Construction of Protograph-Based LDPC Codes With Chordless Short Cycles

Farzane Amirzade, Mohammad-Reza Sadeghi, and Daniel Panario, Senior Member, IEEE

Abstract—There is a concept in graph theory known as a chord which has not been considered before in relation to trapping sets of Tanner graphs. A chord of a cycle is an edge outside the cycle which connects two vertices of that cycle. It is proved that short cycles with a chord are the root of several trapping sets. It is proved that check nodes connected to a, b ∈ S, a set of odd degree (even degree) check nodes connected to v is denoted by O(v)(E(v)). If for each v ∈ S we have |O(v)| < |E(v)|, then the trapping set is an (a, b) absorbing set. If any variable node outside an (a, b) absorbing set has more connections with even degree check nodes of that (a, b) absorbing set than its odd degree check nodes, then it is a fully absorbing set. As in the trapping set definition, an (a, b) absorbing set is elementary (EAS) if all check nodes are of degree 1 or 2.

Graphical structures including trapping sets and absorbing sets are known to be key factors in decoding failures and error floor behavior of LDPC codes [25, 26]. Trapping sets for the additive white Gaussian noise (AWGN) channel [27] and absorbing sets when the bit-flipping algorithm is used to decode [5] significantly influence the performance of an LDPC code. For example, according to [28], the performance of LDPC codes in the high signal-to-noise (SNR) region is mainly influenced by the structure of the smallest absorbing sets.

In order to achieve an appropriate upper bound on the error-correcting performance of LDPC codes at high SNR, several methods are suggested that rely on the relationship between the aforementioned graphical structures and different features of LDPC codes such as the length of the shortest cycles of the Tanner graph and minimum distance d_{min}. These characteristics have been widely studied [11], [16], [18], [21], [30], [31], [32], [33], [35]. In this regard, we have three approaches.

The first approach is based on the relation between trapping sets and the minimum distance of a code. It is known [34, 36] that a code C has minimum distance d_{min} if and only if the Tanner graph contains no (a, 0) trapping set for a < d_{min} and there exists at least one (d_{min}, 0) trapping set. Thus, a large minimum distance guarantees the non-existence of small size quasi-cyclic (QC) LDPC codes. Since these codes are associated with a base matrix and an exponent matrix, they give a simple description of codes and enable hardware-friendly implementation. Thus, QC-LDPC codes, as a special case of the protograph-based construction, have attracted substantial attention [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22].
ETSs which are the roots of the \((a,0)\) trapping set. Moreover, since the size of the smallest absorbing sets, which are the absorbing sets of the smallest size \(a\), is upper-bounded by the minimum distance \([28]\), constructing LDPC codes with a large minimum distance has attracted much attention. On the one hand, in \([37]\) it is proved that the minimum distance of a QC-LDPC code with a \(\gamma \times n\) all-one base matrix, which is a \((\gamma,n)\)-regular QC-LDPC code with column weight \(\gamma\) and row weight \(n\), is upper-bounded by \((\gamma+1)!\). On the other hand, QC-LDPC codes from regular protographs with multiple edges potentially have larger minimum distances \([4]\). Thus, a method to improve the performance of QC-LDPC codes at high SNR is constructing QC-LDPC codes with a large column weight or multi-edge QC-LDPC codes which have potentially large minimum distances.

The second approach is based on the relation between trapping sets and short cycles. In fact, it has been shown empirically that short cycles are the roots of harmful structures. Thus, a method to eliminate the smallest trapping sets is the removal of short cycles. The length of the shortest cycle in the Tanner graph is the \(girth\) of the Tanner graph which is denoted by \(g\). Increasing the girth causes an improvement in the code performance and a great deal of research effort has been devoted to constructing exponent matrices of protograph-based QC-LDPC codes with large girths \([4]\), \([7]\), \([9]\), \([12]\), \([14]\), \([19]\), \([21]\), \([23]\), \([24]\), \([29]\).

The third approach, which is our focus in this paper, is to directly study trapping sets and absorbing sets and avoid them from occurring in the Tanner graph. In Subsection I-A, we summarize some of the achievements in the literature and discuss their merits and drawbacks, where in Subsection I-B we detail our contributions.

### A. Previous Work

In the literature, there are several articles about the smallest size of ETSs and/or EASs as well as methods to remove the most harmful ones of these structures. For example, we can refer to \([30]\) to find the smallest size of ETSs and EASs in the Tanner graph of an LDPC code with a certain girth \(g\) and column weight \(\gamma\). In \([31]\) it is proved that when \(g = 6\), \(\gamma = 3\), and \(d_{\text{min}} \geq 6\), then the smallest fully absorbing set is strictly less than \(d_{\text{min}}\). According to \([5]\), for a special case of QC-LDPC codes known as \(array-based\) \(LDPC\) codes, the minimal absorbing sets are \((4,0)\), \((3,3)\) and \((6,4)\) when the column weights are \(\gamma = 2, 3, 4\), respectively.

Regarding methods to construct an exponent matrix whose corresponding Tanner graph is free of small size ETSs and/or EASs, we refer to \([11]\), \([16]\), \([18]\), \([20]\), \([21]\), \([32]\), and \([33]\), \([35]\). For girth-8 LDPC codes with column weight \(3\), the removal of \((a,b)\) ETSs with \(5 \leq a \leq 8\) and \(b \leq 3\) has been studied in \([11]\), \([16]\), \([21]\), and \([35]\) each of which proposes a method to eliminate these ETSs. Each method results in an improvement in the performance of a QC-LDPC code (and a spatially-coupled LDPC code) with \(g = 8\) and \(\gamma = 3\). Moreover, QC-LDPC codes with short or moderate lengths can outperform random or pseudorandom LDPC codes \([3]\); we observe that the given exponent matrices to construct QC-LDPC codes free of some specific trapping sets also have short lengths. In \([32]\) and \([33]\), it is shown that controlling specific cycles contributes to the removal of harmful trapping sets. In \([18]\) is given, using an edge-coloring technique, a sufficient condition for an exponent matrix to construct a \((3,n)\)-regular algebraic-based QC-LDPC code with girth \(g = 6\) and free of \((a,b)\) ETSs, \(4 \leq a \leq 5\) and \(b \leq 2\). In \([21]\), the edge-coloring technique is applied to spatially-coupled LDPC codes with girth 6 and column weights \(3 \leq \gamma \leq 5\) as well as girth 8 and column weight \(\gamma = 3\).

The following reasons give drawbacks to the methods mentioned above. These drawbacks are some of our motivations for this work.

- Most methods in the literature that remove harmful trapping sets are applied to an all-one base matrix with a specific column weight such as 3 or 4, and there are not many results regarding the removal of harmful trapping sets from the Tanner graph of irregular and multi-edge protographs. However, capacity-approaching LDPC codes require an irregular degree distribution. Thus, an important drawback of the existing methods is that they are not applicable to capacity-approaching LDPC codes such as protograph-based Raptor-like QC-LDPC codes \([38]\), whose protographs are irregular and multi-edge, and 5G LDPC codes in \([15]\), whose protographs are irregular.

- As a result of some methods mentioned above, the removal of ETSs yields a minimum lifting degree that is larger than the minimum lifting degree of a code with the same degree distribution but a higher girth. For example, according to the numerical results in \([20]\), the minimum lifting degree of \((3,5)\)-regular QC-LDPC codes whose Tanner graphs have girth 6 and are free of \((a,b)\) ETSs with \(b \leq 2\) and \(a \leq 5\), \(a \leq 7\), \(a \leq 9\), and \(a \leq 11\) are, \(N = 10, 15, 22\), and \(N = 29\), respectively. Whereas, the minimum lifting degree of a \((3,5)\)-regular QC-LDPC code with girth 8 is 13 \([9]\). In fact, because of the good properties of QC-LDPC codes with short or moderate lengths \([3]\), \([29]\), the construction of QC-LDPC codes with the shortest length has been the focus of several articles \([3]\), \([9]\), \([11]\), \([12]\), \([14]\), \([16]\), \([20]\), \([21]\), \([23]\), \([29]\). Therefore, if codes with the shortest length are desired and increasing girth has better results than using the methods in the literature to remove some trapping sets, then one prefers to raise the girth which originally causes the removal of the desired trapping sets.

- Although there is a direct connection between the size of \((a,0)\) ETSs and the \(d_{\text{min}}\) of an LDPC code, despite the existence of all the mentioned methods to remove small size ETSs, there is no analytic result in the literature about the \(d_{\text{min}}\) of an LDPC code with a certain girth, a given column weight, and free of a specific trapping set.

### B. Contributions

In this paper, to tackle all the above mentioned drawbacks, we propose a novel approach to control harmful trapping sets and to increase the minimum distance. Our approach covers all kinds of protographs, regular or irregular, and simple or multi-edge. Analytical and numerical results prove that our method can be applied to a protograph-based LDPC code with any...
given column weight and row weight. Our results require the following concepts.

In graph theory, a chord of a cycle is an edge that is not part of the cycle but connects two vertices of the cycle. If a cycle is free of a chord, then it is a chordless cycle. A cycle with a chord is denoted by cycle-wc.

We present the results in two parts. In the first part, we analytically consider the influence of the removal of short cycles-wc on increasing the minimum distance and on avoiding small size ETSs from occurring in the Tanner graph of a protograph-based LDPC code with girths 6 and 8. In the second part, we present our method to construct the exponent matrix of a QC-LDPC code with a Tanner graph whose short cycles are all chordless.

1) Contributions of the First Part: To the best of our knowledge, the only lower bound given for the minimum distance of an LDPC code with girth 6 and column weight $\gamma$ is $\gamma + 1$ \cite{36}. It is known that removing trapping sets up to a certain size guarantees tighter lower bounds on the minimum distance. In this first part, we show that short cycles with a chord are the key to several trapping sets, and eliminating these cycles causes the removal of several small size trapping sets and increases the $d_{\text{min}}$. In fact, by conveniently using some theorems from graph theory, we present analytic lower bounds on the minimum distance of an LDPC code whose Tanner graph is free of short cycles with a chord. Our main contributions in this first part are as follows.

- For $g = 6$ and minimum column weight $\gamma$ we show that avoiding 8-cycles-wc causes an increase in the lower bound of the minimum distance from $\gamma + 1$ to $2\gamma$.
- Without increasing the girth from 6 to 8, eliminating 8-cycles-wc results in the removal of several trapping sets and consequently yields an LDPC code in which the lower bounds on the size of the smallest $(a, b)$ ETSs, $b < a$, are equal to the minimum sizes of ETSs in a girth-8 LDPC code.
- For $g = 8$ and column weight $\gamma$, by avoiding 12-cycles-wc, we obtain a new lower bound on the minimum distance which is $d_{\text{min}} \geq \frac{3(\gamma - 1)}{\gamma + 1}$.
- For $g = 8$ and $\gamma = 3$ we show that, as a result of avoiding 12-cycles-wc, the lower bound on the size of the smallest $(a, b)$ ETSs, $b < a$, is equal to the lower bound on the size of ETSs of a girth-10 LDPC code.
- For $g = 8$ and $\gamma = 4$ we provide the minimum sizes of $(a, b)$ ETSs, $b < a$, in a Tanner graph free of cycles-wc of lengths up to 12. Thus, after removing the chords and without increasing the girth the resulting codes inherit the useful features of an LDPC code with a higher girth.

2) Contributions of the Second Part: We provide a new method to construct exponent matrices of QC-LDPC codes with girth 6 whose Tanner graphs are free of 8-cycles-wc and QC-LDPC codes with girth 8 whose Tanner graphs are free of short cycles-wc of lengths up to 12. Our method to control short cycles-wc applies to any exponent matrix. We provide numerical and analytical results to show the applicability of our method to irregular and multi-edge protographs. The analytical conditions to remove 8-cycles-wc and thus the removal of small size ETSs from the Tanner graph of a multi-edge QC-LDPC code have been considered for the first time in this paper. We also apply our method to a Raptor-like QC-LDPC code and construct an exponent matrix with the minimum lifting degree such that its Tanner graph has girth 6 and is free of 8-cycles-wc. Our main contributions in this part are as follows.

- We obtain a necessary and sufficient condition to construct both simple and multi-edge protograph-based LDPC codes with girth 6 and free of 8-cycles-wc. The proposed conditions are implemented on compact QC-LDPC codes as well as array-based LDPC codes. The low complexity of our method allows us to present exponent matrices of regular LDPC codes with column weight $3 \leq \gamma \leq 6$ and row weight $n \leq 18$ as well as LDPC codes with irregular protographs. We also compare the $d_{\text{min}}$ of these codes with the largest $d_{\text{min}}$ of their counterparts in \cite{10} and \cite{29}. For most cases, the $d_{\text{min}}$ of QC-LDPC codes with girth 6 and free of 8-cycles-wc are at least the $d_{\text{min}}$ of their counterpart QC-LDPC codes with girth 8. The simulation results for all simple, regular multi-edge, and irregular multi-edge QC-LDPC codes with a high rate also illustrate the positive impact of avoiding short cycles-wc in the performance curves.

- We present a necessary and sufficient condition to construct girth-8 LDPC codes free of cycles-wc of lengths up to 12. As a result of this condition, we achieve an analytical lower bound on the lifting degree of a QC-LDPC code with girth 8 and free of cycles-wc of lengths up to 12. For QC-LDPC codes with column weight 3 and girth 8, we compare, for different aspects of the code, the influence of avoiding short cycles-wc with the impact of removing $(a, b)$ ETSs with $5 \leq a \leq 8$ and $b \leq 3$. In terms of the length of the code, we show that avoiding short cycles-wc implies in codes with shorter lengths. From the viewpoint of computational complexity in the search space, our approach to remove ETSs has less computational complexity compared to the methods in \cite{11} and \cite{16}. The simulation results also show that the removal of short cycles with a chord can yield the same performance curve as we avoid the occurrence of the mentioned ETSs.

C. Outline

We give the structure of the paper. Section II presents some basic definitions. Section III investigates cycles-wc of short lengths and presents the analytic lower bounds on the $d_{\text{min}}$ of an LDPC code free of short cycles-wc. In Subsections III-A and III-B we consider the influence of the removal of short cycles-wc on increasing the minimum distance and on avoiding small size ETSs from occurring in the Tanner graph of a protograph-based LDPC code with girth 6 and 8, respectively. Section IV presents a necessary and sufficient condition to construct protograph-based LDPC codes with girth 6 in which 8-cycles are all chordless. In Subsections IV-A, IV-B, IV-C, and IV-D we apply our method to simple protographs, compact QC-LDPC codes, array-based LDPC codes, and multi-edge protographs. In Section V, we present necessary and sufficient conditions to avoid short cycles-wc of lengths up to 12. In Section VI, we present simulation results to show the merits of
our approach in the performance of the codes. In Section VII, we summarize our results.

II. PRELIMINARIES

A QC-LDPC code with a lifting degree \( N \) can be associated with an exponent matrix \( B = [\tilde{B}_{ij}] \) and a base matrix \( W = [W_{ij}] \) of the same size \( c \times d \), where \( 0 \leq i \leq c - 1 \) and \( 0 \leq j \leq d - 1 \). If \( W_{ij} = \ell_{ij} \in \mathbb{N} \), then \( [\tilde{B}_{ij}] = \ell_{ij}, \tilde{B}_{ij} = (b_{ij}^{(1)}, b_{ij}^{(2)}, \ldots, b_{ij}^{(s)}), b_{ij}^{(s)} \in \{0,1,\ldots, N-1\} \) and \( b_{ij}^{(s)} \neq b_{ij}^{(r')} \) for \( 1 \leq r < r' \leq \ell_{ij} \), and if \( W_{ij} = 0 \), then \( \tilde{B}_{ij} = 0 \).

If theprotograph is simple, then all entries of \( W \) are 0.1. If the protograph is multi-edge, then \( W \) contains entries bigger than 1. The protograph is fully-connected if all entries of \( W \) are 1. Substituting vectors of \( B \) by \( H_{ij} = I^{b_{ij}^{(1)}} + I^{b_{ij}^{(2)}} + \cdots + I^{b_{ij}^{(s)}} \), where \( I^{b_{ij}^{(s)}} \) is a circulant permutation matrix of dimension \( N \times N \), and \( 0 \) elements by a zero matrix of size \( \prod \) results in a QC-LDPC code. The top row of \( I^{b_{ij}^{(s)}} \) contains 1 in the \( b_{ij}^{(s)} \)-th position and other entries of that row are zero. The \( s \)-th row of the circulant permutation matrix is formed by \( s \) right cyclic shifts of the first row.

**Example 1:** Given a base matrix \( W = \begin{bmatrix} 2 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 \end{bmatrix} \), the following exponent matrix with lifting degree \( N = 5 \) results in an irregular multi-edge QC-LDPC code

\[
B = \begin{bmatrix}
(0,1) & (0,4) & \emptyset \\
(2,4) & (3) & (1,2)
\end{bmatrix}.
\]

A necessary and sufficient condition for the existence of 2k-cycles in the Tanner graph of QC-LDPC codes provided in [3] is

\[
\sum_{i=0}^{k-1} (b_{m,n}^{(i)} - b_{m,n+1}^{(i)}) \equiv 0 \pmod{N}, \tag{1}
\]

where \( b_{m,n}^{(i)} \) is the \( r_i \)-th entry of \( \tilde{B}_{m,n} \), \( \tilde{B}_{m,n} \) is the \( (m,n) \)-th entry of \( B \) with the row index \( m_i \in \{0,1,\ldots, c-1\} \) and the column index \( n_i \in \{0,1,\ldots, d-1\} \), and the \( \ell \)-th entry is \( b_{ij}^{(s)} \) if \( n_i = n_{i+1} \) and \( r_i \neq r' \) if \( n_i = n_{j+1} \) and \( r_i \neq r' \) if \( n_i = n_{j+1} \).

**Example 2:** In the exponent matrix of Example 1 the following equation proves the existence of 4-cycles in the Tanner graph of the code

\[
(b_{01}^{(0)} - b_{02}^{(0)}) + (b_{12}^{(0)} - b_{11}^{(0)}) = (0 - 4) + (3 - 4) \equiv 0 \pmod{5}.
\]

Moreover, the Tanner graph has 6-cycles since

\[
(b_{00}^{(0)} - b_{02}^{(0)}) + (b_{12}^{(1)} - b_{11}^{(1)}) + (b_{01}^{(0)} - b_{03}^{(0)}) = (1 - 0) + (3 - 4) + (0 - 0) \equiv 0 \pmod{5}.
\]

In simple protographs, since the entries of \( W \) are 0, the entries of an exponent matrix \( B \) are defined by \( b_{ij} \) instead of \( \tilde{B}_{ij} \). It should be noticed that the girth of a fully-connected QC-LDPC code, which has an all-one base matrix, is at most 12 [3].

