IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 18, 2018, accepted April 20, 2018, date of publication April 26, 2018, date of current version May 16, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2830406

Lower Bounds on the Lifting Degree of QC-LDPC Codes by Difference Matrices

FARZANE AMIRZADE[1] AND MOHAMMAD-REZA SADEGHI[2]
[1]School of Mathematical Sciences, Shahrood University of Technology, Shahrud 3619995161, Iran
[2]Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran 15875-4413, Iran

Corresponding author: Mohammad-Reza Sadeghi (msadeghi@aut.ac.ir)

ABSTRACT In this paper, we define two "difference matrices" which correspond to an exponent matrix. We present necessary and sufficient conditions for these difference matrices to have quasi-cyclic low-density parity-check codes (QC-LDPC) codes with a certain girth. We achieve all non-isomorphic QC-LDPC codes with the shortest length, girth 6, the column weight, $m = 4$, and the row weight, $5 \leq n \leq 11$. Moreover, a method to obtain an exponent matrix with girth 10 is presented which reduces the complexity of the search algorithm. If the first row and the first column of the exponent matrix are all-zero, then by applying our method we do not need to test Fossorier's lemma to avoid 6-cycles and 8-cycles. For girth 10, we also provide a lower bound on the lifting degree which is tighter than the existing bound. For girth 12, a new lower bound on the lifting degree is achieved.

INDEX TERMS QC-LDPC codes, protographs, girth, difference matrices, lifting degree.

I. 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 practical and simple implementations. One of the most important representations of codes is Tanner graph. The length of the shortest cycles of the Tanner graph, girth, has been known to influence the code performance. According to [1], LDPC codes with large girth and small number of short cycles have good performances and lots of efforts have been put into constructing codes that fulfill the mentioned property.

There are two main approaches for constructing LDPC codes, algebraic-based and graph-theoretic-based. Of the latter the most well-known methods are progressive edge growth (PEG) and protograph-based methods. There is a large body of work devoted to the protograph-based QC-LDPC code structures, the girth of their Tanner graph, the length of the code, the minimum distance of the code and so on. In the protograph-based category, a single-edge QC-LDPC code corresponds to a base matrix, B_{ptg}, in which all entries are ones or zeros. If B_{ptg} contains an all-one submatrix of size 2×3 or 3×2, then the Tanner graph has 12-cycles, [2]. So, the maximum girth of fully-connected single-edge QC-LDPC codes whose base matrix is an all-one matrix is 12. For a single-edge QC-LDPC code, we define an exponent matrix, B, corresponding to its base matrix, B_{ptg}, as follows. We replace 1-components and zero elements of B_{ptg} by some non-negative integers less than N and (∞), respectively. If non-negative integer numbers, b_{ij}s, in the exponent matrix are replaced by $N \times N$ circulant permutation matrices (CPMs), whose first row has 1 in the b_{ij}-th column and zero in other columns, and (∞) is replaced by an $N \times N$ zero matrix (ZM), then we obtain the parity-check matrix. The null space of this parity-check matrix forms a single-edge QC-LDPC code. Hereafter, we use QC-LDPC codes instead of single-edge QC-LDPC codes. An (m, n)-regular QC-LDPC code with the lifting degree, N, is defined as a code represented by an $mN \times nN$ parity-check matrix, H, in which each column has weight m and each row has weight n. The necessary and sufficient condition for the Tanner graph of QC-LDPC codes to have a given girth were presented by Fossorier [3]. He provided the smallest lifting degrees of (m, n)-regular QC-LDPC codes with girth 6 and column weights 3, 4 and 5 and row weight $n \leq 12$. He also presented the smallest lifting degrees of $(3, n)$-regular QC-LDPC codes with girth 8, where $n \leq 12$. There are also some results in [4], [5], and [6]regarding to lifting degrees of QC-LDPC codes with column weights 3 and 4 and girths 6 and 8. O'Sullivan [7], analyzed algebraic conditions that lead to short cycles in the Tanner graph and presented methods to achieve QC-LDPC codes with large girth which results in a good error correction performance. He provided the minimum lifting degrees,

TABLE 1. One of non-isomorphic (4, *n*)-regular QC-LDPC codes with girth 6, row weights 5, 6, 7 and 8 for the existing minimum distances.

Row weight	$n = 5$	$n = 6$	$n = 7$	$n = 8$
Lifting degree	$N = 5$	$N = 7$	$N = 7$	$N = 10$
NI numbers	1	2	2	2996
B with $d_{min} = 10$	-	1 3 4 5 6 5 1 6 4 2 2 6 1 3 5	1 2 3 4 5 6 2 4 6 1 3 5 3 6 2 5 1 4	1 2 3 4 5 6 7 2 1 5 7 9 4 3 5 7 2 6 1 9 4
B with $d_{min} = 8$	1 2 3 4 3 1 4 2 2 4 1 3	1 3 4 5 6 5 1 6 4 2 3 2 5 1 4	1 2 3 4 5 6 2 4 6 1 3 5 4 1 5 2 6 3	1 2 3 4 5 6 7 2 1 5 7 9 4 3 3 6 2 1 8 7 5
B with $d_{min} = 6$	-	-	-	1 2 3 4 5 6 7 2 1 5 8 3 9 4 7 3 6 1 9 8 2

TABLE 2. One of non-isomorphic (4, *n*)-regular QC-LDPC codes with girth 6, row weights 9, 10 and 11 for the existing minimum distances.

Row weight	$n = 9$	$n = 10$	$n = 11$
Lifting degree	$N = 10$	$N = 11$	$N = 11$
NI numbers	29	24	7
B with $d_{min} = 10$	1 2 3 4 5 6 7 8 2 5 7 9 4 8 3 6 5 3 9 6 8 4 2 7	1 2 3 4 5 6 7 9 10 10 9 8 7 6 5 4 2 1 2 4 6 8 10 1 3 7 9	1 2 3 4 5 6 7 8 9 10 7 3 10 6 2 9 5 1 8 4 2 4 6 8 10 1 3 5 7 9
B with $d_{min} = 8$	1 2 3 4 5 6 7 8 2 1 6 8 7 3 5 4 3 6 8 5 1 9 4 7	1 2 3 4 5 6 7 9 10 5 10 4 2 7 9 1 8 6 4 8 1 5 9 2 6 3 7	1 2 3 4 5 6 7 8 9 10 2 6 9 7 4 3 1 10 5 8 3 1 7 9 8 2 4 6 10 5
B with $d_{min} = 6$	1 2 3 4 5 6 7 8 2 5 1 9 7 3 6 4 5 1 9 6 2 4 8 3	-	-

which obtained search-based, for a range of QC-LDPC codes with girths 6, 8, 10 and 12. Regarding to high girth QC-LDPC codes we also refer to [8], [9], and [10]. Tasdighi *et al.* [11], presented a method to find all possible non-isomorphic codes with the same minimum lifting degree, girth and degree distribution. In fact, they achieved a number of isomorphic classes of exponent matrices to obtain an efficient exhaustive search. If an exponent matrix in one such class fails to result in girth, g, then one can prune the search space by eliminating the whole class without affecting the exhaustiveness of the search. They applied their method to achieve non-isomorphic fully connected (3, n)-regular QC-LDPC codes with the minimum lifting degree and girth up to 12. The analytical lower bounds obtained in [3] and [12] on the lifting degree of (m, n)-regular QC-LDPC codes whose Tanner graphs have girth 6, 8 and 10 are n, $(m-1)(n-1)+1$ and $n(n-1)(m-1)+1$, respectively. We also point out the articles [1], [7], [13] and [14] for algebraic-based category. There are also some other approaches to obtain LDPC codes such as cylinder-type block-circulant (CTBC) codes whose parity-check matrices have a cylindrical structure in their base matrices. The comparisons, in [15], between CTBC codes and some QC-LDPC codes with girth 6 and the same column and row weights show that CTBC codes with girth 6 have some advantages over 4-cycle free QC-LDPC codes in terms of the lower bound, minimum distance and 6-cycle multiplicity. Other structure of LDPC codes is obtained from affine permutation matrices, called APM-LDPC codes, which are a class of LDPC codes whose parity-check matrices consist of zero matrices or APMs of the same orders. APM-LDPC codes presented in [16] have shorter lengths than QC-LDPC codes with the same base matrices. Moreover, the constructed APM-LDPC codes have fewer cycle multiplicities compared to QC-LDPC codes with the same base matrices and the same lengths. Regarding to short-length LDPC codes we also refer to [17].

The main contribution of this paper is to provide a method to obtain QC-LDPC codes with a given girth and the minimum lifting degree. This approach reduces the size of the search space and the complexity of the search algorithm. Moreover, it gives us a chance to achieve new lower bounds on the lifting degree which improve the existing bounds in the literature. In the following we summarize our goals in more details.

In this paper, we define two matrices named as "difference matrices", denoted by D and DD, from an exponent matrix. We provide the necessary and sufficient conditions for the difference matrices of a QC-LDPC code to have a Tanner graph with a given girth. One of the advantages of these matrices is a reduction in the complexity of the search algorithm to obtain the minimum lifting degree that achieves a certain girth. Using these matrices we obtain all non-isomorphic fully connected (4, n)-regular QC-LDPC codes with girth 6 and the shortest length for $5 \le n \le 11$. We also obtain their minimum distances and for each minimum distance we present an exponent matrix in Tables 1 and 2. Using difference matrices, we present a method to obtain an exponent matrix with girth 10. Our proposed method demonstrates that if the first row and the first column of the exponent matrix are all-zero, then the non-existence of 8-cycles guarantees the non-existence of some 6-cycles too. In fact, to avoid 6-cycles we do not need to test 3×3 submatrices whose first rows are all-zero. This merit significantly reduces the complexity of the search algorithm. Additionally, the necessary and sufficient conditions for difference matrices to have QC-LDPC codes with girth 10 give rise to the following results.

1) The number of non-isomorphic QC-LDPC codes with the same lifting degree and girth has a direct connection to the search-based method which one applies. In [11], in order to make the search efficient, the size of the search space has been reduced by pruning cases that are isomorphic to those previously examined in the search process. However, this pruning-based search method leads to miss some non-isomorphic cases. For example, the number of non-isomorphic $(3, n)$-regular QC-LDPC codes reported in [11] with girth 10 for $n = 5, 6$ are 3 and 1, respectively, whereas using difference matrices we obtain more non-isomorphic codes in these two cases. We demonstrate that there are 4 non-isomorphic $(3, 5)$-regular QC-LDPC codes with girth 10 and 2 non-isomorphic $(3, 6)$-regular QC-LDPC codes with girth 10. Therefore, our technique seems to be more precise and comprehensive.

