QC-LDPC CONSTRUCTION FREE OF SMALL SIZE ELEMENTARY TRAPPING SETS BASED ON MULTIPLICATIVE SUBGROUPS OF A FINITE FIELD

Farzane Amirzade
Department of Mathematics and Computer Science
Amirkabir University of Technology
Tehran, 1591634312, Iran

Mohammad-Reza Sadeghi∗
Department of Mathematics and Computer Science
Amirkabir University of Technology
Tehran, 1591634312, Iran

Daniel Panario
School of Mathematics and Statistics
Carleton University
Ottawa, K1S 5B6, Canada

Abstract. Trapping sets significantly influence the performance of low-density parity-check codes. An \((a, b)\) elementary trapping set (ETS) causes high decoding failure rate and exert a strong influence on the error floor of the code, where \(a\) and \(b\) denote the size and the number of unsatisfied check-nodes in the ETS, respectively. The smallest size of an ETS in \((3, n)\)-regular LDPC codes with girth 6 is 4. In this paper, we provide sufficient conditions to construct fully connected \((3, n)\)-regular algebraic-based QC-LDPC codes with girth 6 whose Tanner graphs are free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\). We apply these sufficient conditions to the exponent matrix of a new algebraic-based QC-LDPC code with girth at least 6. As a result, we obtain the maximum size of a submatrix of the exponent matrix which satisfies the sufficient conditions and yields a Tanner graph free of those ETSs with small size. Some algebraic-based QC-LDPC code constructions with girth 6 in the literature are special cases of our construction. Our experimental results show that removing ETSs with small size contribute to have better performance curves in the error floor region.

1. Introduction

Quasi-cyclic low-density parity-check (or simply QC-LDPC) codes are among the most popular channel coding schemes due to their good performance under iterative decoding. This type of LDPC codes are divided into two categories: algebraic-based and graph-theoretic-based constructions. Of the latter, progressive-edge-growth (PEG) and protograph-based are the most well-known methods. Among several works devoted to algebraic-based QC-LDPC code structure, we point out [8, 13, 14, 15, 16, 19, 22, 29, 30], to name a few.
A Tanner graph associated to an LDPC code is a bipartite graph in which one part consists of the variable-nodes and the other part consists of the check-nodes. If each variable-node and each check-node has degree $\gamma$ and $n$, respectively, then Tanner graph corresponds to a $(\gamma, n)$-regular LDPC code.

Each algebraic-based QC-LDPC code is developed from an exponent matrix. Each non-zero element of an exponent matrix is replaced by a circulant permutation matrix and every zero element by a zero matrix. The null space of the resulting matrix is the parity-check matrix of an $(\ell, k)$ QC-LDPC code in which $\ell, k$, respectively, are the length of the code and the rank of the parity-check matrix. A $\gamma \times n$ exponent matrix free of zero element results in a fully-connected $(\gamma, n)$-regular QC-LDPC code.

Different features influence the performance of an LDPC code. Among them, those related to graphical structures in the Tanner graph are short cycles, girth (that is the length of the shortest cycle), trapping sets, absorbing sets and stopping sets. For example, it is well recognized that short cycles in the Tanner graph deteriorate the performance of a code, so constructions leading to the existence of 4-cycles in their Tanner graphs are prevented. Consequently, almost all of explicit structures proposed for algebraic-based QC-LDPC codes produce a Tanner graph with girth at least 6. However, obtaining Tanner graphs with larger girth has become a subject of research interest [2, 5, 6, 11, 14, 18, 19, 20, 21, 23, 25, 27, 28]. In order to decrease the number of short cycles, and probably raise the girth from 6 to at least 8, a technique known as masking has been employed by which some nonzero elements of an exponent matrix are turned into zero. In [14], an algorithm is presented which determines whether an exponent matrix after being masked constructs a $(3, 6)$-regular QC-LDPC code whose Tanner graph has girth at least 8. For example, it is shown that an exponent matrix over $\mathbb{F}_{331}$ which contains $\binom{330}{4}\binom{330}{8}$ (or approximately $1.6 \times 10^{24}$) $4 \times 8$ submatrices has only 74336 $(4 \times 8)$ submatrices that after being masked result in QC-LDPC codes with girth at least 8. This implies that the number of desired $4 \times 8$ submatrices are a very small fraction of all $4 \times 8$ submatrices of the exponent matrix.

As mentioned above, another phenomena that influence the performance of LDPC codes are known as trapping sets and absorbing sets. An $(a, b)$ trapping set is a set of $a$ variable-nodes in the Tanner graph which induce a subgraph of the Tanner graph with exactly $b$ check-nodes of odd degrees, named as unsatisfied check-nodes, and any number of even degree check-nodes. The even degree check-nodes are the satisfied check-nodes. Empirical results in the literature show that among all trapping sets, the most harmful ones are those with check-nodes of degree 1 or 2. This category is called elementary trapping sets (or simply ETSs). All unsatisfied check-nodes in an elementary trapping set have degree one.

Given an $(a, b)$ trapping set, the set of variable-nodes is denoted by $S$. We suppose that for each $v \in S$ a set of odd degree check-nodes connected to $v$ is denoted by $O(v)$ and the set of even degree check-nodes connected to $v$ is denoted by $E(v)$. If for each $v \in S$ we have $|O(v)| < |E(v)|$, then the trapping set is an $(a, b)$ absorbing set. We recall that an $(a, b)$ absorbing set is elementary (EAS) if all check-nodes are of degree 1 or 2. Smallest absorbing sets are referred as dominant since an absorbing set is activated when all of its variable-nodes are in error and this activation is more likely for a smaller number of variable-nodes than a large number of variable-nodes [26].
Recently, constructing LDPC codes whose Tanner graph is free of small size ETSs and/or EASs has become an interesting research subject. Increasing the girth can be a technique to eliminate harmful small size trapping sets since, according to [3], as the girth increases, the lower bound on the size of trapping sets increases too. For example, for variable regular LDPC codes whose Tanner graphs have girths 6 and 8, the lower bound on the size of \((a, b)\) ETSs with \(\frac{b}{a} < 1\) is \(\gamma + 1\) and \(2\gamma - 1\), respectively.

Another technique is the PEG algorithm which was used in [17] to construct QC-LDPC codes whose Tanner graphs are free of some small trapping sets. An improved PEG algorithm [10] results in a \((3, n)\)-regular LDPC code with girth 8 whose Tanner graph is free of \((6, 4)\) trapping sets and contains a minimum number of \((6, 4)\) trapping sets. To avoid \((a, b)\) ETSs in \((3, n)\)-regular QC-LDPC codes with girth 8, where \(a \leq 8\) and \(b \leq 3\), see [24]. Moreover, a method named as edge-coloring technique was proposed in [4] which contributes to obtain sufficient conditions for an exponent matrix to avoid a specific ETS and/or EAS from occurrence in the Tanner graph. This technique was applied to fully-connected protograph-based QC-LDPC codes to obtain sufficient conditions for exponent matrices to construct a girth-6 fully-connected QC-LDPC code with column weight 3 and free of \((a, b)\) ETSs with \(a \leq 5, b \leq 2\) as well as a girth-8 fully-connected QC-LDPC code with column weight 3 and free of \((a, b)\) ETSs with \(a \leq 8\) and \(b \leq 3\). The proposed sufficient conditions are based on controlling some 8-cycles in the Tanner graphs.