**Example 3:** Let \( B \) with lifting degree \( N = 5 \) be the exponent matrix of a fully-connected \((3,4)\)-regular QC-LDPC code

\[
B = \begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 2 & 3 & 4 \\
0 & 3 & 2 & 1
\end{bmatrix}.
\]

The Tanner graph has 6-cycles since \((b_{00} - b_{03}) + (b_{13} - b_{11}) + (b_{21} - b_{20}) = (0 - 0) + (4 - 2) + (3 - 0) \equiv 0 \pmod{5} \).

To construct an exponent matrix that results in a QC-LDPC code with lifting degree \( N \) and girth \( g \) we use Equation (1). In fact, an exhaustive search algorithm is required to obtain the entries of the exponent matrix and to avoid specific 2k-cycles of the Tanner graph, \( 2k < g \). To obtain a fully-connected \( \gamma \times n \) exponent matrix with girth \( g \), the number of entries of the exponent matrix which have to be identified is \( \gamma n \). Since each entry of the exponent matrix with lifting degree \( N \) is chosen from the set \{0,1,\ldots, N-1\}, the number of options for each entry is \( N \). Thus, the size of the search space when using an exhaustive search algorithm is \( N^{\gamma n} \). Hence, in the search space, we have \( N^{\gamma n} \) exponent matrices and for each of them, we should check Equation (1) for all 2k-cycles, \( 2k < g \).

**Definition 1:** For a bipartite graph \( G \) corresponding to an ETS, a variable node (VN) graph (also called normal graph) is constructed by removing all 1-degree check nodes, defining variable nodes of \( G \) as its vertices and 2-degree check nodes connecting the variable nodes in \( G \) as its edges.

We note that a chord of a cycle is an edge that is not part of the cycle but connects two vertices of the cycle. For example, Fig. 1 (e) is a 6-cycle with a chord. We adapt this concept to the Tanner graph as follows. We recall that Tanner graphs are bipartite graphs with vertices split into variable nodes and check nodes.

**Definition 2:** A cycle is a chordless cycle if outside the cycle there is no check node connecting two variable nodes of the cycle, and outside the cycle there is no edge between a variable node and a check node of that cycle. Otherwise, it is defined as a cycle with a chord, which is denoted by cycle-wc.

Thus, we take a cycle as a cycle-wc if the cycle or its VN graph contains a chord. Therefore, we cannot take a cycle in which two check nodes are connected by a variable node outside the cycle as a cycle-wc. Because on the one hand, the cycle has no chord, but on the other hand, since this cycle has a check node of degree 3, it is not an ETS and we cannot obtain a VN graph for it. Fig. 1 (a) and (b) show an 8-cycle-wc and its corresponding VN graph, where squares are check nodes and circles are variable nodes. In Fig. 1 (a) two variable nodes are connected by a check node outside the cycle. Fig. 1 (c) is a 6-cycle-wc in which a variable node and a check node are connected by an edge outside the cycle. Fig. 1 (d) shows a cycle in which two check nodes are connected by a variable node outside the cycle. Thus, Fig. 1 (d) is not a cycle-wc. Fig. 1 (e) is a 12-cycle-wc, where two variable nodes of the cycle are connected by a check node outside the cycle.
III. Theoretical Results

In this section, cycles in terms of their chords are considered. In a girth-6 LDPC code, all 6-cycles are chordless otherwise the girth of the Tanner graph would be equal to 4. Similarly, in a girth-8 LDPC code, all 8-cycles and 10-cycles are free of a chord otherwise the girth of the Tanner graph would be equal to 6. We investigate the consequences of avoiding 8-cycles-wc from Tanner graphs with girth 6, and 12-cycles-wc from Tanner graphs with girth 8. It is analytically shown that without increasing the girth we can improve the results related to different features of an LDPC code such as lower bounds on results related to different features of an LDPC code such as the well-known Turan’s theorem, from graph

A. Chordless Short Cycles in Tanner Graphs With Girth 6

To prove Theorem 2 we need some definitions and theorems, such as the well-known Turan’s theorem, from graph theory which are presented below.

A complete graph on \( n \) vertices is a graph in which every pair of distinct vertices are connected by a unique edge. A complete graph on these \( n \) vertices is denoted by \( K_n \). A \( K_n \)-free graph is a graph in which no induced subgraph on \( n \) vertices forms a complete graph on \( n \) vertices. A triangle-free graph is a \( K_3 \)-free graph.

Theorem 1 [39]: Let \( G \) be any graph on \( n \) vertices, such that \( G \) is \( K_{r+1} \)-free. Then the number of edges in \( G \) is at most \( \frac{(2r-1)}{r} \times \frac{n^2}{4} = (1 - \frac{1}{r}) \times \frac{n^2}{4} \).

According to Theorem 1, a triangle-free graph on \( n \) vertices has at most \( \frac{n^2}{4} \) edges. A \( K_4 \)-free graph on \( n \) vertices has at most \( \frac{n^2}{4} \) edges.

Lemma 2 [39]: In a graph with \( n \) vertices and \( |E| \) edges, where \( \frac{n^2}{4} \leq |E| \leq \frac{n^2}{2} \), the minimum number of triangles is \( \frac{n}{9} (4|E| - n^2) \).

Lemma 3 [30]: An \((a, b)\) ETS and its VN graph in an LDPC code with column weight \( \gamma \) fulfill the following conditions.

(a) If \( \frac{b}{\gamma} < 1 \), then a Tanner graph with girth 6 contains no \((a, b)\) ETSs with \( a \leq \gamma \).

(b) If the VN graph contains \(|E|\) edges, then \( b = a\gamma - 2|E|\).

Theorem 2: Let a Tanner graph with girth 6 and \( \gamma \)-degree variable nodes be given. Then, in an \((a, b)\) ETS in which the 8-cycles are all chordless

- the number \(|E|\) of edges of the VN graph satisfies the inequality \(|E| \leq \frac{a^2}{4a - 3}\); and
- the parameters \(a, b, \gamma\) satisfy the inequality \( b \geq a\gamma - \frac{2a^2}{4a - 3}\), and if \( b < a \), then \( a \geq 2\gamma - 2\).

Proof: If we include all triangle-free VN graphs of \((a, b)\) ETSs in a set \( R \) and put all VN graphs of ETSs in which 8-cycles are all chordless in a set \( Y \), then \( R \subset Y \). The VN graph with the maximum number of edges in the set \( R \), which we call the largest VN graph in \( R \), belongs to the set \( Y \) too since a triangle-free VN graph is also a VN graph free of 8-cycles-wc. Thus, the number of edges of the largest VN graph in \( Y \) is at least the number of edges of \(|E|\) of an \((a, b)\) ETS free of 8-cycles-wc, we have \(|E| \geq \frac{a^2}{4a - 3}\). On the other hand, since the VN graph of an \((a, b)\) ETS in which the 8-cycles are all chordless is \( K_4 \)-free, its maximum number of edges is \( a^2 \). Consequently, the largest VN graph containing triangles of an \((a, b)\) ETS in which any 8-cycles do not have a chord satisfies \( \frac{a^2}{4a - 3} < |E| \leq \frac{a^2}{2} \). Hence, according to Lemma 2, the number of triangles in this VN graph with the maximum number of edges \(|E|\) is at least \( \frac{a^2}{2} - a^2 \).

Since the VN graph is free of the graphs in Fig. 2 \((a) \) and \((b) \), no two triangles in the VN graph have an edge in common. In fact, all triangles in the VN graph are edge-disjoint. Thus, the maximum number of triangles is \( \frac{|E|}{3} \). Since the number of triangles is at least \( \frac{a^2}{2} - a^2 \) and the VN graph may contain the maximum number of triangles which is \( \frac{|E|}{3} \), we have \(|E| \geq \frac{a^2}{2} - a^2 \).

This yields \(|E| \leq \frac{a^2}{4a - 3}\). Hence, using equality \( b = a\gamma - 2|E| \) we have \( b \geq a\gamma - \frac{2a^2}{4a - 3} \). Now, if \( b < a \), then we have \( 1 > b > \frac{a}{\gamma} > \gamma - \frac{2a^2}{4a - 3} \). Implies

\[
2a(a + 2 - 2\gamma) > 3 - 3\gamma.
\]
In the left-hand side of inequality (2) we substitute $a$ by $2\gamma - 3$ which implies

$$2a(a + 2 - 2\gamma) = 2(2\gamma - 3)/(2\gamma - 3 + 2 - 2\gamma) = (4\gamma - 6)(-1).$$

Therefore, inequality (2) for $a = 2\gamma - 3$ is $(4\gamma - 6)(-1) > 3 - 3\gamma$ which yields $\gamma < 3$. This proves that inequality (2) is not satisfied if $\gamma \geq 4$ and $a = 2\gamma - 3$.

For $\gamma = 1, 2, 3$, using the inequality $a \geq \gamma + 1$ from Lemma 3 (a), we have $a \geq 2, a \geq 3, a \geq 4$, respectively. Hence, for each $\gamma$ we have $a \geq 2\gamma - 2$. 

The results of Theorem 2 can be also extended to irregular LDPC codes as follows.

**Corollary 1:** Let an irregular LDPC code with girth 6, column weights $\{d_1, \ldots, d_t\}$ and free of 8-cycles-wc be given where the minimum variable node degree is $d_1 = \gamma$. The lower bound on the smallest size of an $(a, b)$ ETS, $b < a$, is $2\gamma - 2$.

**Proof:** The proof is given in Appendix A.

In Table I, using Theorem 2, we present the lower bound on the size of an ETS for an LDPC code with $3 \leq \gamma \leq 6$ and $g = 6$ in which the 8-cycles are all chordless. In this table, for different values of parameters $\gamma$ and $b$, we also compare the lower bound on the size of $(a, b)$ ETSs for girth-6 LDPC codes whose 8-cycles are all chordless with the minimum size of $(a, b)$ ETSs for girth-6 LDPC codes in [30] which are presented in the last row of Table I. By this comparison, we conclude that eliminating 8-cycles-wc causes the removal of small size ETSs which are also removed by eliminating all 6-cycles. Thus, to remove small size ETSs we do not need to remove all 6-cycles; the removal of 8-cycles-wc results in the desired consequences. We provide a detailed explanation for $\gamma = 3, 4$ in Examples 4, 5.

**Example 4:** Let $\gamma = 3$. For different values of $b$, we find the smallest size of an ETS containing at least one 6-cycle and free of an 8-cycle-wc. Suppose $b = 0$, then the smallest $a$ satisfying $b \geq 3a - \frac{2a^3}{3a - 3}$ is $a = 6$ whose VN graph with the maximum number of edges is in Fig. 2 (c). Thus, for $b = 0$, the bound $b \geq 3a - \frac{2a^3}{3a - 3}$ is tight. However, this is not true for $b = 1, 2$. In fact, although for $b \geq 1$ the smallest $a$ satisfying $1 \geq 3a - \frac{2a^3}{3a - 3}$ is $a = 5$, the minimum $a$ obtained for $b = 1, 2$ is $7$, respectively. The VN graph with the maximum number of edges of a $(7, 1)$ ETS with $g = 6$ and free of an 8-cycle-wc is in Fig. 2 (d). Removing an edge from Fig. 2 (c) results in the VN graph of a $(6, 2)$ ETS. Fig. 2 (c) is the VN graph of a $(5, 3)$ ETS.

The following remark gives us the reason for considering the smallest size of an ETS in a girth-8 LDPC code when obtaining the smallest size of an ETS free of 8-cycles-wc.

**Remark 1:** We suppose that for specific $\gamma$ and $b$ the smallest size of an ETS in a girth-8 Tanner graph is $x$ and the smallest size of an ETS containing 6-cycles but free of an 8-cycle-wc is $y$. Since in a girth-8 Tanner graph all 8-cycles are chordless, both ETSs with sizes $x$ and $y$ are free of 8-cycles-wc. Therefore, if $x < y$, then we consider $x$ as the smallest size of an ETS in which any 8-cycles that appear do not have a chord.

**Example 5:** Let $\gamma = 4$. If $b = 0$, then in a girth-8 LDPC code we have $a \geq 8$; see [30]. Now, we prove that if an ETS in which the 8-cycles are all chordless contains a 6-cycle, then the smallest size is more than 8. Since $b = 0$, all variable nodes of the VN graph have degree 4. Suppose $v_0$ is a variable node connected to four check nodes $c_1, c_2, c_3, c_4$. Since all check nodes have degree 2, each check node is connected to another variable node. Let $v_1$ be connected to $c_i$ for $1 \leq i \leq 4$. Without loss of generality, suppose $v_0, v_1, v_2$ are the variable nodes of a 6-cycle. If a check node connects $v_1$ or $v_2$ to one of the variable nodes $v_3, v_4$, then an 8-cycle-wc is obtained, Fig. 3 (a), which is impossible. Thus, there must be variable nodes $v_5$ and $v_6$ for two different check nodes connected to $v_1$. If there is a check node between $v_2$ and $v_5$, or between $v_2$ and $v_6$, then we have an 8-cycle-wc with variable nodes $v_0, v_1, v_5, v_6$, which is shown in Fig. 3 (b), or $v_0, v_1, v_6, v_2$, respectively. Therefore, there is no check node between $v_2$ and any of the variable nodes $v_3, v_4, v_5, v_6$. Hence, there must be two variable nodes $v_7, v_8$ for two different check nodes connected to $v_2$, Fig. 3 (c). This process guarantees the non-existence of an $(8, 0)$ ETS which contains 6-cycles and its 8-cycles are all chordless. Thus, according to Remark 1, the smallest size of an ETS with $\gamma = 4$ and $b = 0$ in which all 8-cycles are chordless is 8.

In general, in an LDPC code with $g = 6, \gamma = 4$ all $(a, b)$ ETSs, $5 \leq a \leq 8, b \leq 2$, and $(6, 4), (7, 4)$ ETSs which contain 6-cycles have at least one 8-cycle-wc. Fig. 3 (d) and (e) show that there are $(8, 4)$ and $(9, 0)$ ETSs in which the 8-cycles are all chordless and these ETSs contain a 6-cycle. Since an LDPC code with $g = 8, \gamma = 4$ is free of all $(a, b)$ ETSs, $5 \leq a \leq 8, b \leq 2$, and $(6, 4)$ ETSs but contains $(8, 0), (8, 2), (7, 4)$ ETSs, according to Remark 1, the minimum size of an $(a, b)$ ETS whose 8-cycles are all chordless for $b = 0, 2, 4$ is $a = 8, 8, 7$, respectively.

Theorem 3 yields an analytical lower bound on the minimum distance of an LDPC code whose Tanner graph has girth at least 6 and is free of 8-cycles-wc. We know that in an LDPC code with column weight $\gamma$ the lower bound on the minimum distance is $\gamma + 1$ when the girth is at least 6. We analytically prove that eliminating 8-cycles-wc causes an increase in the minimum distance from $\gamma + 1$ to $2\gamma$.

**Theorem 3:** For an LDPC code with column weight $\gamma \geq 3$ and a girth-6 Tanner graph whose 8-cycles are all chordless we have $d_{\min} \geq 2\gamma$.

**Proof:** The proof is given in Appendix B.

It should be noticed that avoiding 8-cycles-wc is not the only way to increase the $d_{\min}$. For example, the lower bound on the minimum distance of a girth-6 LDPC code with column weight 3 is 4, thus for array-based LDPC codes with column weight 3 which have girth 6 we have $d_{\min} \geq 4$. Whereas according to [40], [41], it is possible to construct an array-based LDPC code with $\gamma = 3$ whose Tanner graph contains 8-cycles-wc and the code has $d_{\min} = 6$.
TABLE I  
LOWER BOUNDS ON THE SIZE OF (a, b) ETSs OF VARIABLE-REGULAR LDPC CODES WITH 3 ≤ γ ≤ 6 in WHICH THE 8-CYCLES ARE ALL CHORDLESS. THE SIGN “−” IN A COLUMN INDICATES THAT FOR THE b AND γ OF THAT COLUMN THERE IS NO ETS. THE LAST ROW GIVES THE MINIMUM SIZE OF AN (a, b) ETS FOR A VARIABLE-LDPC CODE WITH Girth 8

| γ | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 6 | 6 | 6 | 6 | 6 | 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | 0 | 1 | 2 | 3 | 0 | 1 | 2 | 3 | 4 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| a ≥ 6 | 7 | 6 | 5 | 8 | − | 8 | − | 7 | 10 | 11 | 10 | 11 | 9 | 12 | − | 12 | − | 12 | − | 12 | − | 11 |
| a = 6 | 7 | 6 | 5 | 8 | − | 8 | − | 7 | 10 | 11 | 10 | 11 | 9 | 12 | − | 12 | − | 12 | − | 12 | − | 11 |

Fig. 3. Figures (a) and (b) are subgraphs of an (a, 0) ETS with γ = 4 which contain 8-cycles-wc and 6-cycles. Figure (c) is a subgraph of an (a, 0) ETS with γ = 4 which has 6-cycles and is free of an 8-cycle-wc. Figures (d) and (e) are the VN graphs of (8, 4) and (9, 0) ETSs with γ = 6, γ = 4, respectively.

B. Chordless Short Cycles in Tanner Graphs With Girth 8

Now, we present a new lower bound on the \( d_{\text{min}} \) of a protograph-based LDPC code with a column weight \( γ \) and girth 8 in which cycles of lengths up to 12 are all chordless. Then, we give tighter lower bounds on the minimum distances of girth-8 LDPC codes with column weights 3 and 4. To prove Theorem 4 we need some definitions and concepts from graph theory.

Definition 3: An independent set of a graph \( G \) is a set of pairwise non-adjacent vertices. The size of the largest independent set is the independence number denoted by \( α \).

In [42], it is proved that if \( G \) is a triangle-free graph on \( n \) vertices with average degree \( d \) then the independence number of \( G \) is at least \( n \frac{\ln d - d - 1}{(d - 1)^2} \).