2) The smallest size of lifting degrees found in [7] for a $(3, 7)$-regular QC-LDPC code and a $(3, 8)$-regular QC-LDPC code with girth 10 are 159 and 219, respectively. Whereas, applying difference matrices results in a $(3, 7)$-regular QC-LDPC code and a $(3, 8)$-regular QC-LDPC code with girth 10 and smaller lifting degrees. In these cases lifting degrees are 145 and 211, respectively.

3) The analytical lower bound on the lifting degree of (m, n)-regular QC-LDPC codes with girth 10 proposed in [12] is $n(n-1)(m-1)+1$. Applying our proposed method, we demonstrate that $N \geq \binom{m}{2}n(n-1)+1$ which is $\frac{m}{2}$ times as many as the existing one. Moreover, numerical results reported in [11] for the lifting degrees of $(3, n)$-regular QC-LDPC codes with girth 10 and $n = 4, 5, 6$ show the tightness of our proposed lower bound.

We also consider all conditions for difference matrices to obtain (m, n)-regular QC-LDPC codes with girth 12.

For the first time, a lower bound on the lifting degree of (m, n)-regular QC-LDPC codes with girth 12 is presented. We prove that if $\mathcal{A}$ is a set consisting of the values obtained from the left side of the equation in Fossorier's Lemma to avoid 6-cycle, then $N \geq \mathcal{A} + \binom{m}{2}n(n-1)+1$.

The rest of the paper is organized as follows. Section II presents some basic notations. Section III includes four subsections for QC-LDPC codes with girths 6, 8, 10 and 12. In the last section we summarize our results.

II. PRELIMINARIES

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

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

If the ij-th element of the matrix, B, is an integer number, then it is substituted by an $N \times N$ matrix $I^{b_{ij}}$. This matrix is a circulant permutation matrix (CPM) in which the single 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 the circulant permutation matrix 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 provides us with a QC-LDPC code.

The necessary and sufficient condition for the existence of cycles of the length $2k$ in the Tanner graph of QC-LDPC codes was provided in [3]. This well-known result is our principle tool and we summarize it as follows. If

$$\sum_{i=0}^{k-1}(b_{m_in_i} - b_{m_in_{i+1}}) = 0 \mod N, \quad (2)$$

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 the length $2k$. According to [18], if the girth of Tanner graph is g, then the necessary and sufficient condition for the existence of $2k$-cycles in Equation (2) satisfies for $g \leq 2k \leq 2g-2$. Moreover, Equation (2) proves that the cycle distribution of a code is fully described by its exponent matrix and lifting degree. If the goal is to find a QC-LDPC code with girth, g, and the lifting degree, N, from the exponent matrix, B, one will have to be able to find the elements $b_{ij} \in \{0, \ldots, N-1\}$ such that Equation (2) are avoided for values of $k < \frac{g}{2}$.

To consider the existence of 4-cycles, 2×2 submatrices of the exponent matrix have to be investigated. For 6-cycles, 3×3 submatrices of the exponent matrix are considered. But, computing Equation (2) is time-consuming especially when $2k$ is more than 6. For example, in order to investigate the existence or non-existence of 8-cycles we have to consider all submatrices with sizes $2 \times 2, 2 \times 3, 2 \times 4, 3 \times 2, 3 \times 3, 3 \times 4, 4 \times 2, 4 \times 3$ and 4×4. In this paper, our goal is to reduce the number of inequalities that have to be tested for each exponent matrix to ensure that cycles with the size smaller than the girth do not exist. For example, we prove that in order to construct an exponent matrix with girth 10 we do not need to investigate the mentioned submatrices of the exponent matrix. To reach our goal we define matrices named as "difference matrices" which are denoted by D and DD.

III. DIFFERENCE MATRICES OF QC-LDPC CODES WITH DIFFERENT GIRTHS

Equation (2) is applicable to the exponent matrix. In this section, we obtain an equivalence of Equation (2) which is applicable to difference matrices D and/or DD for cycles of the length $2k$, especially for cycles of lengths 4, 6, 8 and 10. We also provide lower bounds on the lifting degree, where the Tanner graph is free of 8-cycles or 10-cycles. Moreover, we compare the complexity of the search algorithm between the application of Equation (2) to the exponent matrix, B, and using the difference matrices, D and DD. In the following, we explain how to construct two difference matrices.

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

$$D = \begin{bmatrix} b_{00} - b_{10} & \dots & b_{0(n-1)} - b_{1(n-1)} \\ \vdots & \ddots & \vdots \\ b_{00} - b_{(m-1)0} & \dots & b_{0(n-1)} - b_{(m-1)(n-1)} \\ b_{10} - b_{20} & \dots & b_{1(n-1) - b_{2(n-1)}} \\ \vdots & \ddots & \vdots \\ b_{10} - b_{(m-1)0} & \dots & b_{1(n-1)} - b_{(m-1)(n-1)} \\ \vdots & \ddots & \vdots \\ b_{(m-2)0} - b_{(m-1)0} & \dots & b_{(m-2)(n-1)} - b_{(m-1)(n-1)} \end{bmatrix}. \tag{3}$$

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

We also utilize another matrix to reduce the complexity. It is obtained from D which we denote it by DD.

Definition 2: Suppose D is a $\binom{m}{2} \times n$ difference matrix obtained from an $m \times n$ exponent matrix. A $\binom{m}{2} \times \binom{n}{2}$ difference matrix DD is constructed by subtracting every two columns of D as follows. Suppose D_{ij} and $D_{ij'}$ are two elements of the difference matrix, D, which occur in the same row, i, and disjoint columns, j and j', respectively, where $j < j'$. If we subtract j'-th column of D from j-th column of D, then $(D_{ij} - D_{ij'}, D_{ij'} - D_{ij}) \mod N$ is defined as an element of the i-th row and l-th column of DD, where $0 \leq l \leq \binom{n}{2} - 1$.

Example 1: Let B be a 3×4 exponent matrix with the lifting degree $N = 37$ as follows:

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 24 \\ 0 & 27 & 7 & 19 \end{bmatrix}. \tag{4}$$

According to Definitions 1 and 2 we construct two difference matrices D and DD:

$$D = \begin{bmatrix} 0 & -1 & -3 & -24 \\ 0 & -27 & -7 & -19 \\ 0 & -26 & -4 & 5 \end{bmatrix}, \tag{5}$$

$$DD = \begin{bmatrix} (1,36) & (3,34) & (24,13) & (2,35) & (23,14) & (21,16) \\ (27,10) & (7,30) & (19,18) & (17,20) & (29,8) & (12,25) \\ (26,11) & (4,33) & (32,5) & (15,22) & (6,31) & (28,9) \end{bmatrix}. \tag{6}$$

A. 4-CYCLES

In order to consider 4-cycles, Equation (2) has to be investigated for every 2×2 submatrix of the exponent matrix. Consider a 2×2 submatrix of the exponent matrix in two rows i_1 and i_2 and two columns j_1 and j_2. If the submatrix leads to 4-cycles in the Tanner graph, then Equation (2) gives $(b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_1}) = 0 \mod N$. But, in order to consider 4-cycles using the difference matrix, D, we rearrange the left side of the equality as follows:

$$(b_{i_1j_1} - b_{i_2j_1}) - (b_{i_1j_2} - b_{i_2j_2}) = 0 \mod N.$$

Proposition 1: A Tanner graph is 4-cycle free if and only if each row of the difference matrix, D, is free of repeated elements.

Proof: Given $0 \leq i_1, i_2 \leq m-1$ $(i_1 < i_2)$. The expression $(b_{i_1j_1} - b_{i_2j_1})$ is an element of D in the i-th row and the j_1-th column, where $i = \binom{m}{2} - \binom{m-i_1}{2} + i_2 - i_1$, and $(b_{i_1j_2} - b_{i_2j_2})$ is another element of D in the i-th row and the j_2-th column. So, we conclude that if $b_{i_1j_1} - b_{i_2j_1} = b_{i_1j_2} - b_{i_2j_2} \mod N$, then the Tanner graph has 4-cycles. □

Corollary 1: A Tanner graph is 4-cycle free if and only if the difference matrix, DD, has no zero element.

Let B_1 and B_2 be two exponent matrices with the same lifting degree. B_1 and B_2 are non-isomorphic if there is no permutation between entries of B_1 and entries of B_2. In [11] all possible non-isomorphic $(3, n)$-regular QC-LDPC codes with girth 6 for $4 \leq n \leq 12$ along with their minimum distances were represented. In order to extend the results we use difference matrices and provide the number of non-isomorphic (or simply NI numbers) $(4, n)$-regular QC-LDPC codes with girth 6 for $5 \leq n \leq 11$. We present one exponent matrix for each of the existing minimum distances in Tables 1 and 2. The first row and the first column of the exponent matrices are all-zero and are omitted.

B. 6-CYCLES

In this subsection we first consider 6-cycles for three types of exponent matrices with column weights 3, 4 and 5. We provide a substitution of the left side of Equation (2) with expressions whose elements belong to the difference matrix, D. Afterwards, we extend the results to $m \times n$ exponent matrices.

Suppose B has three rows. We should investigate Equation (2) for each three columns of B. Let B' be a 3×3 submatrix of the exponent matrix. According to Definition 1, we obtain a 3×3 matrix D' which is a submatrix of the difference matrix D.

$$B' = \begin{bmatrix} b_{i_0j_0} & b_{i_0j_1} & b_{i_0j_2} \\ b_{i_1j_0} & b_{i_1j_1} & b_{i_1j_2} \\ b_{i_2j_0} & b_{i_2j_1} & b_{i_2j_2} \end{bmatrix}, \tag{7}$$

$$D' = \begin{bmatrix} b_{i_0j_0} - b_{i_1j_0} & b_{i_0j_1} - b_{i_1j_1} & b_{i_0j_2} - b_{i_1j_2} \\ b_{i_0j_0} - b_{i_2j_0} & b_{i_0j_1} - b_{i_2j_1} & b_{i_0j_2} - b_{i_2j_2} \\ b_{i_1j_0} - b_{i_2j_0} & b_{i_1j_1} - b_{i_2j_1} & b_{i_1j_2} - b_{i_2j_2} \end{bmatrix} \tag{8}$$

The left side of the following equalities demonstrate the left side of Equation (2) for 6-cycles. We rearrange terms of each expression in the left to obtain the expressions in the right whose terms belong to the difference matrix, D.

