construction of high-girth QC-LDPC codes, *Proc. 5th Int. Symp. Turbo Codes Rel. Topics*, (2008), 180–185.
14. G. Zhang, R. Sun and X. Wang, Explicit construction of girth-eight QC-LDPC codes and its application in CRT methods, *J. Commun.*, **33**(3) (2012), 171–176.

Farzane Amirzade
Faculty of Mathematical Sciences, Shahrood University of Technology, Shahrood, Iran.
Email: famirzade@gmail.com

Meysam Alishahi
Faculty of Mathematical Sciences, Shahrood University of Technology, Shahrood, Iran.
Email: meysam_alishahi@shahroodut.ac.ir

Mohammad-Reza (Rafsanjani) Sadeghi
Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran.
Email: msadeghi@aut.ac.ir

5. Appendix

Table 1. The second row of an exponent matrix of $(3,n)$-regular QC-LDPC codes with girth 8, $4 \leq n \leq 6$. The third row is the multiplication of the second row by d. The first row is all-zero.

Row weight	$n=4$	$n=5$	$n=6$
Lifting Degree	$N=9$	$N=13$	$N=19$
Multiple	$d=2$	$d=4$	$d=2$
Second Row	0 1 4 6	0 1 3 5 6	0 1 3 12 14 15

Table 2. The second row of an exponent matrix of $(3,n)$-regular QC-LDPC codes with girth 8, $n = 7, 8$. The third row is the multiplication of the second row by d. The first row is all zero.

Row weight	$n=7$	$n=8$
Lifting Degree	$N=21$	$N=27$
Multiple	$d=5$	$d=2$
Second Row	0 1 3 8 13 18 20	0 1 3 4 9 10 12 13

TABLE 3. The second row of an exponent matrix of $(3, n)$-regular QC-LDPC codes with girth 8, $n = 9$. The third row is the multiplication of the second row by d. The first row is all zero.

Row weight	$n = 9$								
Lifting Degree	$N = 31$								
Multiple	$d = 6$								
Second Row	0	1	3	5	7	9	10	20	21

TABLE 4. The second row of an exponent matrix of $(3, n)$-regular QC-LDPC codes with girth 8, $n = 10$. The third row is the multiplication of the second row by d. The first row is all zero.

Row weight	$n = 10$									
Lifting Degree	$N = 37$									
Multiple	$d = 2$									
Second Row	0	1	3	7	17	24	25	28	29	35

Journal of Algebraic Systems

A REDUCTION IN THE SEARCH SPACE OF QC-LDPC CODES WITH GIRTH 8

F. AMIRZADE, M. ALISHAHI AND M.-R. (RAFSANJANI) SADEGHI

کاهش در فضای جستجوی کدهای کم‌چگال شبه‌دوری با کمر ۸

فرزانه امیرزاده[۱]، میثم علیشاهی[۱] و محمدرضا رفسنجانی صادقی[۲]
[۱]دانشکده علوم ریاضی، دانشگاه صنعتی شاهرود، شاهرود، ایران
[۲] دانشکده ریاضی و علوم کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران، ایران

در این مقاله، ساختاری برای به دست آوردن ماتریس نمایه‌ی کدهای کم چگال شبه دوری با کمر ۸ و وزن ستونی ۳ ارائه می‌دهیم. با استفاده از ماتریس‌های تفاضلی معرفی شده توسط امیرزاده و صادقی شرایط لازم و کافی را برای به دست آوردن گراف تنر با کمر ۸ ارائه می‌دهیم. روش مطرح شده در این مقاله به کاهش فضای جستجو در تشخیص درایه‌های ماتریس نمایه کمک می‌کند. درواقع، در این روش فقط یک سطر از ماتریس نمایه را می‌یابیم. سطرهای دیگر مضربی از سطر جستجو شده است.

کلمات کلیدی: کدهای کم چگال شبه دوری، گراف تنر، ماتریس تفاضلی.