Theorem 4: The \( d_{\text{min}} \) of an LDPC code with girth 8 and column weight \( γ \geq 2 \) whose Tanner graph is free of cycles-wc of lengths up to 12 is lower bounded by \( \frac{3(\gamma - 1)^2}{\ln γ - γ + 1} \).

Proof: The proof is given in Appendix C.

In Theorem 5 and its following Remark 2, we prove that avoiding 12-cycles-wc from occurring in the Tanner graph of an LDPC code with girth 8 and \( γ = 3 \) results in a girth-8 LDPC code for which the minimum size of small \((a, b)\) ETSs, \( b < a \), and the lower bound on \( d_{\text{min}} \) are equal to the ones of an LDPC code with girth 10. Thus, without removing all 8-cycles and only by avoiding 12-cycles-wc we can achieve the positive features of a girth-10 LDPC code.

Theorem 5: The smallest \((a, b)\) ETSs, \( b < a \) and \( b = 0, 1, 2, 3 \), in an LDPC code with \( g = 8, γ = 3 \) and free of cycles-wc of lengths up to 12 are \((10, 0), (9, 1), (8, 2), (5, 3)\) ETSs.

Proof: The smallest \((a, b)\) ETSs with \( b < a \) and \( b = 0, 1, 2, 3 \) in an LDPC code with \( g = 8, γ = 3 \) are \((6, 0), (7, 1), (6, 2), (5, 3)\) ETSs; see [30]. According to Lemma 1 part (b), if \( g = 8 \), then the shortest cycle-wc is of length 12. Avoiding 12-cycles-wc causes the removal of all \((6, 0), (7, 1), (6, 2), (8, 0)\) ETSs. Consequently, if \( b < a \), then the smallest ETSs for \( b \leq 3 \) are \((10, 0), (9, 1), (8, 2), (5, 3)\) ETSs.

Remark 2: The smallest \((a, b)\) ETSs with \( b < a \) in the Tanner graph of a girth-8 LDPC code with \( γ = 4 \) is \((7, 4)\) ETS [30]. In Theorem 6, it is proved that avoiding 12-cycles-wc causes the removal of all \((a, b)\) ETSs with \( b < a \) and \( a < 9 \) as well as \((9, b)\) ETSs with \( b < 8 \).

Theorem 6: The smallest \((a, b)\) ETS with \( b < a \) in the Tanner graph of a girth-8 LDPC code with \( γ = 4 \) and free of cycles-wc of lengths up to 12 is \((9, 8)\) ETS.

Proof: If \( b < a \), then in a regular LDPC code with column weight \( γ \) and girth at least 6 the VN graph of an \((a, b)\) ETS must contain at least one variable node of degree \( γ \) [30]. We suppose \( v_1 \) is a variable node with degree 4 whose neighbours in the VN graph of the ETS are \( v_2, v_3, v_4, v_5 \). Because of the non-existence of triangles, no pair of these vertices in the neighbour set of \( v_1 \) is connected. Since the number of variable nodes is at least 7, we suppose that \( v_6 \) is connected to \( v_2, v_3 \) and \( v_7 \) is connected to \( v_4, v_5 \). Clearly, the existence of a 12-cycle-wc in an ETS is equivalent to the existence of a 6-cycle-wc in the VN graph of that ETS. Thus, as shown in Fig. 4 (a), connecting one of the variable nodes \( v_2, v_3 \) to \( v_7 \) or one of \( v_4, v_5 \) to \( v_6 \) causes a 6-cycle-wc. Consequently, to construct the VN graph of an ETS satisfying the desired conditions, we need to add other nodes. Suppose, \( v_8 \) is a new variable node connected to both \( v_2, v_3 \); see Fig. 4 (b). Now, we take the induced subgraph of Fig. 4 (b) on the variable nodes, \( v_1, v_2, v_3, v_6, v_8 \). As shown in Fig. 4 (c), connecting a variable node outside the induced subgraph such as \( v \) to both \( v_6, v_8 \) causes a 6-cycle-wc. Therefore, we can only connect \( v_7 \) to one of the variable nodes \( v_6, v_8 \). We suppose that \( v_7 \) is
connected to $v_8$; see Fig. 4 (d). The obtained VN graph up to now is with regard to an $(8,10)$ ETS. In order to construct the VN graph of an $(a,b)$ ETS with $b < a$, we have to add another variable node to the graph in Fig. 4 (d). The only option we have is to connect $v_9$ to $v_4, v_5$. According to the above explanation, we can connect $v_9$ to only one of $v_4, v_5$. Since the connection between $v_9$ and $v_8$ causes a 6-cycle-wc, we have to connect $v_9$ to $v_6$; see Fig. 4 (e). Hence, the smallest $(a,b)$ ETS obtained with $b < a$ has nine variable nodes.

**Theorem 7:** The minimum sizes of an $(a,b)$ ETS, $b < a$, in an LDPC code with $g = 8, \gamma = 4$ and free of cycles-wc of lengths up to 12 for $b = 0, 2, 4, 6, 8$ are $a = 15, 14, 13, 11, 9$, respectively.

**Proof:** We know, because of the equality $b = a\gamma - 2|E|$, that if $\gamma$ is an even number, then $b$ is also an even number. Thus, for $\gamma = 4$ there is no $(a,b)$ ETS with an odd $b$. As proved in Theorem 6 that if $b = 8$, then the smallest size of an ETS with $b < a$ is $a = 9$. Applying the method we used for the construction of a $(9, 8)$ ETS to any other values of $b = 0, 2, 4, 6$, we obtain the VN graphs shown in Fig. 5.

**Remark 3:** The $d_{\text{min}}$ of an LDPC code with $g = 8, \gamma = 4$ and free of cycles-wc of lengths up to 12 is lower bounded by 15. Indeed, according to Theorem 7 and the proof of Theorem 3, the minimum sizes of an $(a,0)$ ETS and an $(a,0)$ non-elementary trapping set are 15 and 16, respectively. Thus, $d_{\text{min}} \geq 15$.

IV. DESIGNS AND EXAMPLES FOR CODES WITH GIRTH 6

In Section IV, we present a necessary and sufficient condition to construct protograph-based LDPC codes with girth 6 in which 8-cycles are all chordless. The proposed condition is applicable to both simple and multi-edge protographs.

As explained in Section II, in a protograph-based QC-LDPC code with a fully-connected $\gamma \times n$ exponent matrix $B$ if the lifting degree is $N$, then the size of the search space for $B$ is $N^{\gamma n}$. In order to reduce the size of the search space we apply our method to the exponent matrix of a compact QC-LDPC code and the exponent matrix of an array-based LDPC code which are stated in Definition 4; see [14], and Definition 5, respectively. These types of exponent matrices considerably contribute to reducing the size of the search space to $(N-2)^{\gamma+n-4}$. The computational complexity to obtain exponent matrices also reduces, especially for large $n$ and $N$.

**Definition 4:** Let $n,N$ be positive integers with $N > n$, $\bar{0}$ be an all-zero column vector of size $\gamma$, $B_{\bar{0}} = [0,1,b_{21},\ldots,b_{(\gamma-1)}]^T$ be a $\gamma$-entry column vector, where for $2 \leq i \leq \gamma - 1$, $b_{ij} \in \{2,\ldots,N-1\}$, and $T$ represents the transpose. The following $\gamma \times n$ exponent matrix $B = [\bar{0} B_{\bar{1}} B_{\bar{2}} \cdots B_{\bar{n-1}} B_{\bar{1}}]$

(3)

gives a compact QC-LDPC code with lifting degree $N$, where $\gamma_j \otimes B_{\bar{1}}$ with $\gamma_j \in \{2,\ldots,N-1\}$, $\gamma_j < \gamma_j+1$ is the $j$-th column vector of $B$ and $\otimes$ denotes the multiplication modulo $N$.

Let $p$ be a prime number. The set $\{0,1,\ldots,p-1\}$ forms a finite field $\mathbb{F}_p$ with modulo $p$ addition and multiplication. Such a field is a prime field.

**Definition 5:** Given a prime field $\mathbb{F}_p$, any $\gamma \times n$ submatrix of a $p \times p$ matrix $W_p$ with $[W_p]_{ij} = i \cdot j \pmod{p}$ yields an exponent matrix of an array-based LDPC code.

It is important to notice that when $N$ is a prime number, then $B$ in Equation (3) is also an exponent matrix of an array-based LDPC code.

The VN graph of an 8-cycle-wc, which is shown in Fig. 1 (b), consists of two triangles that have one edge in common. Each triangle in the VN graph corresponds to a 6-cycle-wc in the Tanner graph. Thus, a necessary and sufficient condition to remove an 8-cycle-wc with a VN graph in Fig. 1 (b) is to avoid the occurrence of two 6-cycles that share one check node and two variable nodes connected to that check node. The constraints to avoid these 6-cycles for QC-LDPC codes with a simple protograph, QC-LDPC codes with compact exponent matrices, array-based LDPC codes, and multi-edge QC-LDPC codes are given in Subsections IV-A, IV-B, IV-C, and IV-D, respectively. We propose a condition for the exponent matrix to provide an explicit technique to avoid these 8-cycles-wc.

A. QC-LDPC Codes With Simple Protographs and Tanner Graphs in Which 8-Cycles Are All Chordless

When checking 6-cycles by Equation (1), if two equations with zero in their right-hand side (equivalent to two 6-cycles) have one equal term like $b_{ij} = b_{ij}$ for $W_{ij} = 1$ and $B_{ij} = 0$ for $W_{ij} = 0$ all $3 \times 3$ and $3 \times 4$ submatrices of $B$ have to be checked. In fact, when checking 6-cycles, the existence of a common term $b_{ij} = b_{ij}$ in two equations regarding 6-cycles proves that there are two $3 \times 3$ submatrices of $B$ each of which has two column indices $j_1$ and $j_2$. There are two cases for the third column indices.
If the third column indices of these submatrices are equal to $j_3$, then the 8-cycle-wc occurs in a $3 \times 3$ submatrix of $B$ with column indices $j_1, j_2, j_3$. Thus, all $3 \times 3$ submatrices of the exponent matrix have to be checked for 8-cycles-wc.

If the third column index of one of $3 \times 3$ submatrices is $j_3$ and of another is $j_4$, then the 8-cycle-wc occurs in a $3 \times 4$ submatrix of $B$ with column indices $j_1, j_2, j_3, j_4$. Thus, all $3 \times 4$ submatrices of the exponent matrix have to be checked for avoiding 8-cycles-wc.

**Definition 6:** For each $3 \times 3$ submatrix of $B$, we consider a 6-entry vector $\mathbf{e} = [e_1, e_2, \ldots, e_6]$ using the following six equations regarding Equation (1) to check 6-cycles in the $3 \times 3$ submatrix

1. $((b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_1})) = e_1$,
2. $((b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_1})) = e_2$,
3. $((b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_1})) = e_3$,
4. $((b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_1})) = e_4$,
5. $((b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_1})) = e_5$,
6. $((b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_3j_3} - b_{i_3j_1})) = e_6$.

**Example 6:** Consider the exponent matrix of the $(3,4)$-regular QC-LDPC code given in Example 3. The exponent matrix has four $3 \times 3$ submatrices. For each submatrix, we obtain its 6-entry vector. This vector for a $3 \times 3$ submatrix with column indices $j_1 = 0, j_2 = 1, j_3 = 2$ is $\mathbf{e} = (1, 4, 0, 0, 4, 1)$, for $j_1 = 0, j_2 = 1, j_3 = 3$ it is $\mathbf{e} = (4, 0, 1, 1, 0, 4)$, for $j_1 = 0, j_2 = 2, j_3 = 3$ it is $\mathbf{e} = (0, 3, 2, 2, 3, 0)$ and for $j_1 = 1, j_2 = 2, j_3 = 3$ it is $\mathbf{e} = (2, 0, 3, 3, 0, 2)$.

It is clear that to have an 8-cycle-wc from a $3 \times 3$ submatrix, its corresponding 6-entry vector should have at least two zeros.

**Theorem 8:** A necessary and sufficient condition to avoid an 8-cycle-wc in each $3 \times 3$ submatrix of $B$ is that its equivalent 6-entry vector $\mathbf{e}$ does not satisfy any of the following nine equalities:

\[
\begin{align*}
(a) \quad & e_1 = e_6 = 0, \\
(b) \quad & e_1 = e_2 = 0, \\
(c) \quad & e_1 = e_4 = 0, \\
(d) \quad & e_2 = e_5 = 0, \\
(e) \quad & e_3 = e_4 = 0, \\
(f) \quad & e_3 = e_4 = 0, \\
(g) \quad & e_3 = e_6 = 0, \\
(h) \quad & e_4 = e_5 = 0, \\
(i) \quad & e_5 = e_6 = 0.
\end{align*}
\] (4)

**Proof:** First, we prove that if one of the equalities $(a)$ to $(i)$ in Equation (4) occurs, then the Tanner graph contains an 8-cycle-wc. For example, if $e_1 = e_2 = 0$, then, since the first two equations in Definition 6 contain a term $(b_{i_1j_1} - b_{i_1j_2})$ or $-(b_{i_2j_2} - b_{i_2j_3})$, these two 6-cycles belong to an 8-cycle-wc. It can be similarly proved that the occurrence of any of the nine equalities in Equation (4) shows the existence of an 8-cycle-wc. Now, we suppose that the Tanner graph contains an 8-cycle-wc from a $3 \times 3$ submatrix of the exponent matrix. Thus, according to the definition of an 8-cycle-wc, the 6-entry vector corresponding to the $3 \times 3$ submatrix of $B$ contains at least two zeros. The number of possibilities for two zeros in the 6-entry vector is $\binom{6}{2} = 15$. However, a pair of zeros in the 6-entry vector results in an 8-cycle-wc in which the left-hand sides of Equation (1) contain a common term. Thus, $e_1 = e_3 = 0$ does not cause an 8-cycle-wc. It is not difficult to check that each pair of zeros that results in an 8-cycle-wc gives one of the equalities in Equation (4).

**Definition 7:** Given a $c \times d$ exponent matrix $B$, for every zero element of a 6-entry vector regarding a $3 \times 3$ submatrix of $B$ with row indices $i_1, i_2, i_3$ we allocate a column-index vector with $c$ elements as follows. The elements in positions $i_1, i_2, i_3$ of this vector are pairs of column indices of $B$ which appear in Equation (1). Other entries of the vector are empty sets which are for the positions corresponding to the row indices of $B$ which are not among the three row indices $i_1, i_2, i_3$ appearing in Equation (1).

For example, if Equation (1) is checked for three rows with indices $1, 3, 4$ of a $4 \times d$ exponent matrix and three columns with indices $j_1, j_2, j_3$, then we assign $e_1 = 0$ to $[(j_1, j_2), (j_2, j_1), (j_1, j_3)]$.

**Theorem 9:** A necessary and sufficient condition to remove an 8-cycle-wc from each $3 \times 4$ submatrix of $B$ is that no two 6-entry vectors of it yield two column-index vectors containing a common pair in the same position.

**Proof:** A $3 \times 4$ submatrix of $B$ contains four $3 \times 3$ submatrices. Among the $3 \times 4$ submatrices, we consider those containing at least two $3 \times 3$ submatrices whose 6-entry vectors have a zero element. Suppose $U$ is a $3 \times 4$ submatrix of $B$, and $V$ and $W$ are two $3 \times 3$ submatrices of $U$ with the above property.

First, we prove that if two column-index vectors contain a common pair in the same position, then the Tanner graph has an 8-cycle-wc. If the column-index vector assigned to a zero from the 6-entry vector of $V$ and the column-index vector allocated to a zero from the 6-entry vector of $W$ have a common pair in the same position, then the left-hand sides of Equation (1) for these 6-cycles have a common term $(b_{ij_1} - b_{ij_2})$ in which $i$ indicates the existence of a common check node in these 6-cycles and $j, j'$ indicate the common variable nodes connected to that check node. Thus, these 6-cycles have a common check node with two common variable nodes connected to that check node and therefore they belong to an 8-cycle-wc.

Now, we suppose that the Tanner graph has an 8-cycle-wc from a $3 \times 4$ submatrix of $B$. Therefore, there are two 6-cycles for which the left-hand sides of Equation (1) contain a common term. If these two 6-cycles belong to one 6-entry vector, then the 8-cycle-wc is from a $3 \times 3$ submatrix of $B$. Hence, these 6-cycles belong to two 6-entry vectors containing a zero. According to Definition 7 there is a column-index vector for each of these 6-cycles. Since these 6-cycles have a common check node with two common variable nodes connected to that check node, their corresponding column-index vectors should have a common pair (which indicates two common variable nodes) appearing in the same position (which is for the common check node connected to those variable nodes).

It is worth noting that Theorem 9 gives a necessary and sufficient condition to avoid 8-cycles-wc in any simple protograph.

**Remark 4:** As considered in Table I and Theorem 3, avoiding 8-cycles-wc from occurring in the Tanner graph of a girth-6 LDPC code causes the removal of small size ETSs as well as increasing the lower bound on $d_{\text{min}}$. For example, for $\gamma = 3$ the elimination of 8-cycles-wc results in the removal of $(a, b)$ ETSs with $a \leq 5, b \leq 2$ and the lower bound on $d_{\text{min}}$ increases from 4 to 6. For $\gamma = 4$, avoiding 8-cycles-wc causes the removal of $(a, b)$ ETSs with $a \leq 8, b \leq 2, (6, 4), (7, 4)$
ETSs and the lower bound on $d_{\text{min}}$ increases from 5 to 8. Thus, a sufficient condition to construct a $(\gamma, n)$-regular QC-LDPC code with $g = 6$ and $d_{\text{min}} \geq 2\gamma$ whose Tanner graph is free of small size $(a, b)$ ETSs, $b < a$, is to apply Theorems 8 and 9 to the exponent matrix.