- $b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_0} = (b_{i_0j_0} - b_{i_2j_0}) - (b_{i_0j_1} - b_{i_1j_1}) - (b_{i_1j_2} - b_{i_2j_2})$
- $b_{i_0j_1} - b_{i_0j_0} + b_{i_1j_0} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_1} = -(b_{i_0j_0} - b_{i_1j_0}) + (b_{i_0j_1} - b_{i_2j_1}) - (b_{i_1j_2} - b_{i_2j_2})$
- $b_{i_0j_0} - b_{i_0j_2} + b_{i_1j_2} - b_{i_1j_1} + b_{i_2j_1} - b_{i_2j_0} = (b_{i_0j_0} - b_{i_2j_0}) - (b_{i_1j_1} - b_{i_2j_1}) - (b_{i_0j_2} - b_{i_1j_2})$
- $b_{i_0j_2} - b_{i_0j_0} + b_{i_1j_0} - b_{i_1j_1} + b_{i_2j_1} - b_{i_2j_2} = -(b_{i_0j_0} - b_{i_1j_0}) - (b_{i_1j_1} - b_{i_2j_1}) + (b_{i_0j_2} - b_{i_2j_2})$
- $b_{i_0j_1} - b_{i_0j_2} + b_{i_1j_2} - b_{i_1j_0} + b_{i_2j_0} - b_{i_2j_1} = -(b_{i_1j_0} - b_{i_2j_0}) + (b_{i_0j_1} - b_{i_2j_1}) - (b_{i_0j_2} - b_{i_1j_2})$

- $b_{i_0j_2} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_0} + b_{i_2j_0} - b_{i_2j_2} = -(b_{i_1j_0} - b_{i_2j_0}) - (b_{i_0j_1} - b_{i_1j_1}) + (b_{i_0j_2} - b_{i_2j_2})$.

As we see, each expression in the right side of the above equalities includes three elements of a distributed diagonal of D'. In these expressions the elements in the first and the third rows are multiplied by -1. So we proved the following lemma.

Lemma 1: 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 $-D_{0j_0} + D_{1j_1} - D_{2j_2} \neq 0 \mod N$ for all $j_0 \neq j_1, j_0 \neq j_2, j_1 \neq j_2$ $(j_0, j_1, j_2 \in \{0, 1, \ldots, (n-1)\})$.

Now, we consider 6-cycles in a $4 \times n$ exponent matrix. Take a 4×3 submatrix of B and its corresponding submatrix of D as follows:

$$B' = \begin{bmatrix} b_{i_0j_0} & b_{i_0j_1} & b_{i_0j_2} \\ b_{i_1j_0} & b_{i_1j_1} & b_{i_1j_2} \\ b_{i_2j_0} & b_{i_2j_1} & b_{i_2j_2} \\ b_{i_3j_0} & b_{i_3j_1} & b_{i_3j_2} \end{bmatrix}, \tag{9}$$

$$D' = \begin{bmatrix} b_{i_0j_0} - b_{i_1j_0} & b_{i_0j_1} - b_{i_1j_1} & b_{i_0j_2} - b_{i_1j_2} \\ b_{i_0j_0} - b_{i_2j_0} & b_{i_0j_1} - b_{i_2j_1} & b_{i_0j_2} - b_{i_2j_2} \\ b_{i_0j_0} - b_{i_3j_0} & b_{i_0j_1} - b_{i_3j_1} & b_{i_0j_2} - b_{i_3j_2} \\ b_{i_1j_0} - b_{i_2j_0} & b_{i_1j_1} - b_{i_2j_1} & b_{i_1j_2} - b_{i_2j_2} \\ b_{i_1j_0} - b_{i_3j_0} & b_{i_1j_1} - b_{i_3j_1} & b_{i_1j_2} - b_{i_3j_2} \\ b_{i_2j_0} - b_{i_3j_0} & b_{i_2j_1} - b_{i_3j_1} & b_{i_2j_2} - b_{i_3j_2} \end{bmatrix}. \tag{10}$$

The matrix B' contains four 3×3 submatrices. Suppose the first three rows are chosen to apply Equation (2) in order to avoid 6-cycles. If we rearrange the elements of the left side of Equation (2) to obtain expressions whose terms belong to the difference matrix, D, then the obtained equalities are as the same as 6 equalities mentioned above. The right side of the first equality and the matrix D' imply the equality $-(b_{i_0j_1} - b_{i_1j_1}) + (b_{i_0j_0} - b_{i_2j_0}) - (b_{i_1j_2} - b_{i_2j_2}) = -D'_{0j_1} + D'_{1j_0} - D'_{3j_2}$. Investigating four 3×3 submatrices results in the following lemma.

Lemma 2: Let D be a difference matrix corresponding to a $4 \times n$ exponent matrix, B. The Tanner graph is 6-cycle free if and only if for all $j_0 \neq j_1, j_0 \neq j_2, j_1 \neq j_2$ $(j_0, j_1, j_2 \in \{0, 1, \ldots, (n-1)\})$ we have:

$$\begin{aligned} &1)\ -D_{0j_0}+D_{1j_1}-D_{3j_2} \neq 0 \quad 2)\ -D_{0j_0}+D_{2j_1}-D_{4j_2} \neq 0 \\ &3)\ -D_{1j_0}+D_{2j_1}-D_{5j_2} \neq 0 \quad 4)\ -D_{3j_0}+D_{4j_1}-D_{5j_2} \neq 0. \end{aligned} \tag{11}$$

All inequalities are computed in modulo N.

Similarly, we consider all 3×3 submatrices of the difference matrix corresponding to a $5 \times n$ exponent matrix. The results are presented in the following lemma.

Lemma 3: Let D be a difference matrix corresponding to a $5 \times n$ exponent matrix, B. The Tanner graph is 6-cycle free if and only if for all $j_0 \neq j_1, j_0 \neq j_2, j_1 \neq j_2$ $(j_0, j_1, j_2 \in \{0, 1, \ldots, (n-1)\})$ we have:

$$\begin{aligned} &1)\ -D_{0j_0}+D_{1j_1}-D_{4j_2} \neq 0 \quad 2)\ -D_{0j_0}+D_{2j_1}-D_{5j_2} \neq 0 \\ &3)\ -D_{0j_0}+D_{3j_1}-D_{6j_2} \neq 0 \quad 4)\ -D_{1j_0}+D_{2j_1}-D_{7j_2} \neq 0 \\ &5)\ -D_{1j_0}+D_{3j_1}-D_{8j_2} \neq 0 \quad 6)\ -D_{2j_0}+D_{3j_1}-D_{9j_2} \neq 0 \\ &7)\ -D_{4j_0}+D_{5j_1}-D_{7j_2} \neq 0 \quad 8)\ -D_{4j_0}+D_{6j_1}-D_{8j_2} \neq 0 \\ &9)\ -D_{5j_0}+D_{6j_1}-D_{9j_2} \neq 0 \quad 10)\ -D_{7j_0}+D_{8j_1}-D_{9j_2} \neq 0. \end{aligned} \tag{12}$$

All inequalities are computed in modulo N.

As we see in lemmas 2 and 3, the row indices of 3×3 submatrices of D which have to be tested to avoid 6-cycles in a $4 \times n$ exponent matrix are completely different from those in a $5 \times n$ exponent matrix. Let a triple (i, j, k), where $i, j, k \in \{0, 1, \ldots, \binom{m}{2} - 1\}$, characterize a submatrix of the difference matrix, D, with row indices i, j, k, which have to be tested to avoid 6-cycles. For example, as mentioned in lemmas 2 and 3, triples for exponent matrices with four rows are (0,1,3), (0,2,4), (1,2,5) and (3,4,5). And triples for exponent matrices with five rows are (0,1,4), (0,2,5), (0,3,6), (1,2,7), (1,3,8), (2,3,9), (4,5,7), (4,6,8), (5,6,9) and (7,8,9). Generally, to obtain an (m, n)-regular QC-LDPC code with girth 8 using difference matrix, D, it is important to determine all (i, j, k) triples in order to investigate 3×3 submatrices of the difference matrix, D, with row indices i, j, k to avoid 6-cycles. In the following, we explain how we recognize such triples.

Let D be a difference matrix corresponding to an $m \times n$ exponent matrix, B. The application of Equation (2) to a 3×3 submatrix of B to avoid 6-cycles implies that two elements of each row and each column of the submatrix occur in the left side of Equation (2). So, there are two elements with a row index i, two elements with a row index i' and two elements with a row index i''. Suppose one of the two terms $(b_{ij} - b_{i'j})$ and $-(b_{ij} - b_{i'j})$ and one of the two terms $(b_{ij'} - b_{i''j'})$ and $-(b_{ij'} - b_{i''j'})$ appear in Equation (2). If they occur in the i_1-th row and the i_2-th row of D, respectively, then the third row is the one which includes $(b_{i'j''} - b_{i''j''})$ or $-(b_{i'j''} - b_{i''j''})$. If it appears in the i_3-th row of D, then the corresponding triple is (i_1, i_2, i_3).

The application of Equation(2) to $3 \times n$ exponent matrices whose first row and first column are all-zero to avoid 6-cycles were simplified into three types of inequalities in [11]. In the following lemma we demonstrate that using the difference matrix, DD, it is sufficient to investigate just one type. Moreover, this type can be utilized for all $m \times n$ exponent matrices whose first row and first column are all-zero.

Lemma 4: Let DD be a difference matrix corresponding to an $m \times n$ exponent matrix, B. Take DD_{ij} and $N - DD_{ij}$ as the first and the second components of the ij-th element of DD, respectively. If the Tanner graph is 6-cycle free, then the submatrix of DD corresponding to 3×3 submatrix of B whose first row is all-zero fulfills the following inequalities:

$$\begin{aligned} &1)\ DD_{ij_0} \neq DD_{i'j_1} \quad 2)\ DD_{ij_0} \neq N - DD_{i'j_2} \\ &3)\ DD_{ij_1} \neq DD_{i'j_2} \quad 4)\ DD_{ij_1} \neq DD_{i'j_0} \\ &5)\ DD_{ij_2} \neq N - DD_{i'j_0} \quad 6)\ DD_{ij_2} \neq DD_{i'j_1}, \end{aligned} \tag{13}$$

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

Suppose the first row and the first column of the exponent matrix are all-zero. Lemma 4 is applicable to 3×3 submatrices of the difference matrix, DD, in which two row indices belong to $\{0, \dots, m-2\}$ or equivalently, it is applicable to (i, j, k) triples which i, j belong to $\{0, \dots, m-2\}$. Therefore, for a $3 \times n$ exponent matrix whose first row and first column are all-zero we consider the inequalities of Lemma 4 to avoid 6-cycles instead of applying Equation (2) or testing the inequality of Lemma 1. As mentioned above, (i, j, k) triples to avoid 6-cycles in a $4 \times n$ exponent matrix are (0,1,3), (0,2,4), (1,2,5) and (3,4,5) which have to be tested by inequalities 1, 2, 3 and 4 of Lemma 2, respectively. The first three triples contain two elements of $\{0, 1, 2\}$. Therefore, to investigate 6-cycles in a $4 \times n$ exponent matrix whose first row and first column are all-zero we prefer using Lemma 4 to testing inequalities 1, 2 and 3 of Lemma 2. Hence, in order to construct a $(4, n)$-regular QC-LDPC code which is free of 6-cycles, there are two types of inequalities which have to be tested to avoid 6-cycles. First type is the application of Lemma 4 to triples (0,1,3), (0,2,4) and (1,2,5). The second type is $-D_{4j_1} + D_{5j_2} - D_{6j_3} \neq 0$. In addition, for a $5 \times n$ exponent matrix, inequalities 1 to 6 in Lemma 3 are investigated by the difference matrix, DD. So just the last four inequalities in Lemma 3 are considered by the difference matrix, D. Besides decreasing the complexity of the search algorithm, Lemma 4 has significant contribution which we will see in finding exponent matrices with girth 10. This merit will be proposed in the next subsection.