In this paper, our main goal is to extend the results of [4] to algebraic-based QC-LDPC codes. We provide sufficient conditions for an exponent matrix of an algebraic-based girth-6 QC-LDPC code whose Tanner graph is free of \((a, b)\) ETSs with \(a \leq 5, b \leq 2\) as well as a girth-8 fully-connected QC-LDPC code with column weight 3 and free of \((a, b)\) ETSs with \(a \leq 8\) and \(b \leq 3\). The proposed sufficient conditions are based on controlling some 8-cycles in the Tanner graphs.

In [30], a method is proposed to construct an exponent matrix based on two multiplicative subgroups of the finite field \(\mathbb{F}_q\) in which \(q - 1\) can be factored into two relatively prime integers and the exponent matrix contains \((q - 1)^2\) elements from which \(q - 1\) entries are zeros. In this paper, we present a new construction of QC-LDPC codes based on multiplicative cyclic subgroups of a finite field in which \(q - 1\) is factored into more than two integer numbers. The Tanner graph corresponding to the exponent matrix has girth 6. Our purpose is to achieve a submatrix of the exponent matrix whose corresponding parity-check matrix has a Tanner graph free of \((a, b)\) ETSs with \(a \leq 5, b \leq 2\). We specifically consider a finite field \(\mathbb{F}_q\) in which \(q - 1\) can be factored into three relatively prime integers.
The rest of the paper is organized as follows. Section 2 presents some basic notation and definitions. Section 3 is devoted to obtaining sufficient conditions for the exponent matrix of an algebraic-based QC-LDPC code whose corresponding Tanner graph has girth 6 and is free of ETSs with small size. Moreover, in this section we consider necessary and sufficient conditions to have a Tanner graph with a certain girth. In Section 4, we give our method for constructing a QC-LDPC code based on cyclic multiplicative subgroups of a finite field. This section contains three subsections. In the first subsection we consider algebraic QC-LDPC codes over finite fields $\mathbb{F}_q$, where $q - 1$ is the product of three relatively prime numbers. In the second subsection, we prove the girth of the Tanner graph is at least 6. Finally, in the third subsection, we apply the sufficient condition proposed in Section 3 to the exponent matrix to obtain the maximum size of a submatrix which yields a girth-6 column weight three QC-LDPC code free of small size ETSs. In the last section of the paper we summarize our results.

2. Preliminaries

Consider the finite field $\mathbb{F}_q$, where $q$ is a power of a prime. Let $\alpha \in \mathbb{F}_q$ be a primitive element. The powers of $\alpha$, $\alpha^{-\infty} = 0, \alpha^0 = 1, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}$ give all elements of $\mathbb{F}_q$ and $\alpha^{q-1} = 1$. For each nonzero element $\alpha^j$ of $\mathbb{F}_q$, $0 \leq j < q$, we construct a $(q - 1) \times (q - 1)$ circulant permutation matrix (or CPM) in which the only nonzero element of its top row is located at the $j$-th position. The $i$-th row of the matrix is formed by $i$ right cyclic shifts of the first row. It is clear that the first row is a right cyclic shift of the last row. Moreover, for the zero element of $\mathbb{F}_q$ we have a $(q - 1) \times (q - 1)$ zero matrix (ZM).

In order to investigate 4-cycles in Tanner graph, every two columns and two rows of the parity-check matrix have to be checked. If the parity-check matrix $H$ is free of $2 \times 2$ all-one submatrix, then $H$ has the property of row-column (RC)-constraint. Let $B$ be the exponent matrix of an algebraic-based QC-LDPC code whose elements belong to a finite field $\mathbb{F}_q$. In order to obtain a QC-LDPC code with the property of (RC)-constraint, we consider a submatrix of an exponent matrix $B$ whose elements hold the following necessary and sufficient conditions.

**Theorem 2.1.** ([9]) Let $B$ be the exponent matrix of a QC-LDPC code whose parity-check matrix is constructed by substituting every entry of $B$ by its corresponding CPM or ZM. A necessary and sufficient condition for the Tanner graph to have girth at least 6 is that every $2 \times 2$ submatrix in the exponent matrix $B$ contains at least one zero entry or is non-singular.

Let a QC-LDPC code be 4-cycle free. The Tanner graph has 6-cycles if and only if the parity-check matrix has one of the following six formats for each $3 \times 3$ submatrix:

\[
\begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 1 \\
1 & 0 & 1
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & 1 & 0 \\
1 & 1 & 0 \\
1 & 1 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & 1 & 0 \\
0 & 0 & 1 \\
1 & 1 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & 0 & 1 \\
1 & 0 & 1 \\
1 & 0 & 1
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & 1 & 0 \\
1 & 1 & 0 \\
1 & 1 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & 1 \\
0 & 1 & 1 \\
1 & 1 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
0 & 1 & 1 \\
0 & 1 & 1 \\
1 & 1 & 0
\end{bmatrix}
\]

Using the following theorem, we can check the 6-cycles in the exponent matrix.

**Theorem 2.2.** ([9]) A necessary and sufficient condition for the Tanner graph to have girth at least 8 is that no $2 \times 2$ and $3 \times 3$ submatrix in the exponent matrix $B$ has two identical nonzero terms in its determinant expansion.
In order to improve the performance curve of a code, instead of raising the girth, we can remove the most harmful trapping sets and/or absorbing sets in its Tanner graph. Therefore, we need some important definitions related to trapping sets, absorbing sets and their graphical structures.

**Definition 2.3.** For a bipartite graph $G$ corresponding to an ETS and/or EAS, a **variable node (VN) graph** is constructed by removing all degree-one check-nodes, defining variable-nodes of $G$ as its vertices and degree-two check-nodes connecting the variable-nodes in $G$ as its edges.

Any cycle of length $k$ in the VN graph is equivalent to a $2k$-cycle in its corresponding ETS and/or EAS. For example, a sequence of $v_0, c_0, v_1, c_1, v_2, c_2, v_0$ as a 6-cycle in an ETS, where $v_i \in V$ and $c_i \in C$, is equivalent to a triangle with vertices $v_1, v_2, v_3$ in the VN graph. Therefore, in a Tanner graph with girth at least 8, the VN graph of each ETS is a triangle-free graph. For example, in Fig. 1 the EAS contains no 6-cycles and its corresponding VN graph is triangle-free. Variable-nodes, satisfied and unsatisfied check-nodes are denoted by circles, empty squares and full squares, respectively.