**B. Compact QC-LDPC Codes With Tanner Graphs Whose 8-Cycles Are All Chordless**

As explained in Section II, to construct an exponent matrix that gives a QC-LDPC code whose Tanner graph has girth 6 and is free of 8-cycles-wc, an exhaustive search algorithm is used. If we use the compact method in Definition 4, which has a fully-connected protograph, the size of the search space is $(N - 2)^{2} + n - 1$ since only the entries of the second column and the second row except for $b_{01}, b_{10}, b_{11}$ have to be obtained. Thus, since the compact method has less complexity and accelerates the process of finding the entries of $B$, we prefer to use this method to propose Algorithm 1 which yields the exponent matrix of a compact QC-LDPC code with girth 6 whose 8-cycles are all chordless. In order to present Algorithm 1 we need Lemma 4 and Theorem 10 which are given below. Lemma 4 is obtained by applying Theorem 8 to each $3 \times 3$ submatrix of an exponent matrix of a compact QC-LDPC code. In Theorem 10, we provide a necessary and sufficient condition to avoid 8-cycles-wc from occurring in a $3 \times 4$ submatrix of an exponent matrix of a fully-connected QC-LDPC code. Theorem 10 can be also used for the compact method. Hence, Algorithm 1 is only applicable to a compact QC-LDPC code since it is based on Lemma 4 and Theorem 10 where Lemma 4 is only applicable to the compact method.

**Lemma 4.** Let an exponent matrix $B$ of a compact QC-LDPC code be given by a vector of coefficients $[0, 1, \gamma_2, \ldots, \gamma_{n-1}]$ and a vector $\vec{B}_1$. If for each three elements $x, y, z \in \vec{B}_1$ and $0 \leq i, j \leq n - 1$, the terms $(2x - y - z)(\gamma_i - \gamma_j), (2y - x - z)(\gamma_i - \gamma_j)$, and $(2z - x - y)(\gamma_i - \gamma_j)$ are nonzero modulo $N$, then no $3 \times 3$ submatrix of $B$ causes an 8-cycle-wc.

**Proof.** We suppose that the terms mentioned in the lemma are nonzero and the Tanner graph has an 8-cycle-wc from a $3 \times 3$ submatrix of $B$. Then, according to Theorem 8, the corresponding 6-entry vector contains at least two zeros and at least one of the equalities in Equation (4) is satisfied.

We let the entries of the $3 \times 3$ submatrix of $B$ be $s \cdot t \pmod{N}$, where $s \in \{x, y, z\}$ and $t \in \{\gamma_i, \gamma_j, \gamma_k\}$. We show that each equality in Equation (4) results in one of the equations $(2x - y - z)(\gamma_i - \gamma_j) \equiv 0 \pmod{N}$, $(2y - x - z)(\gamma_i - \gamma_j) \equiv 0 \pmod{N}$, or $(2z - x - y)(\gamma_k - \gamma_i) \equiv 0 \pmod{N}$ for $0 \leq i, j \leq n - 1$. We cannot have $2x - y - z = 0$, $2y - x - z = 0$, or $2z - x - y = 0$ for $0 \leq i, j \leq n - 1$, which contradicts our assumption. Let the 6-entry vector satisfy $e_1 = e_6 = 0$. From $e_1 = (x\gamma_i - x\gamma_j) + (y\gamma_j - y\gamma_k) + (z\gamma_k - z\gamma_i) \equiv 0$, and $e_6 = (x\gamma_j - x\gamma_i) + (y\gamma_j - y\gamma_k) + (z\gamma_k - z\gamma_i) \equiv 0$, we conclude that $e_1 - e_6 = (2x - y - z)(\gamma_i - \gamma_j) \equiv 0$. If $e_1 = e_2 = 0$, then from $e_1 = 0$ and $e_2 = (x\gamma_j - x\gamma_i) + (y\gamma_j - y\gamma_k) + (z\gamma_k - z\gamma_i) \equiv 0$ we have $e_1 - e_2 = (2y - x - z)(\gamma_i - \gamma_j) \equiv 0$. If $e_2 = e_4 = 0$, then from $e_2 = 0$ and $e_4 = (x\gamma_j - x\gamma_i) + (y\gamma_j - y\gamma_k) + (z\gamma_k - z\gamma_i) \equiv 0$ we have $e_1 - e_4 = (2z - x - y)(\gamma_k - \gamma_i) \equiv 0$. Similarly, we can continue this process for other equalities in Equation (4).

Thus, if for each pair of coefficients $\gamma_i$ and $\gamma_j$ the terms in the lemma are nonzero modulo $N$, then $3 \times 3$ submatrices of $B$ are free of 8-cycles-wc.

In Theorem 10 we assume that the right-hand side of Equation (1) regarding a $2 \times 2$ submatrix of $B$ with row indices $i_1, i_2$ and two column indices $j_1, j_2$ is denoted by $q_{i_1, i_2, j_1, j_2}$. Theorem 10: A necessary and sufficient condition to avoid 8-cycles-wc from occurring in any $3 \times 4$ submatrix of the exponent matrix $B$ of a fully-connected QC-LDPC code with girth 6 is that for every two rows of $B$ with indices $i, i'$ and four columns with indices $j, j', k, k'$ we have $q_{i, i', j, j', k, k'} \neq 0 \pmod{N}$, where $j, j', k, k'$ are four two-by-two distinct column indices.

**Proof:** Without loss of generality, we assume that the following submatrix of $B$

\[
\begin{bmatrix}
 b_{i_1 j_1} & b_{i_1 j_2} & b_{i_1 j_3} & b_{i_1 j_4} \\
 b_{i_2 j_1} & b_{i_2 j_2} & b_{i_2 j_3} & b_{i_2 j_4} \\
 b_{i_3 j_1} & b_{i_3 j_2} & b_{i_3 j_3} & b_{i_3 j_4} \\
 b_{i_4 j_1} & b_{i_4 j_2} & b_{i_4 j_3} & b_{i_4 j_4}
\end{bmatrix}
\]

contains two 6-cycles one from columns with indices $j_1, j_2, j_3$ and the other from columns with indices $j_1, j_2, j_4$ whose equations from Equation (1) share the term $(b_{i_1 j_1} - b_{i_2 j_2})$. Each of these equations contains six entries. If they have more than two elements in common, then the Tanner graph contains a 4-cycle, which contradicts the assumptions. For example, we let the equations of 6-cycles be

\[
(b_{i_3 j_1} - b_{i_3 j_2}) + (b_{i_2 j_2} - b_{i_2 j_3}) + (b_{i_1 j_3} - b_{i_1 j_4}) \equiv 0, \quad (6)
\]

\[
(b_{i_3 j_1} - b_{i_3 j_2}) + (b_{i_2 j_2} - b_{i_2 j_4}) + (b_{i_1 j_4} - b_{i_1 j_1}) \equiv 0. \quad (7)
\]

By subtracting the left-hand sides of Equations (6) and (7), we obtain $-b_{i_2 j_3} + b_{i_1 j_3} + b_{i_2 j_4} - b_{i_1 j_4} \equiv 0$. This equation proves the existence of a 4-cycle from the rows with indices $i_1, i_2$ and columns with indices $j_1, j_4$.

Thus, we assume that the $3 \times 4$ submatrix in (5) contains two 6-cycles whose equations from (1) share two entries, the common term $(b_{i_3 j_1} - b_{i_3 j_2})$. If two 6-cycle equations containing $(b_{i_3 j_1} - b_{i_3 j_2})$ are as follows,

\[
(b_{i_3 j_1} - b_{i_3 j_2}) + (b_{i_2 j_2} - b_{i_2 j_3}) + (b_{i_1 j_3} - b_{i_1 j_4}) \equiv 0, \quad (8)
\]

\[
(b_{i_3 j_1} - b_{i_3 j_2}) + (b_{i_2 j_2} - b_{i_2 j_4}) + (b_{i_1 j_4} - b_{i_1 j_1}) \equiv 0, \quad (9)
\]

then by subtracting the left-hand sides of Equations (8) and (9), we obtain

\[
[(b_{i_2 j_2} - b_{i_1 j_4}) + (b_{i_1 j_3} - b_{i_2 j_3})] - [(b_{i_1 j_3} - b_{i_2 j_3}) + (b_{i_2 j_4} - b_{i_1 j_4})]
\]

which is $q_{i_1, i_2, j_1, j_3} - q_{i_1, i_2, j_2, j_4} \equiv 0$ or $q_{i_1, i_2, j_1, j_3} - q_{i_1, i_2, j_3, j_4} \equiv 0$. We obtain similar results when considering other terms as the common term in the equations of two 6-cycles from the above $3 \times 4$ submatrix of $B$. These equalities prove that the existence of an 8-cycle-wc in a $3 \times 4$ submatrix of $B$ is equivalent to the existence of an equality $q_{i, i', j, j'} \equiv 0 \pmod{N}$, where $i, i' \in \{i_1, i_2, i_3\}$ and $j, j', k, k'$ are two-by-two distinct values in $\{j_1, j_2, j_3, j_4\}$.

As mentioned before, Algorithm 1 is a greedy search algorithm based on Lemma 4 and Theorem 10 to construct an exponent matrix of a compact QC-LDPC code whose Tanner graph has girth 6 and 8-cycles are all chordless. In this algorithm, the first column of the exponent matrix $B$ is
all-zero and other columns of $B$ are obtained gradually in $n - 1$ steps by checking Lemma 4 and Theorem 10 for the obtained exponent matrix $B'$ in each step.

**Algorithm 1: Greedy search algorithm to avoid 8-cycles-wc**

**Input:** $\gamma, n, N$

**Output:** A coefficient vector $\Gamma = [0, 1, \gamma_2, \ldots, \gamma_{n-1}]$ and $B_1 = [0, 1, b_2, \ldots, b_{(n-1)}]

All computations are modulo $N$

put $\Gamma = [0, 1], n' = 2, \gamma_0 = 0, \gamma_1 = 1$;
while $n' < n$ do
pick $\gamma_{n'}$ from $[2, N - 1]$ such that $\gamma_{n'} > \gamma_\ell$ for $0 \leq \ell < n'$;
for $k = 2$ to $N - 1$ do
put $C_2 = [0, 1]$;
if for $\gamma_\ell, \gamma_j \in \Gamma$, $(1 - 2k)(\gamma_\ell - \gamma_j) \neq 0$ and $(k - 2)(\gamma_\ell - \gamma_j) \neq 0$ and $(k + 1)(\gamma_\ell - \gamma_j) \neq 0$ then
$C_2 + = [k]$;
if $|C_2| \geq \gamma$ then
pick $B_1 = (0, 1, b_2, \ldots, b_{(n-1)})$ from $C_2$;
if for $x, y, z \in B_1$ and $\gamma, \gamma_j \in \Gamma$ we have $\langle x + y - 2z \rangle(\gamma - \gamma_j) \neq 0$, $\langle x + z - 2y \rangle(\gamma - \gamma_j) \neq 0$, and $\langle y + z - 2x \rangle(\gamma - \gamma_j) \neq 0$ then
$B' = [0, 1, b_2, \ldots, b_{(n-1)}] \otimes \Gamma$;
if $B'$ satisfies Theorem 10, then
$\Gamma + = [\gamma_{n'}]$;
$n' + 1$;
if $n' < n$ then
return $\Gamma$
else if $n' = n$ then
return $\Gamma$ and $B_1$.

1) Computational Complexity of Algorithm 1: We measure the cost of Algorithm 1 in the number of arithmetic operations, that is, “+”, “−”, “×”, and “≡”. The computational complexity of avoiding 8-cycles-wc is less than that of avoiding all 6-cycles (raising the girth). In fact, the number of operations to avoid 4-cycles and 6-cycles by checking Equation (1) in a $\gamma \times n$ exponent matrix is

$$5 \times \binom{\gamma}{2} \binom{n}{2} + 6 \times 7 \times \binom{\gamma}{3} \binom{n}{3}.$$  

(10)

Whereas, the number of operations to avoid 4-cycles and 8-cycles-wc is

$$5 \times \binom{\gamma}{2} \binom{n}{2} + 3 \times 6 \times \binom{\gamma}{3} \binom{n}{2} + \binom{\gamma}{2} \binom{n}{2} \binom{n-2}{2},$$  

(11)

where $3 \times 6 \times \binom{\gamma}{3} \binom{n}{2}$ comes from Lemma 4 and $\binom{\gamma}{2} \binom{n}{2} \binom{n-2}{2}$ comes from Theorem $\gamma$.

In general, from comparing the number of operations to check Equation (1) between an exponent matrix with girth 8 and an exponent matrix with girth 6 and free of 8-cycles-wc, we conclude that for each $\gamma$ and $n$ satisfying $\binom{\gamma}{2}(\gamma - 2)(n - 2) - 3(\gamma - 2) - \binom{n-2}{2} < 0$ the number of operations to avoid 4-cycles and 6-cycles is larger than the one to obtain a girth-6 QC-LDPC code free of 8-cycles-wc. Thus, as shown in Table II, for $\gamma = 3$ and $n \leq 10$ the number of operations when using Equation (10) is larger than the number of operations when using Equation (11). In Table II, we also compare the computational complexity of our method with the one which is proposed in [29] (Algorithm B). In Table I of [29] the number of operations to construct a $(3, n)$-regular QC-LDPC code with girth 8 and $4 \leq n \leq 12$ is provided. According to the comparison in Table II, for $\gamma = 3$ and $n \leq 7$ the number of operations when using Equation (11) is less than the number of operations when using Algorithm B in [29]. For all these cases, it should be noted that, as shown in Table IV, our method implies a code with a shorter length than the one in [29].

In Table III, we apply Equation (10) and Equation (11) to compact exponent matrices with column weights 4 and 5 and different row weights. In all cases, the number of operations when using Equation (11) is less than the number of operations when using Equation (10).

2) Exponent Matrices of Compact QC-LDPC Codes: In Table IV, using Algorithm 1, we provide exponent matrices $B$ for compact QC-LDPC codes with $g = 6$, column weights 3 and 4, and row weights less than 10. As shown in Table IV, using the compact technique and Algorithm 1 it takes the search algorithm less than 10 seconds to find each exponent matrix. We also in Table V present exponent matrices of compact QC-LDPC codes with column weight 3 and large row weights $10 \leq n \leq 18$, with column weight 4 and large row weights $10 \leq n \leq 12$ as well as with column weight 5 and row weights $n = 6, 7, 8$. We take the lifting degree achieved for each $n$ as an upper bound on $N$ of a $(\gamma, n)$-regular QC-LDPC code with the shortest length, $g = 6$, and a Tanner graph whose 8-cycles are all chordless. In each case, we only present the second row of $B$ as well as $B_1$.

Now using the numerical results in Tables IV, V and Remark 4 as well as analytical results in Lemma 4 and Theorem 10 we present the advantages of avoiding 8-cycles-wc over avoiding all 6-cycles.

- The length of a QC-LDPC code with girth 6 whose 8-cycles are all chordless is less than the length of a QC-LDPC code with girth 8. In the last column of Tables IV and V, it is shown that in all cases the obtained lifting degree for a $(\gamma, n)$-regular QC-LDPC code with girth 6 and free of 8-cycles-wc is much less than the lifting degree of a $(\gamma, n)$-regular QC-LDPC code with girth 8.

- Without increasing the girth from 6 to 8, the resulting codes from Algorithm 1 inherit the useful features of an LDPC code with girth 8 such as the non-existence of small size ETSs (Remark 4) and a better lower bound on $d_{\text{min}}$. For example, as it can be seen in Table IV, for $\gamma = 3$ and $n = 5, 7, 8, 9$, avoiding 8-cycles-wc results in girth-6 codes whose minimum distances are equal to the maximum minimum distances reported in [29] and [10] for girth-8 QC-LDPC codes with the same degree distribution. Moreover, for $\gamma = 4$ and $n = 6, 7$, the minimum distances of girth-6 codes free of 8-cycles-wc (consequently free of small size ETSs) are larger than those with $g = 8$. The minimum distances of all the codes were found using the “MinimumDistance” command in MAGMA.

### C. Array-Based LDPC Codes With Tanner Graphs Whose 8-Cycles Are All Chordless

According to Definition 5, if $p$ is a prime number, then any submatrix of a $p \times p$ matrix $W_p$ with entries $[W_p]_{ij} = i \cdot j$
TABLE II
COMPARISON OF THE NUMBER OF OPERATIONS TO CONSTRUCT A (3, n)-REGULAR QC-LDPC CODE WHEN WE REMOVE ALL 4-CYCLES AND 6-CYCLES (USING EQUATION (10)), WHEN WE AVOID 4-CYCLES AND 8-CYCLES-WC FROM OCCURRING IN THE TANNER GRAPH (USING EQUATION (11)), AND WHEN WE USE ALGORITHM B IN [29]. THE SIGN "—" IN A COLUMN INDICATES THAT FOR THE n OF THAT COLUMN THERE IS NO NUMERICAL RESULTS IN [29]

| (γ, n) | (3, 4) | (3, 5) | (3, 6) | (3, 7) | (3, 8) | (3, 9) | (3, 10) | (3, 11) | (3, 12) | (3, 13) | (3, 14) | (3, 15) | (3, 16) |
|--------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| Equation (10) | 308 | 608 | 1015 | 1528 | 2152 | 2848 | 3741 | 4712 | 5805 | — | — | — | — |
| Equation (11) | 258 | 570 | 1065 | 1575 | 2172 | 2872 | 3765 | 4755 | 5845 | 6930 | 7920 | 8910 | 9900 |

TABLE III
COMPARISON OF THE NUMBER OF OPERATIONS TO CONSTRUCT A (γ, n)-REGULAR COMPACT QC-LDPC CODE WHEN WE REMOVE ALL 4-CYCLES AND 6-CYCLES (USING EQUATION (10)) AND WHEN WE AVOID 4-CYCLES AND 8-CYCLES-WC FROM OCCURRING IN THE TANNER GRAPH (USING EQUATION (11))

| (γ, n) | (4, 5) | (4, 6) | (4, 7) | (4, 8) | (4, 9) | (4, 10) | (4, 11) | (4, 12) | (4, 13) | (4, 14) | (4, 15) | (4, 16) |
|--------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| Equation (10) | 1990 | 3810 | 6510 | 10248 | 15192 | 21310 | 29370 | 38490 | 50388 | 63882 | 79590 | 97680 |
| Equation (11) | 1200 | 2070 | 3402 | 5376 | 8208 | 12150 | 17490 | 25552 | 33696 | 45318 | 59890 | 77760 |