C. 8-CYCLES

The number of different types of submatrices that need to be tested in order to obtain a QC-LDPC code avoiding 8-cycles is nine. The mentioned submatrices have sizes 2×2, 2×3, 2×4, 3×2, 3×3, 3×4, 4×2, 4×3 and 4×4. Using two matrices D and DD we present a method to obtain an exponent matrix with girth 10. Our proposed method reduces the complexity of the search algorithm. The reason behind this fact is that by applying our method to avoid 8-cycles we do not need to investigate Equation (2) for the mentioned submatrices. More importantly, if the first row and the first column of the exponent matrix are all-zero, then our method proves that the non-existence of 8-cycles guarantees the non-existence of some 6-cycles too. So, to avoid 6-cycles we do not need to test 3×3 submatrices whose first rows are all-zero. In this subsection we also provide a lower bound on the lifting degree of QC-LDPC codes whose Tanner graphs have girth at least 10. We prove that the lower bound on the lifting degree of QC-LDPC codes with girth 10 is $2\binom{n}{2}\binom{m}{2}+1$. In the following lemma we provide our principle tool to consider 8-cycles.

Lemma 5: If the left side of Equation (2) to consider an 8-cycle contains more than two elements of a column of the exponent matrix, then the elements which occur in the expression can be taken as elements which appear in two 2×2 submatrices of the exponent matrix.

Proof: We investigate one type of submatrices which satisfies the condition of Lemma, others are alike and are omitted. Suppose we apply Equation (2) on a 4×3 submatrix of the exponent matrix. Let the left side of the equality be

$$b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_1} + b_{i_3j_1} - b_{i_3j_0} \qquad (14)$$

whose elements are in the following matrix,

$$B' = \begin{bmatrix} b_{i_0j_0} & b_{i_0j_1} & * \\ * & b_{i_1j_1} & b_{i_1j_2} \\ * & b_{i_2j_1} & b_{i_2j_2} \\ b_{i_3j_0} & b_{i_3j_1} & * \end{bmatrix}.$$

The terms of the expression can be located in the following two 2×2 submatrices:

$$B' = \begin{bmatrix} b_{i_0j_0} & b_{i_0j_1} \\ b_{i_3j_0} & b_{i_3j_1} \end{bmatrix} \quad \text{and } B'' = \begin{bmatrix} b_{i_1j_1} & b_{i_1j_2} \\ b_{i_2j_1} & b_{i_2j_2} \end{bmatrix}.$$

□

The benefit of Lemma 5 is that we can obtain an equivalence for Equation (2) whose terms belong to two rows of the difference matrix, D. Whereas, the left side of Equation (2) can be rearranged in a way that more than two rows of the difference matrix are involved. For example,

$$\begin{aligned} & b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_1} + b_{i_3j_1} - b_{i_3j_0} \\ & = b_{i_0j_0} - b_{i_3j_0} - (b_{i_0j_1} - b_{i_1j_1}) - (b_{i_1j_2} - b_{i_2j_2}) - (b_{i_2j_1} - b_{i_3j_1}) \\ & = D_{i'j_0} - D_{ij_1} - D_{i''j_2} - D_{i'''j_1} \qquad (15) \end{aligned}$$

which contains four rows of the difference matrix, where $i < i' < i'' < i'''$.

In the following theorem we clarify the merit of using the difference matrix, DD, to obtain QC-LDPC codes avoiding 8-cycles. The proof of the theorem is provided in Appendix A.

Theorem 1: A QC-LDPC code has no 8-cycles if:

- (i) the matrix obtained by multiplying the difference matrix, DD, by 2 (or simply $2DD$) has no zero element,
- (ii) the matrix DD has no repeated elements and
- (iii) for each 4×4 submatrix of the exponent matrix, B, the left side of Equation (2) is non-zero.

According to Theorem 1, if we use the matrix DD, then we do not need to consider all submatrices with sizes 2×3, 2×4, 3×2, 3×3, 3×4, 4×2 and 4×3, instead, we consider the non-existence of repeated elements in the matrix, DD, and the zero element in the matrix, $2DD$.

Example 2: Suppose B is the 3×4 exponent matrix given in Example 1. As $N = 37$ is an odd number, for the ij-th element of $2DD$ we have $2DD_{ij} \neq 0 \mod N$. So, B fulfills the first condition of Theorem 1. As we see, in this case no computation is required. By comparing each two elements of the matrix, DD, we conclude that there are no repeated elements in DD. Hence, B holds in the second condition of Theorem 1. Moreover, the last condition of Theorem 1 is applicable to exponent matrices with at least four rows. So, Theorem 1 part (iii) is not considered for the given exponent matrix. According to Theorem 1 we conclude that the Tanner graph corresponding to the given exponent matrix is 8-cycle free.

TABLE 3. The number of operations of Equation (2) to avoid 8-cycles and the number of operations of Theorem 1 to consider 8-cycles in (m, n)-regular QC-LDPC codes whose column weight values are $m = 3, 4, 5, 6$.

	Equation (2)	Theorem 1 when N is odd	Theorem 1 when N is odd
$m=3$	$9(6\binom{n}{2}+27\binom{n}{3}+24\binom{n}{4})$	$3n+9\binom{n}{2}+\binom{3\binom{n}{2}}{2}$	$3n+15\binom{n}{2}+\binom{3\binom{n}{2}}{2}$
$m=4$	$9(24\binom{n}{2}+102\binom{n}{3}+68\binom{n}{4})$	$6n+18\binom{n}{2}+\binom{3n(n-1)}{2}+5\binom{n}{4}$	$6n+18\binom{n}{2}+\binom{3n(n-1)}{2}+5\binom{n}{4}$
$m=5$	$9(70\binom{n}{2}+270\binom{n}{3}+160\binom{n}{4})$	$10n+30\binom{n}{2}+\binom{5n(n-1)}{2}+25\binom{n}{4}$	$10n+50\binom{n}{2}+\binom{5n(n-1)}{2}+25\binom{n}{4}$
$m=6$	$9(165\binom{n}{2}+585\binom{n}{3}+330\binom{n}{4})$	$15n+45\binom{n}{2}+\binom{15\binom{n}{2}}{2}+75\binom{n}{4}$	$15n+45\binom{n}{2}+\binom{75\binom{n}{2}}{2}+75\binom{n}{4}$

TABLE 4. Comparison of the number of operations between applying Fossorier's Lemma on the exponent matrix and using difference matrices.

	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$	$n=9$	$n=10$	$n=11$	$n=12$
$m=3$, Equation (3)	1770	4620	9975	18984	33012	53640	82665	122100	174174
$m=3$, difference matrices	273	570	1278	2226	4014	6237	9885	14223	20727
$m=4$, Equation (3)	-	16380	34590	64596	110544	177192	269910	394680	558096
$m=4$, difference matrices	-	2245	5046	9310	16610	26568	41655	60951	88017

If all submatrices with sizes $2\times 2, 2\times 3, 2\times 4, 3\times 2, 3\times 3$ and 3×4 were considered, then 168 inequalities had to be investigated to avoid 8-cycles.

In appendix A, we present the number of inequalities which have to be tested to avoid 8-cycles when we apply Equation (2) in the exponent matrix. Moreover, in Table 3 we provide the number of operations in the application of Equation (2) to avoid 8-cycles and the number of operations to check conditions of Theorem 1 to avoid 8-cycles in (m, n)-regular QC-LDPC codes with the column weight $m = 3, 4, 5, 6$. In the following corollary we present the comparison for all values of m and n.

Corollary 2: Let B be an exponent matrix whose Tanner graph is 4-cycle free. The number of operations required to obtain a QC-LDPC code whose Tanner graph is 8-cycle free using Equation (2) is

$$9\binom{n}{2}\binom{m}{2}(\binom{n-2}{2}(\frac{2}{9}\binom{m-2}{2}+3m-4) + \binom{n-2}{1}(\frac{2}{3}\binom{m-2}{2}+2m-3)+m). \quad (16)$$

If we utilize the matrix DD, then the number of operations is

$$\begin{cases} n\binom{m}{2}+3\binom{n}{2}\binom{m}{2}+\binom{\binom{n}{2}\binom{m}{2}}{2}+5\binom{n}{4}\binom{m}{4}, & N \text{ is odd}, \\ n\binom{m}{2}+5\binom{n}{2}\binom{m}{2}+\binom{\binom{n}{2}\binom{m}{2}}{2}+5\binom{n}{4}\binom{m}{4}, & N \text{ is even}. \end{cases} \quad (17)$$

Note that in Corollary 2 the number of operations to construct the matrices D and DD are also taken into account, which are $n\binom{m}{2}$ and $3\binom{n}{2}\binom{m}{2}$, respectively. Moreover, in order to ensure the non-existence of repeated elements in DD, it is sufficient to consider the smaller element of each pair in DD. If they provide a subset of $\{1, 2, \ldots, [\frac{N}{2}]\}$ with the cardinality $\binom{n}{2}\binom{m}{2}$, then the exponent matrix satisfies in the second condition of Theorem 1. The number of operations in this case is $\binom{\binom{n}{2}\binom{m}{2}}{2}$. More importantly, in the following, we demonstrate other benefit of using difference matrices to obtain regular QC-LDPC codes.

Corollary 3: Suppose B is a $3\times n$ exponent matrix. If the first row and the first column of B are all-zero and difference matrix, DD, fulfills Theorem 1, then the Tanner graph is 6-cycle free.

Proof: According to Theorem 1, the difference matrix, DD, has no repeated elements. Therefore, all inequalities in Lemma 4 occur and the Tanner graph is free of 6-cycles. □

Using the above discussions, we propose our method to construct $3\times n$ exponent matrices with girth 10 whose first column and first row are all-zero. In this method, no submatrix of the exponent matrix needs to be tested to avoid cycles with the size less than 10. In fact, we search for an exponent matrix with girth 10 and lifting degree N whose difference matrix, DD, contains disjoint non-zero elements and $2DD \neq 0 \mod N$. If difference matrix, DD, is free of repeated elements and $2DD \neq 0 \mod N$, then according to Theorem 1 the Tanner graph is 8-cycle free. Corollary 3 implies that the Tanner graph has no 6-cycles and since DD has no zero element, Corollary 1 indicates that the Tanner graph is 4-cycle free. We generalize the corollary for all $m\times n$ exponent matrices whose first row and first column are all-zero.