### 3. Algebraic-based QC-LDPC codes with column weight 3, girth 6 and free of ETSs of small size

In [4] it is proved that one of the sufficient conditions to construct a QC-LDPC code with column weight 3 and girth 6 whose Tanner graph is free of small ETSs is the removal of 8-cycles obtained from two rows of the exponent matrix. In this section, we revise this sufficient condition and then we provide an equivalent result for algebraic-based QC-LDPC codes. We need the following definition.

**Definition 3.1.** An **edge coloring of a graph**, $G$, is an assignment of colors (labels) to the edges of the graph so that no two adjacent edges have the same color (label). The minimum required number of colors for the edges of a given graph is the **chromatic index of the graph** which is denoted by $\chi'(G)$, or simply $\chi'$, which indicates the graph has a $\chi'$-edge-coloring.

The following theorem known as Vizing theorem gives the chromatic index of a graph.

**Theorem 3.2.** [7] If $\Delta(G)$ is the maximum degree of a graph $G$, then $\Delta(G) \leq \chi' \leq \Delta(G) + 1$.
Definition 3.3. An algebraic-based fully connected \((\gamma, n)\)-regular QC-LDPC code is an algebraic-based QC-LDPC code whose \(\gamma \times n\) exponent matrix contains no zeros.

Consider a fully connected QC-LDPC code. Every vertex of a VN graph corresponds to a column of \(B\) and each edge of a VN graph corresponds to a row of \(B\). The degree of each vertex in a VN graph determines the number of rows of the exponent matrix which are involved in an ETS.

Suppose \(r_1, r_2, \ldots, r_\gamma\) are row indices of a \(\gamma \times n\) exponent matrix. Clearly, the degree of each variable-node in the VN graph is at most \(\gamma\). We characterize each edge of the VN graph by a row index of \(B\). The existence of two adjacent edges with the same row indices in the VN graph indicates that a column of the parity-check matrix contains two 1-components which belong to a CPM which is impossible because of the definition of CPM. If characterizing each edge of the VN graph by a row index of the exponent matrix results in an edge-coloring for the VN graph, then row indices can be taken as the required colors for the edges of the VN graph. Otherwise, Vizing theorem proves that we need \(\gamma + 1\) colors for the edges of VN graph.

Proposition 1. [4] Given a fully connected \((\gamma, n)\)-regular QC-LDPC code, a necessary condition for the Tanner graph to contain an \((a, b)\) ETS is that the VN graph has a \(\gamma\)-edge-coloring.

From Proposition 1, which is independent of the girth of the Tanner graph, we conclude that in a fully connected \((\gamma, n)\)-regular QC-LDPC code, the number of colors we use for the edges of the VN graph existing in the Tanner graph has to be equal to the number of rows of the exponent matrix. For example, suppose \(u, v, w\) are three row indices of a \(3 \times n\) exponent matrix. The smallest size of ETSs in the Tanner graph of LDPC codes with column weight 3 is 4 [12]. They are \((4, 0)\) and \((4, 2)\) ETSs whose VN graphs are shown in Fig.2 (a) and (b). Each edge of the VN graphs of \((4, 0)\) and \((4, 2)\) ETSs is labeled by a row index of the exponent matrix and no two adjacent edges have the same label. Thus, we conclude that these two VN graphs which have 3-edge-coloring exist in Tanner graph. However, since using every coloring method to color the edges of the VN graph corresponding to the \((5, 1)\) ETS shown in Fig.2 (c) with three row indices \(u, v, w\) we end up with a vertex containing two adjacent edges with the same color, we conclude that the VN graph of \((5, 1)\) ETS has no 3-edge-coloring and so the Tanner graph of a fully connected \((3, n)\)-regular QC-LDPC code with girth 6 contains no \((5, 1)\) ETS.

One of the main contributions of this section is that instead of using the PEG algorithm and the masking technique, we provide sufficient conditions for the exponent matrix \(B\) to obtain fully connected \((3, n)\)-regular algebraic-based QC-LDPC codes with girth 6 whose Tanner graphs are free of \((4, 0)\) and \((4, 2)\) ETSs. To provide an explicit method to remove these ETSs we have to obtain a necessary and sufficient condition for the exponent matrix of an algebraic-based QC-LDPC code to avoid 8-cycles which is proposed for the first time in this paper.

Let \(B\) be an exponent matrix of an algebraic-based QC-LDPC code. We substitute each element \(b_{m,n}^{b_{m,n}}\) in the exponent matrix \(B\) by \(b_{m,n}\), where \(b_{m,n} \in \{1, 2, \ldots, q - 1\}\), and zero elements by \((\infty)\) to obtain an equivalent matrix \(B'\) which can be used to check different \(2k\)-cycles in the Tanner graph using Fossorier’s Lemma [11]. If
Figure 2. The variable node graphs of $(4, 0)$, $(4, 2)$ and $(5, 1)$ ETSs with girth 6.

\[\sum_{i=0}^{k-1} (b_{m_i n_i} - b_{m_{i+1} n_{i+1}}) \equiv 0 \pmod{q - 1},\]

where $n_k = n_0$, $m_i \neq m_{i+1}$, $n_i \neq n_{i+1}$ and $b_{m_i n_i}$ is the $(m_i, n_i)$-th entry of $B'$, then the Tanner graph of the parity-check matrix has cycles of length $2k$. This approach allows us to use the results obtained in protograph-based QC-LDPC codes related to cycles with larger lengths, such as 8-cycles and 10-cycles. For example, the following proposition provides an equivalent version of Theorem 2.2 to check 6-cycles using Fossorier’s Lemma.

**Proposition 2.** If a $3 \times 3$ submatrix of an exponent matrix $B'$ has two diagonals, either broken diagonals or main diagonal, that sum to an identical value, then the Tanner graph has 6-cycles.

**Proof.** Let $P$ be a $3 \times 3$ submatrix of an exponent matrix $B$ in which the exponents of elements form the $3 \times 3$ submatrix $P'$ of $B'$

\[P' = \begin{bmatrix} b_{i_1 j_1} & b_{i_1 j_2} & b_{i_1 j_3} \\ b_{i_2 j_1} & b_{i_2 j_2} & b_{i_2 j_3} \\ b_{i_3 j_1} & b_{i_3 j_2} & b_{i_3 j_3} \end{bmatrix}.\]

According to Theorem 2.2, if a determinant expansion of $P$ has two identical terms, then the Tanner graph has 6-cycles. Each term in the determinant expansion is obtained by multiplying elements in a diagonal of $P$. If $\alpha^{b_{i_1 j_1} + b_{i_2 j_2} + b_{i_3 j_3}} = \alpha^{b_{i_1 j_2} + b_{i_2 j_3} + b_{i_3 j_1}}$, then we have the equality $b_{i_1 j_1} + b_{i_2 j_2} + b_{i_3 j_3} = b_{i_1 j_2} + b_{i_2 j_3} + b_{i_3 j_1}$ which can be also obtained from Fossorier’s Lemma

\[b_{i_1 j_1} - b_{i_1 j_2} + b_{i_2 j_2} - b_{i_2 j_3} + b_{i_3 j_3} - b_{i_3 j_1} = 0.\]

Clearly the three terms $b_{i_1 j_1}, b_{i_2 j_2}$ and $b_{i_3 j_3}$ are on a diagonal and the other terms $b_{i_1 j_2}, b_{i_2 j_3}$ and $b_{i_3 j_1}$ are on another (broken) diagonal. The same happens with any two diagonals. Hence, Theorem 2.2 and Fossorier’s Lemma prove that if among six diagonals, there are two diagonals whose elements sum to an identical value, then the Tanner graph has 6-cycles. \qed
Using Fosserier’s Lemma, we also present the necessary and sufficient condition to remove 8-cycles obtained from two rows of an exponent matrix.