TABLE IV
AN EXPONENT MATRIX B OF A (γ, n)-REGULAR COMPACT QC-LDPC CODE FREE OF 8-CYCLES-WC, WITH γ = 6 AND MINIMUM N WHOSE d_min IS COMPARED TO THE HIGHEST d_min OF THE CODE WITH γ = 8 IN [10] AND [29]. THE MINIMUM LIFTING DEGREE N AND THE HIGHEST d_min FROM [10] AND [29] ARE PRESENTED IN THE LAST COLUMN

| γ, n | Second row of B | B_1 | N | d_min | Runtime | N, d_min, γ = 8 |
|------|----------------|-----|---|-------|---------|----------------|
| 3.5  | 0, 1, 2, 4, 7, 10 | 0, 1, 3 | 10 | 0.03 | 13, 10 |
| 3.6  | 0, 1, 2, 3, 5, 8 | 0, 1, 4 | 8 | 0.14 | 18, 10 |
| 3.7  | 0, 1, 2, 4, 7, 15, 16 | 0, 1, 8 | 10 | 0.31 | 21, 10 |
| 3.8  | 0, 1, 2, 3, 5, 7, 12, 13 | 0, 1, 4 | 8 | 0.76 | 25, 8 |
| 3.9  | 0, 1, 2, 3, 5, 7, 12, 13, 16 | 0, 1, 4 | 8 | 0.75 | 30, 8 |
| 4.5  | 0, 1, 2, 4, 7 | 0, 1, 3, 9 | 13 | 0.5 | 23, 24 |
| 4.6  | 0, 1, 2, 3, 6, 11 | 0, 1, 4, 5 | 17 | 0.43 | 24, 8 |
| 4.7  | 0, 1, 2, 3, 5, 7, 14 | 0, 1, 4, 5 | 19 | 0.62 | 30, 12 |
| 4.8  | 0, 1, 2, 3, 5, 7, 12, 13 | 0, 1, 4 | 10 | 0.75 | 39, 12 |
| 4.9  | 0, 1, 2, 3, 5, 7, 12, 13, 16 | 0, 1, 4, 5 | 10 | 0.75 | 48, 12 |

TABLE V
AN EXPONENT MATRIX B OF A (γ, n)-REGULAR COMPACT QC-LDPC CODE FREE OF 8-CYCLES-WC, WITH γ = 6 AND MINIMUM N WHICH IS COMPARED TO THE MINIMUM N OF A QC-LDPC CODE WITH γ = 8 IN [10]. THE MINIMUM N FROM [10] IS IN THE LAST COLUMN

| γ, n | Second row of B | B_1 | N, γ = 8 |
|------|----------------|-----|---------|
| 3.10 | 0, 1, 2, 3, 4, 6, 8, 11, 12, 16 | 0, 1, 5 | 21, 35 |
| 3.11 | 0, 1, 2, 3, 4, 5, 7, 9, 12, 13, 17 | 0, 1, 6 | 31, 41 |
| 3.12 | 0, 1, 2, 4, 9, 10, 12, 15, 19, 21, 31, 32 | 0, 1, 3 | 35, 45 |
| 3.13 | 0, 1, 2, 4, 7, 8, 9, 11, 14, 16, 18, 22, 34, 35, 36 | 0, 1, 3 | 43, 50 |
| 3.14 | 0, 1, 2, 4, 7, 8, 9, 11, 14, 15, 16, 21, 34, 35, 36 | 0, 1, 3 | 47, 57 |
| 3.15 | 0, 1, 2, 4, 7, 8, 9, 11, 14, 15, 16, 18, 22, 34, 35, 36, 41 | 0, 1, 3 | 53, 63 |
| 3.16 | 0, 1, 2, 4, 7, 8, 9, 11, 14, 15, 16, 18, 19, 41, 43, 47 | 0, 1, 3 | 59, 71 |
| 3.17 | 0, 1, 2, 4, 7, 8, 9, 11, 14, 15, 16, 18, 34, 35, 36, 41, 43, 47 | 0, 1, 3 | 61, 79 |
| 3.18 | 0, 1, 2, 4, 7, 8, 9, 11, 15, 18, 20, 23, 32, 41, 47, 49, 51, 62, 63 | 0, 1, 3 | 67, 88 |
| 4.10 | 0, 1, 2, 4, 7, 8, 9, 13, 17, 23 | 0, 1, 3, 4 | 37, 57 |
| 4.11 | 0, 1, 2, 4, 7, 8, 9, 13, 22, 25, 28 | 0, 1, 3, 4 | 47, 67 |
| 4.12 | 0, 1, 2, 4, 7, 12 | 0, 1, 3, 4, 9 | 19, 35 |

(\text{mod } p) represents an exponent matrix of an array-based LDPC code. We implement Theorems 8 and 9 to the exponent matrix of this code. As a result, necessary and sufficient conditions to remove 8-cycles-wc from the Tanner graph of array-based LDPC codes are simplified. Moreover, we use the obtained constraints to construct new codes with column weight 6, girth 6, and free of 8-cycles-wc.

**Lemma 5:** Given a $3 \times 3$ submatrix of $W_p$ with row indices $i_1, i_2, i_3$, the corresponding Tanner graph is free of 8-cycles-wc if $(2i_1 - i_2 - i_3), (2i_2 - i_1 - i_3),$ and $(2i_3 - i_1 - i_2)$ are not divisible by $p$.

**Proof:** Suppose $(2i_1 - i_2 - i_3) \not\equiv 0 \pmod{p}, (2i_2 - i_1 - i_3) \not\equiv 0 \pmod{p},$ and $(2i_3 - i_1 - i_2) \not\equiv 0 \pmod{p}$ but the $3 \times 3$ submatrix of $W_p$ causes an 8-cycle-wc. As a
consequence, we have one of the equalities in Equation (4). Without loss of generality, we assume that $c_1 = c_6$. Hence, we have

$$i_1j_1 - i_1j_2 + i_2j_2 - i_2j_3 + i_3j_3 - i_3j_1 = i_1j_2 - i_1j_1 + i_2j_1 - i_2j_3 + i_3j_3 - i_3j_2,$$

which yields $(j_1-j_2)(2i_1 - i_2 - i_3) \equiv 0 \pmod{p}$. Since $\text{gcd}(j_1-j_2, p) = 1$, we conclude that $(2i_1 - i_2 - i_3) \equiv 0 \pmod{p}$, which is a contradiction.

Remark 5: Suppose $i_1, i_2, \ldots, i_n$ are the row indices of $W_p$, which are chosen for a $\gamma \times n$ exponent matrix $B$. If for each $i_x, i_y, i_z \in \{i_1, i_2, \ldots, i_n\}$ we have $(2i_x - i_y - i_z) \not\equiv 0 \pmod{p}$, $(2i_y - i_x - i_z) \not\equiv 0 \pmod{p}$, and $(2i_z - i_x - i_y) \not\equiv 0 \pmod{p}$, then no $3 \times 3$ submatrix of $B$ yields an 8-cycle-wc.

Example 7: Using Remark 5, we can prove that no $3 \times 3$ submatrix of $W_p$ with $p > 19$ and row indices $[0, 1, 3, 4, 9, 10]$ causes an 8-cycle-wc. In fact, each triple chosen from the row indices satisfies Lemma 5 if the lifting degree is $p > 19$. For example, assuming $p = 23$ and three row indices $i_x = 3, i_y = 4, i_z = 9$, we have $(2i_x - i_y - i_z) = 6 - 4 - 9 \neq 0$, $(2i_y - i_x - i_z) = 8 - 3 - 9 \neq 0$, and $(2i_z - i_x - i_y) = 18 - 3 - 4 \neq 0$ when computations are modulo 23. We compute $(2i_x - i_y - i_z), (2i_y - i_x - i_z), (2i_z - i_x - i_y)$ for each triple $(i_x, i_y, i_z)$ from the row indices $[0, 1, 3, 4, 9, 10]$ and put the results of these computations in a set. It is easy to see that the elements of this set vary between $-19$ and $19$. Thus, for any $p > 19$, all of the elements of the set are nonzero modulo $p$ which proves that the row indices $[0, 1, 3, 4, 9, 10]$ with $p > 19$ satisfy Remark 5.

Theorem 11: Let us consider a $3 \times 3$ submatrix of $W_p$ with row indices $i_1, i_2, i_3$ and column indices $j_1, j_2, j_3$. A necessary and sufficient condition for this submatrix to have no 8-cycle-wc is that if one of the integers $(2i_1 - i_2 - i_3), (2i_2 - i_1 - i_3)$, or $(2i_3 - i_1 - i_2)$ is divisible by $p$, then none of $(2j_1 - j_2 - j_3), (2j_2 - j_1 - j_3)$, and $(2j_3 - j_1 - j_2)$ are divisible by $p$.

Proof: We assume that $(2i_1 - i_2 - i_3) \equiv 0 \pmod{p}$ which yields $e_1 = e_6, e_2 = e_5, e_3 = e_4$. According to the equations in (4), a necessary and sufficient condition to remove an 8-cycle-wc is that none of these three equations equals zero. If one of these equations is equal to zero, for example, if $e_1 = e_6 = 0$, then $e_1 = 0$ and $e_6 = 0$ imply

$$i_2j_1 - i_2j_2 + i_3j_3 - i_3j_1 = i_1j_2 - i_1j_1$$

$$-i_2j_2 + i_3j_3 - i_3j_1 = i_1j_2 - i_1j_1,$$

which proves $i_2j_2 = i_3j_3 - i_3j_1 = -i_2j_1 + i_2j_3 - i_3j_3 + i_2j_2$ or $(i_2 - i_3)(2j_1 - j_2 - j_3) \equiv 0 \pmod{p}$. Since $\text{gcd}(i_2 - i_3, p) = 1$ we have $(2j_1 - j_2 - j_3) \equiv 0 \pmod{p}$. Therefore, in this case, the existence of an 8-cycle-wc is associated with the equation $(2j_1 - j_2 - j_3) \equiv 0 \pmod{p}$. Other cases can be considered similarly.

Theorem 12: Given a $3 \times 4$ submatrix of $W_p$ with column indices $j_1, j_2, j_3, j_4 \in \{0, 1, \ldots, p - 1\}$, the corresponding Tanner graph is free of 8-cycles-wc if and only if $\pm(j_1 + j_2) \not\equiv \pm(j_1 + j_3) \pmod{p}, \pm(j_1 + j_3) \not\equiv \pm(j_2 + j_4) \pmod{p}$, and $\pm(j_2 + j_3) \not\equiv \pm(j_1 + j_4) \pmod{p}$.

Proof: The proof is given in Appendix D.

To construct a $(\gamma, n)$-regular array-based LDPC code whose Tanner graph is free of 8-cycles-wc we should find the submatrices of $W_p$ satisfying Theorems 11 and 12. In this regard, to reduce the complexity of the search space we restrict ourselves to those submatrices whose first row and first column are all-zero, each triple $(i_x, i_y, i_z)$, where $x, y, z \in \{1, \ldots, \gamma\}$, satisfies Lemma 5, and each quadruple $\{j_x, j_y, j_u, j_v\}$, where $s, t, u, v \in \{1, \ldots, n\}$, satisfies Theorem 12. In Table VI we present column and row indices which result in $(6, n)$-regular array-based LDPC codes free of 8-cycles-wc. In order to obtain the exponent matrix it is sufficient to consider $B_{kl} = b_k \cdot b_l \pmod{p}$. For $7 \leq n \leq 11$, we use the row indices in Example 7. In all cases, the obtained lifting degree is much less than the minimum lifting degree of a fully-connected QC-LDPC code with girth 8 reported in [10].

D. Multi-Edge QC-LDPC Codes With Tanner Graphs Whose 8-Cycles Are All Chordless

To consider cycles in a multi-edge QC-LDPC code we use the following definition which simplifies checking Equation (1).

Definition 8: A difference matrix $D$ corresponding to an exponent matrix $B$ is a matrix in which the $ij$-th entry is obtained by subtracting every two entries of $B_{ij}$ if $|B_{ij}| > 1$. Instead, for $b_{ij}, b'_{ij} \in B_{ij}$, where $b_{ij} \neq b'_{ij}$, we define $D_{ij}^{(x,y)} = |b_{ij} - b'_{ij}|$ and $-D_{ij}^{(x,y)} = -|b_{ij} - b'_{ij}|$ and in this case $|D_{ij}| = 2(|b_{ij} - b'_{ij}|). The ij-th entry of $D$ is (−) when $|B_{ij}| = 1$ and it is 0 if $B_{ij} = 0$.

Since the Tanner graph is supposed to have girth 6, according to Theorem 1 in [13], for $b_{ij}, b'_{ij} \in B_{ij}$, and $b''_{ij}, b'''_{ij} \in B'_{ij}$, we have $D_{ij}^{(x,y)} \not\equiv D_{ij}'^{(x,y)}$. If $W_{ij} = 2$, then we use $D_{ij}$ instead of $D_{ij}^{(0,1)}$ for $B_{ij} = (b_{ij}, b'_{ij})$ and the $ij$-th entry of $D$ is $D_{ij} = (D_{ij}, -D_{ij})$.

According to [43], to consider 6-cycles in the exponent matrix of a multi-edge protograph, Equation (1) has to be checked for all submatrices of sizes $1 \times 1, 1 \times 2, 2 \times 1, 1 \times 3, 3 \times 1, 2 \times 2, 2 \times 3, 3 \times 2, 3 \times 3$. In this case, if the Tanner graph is free of 8-cycles-wc, then there are no pairs like $(b_{m,n}, b'_{m,n+1})$ which occur in two 6-cycle equations. In the following theorem, we provide, in detail, the conditions to avoid 8-cycles-wc from occurring in the Tanner graph of a girth-6 multi-edge QC-LDPC code.

Theorem 13: Let $W$ and $B$ be a base matrix and an exponent matrix of a multi-edge QC-LDPC code. The necessary conditions for the exponent matrix to have a Tanner graph free of 8-cycles-wc are as follows, where all computations are modulo $N$:

(i) $W_{ij} < 3$.
(ii) For the submatrix $[B_{ij}, B'_{ij}']$ with $W_{ij} = W'_{ij} = 2$ we have $2D_{ij} \neq 0, 4D_{ij} \neq 0, 2D'_{ij} \neq 0, 4D'_{ij} \neq 0$.
(iii) For the submatrix $[B_{ij}, B'_{ij}, B_{ij}', B'_{ij}']$ with $W_{ij} = W'_{ij} = 2$ we have

\[ \begin{array}{l}
\pm D_{ij} \pm D_{ij}' \neq 0, \pm D_{ij} \pm D_{ij}' \neq 0, \pm D_{ij} \pm D_{ij}' \neq 0, \pm D_{ij} \pm D_{ij}' \neq 0, \\
\pm D_{ij} \pm D_{ij}' \neq 0, \pm D_{ij} \pm D_{ij}' \neq 0, \pm D_{ij} \pm D_{ij}' \neq 0, \pm D_{ij} \pm D_{ij}' \neq 0.
\end{array} \]
In the following, we propose two examples that satisfy Theorem 13 and Remark 6. In Examples 8 and 9 we need to define Sidon sequences and Raptor-like LDPC codes. These examples also show the applicability of our method to both regular and irregular multi-edge LDPC codes.

**Definition 9 [17]:** A sequence \( S = \{s_0, s_1, \ldots, s_l\} \) over \( \mathbb{Z}_m \) with \( \binom{t^2}{2} \) distinct sums \((s_i + s_j) \pmod{m}\), where \( i \neq j \), is a Sidon sequence.

**Example 8:** Given the Sidon sequence \( S = \{0, 6, 9, 10, 21, 23, 28\} \) over \( \mathbb{Z}_{48} \), we consider an exponent matrix whose integer entries are chosen from \( S \). For instance, let \( B = [E(0), E(1), E(2)] \) be given by

\[
E^{(k)} = \begin{bmatrix}
(a_0^{(k)}, b_0^{(k)}) & \emptyset & \emptyset \\
(0) & (a_1^{(k)}, b_1^{(k)}) & \emptyset \\
\emptyset & \emptyset & (a_2^{(k)}, b_2^{(k)})
\end{bmatrix},
\]

where all parameters \( a_0^{(k)}, a_1^{(k)} \) and \( b_1^{(k)} \) are in \( S \). Even if there is no constraint on choosing elements from \( S \) for parameters \( a_0^{(k)} \) and \( b_1^{(k)} \), the exponent matrix \( B \) yields a \((3,9)\)-regular multi-edge QC-LDPC code from Sidon sequences with \( N = m \) [17]. Now, we choose those elements from \( S \) over \( \mathbb{Z}_{48} \) such that the obtained exponent matrix \( B \) is free of 4-cycles and 8-cycles-wc. Considering this constraint, the pairs in the diagonal of this \( E^{(k)} \) are \((0, 0), (0, 9), (0, 10)\) for \( k = 0 \), \((6, 9), (6, 23), (6, 21)\) for \( k = 1 \), and \((23, 28), (21, 28), (9, 23)\) for \( k = 2 \). In Equation (12), shown at the bottom of the next page, we provide the obtained exponent matrix which results in a \((3,9)\)-regular multi-edge QC-LDPC code with girth 6, free of 8-cycles-wc, and length 432. We also present the matrix \( D \) to show that it satisfies Theorem 13.

Because of the structure of the base matrix, in order to prove the non-existence of 5-cycles-wc, we only need to check part (ii) and the first condition of part (iii) in Theorem 13 as well as the \( 3 \times 3 \) submatrices of \( B \).