Corollary 4: Suppose B is an $m\times n$ exponent matrix. If the first row and the first column of B are all-zero and difference matrix, DD, fulfills the conditions of Theorem 1, then to avoid 6-cycles we do not need to apply Equation (2) in 3×3 exponent matrices whose first row is all-zero.

In Table 4, we compare the number of operations to obtain an $m\times n$ exponent matrix with girth 10, $m = 3, 4$ and $n \leq 12$ between two cases. For the first case we use Equation (2) and for the second case we use the matrices, D and DD.

As we see, the number of operations when we use the difference matrices is much less than the number of operations when we apply Equation (2). Moreover, our technique seems to be more precise and exhaustive since the number of non-isomorphic $(3, 5)$-regular QC-LDPC codes with girth 10 reported in [11] is 3 whereas we show that there are 4 non-isomorphic $(3, 5)$-regular QC-LDPC codes with girth 10. This also happens for the number of non-isomorphic

TABLE 5. All non-isomorphic (3, n) QC-LDPC codes with girth 10 and $n = 4, 5, 6$. and an obtained exponent matrix with girth 10 for $n = 7, 8$. Minimum lifting degrees obtained in the literature for these two cases are $N = 159, 219$, respectively. (Codes non-isomorphic to those of [11] are shown as matrices).

$n,\ N$	*New exponent matrices*	*Isomorph with* [11]	*Isomorph with* [11]	*Isomorph with* [11]
$n = 4, N = 37$		$\begin{matrix} 1 & 3 & 24 \\ 11 & 33 & 5 \end{matrix}$		
$n = 5, N = 61$	$\begin{bmatrix} 1 & 4 & 11 & 27 \\ 14 & 56 & 32 & 12 \end{bmatrix}$	$\begin{matrix} 1 & 3 & 21 & 55 \\ 5 & 15 & 44 & 31 \end{matrix}$	$\begin{matrix} 1 & 3 & 21 & 55 \\ 14 & 42 & 50 & 38 \end{matrix}$	$\begin{matrix} 1 & 4 & 28 & 44 \\ 14 & 56 & 26 & 6 \end{matrix}$
$n = 6, N = 91$	$\begin{bmatrix} 1 & 6 & 28 & 40 & 48 \\ 10 & 60 & 7 & 36 & 25 \end{bmatrix}$	$\begin{matrix} 1 & 3 & 7 & 25 & 38 \\ 17 & 51 & 28 & 61 & 9 \end{matrix}$		
$n = 7, N = 145$	$\begin{matrix} 1 & 6 & 44 & 71 & 92 & 122 \\ 4 & 20 & 108 & 83 & 123 & 76 \end{matrix}$			
$n = 8, N = 211$	$\begin{matrix} 1 & 5 & 12 & 39 & 56 & 183 & 192 \\ 3 & 13 & 92 & 188 & 106 & 74 & 151 \end{matrix}$			

(3, 6)-regular QC-LDPC codes with girth 10. Furthermore, using difference matrices results in a 3 × 7 exponent matrix and a 3 × 8 exponent matrix with girth 10 and lifting degrees $N = 145$ and 211, respectively, while the existing lower bound on N reported in the literature are 159 and 219, respectively.

In addition to reduce the size of the search space, Theorem 1 provides us with a chance to obtain a lower bound on the lifting degree of QC-LDPC codes with girth 10.

Theorem 2: The lifting degree of an (m, n)-regular QC-LDPC code with girth 10 is at least $2\binom{n}{2}\binom{m}{2} + 1$.

Proof: Since the Tanner graphs of (m, n)-regular QC-LDPC codes with girth 10 are 8-cycle free, from the second condition of Theorem 1, the difference matrix, DD, has no repeated elements. So, the matrix DD contains $\binom{m}{2}n(n-1)$ disjoint elements. As a result, we have $N \geq 2\binom{n}{2}\binom{m}{2} + 1$. □

The minimum lifting degrees of (3,n)-regular QC-LDPC codes with $n = 4, 5, 6$ acknowledge our proposed lower bound. They are $N = 37, 61$ and 91, respectively. So our proposed lower bound is tight.

Moreover, the existence and non-existence of repeated elements in the difference matrix, DD, can determine whether a structure gives a QC-LDPC code with girth 10 or not. In the following example, we demonstrate that the Tanner graph of QC-LDPC codes based on the symmetrical construction presented in [19] has 8-cycles.

Example 3: In [19] it is shown that if n is an even number, then an $m \times \frac{n}{2}$ exponent matrix, M, with girth at least 8, gives an $m \times n$ exponent matrix $B = [M\ -M]$ with girth at least 8. The first row of B is all-zero, if b_{ij} and $-b_{ij}$ are two elements of B, then $(-b_{ij}, b_{ij})$ and $(b_{ij}, -b_{ij})$ are two elements of DD. Therefore, DD has repeated elements and according to Theorem 1 the Tanner graph corresponding to the exponent matrix, B, has 8-cycles.

D. 10-CYCLES

The number of different types of submatrices that have to be tested to obtain a QC-LDPC code avoiding 10-cycles is nine. These submatrices have at least three rows and three columns. Their sizes are 3 × 3, 3 × 4, 3 × 5, 4 × 3, 4 × 4, 4 × 5, 5 × 3, 5 × 4 and 5 × 5. In this case, we also use the difference matrices, D and DD instead of applying Equation (2) on the exponent matrix. In the following, we provide our principle tool to consider 10-cycles.

Lemma 6: If the left side of Equation (2) to consider a 10-cycle contains more than two elements of a column or a row of the exponent matrix, then its equivalent expression whose terms belong to the difference matrix, D, includes three terms occurring in three rows and three columns of D.

Proof: We prove Lemma for one type of submatrices of the exponent matrix which satisfies the condition of Lemma, others are alike and are omitted. Suppose we test a 3 × 5 submatrix to avoid 10-cycles. For example, let the left side of the equality be $b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_3} + b_{i_1j_3} - b_{i_1j_4} + b_{i_2j_4} - b_{i_2j_0}$ whose terms are located in the following matrix

$$B' = \begin{bmatrix} b_{i_0j_0} & b_{i_0j_1} & * & * & * \\ * & b_{i_1j_1} & b_{i_1j_2} & b_{i_1j_3} & b_{i_1j_4} \\ b_{i_2j_0} & * & b_{i_2j_2} & b_{i_2j_3} & b_{i_2j_4} \end{bmatrix}.$$

By rearranging the terms of this expression we conclude that 6 terms of the expression are related to 3 elements of the matrix, D, which occur in three rows and three columns of D. They are $(b_{i_0j_0} - b_{i_2j_0}) = D_{ij_0}$, $(b_{i_0j_1} - b_{i_1j_1}) = D_{i'j_1}$ and $(b_{i_1j_2} - b_{i_2j_2}) = D_{i''j_2}$. The other terms are $(b_{i_1j_3} - b_{i_2j_3})$ and $-(b_{i_1j_4} - b_{i_2j_4})$ whose equivalent elements in the matrix, D, are $D_{i''j_3}$ and $D_{i''j_4}$ and appear in a 2 × 2 submatrix of the matrix, B. □

The merit of Lemma 6 is that in the expression equivalent to Equation (2) whose terms belong to the difference matrix, D, three terms which occur in disjoint rows and columns of the difference matrix, D, have been once investigated in 6-cycle considerations. So, we can utilize our computations in 6-cycle considerations for investigating 10-cycles too.

In the following theorem we provide the necessary and sufficient conditions for a QC-LDPC code whose Tanner graph is free of 10-cycles. The proof is presented in Appendix B.

Theorem 3: A QC-LDPC code has no 10-cycles if and only if:

- (i) by choosing every three rows of the exponent matrix, their equivalent rows in the matrix, DD, have no intersections with the set consisting of the values obtained by the left side of Equation (2) in 6-cycle considerations,

- (*ii*) by choosing every three rows i, i', i'' and three columns j, j', j'' of the difference matrix, D, the set, X, consisting of expressions $-D_{ij} + D_{i'j'} - D_{i''j''}$ has no common elements with a set consisting of the elements occurring in the rows of the matrix, DD, which are different from three rows i, i', i''. In addition, there is no intersections between the set X and the values obtained by adding or subtracting every two elements on the distributed diagonals of 2×2 submatrices of D. (If we use the matrix D to consider 10-cycles, then each expression, which have to be tested to avoid 10-cycles, has five terms. Three terms occur in a 3×3 submatrix of D and two of them belong to the distributed diagonal of a 2×2 submatrices of D.) and
- (*iii*) for each 5×5 submatrix of the exponent matrix, B, the left side of Equation (3) is non-zero.

In Appendix B we compute the number of inequalities which have to be tested to avoid 10-cycles when we use Equation (2). The number of operations is eleven times as many as the number of inequalities. As we see, the submatrices with three rows are considered according to the first condition of Theorem 3, submatrices with four rows are investigated according to the second condition and there is no need to consider the submatrices of sizes 5×3 and 5×4 when the matrices D and DD are used.

Example 4: Suppose

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 13 \\ 0 & 9 & 27 & 44 \end{bmatrix}$$

is the exponent matrix of a (3, 4)-regular QC-LDPC code with the lifting degree $N = 73$.

The difference matrices D and DD are as follows:

$$D = \begin{bmatrix} 0 & -1 & -3 & -13 \\ 0 & -9 & -27 & -44 \\ 0 & -8 & -24 & -31 \end{bmatrix}, \tag{18}$$

$$DD = \begin{bmatrix} (1,72) & (3,70) & (13,60) & (2,71) & (12,61) & (10,63) \\ (9,64) & (27,46) & (44,29) & (18,55) & (35,38) & (17,56) \\ (8,65) & (24,49) & (31,42) & (16,57) & (23,50) & (7,66) \end{bmatrix}. \tag{19}$$

The set $\mathcal{A}$ consists of the left side of Equation (2) when we consider 6-cycles:

$$\mathcal{A} = \{4, 5, 11, 15, 21, 22, 25, 28, 30, 32, 34, 37, 40, 47, 53, 54, 59, 67\}.$$

All elements of the matrix, DD, are accumulated in the set $\mathcal{B}$,

$$\mathcal{B} = \{1, 2, 3, 7, 8, 9, 10, 12, 13, 16, 17, 18, 23, 24, 27, 29, 31, 35, 38, 42, 44, 46, 49, 50, 55, 56, 57, 60, 61, 63, 64, 65, 66, 70, 71, 72\}.$$

Since $\mathcal{A} \cap \mathcal{B} = \emptyset$, the first condition of Theorem 3 fulfills for the given exponent matrix. So, instead of testing Equation (2) on 3×3 and 3×4 submatrices to avoid 10-cycles, which results in testing 648 inequalities, we consider the non-existence of common values in two sets $\mathcal{A}$ and $\mathcal{B}$. Submatrices with four and five rows are required to consider 10-cycles in parts (*ii*) and (*iii*) of Theorem 3, respectively. So, for an exponent matrix with three rows the first part (*i*) is required to be checked, only. Hence, $\mathcal{A} \cap \mathcal{B} = \emptyset$ indicates that the Tanner graph is 10-cycle free.