**Theorem 3.4.** Let $\mathbf{B}$ be an exponent matrix. The necessary and sufficient conditions to remove 8-cycles obtained from two rows of $\mathbf{B}$ are:

(i) if $\alpha^d$ is the division of two nonzero terms in the determinant expansion of a $2 \times 2$ submatrix of $\mathbf{B}$, then $2d \equiv 0 \pmod{q-1}$;

(ii) if $\alpha^d$ and $\alpha^{d'}$ are two divisions of two nonzero terms in the determinant expansion of two $2 \times 2$ submatrices of $\mathbf{B}$ with same row indices, then $d \not\equiv d' \pmod{q-1}$.

**Proof.** Suppose $\mathbf{P} = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$ is a submatrix of $\mathbf{B}$. Then, its corresponding submatrix in $\mathbf{B}'$ is $\mathbf{P}' = \begin{bmatrix} i_1 & i_2 \\ i_3 & i_4 \end{bmatrix}$. Using Fosserier’s Lemma, if $i_1 - i_2 + i_4 - i_3 + i_1 - i_2 + i_4 - i_3 \equiv 0 \pmod{q-1}$, then the Tanner graph has 8-cycles. From $i_1 - i_2 + i_4 - i_3 + i_1 - i_2 + i_4 - i_3 = 2(i_1 + i_4 - i_2 - i_3)$ and $|\mathbf{P}| = \alpha^{(i_1+i_4) - (i_2+i_3)}$ we conclude that if $\alpha^d$ is the division of two nonzero terms of $|\mathbf{P}|$, or equivalently if $\alpha^d = \frac{\alpha^{(i_1+i_4)}}{\alpha^{(i_2+i_3)}} = \alpha^{i_1+i_4-i_2-i_3}$, then an equality $2d \equiv 0 \pmod{q-1}$ proves the existence of 8-cycles in Tanner graph.

For $2 \times 3$ submatrices we have $\mathbf{P} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{14} & \alpha_{15} & \alpha_{16} \end{bmatrix}$ as submatrix of $\mathbf{B}$. Then $\mathbf{P}$ can be viewed as two $2 \times 2$ submatrices $\mathbf{P}_1 = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{14} & \alpha_{15} \end{bmatrix}$ and $\mathbf{P}_2 = \begin{bmatrix} \alpha_{12} & \alpha_{13} \\ \alpha_{15} & \alpha_{16} \end{bmatrix}$.

Applying Fosserier’s Lemma to the submatrix $\mathbf{P}' = \begin{bmatrix} i_1 & i_2 & i_3 \\ i_4 & i_5 & i_6 \end{bmatrix}$ shows that $i_1 - i_2 + i_5 - i_6 + i_3 - i_2 + i_5 - i_4 \equiv 0 \pmod{q-1}$ results in 8-cycles. By rearranging the terms of the left hand side of the last equation we obtain $(i_1 + i_5 - i_2 - i_4) - (i_2 + i_5 - i_3)$. Since $|\mathbf{P}_1| = \alpha^{(i_1+i_5) - (i_2+i_4)}$ and $|\mathbf{P}_2| = \alpha^{(i_2+i_5) - (i_2+i_3)}$, we conclude that if for $\alpha^d = \frac{\alpha^{(i_1+i_5)}}{\alpha^{(i_2+i_4)}}$ and $\alpha^{d'} = \frac{\alpha^{(i_2+i_5)}}{\alpha^{(i_3+i_5)}}$ we have $d \equiv d' \pmod{q-1}$, then the Tanner graph has 8-cycles.

Each submatrix with two rows and at most four columns is equivalent to two $2 \times 2$ submatrices with determinants $\alpha^d$ and $\alpha^{d'}$. Similarly, we can show that rearranging the terms in the left hand side of Fosserier’s Lemma proves that if $d \equiv d' \pmod{q-1}$, then the Tanner graph has 8-cycles.

**Theorem 3.5.** Suppose $\mathbf{Q}$ is a $3 \times n$ submatrix of the exponent matrix $\mathbf{B}$. If $\mathbf{Q}$ satisfies parts (i) and (ii) of Theorem 3.4 and $\mathbf{Q}$ is free of zero element, then $\mathbf{Q}$ results in a fully connected $(3,n)$-regular QC-LDPC code whose Tanner graph is free of $(4,0)$ and $(4,2)$ ETSs.

**Proof.** As it can be shown from Fig.2 (a) and (b), each 4-cycle in the VN graphs of $(4,0)$ and $(4,2)$ ETSs is colored with 2 labels. Therefore, each 8-cycle in the Tanner graph is caused by two rows of the exponent matrix. To remove them, one has to avoid 8-cycles obtained from two rows of the exponent matrix. Since Theorem 3.4 gives necessary and sufficient conditions to remove the mentioned 8-cycles, we conclude that a sufficient condition to construct a fully connected $(3,n)$-regular QC-LDPC code whose Tanner graph is free of $(4,0)$ and $(4,2)$ ETSs is that $\mathbf{Q}$ satisfies parts (i) and (ii) of Theorem 3.4.

Theorem 3.5 enables us to determine the submatrices of an exponent matrix of an algebraic-based QC-LDPC code which result in girth-6 QC-LDPC codes with column
weight $3$ and free of $(a,b)$ ETSs with $a \leq 5$, $b \leq 2$. For example, in [1] Theorem
3.5 is applied to a well-known algebraic-based construction of girth-6 QC-LDPC
code based on powers of a primitive element $\alpha$ in a finite field $\mathbb{F}_q$. In this structure,
m is the largest prime factor of $q - 1$ such that $q - 1 = cn$ and $\beta = \alpha^\psi$. The $ij$-th
element of the exponent matrix in this construction method is $B_{ij} = (\beta^{i-1})^{j-1}$,
where $i, j \in \{0, 1, \ldots, m - 1\}$. The application of Theorem 3.5 to this structure
proves that for $q = 32$ and $q = 256$ the maximum size of $3 \times n$ submatrices of $B$
satisfying Theorem 3.5 are $3 \times 6$ and $3 \times 4$, respectively.