**Definition 10 [38]:** The protograph of a Raptor-like LDPC code consists of two parts: a highest-rate code (HRC) protograph and an incremental redundancy code (IRC) protograph. The adjacency matrices of these two protographs are denoted by \( W_{\text{HRC}} \) and \( W_{\text{IRC}} \), respectively. Assuming that \( 0 \) is the all-zero matrix and \( I \) is an identity matrix of appropriate size,
the base matrix of the Raptor-like LDPC code is defined as
\[ W = \begin{bmatrix} W_{\text{HRC}} & 0 \\ W_{\text{IRC}} & I \end{bmatrix}. \]

\textbf{Example 9:} We present an exponent matrix corresponding to a protograph-based Raptor-like LDPC code given in [38] with the following \( W_{\text{HRC}} \) and \( W_{\text{IRC}} \) which yields an irregular multi-edge QC-LDPC code with girth 6, free of 8-cycles-wc, and with the shortest length from an exhaustive search.

\[ W_{\text{HRC}} = \begin{bmatrix} 1 & 1 & 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 2 & 1 & 2 \end{bmatrix}, \]
\[ W_{\text{IRC}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \]

Avoiding the occurrence of pairs like \( (b_{m_1,n_1}, b_{m_2,n_2}) \) in two 6-cycle equations related to the exponent matrix corresponding to \( W \) in Definition 10 as well as avoiding 4-cycles we obtain the following exponent matrices \( B_{\text{HRC}} \) and \( B_{\text{IRC}} \) with \( N = 78 \), respectively corresponding to \( W_{\text{HRC}} \) and \( W_{\text{IRC}} \):

\[ B_{\text{HRC}} = \begin{bmatrix} (0) & (0) & (0, 27) & (0, 37) & (0) \\ (0, 4) & (21, 61) & (3) & (29, 52) & (76) & (18, 46) \end{bmatrix}, \]
\[ B_{\text{IRC}} = \begin{bmatrix} (3) & (44) & (11) & (31) & (73) & (50) \\ (36) & (60) & (54) & (0) & (18) & (0) \\ (0) & (72) & (0) & (0) & (6) & (18) \\ (63) & (0) & (0) & (1) & (0) & (62) \\ (0) & (0) & (33) & (0) & (63) & (0) \\ (0) & (36) & (0) & (75) & (0) & (48) \\ (36) & (28) & (0) & (44) & (0) \end{bmatrix}. \]

The resulting code is a Raptor-like QC-LDPC code with girth 6, free of 8-cycles-wc, length 1014, and rate 0.307. In the matrix \( D \) corresponding to the exponent matrix of this code the only integer elements occur in the following matrix which we named as \( D_{\text{HRC}} \):

\[ D_{\text{HRC}} = \begin{bmatrix} (-) & (-) & (27, 51) & (-) & (37, 41) & (-) \\ (4, 74) & (38, 40) & (-) & (23, 55) & (-) & (28, 50) \end{bmatrix}. \]

It is easy to check that \( W \) and \( D \) satisfy Remark 6 and Theorem 13, respectively, and similar to Example 8, part (ii) and the first condition of part (iii) in Theorem 13, as well as \( 3 \times 3 \) submatrices of \( B \) have to be checked to remove 8-cycles-wc.

V. DESIGNS AND EXAMPLES FOR CODES WITH GIRTH 8

In this section, we propose a method to remove short cycles-wc of lengths up to 12 such that the resulting QC-LDPC code with girth 8 inherits some merits of codes with girth 10. Moreover, our approach improves its counterparts in the literature for constructing QC-LDPC codes with girth 8 and free of \((a, b)\) ETSs with \(5 \leq a \leq 8\) and \(b \leq 3\).

In a Tanner graph with girth 8 all 8-cycles and 10-cycles are chordless. Thus, to construct a Tanner graph with girth 8 and free of cycles-wc of lengths up to 12 we should only present necessary and sufficient conditions to avoid 12-cycles-wc. Fig. 1 (e) shows a 12-cycle-wc. Its VN graph consists of two 4-cycles with one edge in common. Each 4-cycle in the VN graph corresponds to an 8-cycle in the Tanner graph. Hence, a necessary and sufficient condition to remove a 12-cycle-wc is to avoid the occurrence of two 8-cycles that share one check node and two variable nodes connected to that check node. In the following, we propose our method to construct a protograph-based LDPC code with girth 8 and free of cycles-wc of lengths up to 12 and then we apply our method to fully-connected QC-LDPC codes.

Suppose an exponent matrix \( B \) is given which belongs to a simple protograph. In order to check 12-cycles in terms of their chords, we consider 8-cycles. Therefore, we have to check Equation (1) for all submatrices of sizes \( r \times s \), where \(2 \leq r, s \leq 4 \), from the exponent matrix. According to [12] and [21], to simplify checking 8-cycles, we construct \( \binom{n}{2} \) arrays \( A_{(i_1,i_2)} \), \( 1 \leq i_1, i_2 \leq m \) whose elements are obtained as follows.

Let the right-hand side of Equation (1) regarding a \( 2 \times 2 \) submatrix of \( B \) with row indices \( i_1, i_2 \) and column indices \( j_1, j_2 \) be denoted by \( q_{i_1,i_2,j_1,j_2} \). We define

\[ A_{(i_1,i_2)} = \{ q_{i_1,i_2,j_1,j_2} \mid N - q_{i_1,i_2,j_1,j_2} \leq 1 \leq j_1, j_2 \leq n \}. \]

It is clear that any element of \( A_{(i_1,i_2)} \) is less than or equal to \( n^2 \). Using these arrays, Equation (1) implies the next rules that significantly simplify checking 8-cycles.

- The existence of repeated elements in \( A_{(i_1,i_2)} \) proves the existence of 8-cycles belonging to two rows \( i_1, i_2 \) of \( B \).
- If \( A_{(i_1,i_2)} \cap A_{(i_1,i_3)} \neq \emptyset \), then there are rows \( i_1, i_2, i_3 \), where \( i_2 \) is used twice in Equation (1), contain 8-cycles.

We have a similar scenario for arrays \( A_{(j_1,j_2)} \), \( 1 \leq j_1, j_2 \leq n \), obtained from any two columns \( j_1, j_2 \) of the exponent matrix. Using these rules we obtain our main tools to check 12-cycles-wc.

\textbf{Theorem 14:} A protograph-based LDPC code with an exponent matrix \( B \) is free of 12-cycles-wc if and only if

1. in each of the arrays \( A_{(i_1,i_2)} \cup A_{(i_1,i_3)} \), \( A_{(i_1,i_2)} \cup A_{(i_2,i_3)} \), and \( A_{(i_1,i_3)} \cup A_{(i_2,i_3)} \) with \( 1 \leq i_1, i_2, i_3 \leq m \), any element \( x \) is repeated at most twice;

\[ B = \begin{bmatrix} (0, 6) & 0 & (0) & (9, 10) & 0 & (0) & (0) & (23, 28) & 0 & (0) \\ (0) & (0, 9) & 0 & (0) & (6, 23) & 0 & (0) & (21, 28) & 0 & 0 \\ 0 & (0) & (0, 10) & 0 & (0) & (6, 21) & 0 & (0) & (9, 23) & 0 \end{bmatrix}, \]
\[ D = \begin{bmatrix} (6, 42) & 0 & (-) & (1, 47) & 0 & (-) & (5, 43) & 0 & (-) \\ (-) & (9, 39) & 0 & (-) & (17, 31) & 0 & (-) & (7, 41) & 0 \\ 0 & (-) & (10, 38) & 0 & (-) & (15, 33) & 0 & (-) & (14, 34) & 0 \end{bmatrix}. \]
II. in each of the arrays $A_{(j_1,j_2)} \cup A_{(j_2,j_3)} \cup A_{(j_3,j_2)}$, $A_{(j_1,j_2)} \cup A_{(j_2,j_3)}$ with $1 \leq j_1, j_2, j_3 \leq n$, any element $y$ is repeated at most twice; and

III. each $4 \times 4$ submatrix of $B$ is free of two 8-cycles with one common term such as $\pm(b_{1j_1} - b_{1j_2})$.

**Proof:** We prove the first item. The proof of the second item is similar and is omitted. The third item is the result of the definition of cycles-wc which have to be avoided to construct a girth-8 LDPC code with chordless cycles of lengths up to 12.

We suppose that $A_{(i_1,i_2)} \cup A_{(i_2,i_3)}$ contains an element $x$ which appears three times. Without loss of generality, we assume that $q_{i_1,i_2,j_1} = q_{i_1,i_3,j_2} = q_{i_2,i_3,j_3} = x$. Therefore, we have two 8-cycles for which the left-hand sides of Equation (1) contain exactly one common term. For example, $(b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_1j_3} - b_{i_1j_2}) + (b_{i_2j_3} - b_{i_2j_3})$ and $(b_{i_1j_1} - b_{i_1j_2}) + (b_{i_2j_2} - b_{i_2j_3}) + (b_{i_1j_3} - b_{i_1j_3}) + (b_{i_2j_3} - b_{i_2j_2})$ are left-hand sides of Equation (1) for two 8-cycles that have exactly one check node in common.

**Corollary 2:** Let a $\gamma \times n$ exponent matrix $B$ be given. A necessary condition to have a protograph-based LDPC code with girth 8 and chordless cycles of lengths up to 12 is that the lifting degree $N$ be lower bounded by $n(n-1)$.

**Proof:** There are $(\gamma - 1)$ arrays $A_{(i_1,i_2)}$ with the same row index $i_1$ and $i_2 \neq i_1$. Each of these arrays has $\binom{n}{2}$ elements. The number of elements in the array $\bigcup_{1 \leq i_2 \leq \gamma} A_{(i_1,i_2)}$ is $(\gamma - 1)\binom{n}{2} = n(n-1)(\gamma-1)$. According to Theorem 14, for a row index $i_3$ any element in the array $A_{(i_1,i_2)} \cup A_{(i_1,i_3)}$ appears at most twice. Therefore, if an element appears in any array $A_{(i_1,i_2)}$ twice, then it cannot occur in other arrays $A_{(i_1,i_3)}$ with $i' \neq i$. As a result, the array $\bigcup_{1 \leq i_2 \leq \gamma} A_{(i_1,i_2)}$ contains that element twice. Consequently, if an element appears $\lambda$ times in $\bigcup_{1 \leq i_2 \leq \gamma} A_{(i_1,i_2)}$, where $\lambda > 2$, then there are $\lambda$ arrays like $A_{(i_1,i_2)}$ containing that element. Clearly $\lambda \leq \gamma - 1$. Since the number of arrays $A_{(i_1,i_2)}$ with $i_2 \neq i_1$ is $\gamma - 1$, if an element $x$ appears $\gamma$ times in $\bigcup_{1 \leq i_2 \leq \gamma} A_{(i_1,i_2)}$, then there is an array like $A_{(i_1,i')}$ which contains $x$ at least twice. Therefore, if another array like $A_{(i_1,i')}$ includes $x$ once, then $A_{(i_1,i')} \cup A_{(i_1,i')} \cup A_{(i_1,i')} \cup A_{(i_1,i')} \cup A_{(i_1,i')} \cup A_{(i_1,i')} \cup A_{(i_1,i')} \cup A_{(i_1,i')} \cup A_{(i_1,i')}$ contains $x$ three times which is impossible. Since the array $\bigcup_{1 \leq i_2 \leq \gamma} A_{(i_1,i_2)}$ contains $n(n-1)(\gamma-1)$ elements, even if each element appears exactly $(\gamma - 1)$ times then the number of distinct elements in the last array is $\frac{n(n-1)(\gamma-1)}{2}$.

These distinct elements belong to $\{1, \ldots, N\}$. Hence, we have $\frac{N}{2} \geq \frac{n(n-1)}{2}$ which yields $N \geq n(n-1)$.

**Remark 7:** Each array in Condition I of Theorem 14 contains $2\binom{n}{2}$ elements. Since each element can be repeated at most twice in each array, the cardinality of each set obtained from each array by eliminating repeated elements is at least $\frac{n(n-1)}{2}$ entries. Thus, if each set corresponding to an array has at least $\frac{n(n-1)}{2}$ entries, then the exponent matrix satisfies the first part of Theorem 14. To check the second part we should have sets corresponding to arrays with at least $\frac{n^2(n-1)}{2}$ entries.

Using Theorem 14 and Corollary 2, we provide a greedy search algorithm (Algorithm 2) to obtain an exponent matrix of a QC-LDPC code whose Tanner graph is free of short cycles-wc of lengths up to 12. In this algorithm the first column of $B$ is all-zero and other columns of $B$ are obtained gradually in $n - 1$ steps by checking Theorem 14 and Corollary 2 for the obtained exponent matrix $B'$, which has $n' + 1$ columns, in the $n'$th step. Moreover, in this algorithm we have

$$|A_{0,1}| = | \{ \min \{ q_{0,1,j_1,j_2}, q_{0,1,j_2,j_1} \} : 0 \leq j_1, j_2 < n' \} |,$$

and

$$|A_{q',i} | = | \{ \min \{ q_{q',i,j_1,j_2}, q_{q',i,j_2,j_1} \} : 0 \leq j_1, j_2 < n' \} |.$$

**Algorithm 2:** Greedy search algorithm to avoid 12-cycles-wc

**Input:** $\gamma, n, N$

**Output:** An exponent matrix $B$ with $\gamma$ rows and $n$ columns.

All computations are modulo $N$

- put $n' = 1$, $b_{0j} = 0$ for $0 \leq j \leq n - 1$, $b_{00} = 0$ for $0 \leq i < n - 1$;
  - while $0 < n' < n$
    - put $B' = [0]$, an exponent matrix with $n'$ columns, and $R_1 = [0]$, the second row of $B'$;
    - pick $b_{1n'}$ from $[2, N - 1]$ such that $b_{1n'} > b_{1k}$ for $0 \leq k < n' - 1$ and put $q_{0,1,e_1,e_2} = b_{1n'} - b_{1k}$;
    - if $|A_{0,1}| \geq \frac{n(n-1)}{2}$
      - add $b_{1n'}$ to $R_i$;
      - $R_i = [0, b_{11}, b_{12}, b_{13}]$;
    - for $i = 2$ to $m - 1$
      - put $R_i = [0]$, the $i$th row of $B'$;
      - pick $b_{in'}$, from $[2, N - 1]$ and put $q_{i,e_1,e_2} = b_{in'} - b_{ik}$ for $0 \leq i < j$ and $0 \leq k < n' - 1$;
      - if $|A_{i,e_1,e_2}| \geq \frac{n(n-1)}{2}$
        - the exponent matrix $B'$ with $i + 1$ rows and $n' + 1$ columns satisfies Theorem 14 then
          - add $b_{in'}$ to $R_i$;
          - $R_i = [0, b_{i1}, b_{i2}, b_{i3}]$;
    - $n' + 1$
      - return the matrix $B'$ with $n'$ columns;
      - $B' = [0 R_1 \cdots R_{n-1}]^T$, where $T$ is the transpose.

Applying Algorithm 2, we obtain the minimum lifting degree of fully-connected QC-LDPC codes with girth 8, column weight 3, and row weight $4 \leq n \leq 9$ whose Tanner graphs are free of cycles-wc of lengths up to 12. The exponent matrices of these codes are presented in Table VII.

| $n$ | $N$ | $B$ |
|-----|-----|-----|
| 4   | 19  | 1, 3, 8 |
|     |     | 4, 12, 13 |
| 5   | 24  | 1, 3, 8, 12, 17 |
|     |     | 4, 18, 22, 19 |
| 6   | 31  | 1, 3, 8, 11, 13, 17 |
|     |     | 3, 14, 4, 29, 22 |
| 7   | 52  | 1, 3, 8, 11, 13, 17 |
|     |     | 2, 15, 9, 23, 5, 35 |
| 8   | 75  | 1, 3, 8, 11, 13, 17 |
|     |     | 2, 7, 20, 53, 34, 28, 37 |
| 9   | 110 | 1, 3, 8, 12, 22, 46, 63, 78 |
|     |     | 2, 7, 18, 28, 15, 76, 98, 51 |

**TABLE VII**

AN EXPONENT MATRIX $B$ OF A $(3, n)$-REGULAR QC-LDPC CODE WITH $g = 8, 4 \leq n \leq 9$ AND THE MINIMUM LIFTING DEGREE WHOSE TANNER GRAPH IS FREE OF CYCLES-WC OF LENGTHS UP TO 12.

THE FIRST ROW AND THE FIRST COLUMN OF EACH EXPONENT MATRIX ARE ALL-ZEROS.
Now we compare the impact of avoiding short cycles-wc of lengths up to 12 and the impact of avoiding \((a, b)\) ETSs with \(5 \leq a \leq 8\) and \(b \leq 3\) in the Tanner graph of fully-connected QC-LDPC codes with column weight 3 which have been studied in many articles [11], [16], [20], [21]. In fact, the removal of short cycles-wc of lengths up to 12 or eliminating \((a, b)\) ETSs with \(5 \leq a \leq 8\) and \(b \leq 3\) from a \((3, n)\)-regular QC-LDPC code results in a girth-8 code with the same lower bound on the minimum distance. On the one hand, according to Remark 2, the elimination of 12-cycles-wc yields the lower bound 10 on the minimum distance. On the other hand, the elimination of \((a, b)\) ETSs with \(5 \leq a \leq 8\) and \(b \leq 3\) causes the removal of all \((8, 0)\) ETSs whose size is the largest ETS with \(b = 0\) is 10. Moreover, according to the proof of Theorem 3, the lower bound on the size of an \((a, 0)\) non-elementary trapping set is \(4\gamma\) which is 12 for \(\gamma = 3\). Thus, by the removal of these ETSs the lower bound on the \(d_{\min}\) is also 10.

In the following, we investigate other merits of avoiding short cycles-wc of lengths up to 12 over eliminating the mentioned ETSs. As we mention in the introduction, there are different methods to eliminate those ETSs in the literature. For example, from [11] we conclude that the removal of all 8-cycles obtained from the first two rows of the exponent matrix, 8-cycles obtained from the last two rows, and the 8-cycles obtained from the three rows which use the second row twice cause the elimination of the mentioned ETSs. We refer to this method as \(M_1\). On the other hand, [16] proposes to remove all 8-cycles obtained from two rows of the exponent matrix and some other 8-cycles from three such that any pair of the remaining 8-cycles do not have common check nodes. We refer to this method as \(M_2\).

**Comparison of the Computational Complexity Between Algorithm 2 and the Methods \(M_1\) and \(M_2\)**

In method \(M_1\), which is only applicable to QC-LDPC codes with column weight 3, Equation (1) has to be checked for all \(2 \times 2, 2 \times 3, 2 \times 4, \ldots, 2 \times 4\) submatrices of the first two rows and the last two rows of \(B\) as well as \(3 \times 2, 3 \times 3, 3 \times 4\) submatrices of \(B\). The number of these equations for \(B\) with \(n\) columns is

\[
2 \left( \binom{n}{2} + 3 \binom{n}{3} + 6 \binom{n}{4} \right) + \left( \binom{n}{2} + 6 \binom{n}{3} + 3 \binom{n}{4} \right)
\]

or equivalently \(3\binom{n}{2} + 12\binom{n}{3} + 14\binom{n}{4}\). Since the number of operations for each 8-cycle is 9, the number of operations using the method \(M_1\) is \(9 \left( \binom{n}{2} + 12\binom{n}{3} + 14\binom{n}{4}\right)\).