Theorem 4: Suppose $\mathcal{A}$ is a set including all values obtained by the left side of Equation (2) when we consider 6-cycles and $\mathcal{B}$ contains all elements of the matrix DD. If the Tanner graph of a QC-LDPC code is 10-cycle free, then we have $\mathcal{A} \cap \mathcal{B} = \emptyset$.

Proof: As shown in Theorem 3, if i, i', i'' are three rows of DD corresponding to three rows of the exponent matrix which we test to avoid 6-cycles, then values obtained from the left side of Equation (2) to consider 6-cycles have no intersections with elements of three rows i, i', i'' of the matrix, DD. Moreover, the second part of Theorem 3 shows that these values have also no intersections with other rows of the matrix, DD. As a result, there are no common elements between two sets. □

Corollary 5: A lower bound on the lifting degree of an (m, n)-regular QC-LDPC code whose Tanner graph is 10-cycle free is at least $|\mathcal{A}| + \binom{m}{2} n(n-1) + 1$, where $\mathcal{A}$ is a set including all values obtained by the left side of Equation (2) when we consider 6-cycles

For instance, in Example 4 we have $|\mathcal{A}| = 18$ and $\binom{m}{2} n(n-1) + 1 = 37$ so, $N \geq 55$. Corollary 5 indicates that to obtain a regular QC-LDPC code whose Tanner graph is 10-cycle free the lower bound on the lifting degree can be guessed after applying Equation (2) to avoid 6-cycles.

IV. CONCLUSION

In this paper, we defined two matrices named as "difference matrices", denoted by D and DD which contribute to reduce the complexity of search algorithms to achieve a QC-LDPC code with the shortest length and the certain girth. More importantly, we provided the necessary and sufficient conditions for the difference matrices of a QC-LDPC code with different girths. We proved that the necessary condition to have an exponent matrix with girth 6 is that every row of the difference matrix, D, is free of repeated elements. Having this necessary condition in exponent matrices with the column weight 4 resulted in a range of QC-LDPC codes with the minimum lifting degree and girth 6. We presented a method to obtain an exponent matrix with girth 10 which reduces the complexity of the search algorithm. We demonstrated that if the first row and the first column of the exponent matrix are all-zero, then by applying our method we do not need to test Fossorier's Lemma to avoid 6-cycles and 8-cycles. Using difference matrices, we provided some numerical and analytical results which improved their counterparts in the literature. For example, we proved that the lower bound on the lifting degree of an (m, n)-regular QC-LDPC code with girth 10 is $N \geq \binom{m}{2} n(n-1) + 1$ which is tighter than the existing bound. For QC-LDPC codes with girth 12, for the first time, a lower bound on the lifting degree was proposed which is $N \geq |\mathcal{A}| + \binom{m}{2}n(n-1) + 1$, where $\mathcal{A}$ is a set of values obtained from the left side of equations of Fossorier's Lemma in 6-cycle considerations.

APPENDIX A

In this appendix we simultaneously prove Theorem 1 and compute the number of equations of Fossorier's Lemma for each type of submatrices to avoid 8-cycles.

Proof: We prove the theorem in three steps. For the first step, we consider submatrices with two rows and 2, 3 and 4 columns in three parts, as follows.

Case 1: Submatrices which include two rows of the exponent matrix. Suppose the row indices are i_0 and i_1.

1) Take j_0 and j_1 as two column indices of a 2×2 submatrix of B. The left side of Equation (2) is $b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_0} + b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_0} = 2(b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_0})$. By rearranging the terms of the equation we have $2((b_{i_0j_0} - b_{i_1j_0}) - (b_{i_0j_1} - i_1j_1)) = 2(D_{ij_0} - D_{ij_1})$, where $i \in \{0, 1, \ldots, \binom{m}{2} - 1\}$. So, in the difference matrix of 8-cycle free QC-LDPC codes we have $2(D_{ij_0} - D_{ij_1}) \neq 0$. Since $(D_{ij_0} - D_{ij_1})$ is a component of an element of the matrix, DD, in 8-cycle free QC-LDPC codes we have $2DD \neq 0$. So, the first condition of the theorem is proved. In this item if Equation (2) is used, then $\binom{m}{2}\binom{n}{2}$ inequalities have to be tested to avoid 8-cycles.
2) Take j_0, j_1, j_2 as three column indices of a 2×3 submatrix of B. The left side of Equation (2) and its corresponding expression whose elements belong to D are as follows:

$$\begin{aligned} &b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_2} + b_{i_0j_2} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_0} \\ &= (b_{i_0j_0} - b_{i_1j_0}) - (b_{i_0j_1} - b_{i_1j_1}) + (b_{i_0j_2} - b_{i_1j_2}) \\ &\quad - (b_{i_0j_1} - b_{i_1j_1}) = D_{ij_0} - D_{ij_1} + D_{ij_2} - D_{ij_1}. \end{aligned}$$

   So, the difference matrix of an 8-cycle free QC-LDPC code holds in the inequality $D_{ij_0} - D_{ij_1} + D_{ij_2} - D_{ij_1} \neq 0$ or equivalently, $D_{ij_0} - D_{ij_1} \neq D_{ij_1} - D_{ij_2}$. To obtain this inequality the 8-cycle is started from $b_{i_0j_0}$. If the cycle is started from $b_{i_0j_1}$, then we obtain one of the inequalities $D_{ij_0} - D_{ij_1} \neq -(D_{ij_0} - D_{ij_2})$ or $D_{ij_0} - D_{ij_2} \neq -(D_{ij_1} - D_{ij_2})$. Note that two sides of inequalities are components of two elements of the i-th row of the matrix DD. In this item if Equation (2) is used, then $3\binom{m}{2}\binom{n}{3}$ inequalities have to be tested to avoid 8-cycles.
3) Take j_0, j_1, j_2 and j_3 as four column indices of a 2×4 submatrix of B. Like the previous item by investigating Equation (2) and their equivalences in the difference matrix we conclude that the difference matrix of an 8-cycle free QC-LDPC code holds the inequality: $\pm(D_{ij_0} - D_{ij_1}) \neq \pm(D_{ij_2} - D_{ij_3})$. Note that two sides of inequalities are components of two elements of the i-th row of the matrix DD. If Equation (2) is used, then $6\binom{m}{2}\binom{n}{4}$ inequalities have to be investigated to avoid 8-cycles.

   The items 2 and 3 result in the existence of $2\binom{m}{2}$ disjoint elements for each row of DD. Suppose $(D_{ij} - D_{ij'}, D_{ij'} - D_{ij})$ and $(D_{ij} - D_{ij''}, D_{ij''} - D_{ij})$ are two elements of i-th row of DD. If they have elements in common, then one of the following equalities occurs which contradicts the assumption that the Tanner graph is 8-cycle free. The equalities are $D_{ij'} = D_{ij''}$ or $(D_{ij} - D_{ij'}) + D_{ij} - D_{ij''} = 0$. Item 3 proves that the equality $\pm(D_{ij} - D_{ij'}) = \pm(D_{ij''} - D_{ij'''})$ provides 8-cycles.

Case 2: In the second step, we have to test submatrices which include three rows of the exponent matrix to avoid 8-cycles. Suppose the row indices are i_0, i_1 and i_2.

1) Take j_0, j_1 as two column indices of a 3×2 submatrix of B. The left side of Equation (2) and its corresponding expressions whose elements belong to D are as follows:

$$\begin{aligned} &I)\ b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_0} + b_{i_2j_0} - b_{i_2j_1} + b_{i_1j_1} - b_{i_1j_0} \\ &\quad = (b_{i_0j_0} - b_{i_1j_0}) - (b_{i_0j_1} - b_{i_1j_1}) - (b_{i_1j_0} - b_{i_2j_0}) \\ &\qquad + (b_{i_1j_1} - b_{i_2j_1}) = D_{ij_0} - D_{ij_1} - D_{i'j_0} + D_{i'j_1}, \\ &II)\ b_{i_1j_0} - b_{i_1j_1} + b_{i_0j_1} - b_{i_0j_0} + b_{i_2j_0} - b_{i_2j_1} + b_{i_0j_1} - b_{i_0j_0} \\ &\quad = -(b_{i_0j_0} - b_{i_1j_0}) + (b_{i_0j_1} - b_{i_1j_1}) - (b_{i_0j_0} - b_{i_2j_0}) \\ &\qquad + (b_{i_0j_1} - b_{i_2j_1}) = -D_{ij_0} + D_{ij_1} - D_{i'j_0} + D_{i'j_1}, \\ &III)\ b_{i_1j_0} - b_{i_1j_1} + b_{i_2j_1} - b_{i_2j_0} + b_{i_0j_0} - b_{i_0j_1} + b_{i_2j_1} - b_{i_2j_0} \\ &\quad = (b_{i_0j_0} - b_{i_2j_0}) - (b_{i_0j_1} - b_{i_2j_1}) + (b_{i_1j_0} - b_{i_2j_0}) \\ &\qquad - (b_{i_1j_1} - b_{i_2j_1}) = D_{ij_0} - D_{ij_1} + D_{i'j_0} - D_{i'j_1}. \end{aligned}$$

   So, by considering all of above conditions we conclude that for 8-cycle free QC-LDPC codes we have: $\pm(D_{ij_0} - D_{ij_1}) \neq \pm(D_{i'j_0} - D_{i'j_1})$, where $i \neq i'$; $i, i' \in \{0, 1, \ldots, \binom{m}{2} - 1\}$. Thus, there is no repeated elements in any column of the difference matrix, DD. If Fossorier's equation is used then $3\binom{m}{3}\binom{n}{2}$ inequalities have to be investigated to avoid 8-cycles.
2) Take 3×3 submatrices of the exponent matrix, where j_0, j_1 and j_2 are three column indices. Like the previous item by investigating Equation (2), which contains 9 cases, and their equivalences in the difference matrix we have: $\pm(D_{ij_0} - D_{ij_1}) \neq \pm(D_{i'j_1} - D_{i'j_2})$. In this item if Equation (2) is used, then $18\binom{m}{3}\binom{n}{3}$ inequalities have to be investigated to avoid 8-cycles.
3) Take 3×4 submatrices of the exponent matrix, where j_0, j_1, j_2 and j_3 are four column indices. The left side of Equation (2) is $b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_3} + b_{i_1j_3} - b_{i_1j_0}$. In the following we rearrange the terms of the expression to obtain an expression whose terms belong D.
   $(b_{i_0j_0} - b_{i_1j_0}) - (b_{i_0j_1} - b_{i_1j_1}) - (b_{i_1j_2} - b_{i_2j_2}) + (b_{i_1j_3} - b_{i_2j_3}) = (D_{ij_0} - D_{ij_1}) - (D_{i'j_2} - D_{i'j_3})$. In this case elements in the first term occur in i-th row of D and elements in the second term occur in the i'-th row of D. As a result, if the Tanner graph is 8-cycle free, then for each two rows and four columns of D we have $\pm(D_{ij_0} - D_{ij_1}) \neq \pm(D_{i'j_2} - D_{i'j_3})$. If Equation (2) is used, then $6\binom{m}{3}\binom{n}{4}$ inequalities have to be investigated to avoid 8-cycles.