4. A NEW CONSTRUCTION OF QC-LDPC CODES

In this section we, first, provide our method to construct QC-LDPC codes based
on factors of $q - 1$. Then, we show that some construction methods in the literature
are particular cases of our proposed method. Finally, we apply Theorem 3.5 to the
exponent matrix to obtain submatrices of the maximum size whose Tanner graphs
are free of $(a,b)$ ETSs with $a \leq 5$ and $b \leq 2$.

Let $q$ be a prime power such that $q - 1 = d_1 d_2 \ldots d_\ell$, where for $i, j \in \{1, 2, \ldots, \ell\}$,
$i \neq j$, we have $\gcd(d_i, d_j) = 1$. Let $\alpha$ be a primitive element of $\mathbb{F}_q$ with
$\delta = \alpha^{d_\ell - d_{\ell-1}}$, $\beta_1 = \alpha^{d_\ell - d_{\ell-2}}$, $\ldots$, $\beta_{\ell-2} = \alpha^{d_\ell - d_{\ell-3}}, \gamma = \alpha^{d_\ell - d_{\ell-1}}$. Clearly, the orders
of $\delta, \beta_1, \ldots, \beta_{\ell-2}, \gamma$ are $d_1, d_2, \ldots, d_\ell$, respectively. We have $\ell$ cyclic subgroups
of the multiplicative group of $\mathbb{F}_q$

$$G_1 = \{\delta^0 = 1, \delta, \delta^2, \ldots, \delta^{d_1-1}\}, G_2 = \{\beta_1^0 = 1, \beta_1, \beta_1^2, \ldots, \beta_1^{d_2-1}\}, \ldots,$$
$$G_{\ell-1} = \{\beta_{\ell-2}^0 = 1, \beta_{\ell-2}, \beta_{\ell-2}^2, \ldots, \beta_{\ell-2}^{d_{\ell-2}-1}\} \quad \text{and} \quad G_\ell = \{\gamma^0 = 1, \gamma, \gamma^2, \ldots, \gamma^{d_\ell-1}\}.$$

We choose two factors of $q - 1$ like $d_1$ and $d_\ell$. For each $d_i, 2 \leq i \leq \ell - 1$ we
construct $B_i = [W_{(i,0)}, \ldots, W_{(i,d_i-1)}]$, where $W_{(i,k)}_{m,n} = \delta_{i}^m \beta_{i}^n - \gamma^k$ and $W_{(i,k)}$
is a $d_1 \times d_\ell$ matrix:

$$W_{(i,k)} = \begin{bmatrix}
\delta_{i}^0 \beta_{i}^0 - \gamma^k & \delta_{i}^0 \beta_{i}^1 - \gamma^k & \ldots & \delta_{i}^0 \beta_{i}^{d_1-1} - \gamma^k \\
\delta_{i}^1 \beta_{i}^0 - \gamma^k & \delta_{i}^1 \beta_{i}^1 - \gamma^k & \ldots & \delta_{i}^1 \beta_{i}^{d_1-1} - \gamma^k \\
\vdots & \vdots & \ddots & \vdots \\
\delta_{i}^{d_1-1} \beta_{i}^0 - \gamma^k & \delta_{i}^{d_1-1} \beta_{i}^1 - \gamma^k & \ldots & \delta_{i}^{d_1-1} \beta_{i}^{d_1-1} - \gamma^k
\end{bmatrix},$$

(3)

The exponent matrix is

$$B = [B_2, \ldots, B_{\ell-1}].$$

(4)

Clearly entries of $W_{(i,k)}$ are elements of $\mathbb{F}_q$ and all are nonzero elements with
the exception of $(0,0)$-th entry of $W_0$ which is $\delta_{i}^0 \beta_{i}^0 - \gamma^0 = 0$. In order to illustrate
our proposal structure, we provide in detail in the next subsection the case when
$q - 1$ can be factored into three relatively prime numbers. We also point out some
algebraic-based constructions of QC-LDPC codes in the literature which are special
cases of the proposed construction.

4.1. ALGEBRAIC QC-LDPC CODES BASED ON THREE MULTIPLICATIVE SUBGROUPS

OF A FINITE FIELD. Let $q$ be a prime power such that $q - 1$ can be factored as a
product of three integers $a$, $b$ and $c$ that are relatively prime. Let $\alpha$ be a primitive
element of $\mathbb{F}_q$ with $\delta = \alpha^{bc}$, $\beta = \alpha^{ac}$ and $\gamma = \alpha^{ab}$. Then, the orders of $\delta, \beta$
and $\gamma$ are $a, b$ and $c$, respectively. The three sets $G_1 = \{\delta^0 = 1, \delta, \ldots, \delta^{a-1}\}$,
$G_2 = \{\beta^0 = 1, \beta, \ldots, \beta^{b-1}\}$ and $G_3 = \{\gamma^0 = 1, \gamma, \ldots, \gamma^{c-1}\}$ form three cyclic
subgroups of the multiplicative group of $\mathbb{F}_q$. Since $a, b$ and $c$ are relatively prime, we have $G_1 \cap G_2 \cap G_3 = \{1\}$. For $0 \leq k < c$ consider the following $a \times b$ matrix $W_k$:

\[
W_k = \begin{bmatrix}
\delta^0 \beta^0 - \gamma^k & \delta^0 \beta^1 - \gamma^k & \cdots & \delta^0 \beta^{b-1} - \gamma^k \\
\delta^1 \beta^0 - \gamma^k & \delta^1 \beta^1 - \gamma^k & \cdots & \delta^1 \beta^{b-1} - \gamma^k \\
\vdots & \vdots & \ddots & \vdots \\
\delta^{a-1} \beta^0 - \gamma^k & \delta^{a-1} \beta^1 - \gamma^k & \cdots & \delta^{a-1} \beta^{b-1} - \gamma^k 
\end{bmatrix}.
\]

An $a \times bc$ exponent matrix is formed from $W_k$ as follows:

\[
B = [W_0 \ W_1 \ W_2 \ldots \ W_{e-1}].
\]

**Example 1.** Consider the finite field $\mathbb{F}_{31}$ and $\alpha = 3$ a primitive element. We factor $31 - 1 = 30$ as the product of $2 \times 3 \times 5$. Set $a = 3, \ b = 2$ and $c = 5$. Form three cyclic subgroups of the multiplicative group of $\mathbb{F}_{31}$, $G_1 = \{\delta^0, \delta^1, \delta^2\}, \ G_2 = \{\beta^0, \beta^1\}$ and $G_3 = \{\gamma^0, \gamma^1, \gamma^2, \gamma^3, \gamma^4\}$. To clarify the construction we, first, form $W_0$:

\[
W_0 = \begin{bmatrix}
\delta^0 \beta^0 - \gamma^0 & \delta^0 \beta^1 - \gamma^0 \\
\delta^1 \beta^0 - \gamma^0 & \delta^1 \beta^1 - \gamma^0 \\
\delta^2 \beta^0 - \gamma^0 & \delta^2 \beta^1 - \gamma^0 
\end{bmatrix} = \begin{bmatrix}
0 & \alpha^{15} - 1 \\
\alpha^{10} - 1 & \alpha^{25} - 1 \\
\alpha^{20} - 1 & \alpha^5 - 1 
\end{bmatrix}.
\]

Since $\alpha = 3$, in $\mathbb{F}_{31}$ we have $\alpha^{10} - 1 = \alpha^{13}, \alpha^{20} - 1 = \alpha^{18}, \alpha^{15} - 1 = \alpha^9, \alpha^{25} - 1 = \alpha^{20}$ and $\alpha^{35} - 1 = \alpha^{10}$. Then we have $W_0 = \begin{bmatrix}
0 & \alpha^9 \\
\alpha^{13} & \alpha^{20} \\
\alpha^{18} & \alpha^{10} 
\end{bmatrix}$.