The computational complexity of our method based on Algorithm 2 is lower than that of the method \(M_1\). In fact, using Algorithm 2 we only need to obtain the left-hand side of Equation (1) for all \(2 \times 2\) submatrices of \(B\). If the column weight is 3, then the number of equations is \(3\binom{n}{2}\) and since the number of operations for each \(2 \times 2\) submatrix is 5, the number of operations in this step of Algorithm 2 is \(15\binom{n}{2}\). This is much less than \(9 \left( \binom{n}{2} + 12\binom{n}{3} + 14\binom{n}{4}\right)\) especially for large \(n\) since this gives a drop in order from \(O(n^4)\) to \(O(n^2)\). Then, the next step to avoid 12-cycles-wc is to check Remark 7 for which we should obtain the cardinality of each set corresponding to an array.

The exponent matrix obtained from the method \(M_2\) not only satisfies Theorem 14 and Remark 7 but also its corresponding Tanner graph is free of 8-cycles obtained from any two rows of \(B\). Hence, the method \(M_2\) has \(27 \left( \binom{n}{2} + 3\binom{n}{3} + 6\binom{n}{4}\right)\) more arithmetic operations than Algorithm 2. In Table VIII, we compare the number of operations to construct a \((3, n)\)-regular QC-LDPC code between the above three methods. As we expect, the number of operations for the removal of 12-cycles-wc is significantly less than the number of operations for avoiding small size ETSs when using the methods \(M_1\) and \(M_2\).

**Comparison of the Code Length Between Codes Obtained From Algorithm 2 and the Methods \(M_1\) and \(M_2\)**

The merit of QC-LDPC codes with short or moderate lengths is that they outperform random or pseudorandom LDPC codes. This is the reason for a large body of work in the literature such as [9], [10], [11], [12], [13], [14], [16], [21], and [37] to find QC-LDPC codes with the shortest length. Algorithm 2 which has a lower computational complexity compared to \(M_1\) and \(M_2\) implies a code with a shorter length than its counterpart. For example, as can be seen in Table VII, for \((3, n)\)-regular fully-connected QC-LDPC codes with \(n = 5, 6\), girth 8 and free of 12-cycles-wc the minimum lifting degrees are \(N = 24, 31\), respectively. Whereas, using \(M_2\), the minimum ones obtained for the Tanner graphs free of \((a, b)\) ETSs with \(5 \leq a \leq 8\) and \(b \leq 3\) are \(N = 27, 41\), respectively.

Moreover, the lower bound on the minimum lifting degree using our method is much less than that of \(M_1\). In fact, the lower bound on the lifting degree has a direct connection with the computational complexity of the search algorithm of the method which we use to obtain the entries of the exponent matrix. Using \(M_1\), the array \(A_{1,2} \cup A_{2,3}\) is free of repeated elements and then \(N \geq 4\binom{n}{2} + 1\). Whereas the lower bound of \(N\) using our method is \(n(n - 1)\) which is explained in Corollary 2. It should be noticed that using \(M_2\) the arrays \(A_{1,2}, A_{1,3}\) and \(A_{2,3}\) are free of repeated elements and therefore the lower bound on the lifting degree is \(2\binom{n}{2} + 1\).

To sum up, we consider two approaches, the first approach is the removal of short cycles-wc of lengths up to 12 and the
second approach is the elimination of \((a, b)\) ETSs, \(5 \leq a \leq 8, b \leq 3\). Firstly, the lower bounds on the minimum distances of the codes based on these approaches are equal. Secondly, the computational complexity of the first approach is lower than that of the second approach, Subsection V-A, which yields a code with a shorter length than the code obtained from the second approach, Subsection V-B. Finally, there is a similarity between the behaviour of these codes in their performance curves, which we see in Section VI. Thus, we propose avoiding the occurrence of short cycles-wc in the Tanner graph instead of eliminating specific ETSs. We construct the protograph-based LDPC codes with girth 8, short length, and free of short cycles-wc of lengths up to 12 whose lower bound on the minimum distances and performance curves are similar to those of the codes free of small size ETSs.

### VI. Simulations

In this section, we show another merit of avoiding short cycles with a chord, and consequently the elimination of small size ETSs, in the performance curves of some of the codes whose exponent matrices are given in Sections IV and V. The performances of these codes were decoded using the sum-product algorithm with 50 iterations. The simulations were performed over the additive white Gaussian noise (AWGN) channel using BPSK modulation. The parameters of the codes simulated are given in Table IX.

Fig. 6 shows performances of four codes, \(C_1, C_2, C_3,\) and \(C_4\). In fact, we compare the performances of two \((3, 11)\)-regular QC-LDPC codes \(C_1, C_2\) with girth 6, \(d_{\text{min}} = 8, N = 31,\) and length 341, where the Tanner graph of \(C_1\) is free of 8-cycles-wc and \(C_2\) contains these graphical structures. As we expect \(C_1\) significantly outperforms its counterpart \(C_2\). Moreover, we compare the performance curves of two \((3, 11)\)-regular QC-LDPC codes \(C_3, C_4\) with \(d_{\text{min}} = 8, N = 41,\) and length 451. The code \(C_3\) is a compact code whose exponent matrix has \(B_1 = [0, 1, 6]\) and its second row is \([0, 1, 2, 3, 4, 5, 7, 9, 12, 15, 19]\). The exponent matrix of the code \(C_4\) is given in [29]. The Tanner graph of \(C_3\) has girth 6 and is free of 8-cycles-wc and the Tanner graph of \(C_4\) has girth 8. As it can be seen, the performances of \(C_3, C_4\) are similar. Therefore, girth-8 codes are not better than girth-6 codes with a Tanner graph free of 8-cycles-wc.

Fig. 7 shows the performances of two codes, one with 8-cycles-wc and the other free of these graphical structures. In fact, we compare the performances of two \((3, 18)\)-regular QC-LDPC codes \(C_5, C_6\) with \(N = 67,\) length 1206 and high rate 0.835. The code \(C_5\) which is free of 8-cycles-wc significantly outperforms its counterpart \(C_6\) which contains those 8-cycles-wc and small size ETSs.

In Fig. 8, to show the advantage of avoiding 8-cycles-wc from occurring in the codes with column weight 4 and large row weight, we compare two \((4, 12)\)-regular QC-LDPC codes.
Fig. 7. Bit and frame error rates of (3, 18)-regular QC-LDPC codes \( C_5, C_6 \) with the same girth 6 and length 1206. The exponent matrix of \( C_5 \) with lifting degree \( N = 67 \) is given in Table V which gives a Tanner graph free of 8-cycles-wc. \( C_6 \) is an array-based code with \( p = 67 \) whose Tanner graph contains 8-cycles-wc.

Fig. 8. Bit and frame error rates of (4, 12)-regular QC-LDPC codes \( C_7, C_8 \) with the same girth 6 and length 624. The exponent matrix of \( C_7 \) with lifting degree \( N = 52 \) is given in Table V which gives a Tanner graph free of 8-cycles-wc. \( C_8 \) is a compact QC-LDPC code with \( N = 52 \) whose Tanner graph contains 8-cycles-wc.

Fig. 9. Bit and frame error rates of (3, 9)-regular multi-edge QC-LDPC codes \( C_9, C_{10} \). The exponent matrix of the (3, 9)-regular multi-edge QC-LDPC code \( C_9 \) is given in Example 8 and the exponent matrix of \( C_{10} \) is given in Section VI. The exponent matrix in Equation (13), shown at the bottom of the page, whose Tanner graph contains 8-cycles-wc.

In this comparison, we also see the benefit of avoiding short cycles-wc in regular multi-edge QC-LDPC codes.

To present the behaviour of irregular multi-edge codes with and without 8-cycles-wc, we obtain the simulation results of the Raptor-like LDPC code \( C_{11} \) given in Example 9 with different rates and different lengths. For comparison, we need another Raptor-like LDPC code \( C_{12} \) with the base matrix in [38] and the following \( B_{\text{HRC}} \) and \( B_{\text{IRC}} \) with \( N = 78 \):

\[
B_{\text{HRC}} = \begin{bmatrix}
0 & 0 & 0 & (0,1)
(0) & (1,3) & 0 & (1,2)
(0,1) & (2,4) & (6) & (3,7)
(0) & (2,4) & (12) & 0
\end{bmatrix}
\]

\[
B_{\text{IRC}} = \begin{bmatrix}
(1) & (6) & (3) & (10) & (9) & (4)
(4) & (24) & (12) & 0 & (36)
(0) & (18) & 0 & (27) & (12)
(2) & 0 & 0 & (20) & 0
(0) & 0 & (6) & 0 & (18)
(0) & 24 & 0 & (50) & 0
(0) & 0 & (15) & 0 & (45)
\end{bmatrix}
\]

Both codes \( C_{11} \) and \( C_{12} \) have the same length, rate, and girth but they are different in terms of containing 8-cycles-wc. The 8-cycles in the Tanner graph of the code in Example 9 are all chordless but the Raptor-like code using the above exponent matrices contains 8-cycles-wc.

We first obtain the performance curves of two QC-LDPC codes with exponent matrices \( B_{\text{HRC}} \) of \( C_{11} \) and \( C_{12} \), rate 0.67 and length 468. The results are presented in Fig. 10 that shows \( C_{11} \) which has no 8-cycles-wc significantly outperforms \( C_{12} \) which contains those cycles. Then, in both codes \( C_{11} \) and \( C_{12} \), we add the first row of \( B_{\text{IRC}} \) and the first column of the exponent matrix corresponding to the base matrix.

\[
B = \begin{bmatrix}
(0,1) & 0 & (0,3) & 0 & (0,2)
(0) & (0,3) & 0 & (0) & (0,2)
(1,3) & 0 & (0) & (5,8) & 0
(7) & 0 & (4) & (18) & 0
(9,12) & 0 & (14,18) & 0 & (16)
(0,1) & (0) & (0,2) & 0 & (8,12)
(0) & (0) & (0) & (7) & 0
(0) & (0) & (0) & (7) & 0
(0) & (0) & (0) & (7) & 0
(0) & (0) & (0) & (7) & 0
\end{bmatrix}
\]
B the exponent matrix corresponding to the base matrix $B$ decreases.

The performances of these codes decrease as the rate of the codes decreases, as illustrated in Fig. 10, which shows bit and frame error rates of protograph-based Raptor-like LDPC codes $C_{11}$ and $C_{12}$ with rates 0.67, 0.57, and 0.5. The exponent matrix of the protograph-based Raptor-like LDPC code $C_{11}$ is given in Example 9 and $B_{HRC}$ and $B_{ABC}$ matrices of $C_{12}$ are given in Section VI.

Fig. 10. Bit and frame error rates of protograph-based Raptor-like LDPC codes $C_{11}, C_{12}$ with rates 0.67, 0.57, and 0.5. The exponent matrix of the protograph-based Raptor-like LDPC code $C_{11}$ is given in Example 9 and $B_{HRC}$ and $B_{ABC}$ matrices of $C_{12}$ are given in Section VI.

We continue this process and we add the first two rows of $B_{HRC}$ and the first two columns of the exponent matrix corresponding to the base matrix $[0 \mid I]^T$. Then, adding the first four rows and four columns implies codes with rate 0.4 and length 780. As shown in Fig. 11, in this comparison, $C_{11}$ slightly outperforms $C_{12}$. However, when performing the original Raptor-like codes with rate 0.307 and length 1014 we encounter a different trend in the performances of these codes. In this comparison, $C_{11}$ slightly outperforms $C_{12}$. Thus, we experience mixed behaviours for Raptor-like codes with different rates when avoiding short cycles-wc.

In Fig. 12, we compare the performance curves of two $(3,5)$-regular QC-LDPC codes with girth 8, $N = 27$ and the same $d_{min} = 16$ but different graphical structures. The exponent matrix of one of them, constructed using $M_2$ in [16], is given in Example 9 and the exponent matrix of the other, $C_{13}$, is in Table X. As can be seen, for both of these cases, the performance curves are similar.

Table X

| $n$ | $N$ | $B$ |
|-----|-----|-----|
| 5   | 27  | 0   | 0   | 0   | 0   |
|     |     | 0   | 1   | 2   | 9   | 12  |
| 6   | 41  | 0   | 0   | 1   | 2   | 6   | 17  | 25  |
|     |     | 0   | 3   | 7   | 21  | 9   | 36  |

Fig. 12. Comparison of bit and frame error rates of $(3,n)$-regular QC-LDPC codes with $g = 8$, $n = 5, 6$ and free of cycles-wc of lengths up to 12.

The rest of this process is shown in Fig. 11, when we add the first three rows of $B_{HRC}$ and the first three columns of the exponent matrix corresponding to the base matrix $[0 \mid I]^T$, which yield codes with rate 0.44 and length 702. For this case, $C_{11}$ slightly outperforms $C_{12}$. Then, adding the first four rows and four columns implies codes with rate 0.4 and length 780. As shown in Fig. 11, in this comparison, $C_{11}$ slightly outperforms $C_{12}$ too. However, when performing the original Raptor-like codes with rate 0.307 and length 1014 we encounter a different trend in the performances of these codes. In this comparison, $C_{11}$ slightly outperforms $C_{12}$. Thus, we experience mixed behaviours for Raptor-like codes with different rates when avoiding short cycles-wc.

In Fig. 12, we compare the performance curves of two $(3,5)$-regular QC-LDPC codes with girth 8, $N = 27$ and the same $d_{min} = 16$ but different graphical structures. The exponent matrix of one of them, constructed using $M_2$ in [16], is given in Example 9 and the exponent matrix of the other, $C_{13}$, is in Table X. As can be seen, for both of these cases, the performance curves are similar.

VII. CONCLUSION

We study cycles with a chord in the Tanner graph of an LDPC code and propose the impact of avoiding short cycles.
with a chord on the lower bound of the size of small trapping sets as well as on the minimum distance of the code. We provide new analytic lower bounds on the minimum distance of LDPC codes with girth 6, 8 and free of short cycles with a chord. For any protograph, simple or multi-edge, regular or irregular, we provide conditions to remove 8-cycles with a chord and 12-cycles with a chord from the Tanner graph of an LDPC code with girth 6 and 8, respectively. For girth-8 QC-LDPC codes free of 12-cycles with a chord we also present a lower bound on the lifting degree. The analytic, numerical, and simulation results in this paper prove that without increasing the girth we can improve important factors of an LDPC code that significantly influence the performance curve of the regular codes and also some irregular codes.

APPENDIX A

PROOF OF COROLLARY 1

We consider an \((a, b)\) ETS with \(b < a\) and free of 8-cycles-wc. Then, we remove some check nodes of degrees 1 or 2 connected to variable nodes of degree \(d_i \geq \gamma\) such that in the obtained ETS of size \(a\), which is the size of the original ETS, any variable node has degree at least \(\gamma\). Since through this process some check nodes of degree 1 may be removed from the original ETS, the obtained ETS has \(b'\) check nodes of degree 1, where \(b' \leq b\).

First, we suppose that in the remaining graph, the degree of each variable node is \(\gamma\). Thus, the number of edges removed from each variable node with \(d_i > \gamma\) is \(d_i - \gamma\). In this way we convert the \((a, b)\) ETS to an \((a, b')\) ETS with \(b' \leq b < a\) which belongs to an LDPC code with column weight \(\gamma\) and free of 8-cycles-wc. According to Theorem 2, for the \((a, b')\) ETS with \(b' < a\) we have \(a \geq 2\gamma - 2\). We compare the VN graph of the \((a, b)\) ETS in the irregular LDPC code with the VN graph of the \((a, b')\) ETS in the LDPC code with \(\gamma\)-degree variable nodes. The latter is formed by removing the edges from the former. Since both VN graphs have the same number of variable nodes, the inequality \(a \geq 2\gamma - 2\) is satisfied for both ETSs. Now, we assume that in the remaining graph, there exist variable nodes of degree larger than \(\gamma\), and the size of the \((a, b)\) ETS is \(a < 2\gamma - 2\). Without loss of generality, we can assume that \(a = 2\gamma - 3\). In the original ETS, there is a variable node \(v\) of degree \(d_v \geq \gamma + 1\) such that after removing check nodes the degree of \(v\) in the obtained \((a, b')\) ETS is still larger than \(\gamma\). It is clear that in the \((a, b')\) ETS, the variable node \(v\) is connected to at least \(\gamma + 1\) check nodes of degree 2. Indeed, if it is connected to at most \(\gamma\) check nodes of degree 2, then the removal of check nodes of degree 1 connected to \(v\) causes a variable node of degree \(\gamma\) in the \((a, b')\) ETS, which contradicts our assumption. Thus, in the VN graph of the \((a, b')\) ETS the variable node \(v\) is connected to at least \(\gamma + 1\) variable nodes. We suppose that in this VN graph \(d_v = \gamma + 1\) and \(N_v = \{v_1, v_2, \ldots, v_{\gamma + 1}\}\) is the set of neighbours of \(v\). Since the VN graph has \(a = 2\gamma - 3\) variable nodes, there are \((2\gamma - 3) - (\gamma + 2) = \gamma - 5\) variable nodes \(v'_1, \ldots, v'_{\gamma - 5}\) which have to be connected to some vertices in \(N_v\). Since the ETS is free of 8-cycles-wc, if two vertices \(v_i\) and \(v_j\) in \(N_v\) are connected by an edge in the VN graph, then \(v_i\) and \(v_j\) cannot be connected to a common vertex in \(\{v'_1, \ldots, v'_{\gamma - 5}\}\). Moreover, any vertex \(v_i\) in \(N_v\) can be connected to at most one vertex \(v_j\) in \(N_v\) since if \(v_i\) is connected to two vertices \(v_j\) and \(v'_j\) in \(N_v\), then there exists an 8-cycle-wc. In order to have the maximum number of edges between two sets \(N_v\) and \(\{v'_1, \ldots, v'_{\gamma - 5}\}\), we suppose that each \(v_i \in N_v\) is connected to all vertices \(v'_j\) for \(1 \leq j \leq \gamma - 5\) and \(v_i\) is not connected to \(v_j\) for \(j \in \{1, 2, \ldots, \gamma - 1\}\). Thus, the degree of each vertex \(v_i \in N_v\) is \((\gamma - 5) + 1 = \gamma - 4\). Since in the \((a, b')\) ETS the degree of each variable node is at least \(\gamma\), each vertex in \(N_v\) is connected to \(\gamma - 4\) check nodes of degree 2 and at least 4 check nodes of degree 1. This proves that the \((a, b')\) ETS has at least \(4(\gamma + 1)\) check nodes of degree 1. Thus, \(a \gamma b' \geq 4(\gamma + 1) > 2\gamma - 3 = a\) gives \(b' > a\) which is a contradiction. Other cases which occur when two vertices in \(N_v\) are connected by an edge in the VN graph make the situation worse since the \((a, b')\) ETS will have more 1-degree check nodes than the \((a, b')\) ETS which is explained above.