Case 3: In the third step, we have to test submatrices which include four rows of the exponent matrix to avoid 8-cycles. Suppose the row indices are $i_0,\ i_1,\ i_2$ and i_3.

1) Take j_0, j_1 as two columns of a 4×2 submatrix of B. The left side of Equation (2) and its corresponding expression whose elements belong to D are similar to: $b_{i_0j_0} - b_{i_0j_1} + b_{i_1j_1} - b_{i_1j_0} + b_{i_2j_0} - b_{i_2j_1} + b_{i_3j_1} - b_{i_3j_0} = D_{ij_0} - D_{ij_1} + D_{i'j_0} - D_{i'j_1}$.
   This case is similar to considering 3×2 submatrices. By considering all of them we obtain the same result. So, for 8-cycle free QC-LDPC codes we have: $\pm(D_{ij_0} - D_{ij_1}) \neq \pm(D_{i'j_0} - D_{i'j_1})$, where $i \neq i'; i, i' \in \{0, 1, \ldots, \binom{m}{2} - 1\}$. If Equation (2) is used, then $6\binom{m}{4}\binom{n}{2}$ inequalities have to be tested to avoid 8-cycles. Whereas, since this item is considered in 3×2 submatrices, there is no need to investigate again.
2) Take 4×3 submatrices of the exponent matrix, where $j_0,\ j_1$ and j_2 are the three column indices. By investigating Equation (2) we conclude that 8-cycle free QC-LDPC codes hold the following inequality : $\pm(D_{ij_0} - D_{ij_1}) \neq \pm(D_{i'j_1} - D_{i'j_2})$. Since this case is similar to considering 3×3 submatrices, it can be omitted from testing to avoid 8-cycles. However, if Equation (2) is used then $12\binom{m}{4}\binom{n}{3}$ inequalities have to be investigated to avoid 8-cycles.
   Above items except for the first item of Case 1 result in the non-existence of repeated elements for each two rows of DD. As a whole, the difference matrix, DD, belonging to 8-cycle free QC-LDPC codes has no repeated entries. Consequently, the second condition of the theorem is proved.
3) It is clear. □

APPENDIX B

In this appendix we simultaneously prove Theorem 3 and compute the number of equations of Fossorier's Lemma for each type of submatrices which have to be tested to avoid 10-cycles.

Proof: We prove the theorem in three steps. For the first step, we consider submatrices with three rows and 3, 4 and 5 columns in three parts, as follows.

Case 1: Submatrices which include three rows of the exponent matrix. Suppose the row indices are $i_0,\ i_1$ and i_2.

1) If three column indices are j_0, j_1, j_2, then its equivalent 3×3 submatrix, D', of the difference matrix, D, consists of three rows i, i', i'' and three columns j_0, j_1, j_2. By rearranging the terms of the left side of Equation (2) we obtain an equivalent expression whose terms belong to D and DD. For example:
$$\begin{aligned} & b_{i_1j_0} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_1} \\ &\quad + b_{i_0j_1} - b_{i_0j_2} + b_{i_1j_2} - b_{i_1j_1} + b_{i_0j_1} - b_{i_0j_0} \\ &= -(b_{i_0j_0} - b_{i_1j_0}) + (b_{i_0j_1} - b_{i_2j_1}) - (b_{i_1j_2} - b_{i_2j_2}) \\ &\quad + (b_{i_0j_1} - b_{i_1j_1}) - (b_{i_0j_2} + b_{i_1j_2}) = -D_{ij_0} + D_{i'j_1} \\ &\quad - D_{i''j_2} + D_{ij_1} - D_{ij_2} = -D_{ij_0} + D_{i'j_1} - D_{i''j_2} + DD_{ij}. \end{aligned}$$
   Where, j is a column of the matrix, DD.
   As we see, elements of the exponent matrix which are investigated for 6-cycles are on a distributed diagonal of D' which are the first three terms in the right side of the above equation. For each three elements on a distributed diagonal of D' there are nine 2×2 submatrices of B which are equivalent to an element in the difference matrix, DD. So, instead of considering all nine equations of Fossorier's Lemma for each distributed diagonal, which are 54 equations as a whole, we use our results in 6-cycle consideration and the matrix, DD. In this item if Equation (2) is used, then $54\binom{n}{3}\binom{m}{3}$ inequalities have to be investigated to avoid 10-cycles.
2) Take j_0, j_1, j_2, j_3 as four column indices of a 3×4 submatrix. For this item there are $6 \times \binom{4}{3} \times 9 = 216$ submatrices of size 3×4 to test to avoid 10-cycles. Because, there are $\binom{4}{3}$ choices for obtaining 3×3 submatrices and for each of them there are 6 cases related to 6-cycles. The number of mentioned 2×2 submatrices is $\binom{3}{2} \times \binom{3}{1}$. The left side of Equation (2) related to one of them is presented in the following. $b_{i_1j_0} - b_{i_1j_2} + b_{i_0j_2} - b_{i_0j_3} + b_{i_1j_3} - b_{i_1j_2} + b_{i_2j_2} - b_{i_2j_1} + b_{i_0j_1} - b_{i_0j_0} = -(b_{i_0j_0} - b_{i_1j_0}) + (b_{i_0j_1} - b_{i_2j_1}) - (b_{i_1j_2} - b_{i_2j_2}) + (b_{i_0j_2} - b_{i_1j_2}) - (b_{i_0j_3} - b_{i_1j_3}) = -D_{ij_0} + D_{i'j_1} - D_{i''j_2} + D_{ij_2} - D_{ij_3}$. As a whole, if $-D_{ij_0} + D_{i'j_1} - D_{i''j_2} + DD_{ij} = 0$, then the Tanner graph has 10-cycles. In this item if Equation (2) is used, then $432\binom{m}{3}\binom{n}{4}$ inequalities have to be investigated to avoid 10-cycles.
3) Take j_0, j_1, j_2, j_3, j_4 as five column indices of a 3×5 submatrix of the exponent matrix. For this item there are $3 \times 6\binom{5}{3} = 180$ submatrices to consider. Because, there are $\binom{5}{3}$ choices for obtaining 3×3 submatrices. For each of them there are 6 cases related to 6-cycles. The 2×2 submatrices occur in the other two columns, so, the number of them is $\binom{2}{2} \times \binom{3}{2} = 3$. The left side of Equation (2) related to one of them is presented in the following.
$$\begin{aligned} & b_{i_1j_0} - b_{i_1j_2} + b_{i_0j_2} - b_{i_0j_3} + b_{i_1j_3} - b_{i_1j_4} + b_{i_2j_4} - b_{i_2j_1} \\ &\quad + b_{i_0j_1} - b_{i_0j_0} \\ &= -(b_{i_0j_0} - b_{i_1j_0}) + (b_{i_0j_1} - b_{i_2j_1}) - (b_{i_1j_4} - b_{i_2j_4}) \\ &\quad + (b_{i_0j_2} - b_{i_1j_2}) - (b_{i_0j_3} - b_{i_1j_3}) \\ &= -D_{ij_0} + D_{i'j_1} - D_{ij_4} + D_{i''j_2} + D_{ij_3}. \end{aligned}$$
   As a whole, if $-D_{ij_0} + D_{i'j_1} - D_{i''j_4} + DD_{ij} = 0$, then the Tanner graph has 10-cycle. In this item if Equation (2) is used, then $180\binom{m}{3}\binom{n}{5}$ inequalities are investigated to avoid 10-cycles.

To prove the first condition of the theorem we utilize three items of Case 1 and define two sets $\mathcal{A}$ and $\mathcal{B}$ as follows. The set $\mathcal{A}$ includes the values obtained from the left side of Equation (2) when we consider 6-cycles. The set $\mathcal{B}$ includes elements of three rows of the matrix, DD, which are equivalent to three rows of the exponent matrix. If $\mathcal{A} \cap \mathcal{B} \neq \emptyset$, then the Tanner graph has 10-cycles. Using this technique decreases the size of the search space and values obtained in 6-cycle considerations are utilized which contribute to reduce the complexity.

Case 2: In the second step, we have to test submatrices which include four rows of the exponent matrix to avoid 10-cycles. Suppose the row indices are $i_0,\ i_1,\ i_2$ and i_3.

1) Take j_0, j_1, j_2 as three column indices of a 4×3 submatrix of B. Like the previous items, we rearrange the left side of Equation (2) to obtain an equivalent expression whose terms belong to D and DD. For example:

$$\begin{aligned}&b_{i_0j_0}-b_{i_0j_1}+b_{i_1j_1}-b_{i_1j_2}+b_{i_2j_2}-b_{i_2j_1}+b_{i_3j_1}-b_{i_3j_2}\\&\quad+b_{i_2j_2}-b_{i_2j_0}=(b_{i_0j_0}-b_{i_2j_0})-(b_{i_0j_1}-b_{i_1j_1})\\&\quad-(b_{i_1j_2}-b_{i_2j_2})-(b_{i_2j_1}-b_{i_3j_1})+(b_{i_2j_2}-b_{i_3j_2})\\&=D_{i'j_0}-D_{ij_1}-D_{i''j_2}-D_{i'''j_1}+D_{i'''j_2}.\end{aligned}$$

As we see, three elements of D' which are on a distributed diagonal of a 3×3 submatrix of D' are the first three terms in the right side of the above equality. There are $\binom{4}{3}$ choices for 3×3 submatrices of D'. The last two terms, in the right side, is equivalent to one element of the matrix, DD. If it appears in the j-th column of DD, then the equality $-D_{ij_1}+D_{i'j_0}-D_{i''j_2}-DD_{i'''j}=0$ provides 10-cycles. For this item there are $6 \times 4 \times 3 = 72$ inequalities to consider. So, for an $m \times n$ exponent matrix there are $72 \times \binom{m}{4}\binom{n}{3}$ inequalities which have to be tested to avoid 10-cycles.