After obtaining all $W_k$s, where $0 \leq k < 5$, and concatenating them in a matrix we achieve the following exponent matrix

\[
B = \begin{bmatrix}
0 & \alpha^9 & \alpha^6 & \alpha^{22} & \alpha^{13} & \alpha^{17} & \alpha^{16} & \alpha^5 & \alpha^{15} & \alpha^{16} \\
\alpha^{13} & \alpha^{20} & \alpha^2 & \alpha^{29} & \alpha^7 & \alpha^{29} & \alpha^{24} & \alpha^{27} & \alpha^{18} & \alpha^9 \\
\alpha^{18} & \alpha^{10} & \alpha^8 & \alpha^{14} & \alpha^{16} & \alpha^{26} & \alpha^{30} & \alpha^{17} & \alpha^1 & \alpha^{13} 
\end{bmatrix}.
\]

If we substitute all nonzero elements of $B$ by CPMs and the zero element by the ZM then the null space of the resulting parity-check matrix gives a QC-LDPC code with length 300.

**Example 2.** Take $c = 1$ and $ab = q - 1$. In this case, $\delta = \alpha^b$ and $\beta = \alpha^a$. Then, the orders of $\delta, \beta$ are $a$ and $b$, respectively. The three cyclic subgroups of the multiplicative group of $\mathbb{F}_q$ are $G_1 = \{\delta^0 = 1, \delta^1, \ldots, \delta^{a-1}\}, \ G_2 = \{\beta^0 = 1, \beta^1, \ldots, \beta^{b-1}\}$, and $G_3 = \{1\}$. Therefore, $W_0 = B$ with $B_{ij} = \delta^i \beta^j - 1$. This exponent matrix is given in [29].

**Example 3.** Take $b = 1$ and $ac = q - 1$. In this case $\delta = \alpha^c$ and $\gamma = \alpha^a$. Then, the orders of $\delta$ and $\gamma$ are $a$ and $c$, respectively. The three cyclic subgroups of the multiplicative group of $\mathbb{F}_q$ are $G_1 = \{\delta^0 = 1, \delta^1, \ldots, \delta^{a-1}\}, \ G_2 = \{1\}$, and $G_3 = \{\gamma^0 = 1, \gamma^1, \ldots, \gamma^{c-1}\}$. Therefore

\[
W_k = [\delta^0 - \gamma^k \ \delta^1 - \gamma^k \ \cdots \ \delta^{a-1} - \gamma^k]^T,
\]

and then $B_{ik} = \delta^i - \gamma^k$. This exponent matrix is given in [8].

4.2. Girth of Tanner Graph. In this subsection we first prove that the parity-check matrix of the proposed construction is (RC)-constraint and so the Tanner graph has girth at least 6.

**Theorem 4.1.** There is no singular 2 by 2 submatrix of the exponent matrix $B$. 
Proof. There are three cases to investigate. For the first case, assume that the two columns and two rows, whose entries are involved in the determinant of $2 \times 2$ submatrix, are in the same $W_{(i,k)}$. Also suppose that the indices of these rows and columns are distinct values $m_1$ and $m_2$ from $\{0, 1, \ldots, d_i - 1\}$ and $n_1$ and $n_2$ from $\{0, 1, \ldots, d_k - 1\}$, respectively. The determinant of such a submatrix is

\begin{equation}
D_1 = \begin{vmatrix}
\delta m_1 \beta_{i_1}^{n_1} - \gamma k \\
\delta m_2 \beta_{i_1}^{n_1} - \gamma k
\end{vmatrix}
= \gamma k (\beta_{i_1}^{m_2} - \beta_{i_1}^{m_1}) (\delta m_1 - \delta m_2).
\end{equation}

If $D_1 = 0$, then we have $\beta_{i_1}^{m_2} = \beta_{i_1}^{m_1}$ or $\delta m_1 = \delta m_2$ which contradicts our assumptions. So, every $2 \times 2$ submatrix of $W_{(i,k)}$ is non-singular.

For the second case, suppose the two columns, whose elements are involved in the determinant of $2 \times 2$ submatrix, belong to two distinct $W_{(i,k_1)}$ and $W_{(i,k_2)}$, where $k_1, k_2 \in \{0, 1, \ldots, d_i - 1\}$. The determinant of the matrix is

\begin{equation}
D_2 = \begin{vmatrix}
\delta m_1 \beta_{i_1}^{n_1} - \gamma k_1 \\
\delta m_2 \beta_{i_1}^{n_1} - \gamma k_1
\end{vmatrix}
= (\delta m_1 - \delta m_2) (\gamma k_1 \beta_{i_1}^{m_2} - \gamma k_2 \beta_{i_1}^{m_1}).
\end{equation}

Similar to the previous case we can suppose that $m_1 \neq m_2$. Therefore, if $D_2 = 0$, then we obtain $\gamma \beta_{i_1}^{m_2} = \gamma \beta_{i_1}^{m_1}$ which gives $\gamma = \beta_{i_1}^{m_2} = \beta_{i_1}^{m_1}$. Since $\beta_i$ and $\gamma$ are elements in the cyclic subgroups $G_d$ and $G_d$, respectively, and $G_d \cap G_d = \{1\}$, the equality holds if and only if $n_1 = n_2$ and $k_1 = k_2$ simultaneously, which contradicts our assumption that $k_1 \neq k_2$.

Finally, for the third case, let the indices of the two columns belong to two different matrices $W_{(i_1,k_1)}$ and $W_{(i_2,k_2)}$, where $i_1, i_2 \in \{1, \ldots, \ell - 2\}$ and $k_1, k_2 \in \{0, 1, \ldots, d_k - 1\}$. The determinant is

\begin{equation}
D_3 = \begin{vmatrix}
\delta m_1 \beta_{i_1}^{n_1} - \gamma k_1 \\
\delta m_2 \beta_{i_1}^{n_1} - \gamma k_1
\end{vmatrix}
= (\delta m_1 - \delta m_2) (\gamma \beta_{i_2}^{m_2} - \gamma \beta_{i_2}^{m_1}).
\end{equation}

If $D_3 = 0$, then $\gamma = \beta_{i_1}^{m_2} = \beta_{i_1}^{m_1}$ which contradicts our assumption $\gcd(d_{i_1}, d_{i_2}) = 1$.