APPENDIX B

PROOF OF THEOREM 3

It is known that a code \(C\) has minimum distance \(d_{\text{min}}\) if and only if the Tanner graph contains no \((a, 0)\) trapping set for \(a < d_{\text{min}}\) and there exists at least one \((d_{\text{min}}, 0)\) trapping set. Since the Tanner graph is free of an 8-cycle-wc, according to Theorem 2, for an \((a, b)\) ETS with \(b < a\) we have \(a \geq 2\gamma - 2, b \geq a\gamma - \frac{2a^3}{4a^3 - 3}\). In the following, we show that the latter inequality does not hold for \(b = 0, \gamma \geq 3\) if \(a = 2\gamma - 2\) or \(a = 2\gamma - 1\).

For \(a = 2\gamma - 1\) and \(\gamma \geq 3\) we have the following which proves \(b > 0\) for \(a = 2\gamma - 1\) and \(\gamma \geq 3\):

\[
 b \geq a\gamma - \frac{2a^3}{4a^3 - 3} = (2\gamma - 1)\gamma - \frac{2(2\gamma - 1)^3}{4(2\gamma - 1)^3 - 3} \\
= \frac{2\gamma^2 - 5\gamma + 2}{8\gamma - 7} > 0.
\]

For \(a = 2\gamma - 2\) and \(\gamma \geq 3\) we have

\[
 b \geq a\gamma - \frac{2a^3}{4a^3 - 3} = (2\gamma - 2)\gamma - \frac{2(2\gamma - 2)^3}{4(2\gamma - 2)^3 - 3} \\
= (\gamma - 1) \left[ 2\gamma - \frac{16(\gamma - 1)^2}{8\gamma - 11} \right] \\
= (\gamma - 1) \left[ \frac{16\gamma - 16}{8\gamma - 11} \right] > 0.
\]

Therefore, there is no \((a, 0)\) ETS for \(a < 2\gamma\). Now, we prove the non-existence of \((a, 0)\) non-elementary trapping sets for \(a < 2\gamma\).

The process of the proof is based on a tree bound argument given in [2]. These \((a, 0)\) non-elementary trapping sets contain \(2\ell\)-degree check nodes with \(\ell > 1\). Since \(b = 0\) all check nodes are of even degrees, and since non-elementary trapping sets contain check nodes of degrees greater than 2, they contain at least one check node of degree at least 4. We consider a structure obtained from the tree bound argument and start from a check node. Suppose a trapping set contains a 4-degree check node \(c\) in the starting level. Then, \(c\) is connected to 4 variable nodes \(v_1, v_2, v_3, v_4\) in the second level. Since every variable node has degree \(\gamma\), each variable node connected to \(c\) is connected to \(\gamma - 1\) other check nodes. If two of these variable
nodes such as $v_1, v_2$ are connected to a common check node $c'$, then a 4-cycle $e_1 e_2 e_3 e_4$ (the 4-cycle in Fig. 13 with one dashed line) appears which is impossible. Therefore, there are $4(\gamma - 1)$ distinct check nodes in the third level. Similarly, if two check nodes $c_1, c_2$ in the third level, which are connected to a common variable node such as $v_3$ of the second level, are connected to another variable node $v'$ in the fourth level, then a 4-cycle $e_1 e_2 e_3 e_4$ (the 4-cycle in Fig. 13 with two dashed lines) appears which is impossible. Hence, in the fourth level, there are at least $\gamma - 1$ distinct variable nodes. If a variable node $v$ in the fourth level is connected to two check nodes $c', c''$ in the third level such that $c', c''$ are connected to two different variable nodes like $v_1, v_2$ of the second level, then a trapping set has a 6-cycle $v' e_1 v_1 v_2 e_2 e_3 v$ (the 6-cycle in Fig. 13 with highlighted lines). Thus, if the Tanner graph is free of 6-cycles, then we have $4(\gamma - 1)$ variable nodes in the fourth level and the size of a trapping set is more than or equal to $4(\gamma - 1) + 4 = 4\gamma$.

Let the trapping set have a 6-cycle. As mentioned above, in the fourth level there are $\gamma - 1$ distinct variable nodes for $\gamma - 1$ check nodes connected to $v_1$. If two of these variable nodes are connected to check nodes in the third level connected to $v_2$, then we have an 8-cycle-wc, see Fig. 14 (a). Hence, only one of the check nodes connected to $v_2$ can be connected to one of those $\gamma - 1$ variable nodes. It means that we need $\gamma - 2$ new variable nodes for $\gamma - 2$ check nodes connected to $v_2$. Continuing this process, the number of variable nodes in the fourth level is at least $(\gamma - 1) + (\gamma - 2) + (\gamma - 3) + (\gamma - 4) = 4\gamma - 10$ for $\gamma \geq 5$. Therefore, for $\gamma \geq 5$, the number of variable nodes of a trapping set containing a 4-degree check node is at least $4\gamma - 10 + 4 = 4\gamma - 6 > 2\gamma$. Moreover, considering this explanation for $\gamma = 3, 4$, we conclude that the number of variable nodes of a trapping set containing a 4-degree check node is at least $2\gamma - 3 + 4 = 7$ for $\gamma = 3$ and $3\gamma - 6 + 4 = 10$ for $\gamma = 4$. In Fig. 14 (b), (c) we show that the smallest sizes of trapping sets containing a 4-degree check node for $\gamma = 3, 4$ are 8 and 10, respectively. Thus, we need more than $2\gamma$ variable nodes to construct a trapping set containing a 4-degree check node. Hence, the $d_{\text{min}}$ is lower bounded by $2\gamma$. It is clear that if a non-elementary $(a, 0)$ trapping set does not contain a 4-degree check node, then it has an even degree check node of a degree greater than 4 for which we can have the same scenario as we have for 4-degree check nodes.

Appendix C

Proof of Theorem 4

In the Tanner graph of a girth-8 LDPC code all 8-cycles and 10-cycles are chordless. Moreover, according to Lemma 1 part (b), the necessary and sufficient condition to have a 12-cycle-wc is the existence of a check node outside the cycle which is connected to two variable nodes on the cycle. Thus, if the Tanner graph is free of cycles-wc of lengths up to 12, then the VN graph of each ETS is a triangle-free graph whose cycles of lengths up to 6 are chordless.

If the degree of each vertex in a graph is $\gamma$, then the graph is called $\gamma$-regular. The VN graph of an $(a, 0)$ ETS in the given Tanner graph with girth 8 is a triangle-free $\gamma$-regular graph. Hence, the average degree of this VN graph is $\gamma$. Consequently, the independence number of the VN graph of an $(a, 0)$ ETS in the Tanner graph of an LDPC code with girth 8 is $\alpha \geq a \gamma + 1$. On the other hand, since any 6-cycle in the VN graph is chordless and that 6-cycle has an independent set with cardinality 3, the independence number of any VN graph is at least 3. For example, an independent set corresponding to a 6-cycle on variable nodes $v_1, v_2, v_3, v_4, v_5, v_6$ is $\{v_1, v_3, v_5\}$. As a result, $\alpha \geq a \gamma + 1 \geq 3$, and we have $a \geq \frac{3(\gamma + 1)^2}{\gamma \ln \gamma - \gamma + 1}$. According to the above explanations, the lower bound on the minimum size of an $(a, 0)$ ETS is $\frac{3(\gamma - 1)^2}{\gamma \ln \gamma - \gamma + 1}$.

As shown in the proof of Theorem 3, the number of variable nodes in the fourth level of a non-elementary trapping set containing a check node of degree 4 is $4(\gamma - 1)$ if the Tanner graph is free of 6-cycles. This proves the size of the non-elementary trapping set in a girth-8 Tanner graph is at least $4(\gamma - 1) + 4 = 4\gamma$. We can use the same process for a non-elementary trapping set with a check node of a degree larger than 4. Hence, if $g = 8$, then for $(a, 0)$ non-elementary trapping sets we have $a \geq 4\gamma$ which is bigger than $\frac{3(\gamma - 1)^2}{\gamma \ln \gamma - \gamma + 1}$.

Consequently, since the size of an $(a, 0)$ trapping set is at least $\frac{3(\gamma - 1)^2}{\gamma \ln \gamma - \gamma + 1}$, the minimum distance of a girth-8 LDPC code whose Tanner graph is free of cycles-wc of lengths up to 12 is at least $\frac{3(\gamma - 1)^2}{\gamma \ln \gamma - \gamma + 1}$.

Appendix D

Proof of Theorem 12

An 8-cycle-wc from a $3 \times 4$ submatrix of $W_9$ occurs if two $3 \times 3$ submatrices of it containing 6-cycles have an statement
We should compare every two equations one of which belongs to a 3 × 3 submatrix with column indices \( j_1, j_2, j_3 \) and the other which belongs to a 3 × 3 submatrix with column indices \( j_1, j_2, j_4 \). Let us denote two equations \( \{u\} \) and \( \{v\} \) which we consider simultaneously by a pair \( \{u, v\} \). If one of the equations \( \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\} \) occurs, then \( i = j \equiv 0 \pmod{p} \) is not possible, since \( i = j \) and \( j = 3j \) modulo \( p \) are less than \( p \) and \( p \) cannot divide their products. If one of the equations \( \{1, 4\}, \{1, 6\}, \{2, 3\}, \{2, 5\}, \{3, 6\}, \{4, 5\}, \{5, 6\}, \{6, 7\} \) happens, then \( i = j \equiv 0 \pmod{p} \) \( \{2, 3\} \) or \( \{2, 6\} \) \( \{2, 3\} \) or \( \{2, 6\} \) \( \{2, 3\} \) or \( \{2, 6\} \) \( \{2, 3\} \) or \( \{2, 6\} \) \( \{2, 3\} \) or \( \{2, 6\} \). Thus, after considering all these pairs we conclude that \( \pm(j_1 + j_2) \neq \pm(j_3 + j_4) \pmod{p} \) if and only if there exists no 8-cycle-wc from two equations with \( \pm(i_1j_1 - i_2j_2) \) and \( \pm(i_1j_3 - i_2j_4) \) in common.

Finally, we obtain eight equations containing \( (i_1j_1 - i_2j_2) \) or \( (i_1j_3 - i_2j_4) \) from two \( 3 \times 3 \) submatrices of \( W_p \) one with column indices \( j_1, j_2, j_3 \) and the other with column indices \( j_1, j_2, j_4 \). By comparing all pairs of equations we conclude that \( \pm(j_2 + j_3) \neq \pm(j_1 + j_4) \pmod{p} \) if and only if there exists no 8-cycle-wc from two equations with \( \pm(i_1j_3 - i_2j_2) \) in common. Thus, a necessary and sufficient condition for a \( 3 \times 4 \) submatrix of \( W_p \) to be free of 8-cycles-wc is that \( \pm(j_1 + j_2) \neq \pm(j_3 + j_4) \pmod{p} \), \( \pm(j_1 + j_3) \neq \pm(j_2 + j_4) \pmod{p} \), and \( \pm(j_2 + j_3) \neq \pm(j_1 + j_4) \pmod{p} \).

ACKNOWLEDGMENT

The authors would like to thank the editor and the reviewers for their many helpful comments and suggestions that improved the article considerably.

REFERENCES

[1] J. Thrope, “Low-density parity-check (LDPC) codes constructed from protographs,” INP Prog. Rep., pp. 42-154, Aug. 2005, vol. 53, no. 8.
[2] R. Tanner, “A recursive approach to low complexity codes,” IEEE Trans. Inf. Theory, vol. IT-27, no. 5, pp. 533–547, Sep. 1981.
[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] R. Smarandache and P. O. Vontobel, “On regular quasi-cyclic LDPC codes from binomials,” in Proc. Int. Symp. Inf. Theory (ISIT), Jun. 2004, p. 274.
[5] L. Dolecek, Z. Zhang, V. Anantharam, M. J. Wainwright, and B. Nikolic, “Analysis of absorbing sets and fully absorbing sets of array-based LDPC codes,” IEEE Trans. Inf. Theory, vol. 56, no. 1, pp. 181–201, Jan. 2010.
[6] J. Wang, L. Dolecek, and R. D. Wesel, “The cycle consistency matrix approach to absorbing sets in separable circulant-based LDPC codes,” IEEE Trans. Inf. Theory, vol. 59, no. 4, pp. 2293–2314, Apr. 2013.
[7] D. G. M. Mitchell, R. Smarandache, and D. J. Costello, “Quasi-cyclic LDPC codes based on pre-lifted protographs,” IEEE Trans. Inf. Theory, vol. 60, no. 10, pp. 5856–5874, Oct. 2014.
[8] J. Li, S. Lin, K. Abdel-Ghaffar, W. Ryan, and D. J. Costello, LDPC Code Designs, Constructions, Unification. Cambridge, U.K.: Cambridge Univ. Press, 2016.
[9] 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.
[10] A. Tasdighi, A. H. Banihashemi, and M.-R. Sadeghi, “Symmetrical constructions for regular girth-8 QC-LDPC codes,” IEEE Trans. Comm., vol. 65, no. 1, pp. 14–22, Jan. 2017.
[11] X. Tao, Y. Li, Y. Liu, and Z. Hu, “On the construction of LDPC codes free of small trapping sets by controlling cycles,” IEEE Commun. Lett., vol. 22, no. 1, pp. 9–12, Jan. 2018.
[12] F. Amirzade and M.-R. Sadeghi, “Lower bounds on the lifting degree of QC-LDPC codes with difference matrices,” IEEE Access, vol. 6, pp. 23688–23700, 2018.
[13] M.-R. Sadeghi and F. Amirzade, “Analytical lower bound on the lifting degree of multiple-edge QC-LDPC codes with girth 6,” IEEE Commun. Lett., vol. 22, no. 8, pp. 1528–1531, Aug. 2018.
[14] M. H. Tadayon, A. Tasdighi, M. Battaglioni, M. Baldi, and F. Chiaraluce, “Efficient search of compact QC-LDPC and SC-LDPC convolutional codes with large girth,” IEEE Commun. Lett., vol. 22, no. 6, pp. 1156–1159, Jun. 2018.
[15] H. Li, B. Bai, X. Mu, J. Zhang, and H. Xu, “Algebra-assisted construction of quasi-cyclic LDPC codes for 5G new radio,” IEEE Access, vol. 6, pp. 50229–50244, 2018.
[16] S. Naseri and A. H. Banihashemi, “Construction of girth-8 QC-LDPC codes free of small trapping sets,” IEEE Commun. Lett., vol. 23, no. 11, pp. 1904–1908, Nov. 2019.
[17] C. Zhang, Y. Hu, Y. Fang, and J. Wang, “Constructions of type-II QC-LDPC codes with girth eight from Sidon sequence,” IEEE Trans. Commun., vol. 67, no. 6, pp. 3865–3878, Jun. 2019.
[18] F. Amirzade, M.-R. Sadeghi, and D. Panario, “QC-LDPC construction free of small size elementary trapping sets based on multiplicative subgroups of a finite field,” Adv. Math. Commun., vol. 14, no. 3, pp. 397–411, Aug. 2020.
[19] S. Mo, L. Chen, D. J. Costello, D. G. M. Mitchell, R. Smarandache, and J. Qiu, “Designing protograph-based quasi-cyclic spatially coupled LDPC codes with large girth,” IEEE Commun. Lett., vol. 22, no. 9, pp. 5326–5337, Sep. 2020.
[20] B. Karimi and A. H. Banihashemi, “Construction of QC LDPC codes with low error floor by efficient systematic search and elimination of trapping sets,” IEEE Trans. Commun., vol. 68, no. 2, pp. 697–712, Feb. 2020.
[21] M.-R. Sadeghi and F. Amirzade, “Edge-coloring technique to analyze elementary trapping sets of spatially-coupled LDPC convolutional codes,” IEEE Commun. Lett., vol. 24, no. 4, pp. 711–715, Apr. 2020.
[22] F. Amirzade, M.-R. Sadeghi, and D. Panario, “QC-LDPC codes with large column weight and free of small size ETSs,” IEEE Commun. Lett., vol. 26, no. 3, pp. 500–504, Mar. 2022.
[23] 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, Sep. 2008, pp. 180–185.
[24] Y. Wang, S. C. Draper, and J. S. Yedidia, “Hierarchical and high-girth QC LDPC codes,” IEEE Trans. Inf. Theory, vol. 59, no. 7, pp. 4553–4583, Jul. 2013.
[25] S. K. Chilappagari, M. Chertkov, M. G. Stepanov, and B. Vasic, “Instanton-based techniques for analysis and reduction of error floors of LDPC codes,” IEEE J. Sel. Areas Commun., vol. 27, no. 6, pp. 855–865, Aug. 2009.
Farzane Amirzade received the M.Sc. degree in mathematics from Alzahra University, Tehran, Iran, in 2006, and the Ph.D. degree in mathematics from the Shahrood University of Technology, Shahrood, Iran, in 2019. Since May 2019, she has been a Post-Doctoral Fellow with the Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran. From November 2017 to August 2018 and from May 2019 to October 2019, she was a Visitor with the School of Mathematics and Statistics, Carleton University, Ottawa, Canada, where she has been a Post-Doctoral Fellow with the School of Mathematics and Statistics, since June 2020. Her research interests include coding and information theory, graph theory, and combinatorics.

Mohammad-Reza Sadeghi received the Ph.D. degree 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, and an Adjunct Professor with Carleton University. His research interests include coding theory, lattice codes, and post-quantum 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. He serves as an Associate Editor for IEEE Communications Letters since 2019 and was awarded IEEE Communications Society as an Exemplary Editor in 2020.

Daniel Panario (Senior Member, IEEE) was born in Uruguay. He received the degree in mathematics and computer science in Uruguay, the M.Sc. degree from the University of Sao Paulo, Brazil, and the Ph.D. degree from the University of Toronto, Canada. He is currently a Professor in mathematics with Carleton University, Ottawa, ON, Canada. His main research interests are in finite fields and their applications in information theory and communications and in the analysis of algorithms.