2) Take a 4×4 submatrix, B', of the exponent matrix, where $j_0,\ j_1,\ j_2$ and j_3 are four column indices. It is equivalent to a 6×4 submatrix of the difference matrix, D, which we denote it by D'. We first choose a 3×3 submatrix of D' which corresponds to a 3×3 submatrix of B'. D' includes a row and a column different from those chosen in the 3×3 submatrix. The mentioned row and column have an element in their cross point which appears in the expression whose elements belong to D'. The expression based on D' also contains a term which belong a column of D' which is different from the one in the cross point. For this element there are 9 possibilities to choose. So for each 4×4 submatrix of the difference matrix, D, there are $9 \times 6\binom{4}{3}\binom{4}{3} = 864$ equations to consider. And as a whole, the number of inequalities to avoid 10-cycles for this item is $864 \times \binom{m}{4}\binom{n}{4}$. The left side of Equation (2) and the corresponding expression whose elements belong to D for two cases are as follows:

$$\begin{aligned}&I)\ b_{i_0j_0}-b_{i_0j_1}+b_{i_1j_1}-b_{i_1j_2}+b_{i_2j_2}-b_{i_2j_3}+b_{i_3j_3}\\&\quad-b_{i_3j_2}+b_{i_1j_2}-b_{i_1j_0}=-(b_{i_0j_1}-b_{i_1j_1})+(b_{i_1j_2}-b_{i_3j_2})\\&\quad-(b_{i_2j_3}-b_{i_3j_3})+(b_{i_0j_0}-b_{i_1j_0})-(b_{i_1j_2}-b_{i_2j_2})\\&=-D_{ij_1}+D_{i''j_2}-D_{i'''j_3}+D_{ij_0}-D_{i'j_2},\\&II)\ b_{i_0j_0}-b_{i_0j_1}+b_{i_1j_1}-b_{i_1j_3}+b_{i_3j_3}\\&\quad-b_{i_3j_2}+b_{i_1j_2}-b_{i_1j_3}+b_{i_2j_3}-b_{i_2j_0}\\&=-(b_{i_0j_1}-b_{i_1j_1})+(b_{i_0j_0}-b_{i_2j_0})-(b_{i_1j_3}-b_{i_3j_3})\\&\quad-(b_{i_1j_3}-b_{i_2j_3})+(b_{i_1j_2}-b_{i_3j_2})\\&=-D_{i'j_1}+D_{ij_0}-D_{i''j_3}-D_{i'''j_3}+D_{i'''j_2}.\end{aligned}$$

As we see, in the first case the last two terms do not occur in the same row but for the second case they do. Therefore, in the second case we replace these two terms by one element of the matrix, DD.

3) Take a 4×5 submatrix, B', of the exponent matrix, where $j_0,\ j_1,\ j_2,\ j_3$ and j_4 are five column indices. It is equivalent to a 6×5 submatrix of the difference matrix, D, which we denote it by D'. We first choose a 3×3 submatrix of D' which corresponds to a 3×3 submatrix of B'. D' contains a row and two columns which are different from those in the chosen 3×3 submatrix. The mentioned row and columns have two elements in their cross points which appear in the expression whose elements belong to D'. For these elements there are 4 possibilities to choose. So, for each 4×5 submatrix of the exponent matrix, D, there are $4 \times 6\binom{4}{3}\binom{5}{3} = 960$ inequalities to consider. As a whole, the number of inequalities which have to be tested to avoid 10-cycles for this item is $960 \times \binom{m}{4}\binom{n}{4}$.
The left side of one of Equations (2) and its corresponding equation whose elements belong to D is as follows:

$$\begin{aligned}&b_{i_1j_0}-b_{i_1j_2}+b_{i_3j_2}-b_{i_3j_3}+b_{i_2j_3}-b_{i_2j_4}+b_{i_3j_4}\\&\quad-b_{i_3j_1}+b_{i_0j_1}-b_{i_0j_0}=-(b_{i_0j_0}-b_{i_1j_0})+(b_{i_0j_1}\\&\quad-b_{i_3j_1})-(b_{i_1j_2}-b_{i_3j_2})+(b_{i_2j_3}-b_{i_3j_3})-(b_{i_2j_4}-b_{i_3j_4})\\&=-D_{ij_0}+D_{i'j_1}-D_{i''j_2}+D_{i'''j_3}-D_{i'''j_4}.\end{aligned}$$

As we see, the last two terms can be taken as an element of the matrix, DD. So, if it occurs in the i'''-th row and the j-th column of DD, then the equality $-D_{ij_0}+D_{i'j_1}-D_{i''j_2}+DD_{i'''j}=0$ provides 10-cycles.

Case 3: In the third step, we have to test submatrices which include five rows of the exponent matrix to avoid 10-cycles. Suppose the row indices are $i_0,\ i_1,\ i_2,\ i_3$ and i_4.

1) Take 5×3 submatrices of the exponent matrix, where $j_0,\ j_1$ and j_2 are three column indices. In order to show that this item is similar to the item 2 of Case 2, we obtain the left side of Equation (2) for two cases and rearrange their terms to obtain the expressions whose elements belong to D. So this item can be omitted from testing to avoid 10-cycles which reduces the size of the search space.

$$\begin{aligned}&I)\ b_{i_0j_0}-b_{i_0j_1}+b_{i_1j_1}-b_{i_1j_2}+b_{i_2j_2}-b_{i_2j_1}+b_{i_3j_1}-b_{i_3j_2}\\&\quad+b_{i_4j_2}-b_{i_4j_0}=(b_{i_0j_0}-b_{i_4j_0})-(b_{i_0j_1}-b_{i_3j_1})-(b_{i_3j_2}\\&\quad-b_{i_4j_2})+(b_{i_1j_1}-b_{i_2j_1})-(b_{i_1j_2}-b_{i_2j_2})=D_{ij_0}-D_{i'j_1}\\&\quad-D_{i''j_2}-D_{i'''j_1}-D_{i'''j_2}.\\&II)\ b_{i_0j_0}-b_{i_0j_1}+b_{i_2j_1}-b_{i_2j_2}+b_{i_3j_2}-b_{i_3j_1}+b_{i_4j_1}-b_{i_4j_2}\\&\quad+b_{i_1j_2}-b_{i_1j_0}=(b_{i_0j_0}-b_{i_1j_0})-(b_{i_0j_1}-b_{i_2j_1})-(b_{i_2j_2}\\&\quad-b_{i_3j_2})+(b_{i_1j_2}-b_{i_4j_2})-(b_{i_3j_1}-b_{i_4j_1})\\&=D_{ij_0}-D_{i'j_1}-D_{i''j_2}+D_{i'''j_1}-D_{i''''j_2}.\end{aligned}$$

2) Take 5×4 submatrices of the exponent matrix, where $j_0,\ j_1,\ j_2$ and j_3 are four column indices. This item is also similar to the item 2 of Case 2 and is omitted from testing to avoid 10-cycles.

To prove the second condition of the theorem we use the items 1 of Case 2 to 2 of Case 3. According to the examples provided in the mentioned items we result the condition.

3) It is clear. □

REFERENCES

[1] 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. 2626–2637, Aug. 2014.

[2] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "Design of multiple-edge protographs for QC LDPC codes avoiding short inevitable cycles," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4598–4614, Jul. 2013.

[3] 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, Aug. 2004.

[4] 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. Electron., Commun. Comput. Sci.*, vol. E92.A, no. 11, pp. 2891–2894, 2009.

[5] S. V. S. Ranganathan, D. Divsalar, and R. D. Wesel, "On the girth of (3,L) quasi-cyclic LDPC codes based on complete protographs," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 731–735.

[6] G.-H. Zhang, R. Sun, and X.-M. Wang, "Explicit construction of girth-eight QC-LDPC codes and its application in CRT method," *J. Commun.*, vol. 33, no. 3, pp. 171–176, Mar. 2012.

[7] M. E. O'Sullivan, "Algebraic construction of sparse matrices with large girth," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 718–727, Feb. 2006.

[8] Y. Wang, J. S. Yedidia, and S. C. Draper, "Construction of high-girth QC-LDPC codes," in *Proc. 5th Int. Symp. Turbo Codes Rel. Topics*, 2008, pp. 180–185.

[9] I. E. Bocharova, R. Johannesson, F. Hug, B. D. Kudryashov, and R. V. Satyukov, "Searching for voltage graph-based LDPC tailbiting codes with large girth," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2265–2279, Apr. 2012.

[10] 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, no. 8, pp. 2885–2891, Aug. 2007.

[11] A. Tasdighi, A. H. Banihashemi, and M. R. Sadeghi, "Efficient search of girth-optimal QC-LDPC codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1552–1564, Apr. 2016.

[12] 3M. Karimi and A. H. Banihashemi, "On the girth of quasi-cyclic protograph LDPC codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4542–4552, Jul. 2013.

[13] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Quasi-cyclic LDPC codes on two arbitrary sets of a finite field," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2014, pp. 2454–2458.

[14] S. Song, B. Zhou, S. Lin, and K. Abdel-Ghaffar, "A unified approach to the construction of binary and nonbinary Quasi-cyclic LDPC codes based on finite fields," *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 84–93, Jan. 2009.

[15] M. Gholami, M. Alinia, and Z. Rahimi, "An explicit method for construction of CTBC codes with girth 6," *Int. J. Electron. Commun. (AEU)*, vol. 74, pp. 183–191, Apr. 2017.

[16] M. Gholami and M. Alinia, "High-performance binary and non-binary low-density parity-check codes based on affine permutation matrices," *IET Commun.*, vol. 9, no. 17, pp. 2114–2123, Nov. 2015.

[17] X. Zheng, F. C. M. Lau, C. K. Tse, Y. He, and S. Hau, "Application of complex-network theories to the design of short-length low-density-parity-check codes," *IET Commun.*, vol. 3, no. 10, pp. 1569–1577, Oct. 2009.

[18] H. Xu, D. Feng, R. Luo, and B. Bai, "Construction of quasi-cyclic LDPC codes via masking with successive cycle elimination," *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2370–2373, Dec. 2016.

[19] A. Tasdighi, A. H. Banihashemi, and M.-R. Sadeghi, "Symmetrical constructions for regular girth-8 QC-LDPC codes," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 14–22, Jan. 2017.

FARZANE AMIRZADE received the B.Sc. degree in applied mathematics from Zanjan University, Zanjan, Iran, in 2006, and the M.Sc. degree in applied mathematics from Alzahra University, Tehran, Iran, in 2009. She is currently pursuing the Ph.D. degree with the Department of Mathematics, Shahrood University of Technology, Shahrood, Iran. Her research interests include coding and information theory, combinatorics, and lattice codes.

MOHAMMAD-REZA SADEGHI received the Ph.D. from Carleton University, Ottawa, ON, Canada, in 2003. In 2004, he was a Post-Doctoral Fellow with Carleton University. He is currently an Associate Professor with the Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran. His research interests include coding theory, lattice codes, and lattice-based cryptography. He received the Marwah Award for outstanding graduate (Ph.D.) studies in 2003. He received the Scholarship from the Fields Institute of Mathematical Studies in 2004.