According to the above theorem the Tanner graph of QC-LDPC code constructed by the use of our exponent matrix $B$ has girth at least 6.

**Example 4.** We take a $3 \times 4$ submatrix of the exponent matrix in Example 1.

\[
P = \begin{bmatrix}
\alpha^9 & \alpha^6 & \alpha^{22} & \alpha^{17} \\
\alpha^{10} & \alpha^8 & \alpha^{14} & \alpha^{26}
\end{bmatrix}.
\]

We have $\begin{vmatrix}
\alpha^9 \\
\alpha^{20}
\end{vmatrix} = \alpha^{11} - \alpha^{26}$. Since $\alpha^{11} = \alpha^{15}$ and $2(15) \equiv 0 \pmod{30}$, from Theorem 3.4 we conclude that $\begin{vmatrix}
\alpha^9 \\
\alpha^{20}
\end{vmatrix}$ results in 8-cycles. Moreover,
\[
\begin{bmatrix}
\alpha^9 & \alpha^6 & \alpha^{22} & \alpha^{17} \\
\alpha^{20} & \alpha^2 & \alpha^{29} & \alpha^9 \\
\alpha^6 & \alpha^{22} & \alpha^2 & \alpha^{29} \\
\end{bmatrix}
\]
contains two submatrices \(P_1 = \begin{bmatrix}
\alpha^9 & \alpha^{17} \\
\alpha^{20} & \alpha^9 \\
\end{bmatrix}\) and \(P_2 = \begin{bmatrix}
\alpha^6 \\
\alpha^2 \\
\end{bmatrix}\) whose determinants are \(\alpha^{18} - \alpha^7\) and \(\alpha^5 - \alpha^{24}\), respectively. For \(P_1\) and \(P_2\) we have \(\alpha^{18} = \alpha^{11}\) and \(\alpha^5 = \alpha^{11}\), respectively. Therefore, Theorem 3.4 proves the first two rows of \(P\) cause 8-cycles.

**Corollary 1.** For each \(i \in \{1, 2, \ldots, \ell - 2\}\) and \(k \in \{0, 1, \ldots, d_{i-1}\}\), the matrix \(W_{(i,k)}\) in (3) satisfies part (ii) of Theorem 3.4 if for \(n_1, n_2, n_3, n_4 \in \{0, 1, \ldots, d_{i-1}\}\) we have \(\beta_i^{n_2} - \beta_i^{n_1} + \beta_i^{n_3} - \beta_i^{n_4} \neq 0 \pmod{q-1}\).

**Proof.** Suppose the determinant of two \(2 \times 2\) submatrices of \(W_{(i,k)}\), denoted by \(B_1\) and \(B_2\) with row indices \(m_1, m_2\) and column indices \(n_1, n_2\) and \(n_3, n_4\), respectively, are \(\gamma^k(\beta_i^{n_2} - \beta_i^{n_1}) (\delta_{m_1} - \delta_{m_2})\) and \(\gamma^k(\beta_i^{n_4} - \beta_i^{n_3}) (\delta_{m_1} - \delta_{m_2})\). The Tanner graph corresponding to \(W_{(i,k)}\) has 8-cycles obtained from two rows \(m_1, m_2\) if these two determinants are equal. We have \(\gamma^k(\beta_i^{n_2} - \beta_i^{n_1}) (\delta_{m_1} - \delta_{m_2}) \equiv \gamma^k(\beta_i^{n_4} - \beta_i^{n_3}) (\delta_{m_1} - \delta_{m_2}) \pmod{q-1}\) or equivalently \(\beta_i^{n_2} - \beta_i^{n_1} + \beta_i^{n_4} - \beta_i^{n_3} \equiv 0 \pmod{q-1}\).

**4.3. Submatrices of \(B\) of maximum size satisfying the sufficient condition of Theorem 3.5.** In this subsection, we apply Theorem 3.5 to determine the submatrices of the exponent matrix \(B\) in (6) on the finite field \(\mathbb{F}_q\) which result in QC-LDPC codes with girth 6 and free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\). We factor \(2^7 - 1 = 255 = (3)(5)(17)\). Set \(a = 5\), \(b = 3\) and \(c = 17\). The exponent matrix is presented next. In this matrix, we replace each element \(a^i\) of \(B\) by its power \(i\), and the zero element of \(B\) is replace by \(\infty\). The matrix \(B\) becomes

\[
\begin{bmatrix}
\infty & 33 & 66 & 31 & 132 & 199 & 62 & 248 & 9 & 144 & 143 & 227 & 124 & 72 & 241 & 36 & 18 \\
238 & 240 & 40 & 236 & 171 & 50 & 157 & 4 & 181 & 91 & 64 & 217 & 35 & 186 & 206 & 130 & 15 \\
221 & 182 & 225 & 128 & 80 & 179 & 217 & 70 & 87 & 117 & 100 & 157 & 59 & 5 & 8 & 30 & 107 \\
119 & 20 & 213 & 206 & 218 & 32 & 145 & 103 & 135 & 120 & 118 & 25 & 2 & 173 & 236 & 93 & 65 \\
187 & 234 & 109 & 200 & 195 & 59 & 1 & 118 & 160 & 10 & 103 & 16 & 179 & 60 & 140 & 214 & 174
\end{bmatrix}
\]

We applied Theorem 3.5 and the two conditions of Theorem 3.4 to a computer-based search algorithm to find all \(3 \times n\) submatrices of \(B\) which result in \((3, n)\)-regular QC-LDPC codes with girth 6 and free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\). By checking the conditions in Theorem 3.5, we figured out that if the exponent matrix is \(B\) in (10), then the only submatrices with the mentioned property are those with a row weight 4. We obtain all non-isomorphic \(3 \times 4\) submatrices of \(B\) to construct \((3, 4)\)-regular QC-LDPC codes with girth 6 and free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\). In Table 1, instead of presenting all of these non-isomorphic submatrices of \(B\) we provide their row indices and column indices in \(B\). The first row of the exponent matrix is not used in the submatrices, although the search algorithm takes all rows into account.

In order to demonstrate the positive influence of removing ETSs with small size we compare the performance curves of two \((3, 4)\)-regular QC-LDPC codes with girth 6 whose exponent matrices are submatrices of \(B\) in (10). The Tanner graph of one of them, denoted by \(C_1\), is free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\). The row indices and column indices of \(B\) which give the exponent matrix of \(C_1\) are \((1, 2, 3)\) and \((6, 7, 8, 9)\), respectively. The other one, denoted by \(C_2\), has \((4, 0)\) ETS or \((4, 2)\) ETS or both. The row indices and column indices of \(B\) which give the exponent matrix of \(C_2\) are \((1, 2, 3)\) and \((0, 1, 4, 15)\), respectively. The performance of these codes...
Table 1. Row indices \((i, j, k)\); \(i, j, k \in \{0, 1, 2, 3, 4\}\) and column indices \((c_1, c_2, c_3, c_4)\); \(c_i \in \{0, 1, \ldots, 16\}\) of \(B\) in (10) to construct non-isomorphic \((3, 4)\)-regular QC-LDPC codes with girth 6 and free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\).

| row indices \((i, j, k)\) | column indices \((c_1, c_2, c_3, c_4)\) |
|---------------------------|---------------------------------------------|
| \((1, 2, 3)\)            | \((1, 2, 7, 10), (1, 3, 4, 13), (1, 3, 4, 14), (1, 3, 13, 14)\) |
| \((1, 2, 3)\)            | \((1, 4, 5, 16), (1, 5, 8, 16), (1, 5, 10, 16), (1, 5, 12, 15)\) |

Figure 3. The comparison of the performance curves of two \((3, 4)\)-regular QC-LDPC codes with the same length. The exponent matrices of both codes, \(C_1\) and \(C_2\), are submatrices of \(B\) in (10).

Decoded using the sum-product algorithm with 50 iterations are shown in Fig. 3. Code \(C_1\) which is free of the small ETSs outperforms code \(C_2\).

5. Conclusion

The smallest size of an elementary trapping set (ETS) in an LDPC code with column weight 3 is 4; they are \((4, 0)\) and \((4, 2)\) ETSs. In this paper, using edge-coloring technique as well as a necessary and sufficient condition to avoid some specific 8-cycles, which is proposed in this paper, we provide sufficient conditions to obtain \(3 \times n\) submatrices of an exponent matrix of an algebraic-based QC-LDPC code which give fully connected \((3, n)\)-regular QC-LDPC codes whose Tanner graphs are free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\). We also propose a new algebraic construction to obtain an exponent matrix of QC-LDPC codes based on multiplicative cyclic subgroups of a finite field whose Tanner graph has girth at least 6. Some other algebraic construction methods are particular cases of our proposed one. Then, we apply the sufficient conditions for the removal of small size ETSs to our proposed construction method to obtain \((3, n)\)-regular QC-LDPC codes whose Tanner graphs are free of \((a, b)\) ETSs with \(a \leq 5\) and \(b \leq 2\). Experimental results show the potentiality of removing these ETSs. We are interested in applying the sufficient conditions obtained for eliminating small size ETSs to each algebraic-based construction in the literature. This provides the maximum size of submatrices of...
their exponent matrices which result in girth-6 column weight three QC-LDPC codes free of small ETSs.

REFERENCES

[1] F. Amirzade, M. Alishahi and M.-R. Sadeghi, An algebraic construction of QC-LDPC codes based on powers of primitive elements in a finite field and free of small ETs, *J. Algebraic Struct. The. Appl.*, 6 (2019), 129–140.

[2] F. Amirzade and M.-R. Sadeghi, Lower bounds on the lifting degree of QC-LDPC codes by difference matrices, *IEEE Access*, 6 (2018), 23688–23700.

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

[4] F. Amirzade and M.-R. Sadeghi, Efficient search of QC-LDPC codes with girths 6 and 8 and free of small elementary trapping sets with small size, arXiv:1803.08141.

[5] M. Battaglioni, A. Tasdighi, M. Baldi, M. H. Tadayon and F. Chiaraluce, Compact QC-LDPC block and SC-LDPC convolutional codes for low-latency communications, 2018 IEEE 29th Ann. Int. Symp. PIMRC, (2018), 1–5.

[6] I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov and R. V. Satyukov, Searching for voltage graph-based LDPC tailbiting codes with large girth, *IEEE Trans. Inf. Theory*, 58 (2012), 2265–2270.

[7] J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*, American Elsevier Publishing Co., Inc., New York, 1976.

[8] Q. J. Diao, Q. Huang, S. Lin and K. Abdel-Ghaffar, A matrix-theoretic approach for analyzing quasi-cyclic low-density parity-check codes, *IEEE Trans. Inf. Theory*, 58 (2012), 4030–4048.

[9] Q. J. Diao, Q. Huang, S. Lin and K. Abdel-Ghaffar, A transform approach for analyzing and constructing quasi-cyclic low-density parity-check codes, *IEEE Trans. Inf. Theory Appl. Workshop, San Diego, CA, USA*, (2011), 1–8.

[10] M. Diouf, D. Declercq, S. Ouya and B. Vasic, A PEG-like LDPC code design avoiding short trapping sets, *IEEE Int. Symp. Inf. Theory (ISIT)*, (2015), 1079–1083.

[11] M. P. C. Fossorier, Quasi-cyclic low-density parity-check codes from circulant permutation matrices, *IEEE Trans. Inf. Theory*, 50 (2004), 1788–1793.

[12] Q. Huang, Q. Diao, S. Lin and K. Abdel-Ghaffar, Trapping sets of structured LDPC codes, 2011 IEEE Int. Symp. Inf. Theory, (2011), 1086–1090.

[13] J. Li, K. Liu, S. Lin and K. Abdel-Ghaffar, Algebraic quasi-cyclic LDPC codes: Construction, low error-floor, large girth and a reduced-complexity decoding scheme, *IEEE Trans. Commun.*, 62 (2014), 2626–2637.

[14] J. Li, K. Liu, S. Lin and K. Abdel-Ghaffar, Quasi-cyclic LDPC codes on two arbitrary sets of a finite field, *IEEE Int. Symp. Inf. Theory*, (2014), 2454–2458.

[15] J. Li, K. Liu, S. Lin and K. Abdel-Ghaffar, A matrix-theoretic approach to the construction of non-binary quasi-cyclic LDPC codes, *IEEE Trans. Commun.*, 63 (2015), 1057–1068.

[16] K. Liu, Q. Huang, S. Lin and K. Abdel-Ghaffar, Quasi-cyclic LDPC codes: Construction and rank analysis of their parity-check matrices, *IEEE Inf. Theory and Appl. Workshop*, (2012), 227–233.

[17] D. V. Nguyen, S. K. Chilappagari, N. W. Marcellin and B. Vasic, On the construction of structured LDPC codes free of small trapping sets, *IEEE Trans. Inf. Theory*, 58 (2012), 2280–2302.

[18] M. E. O’Sullivan, Algebraic construction of sparse matrices with large girth, *IEEE Trans. Inf. Theory*, 52 (2006), 718–727.

[19] M.-R. Sadeghi, Optimal search for girth-8 quasi cyclic and spatially coupled multiple-edge LDPC codes, *IEEE Commun. Letters*, 23 (2019), 1466–1469.

[20] M.-R. Sadeghi and F. Amirzade, Analytical lower bound on the lifting degree of multiple-edge QC-LDPC codes with girth 6, *IEEE Commun. Letters*, 22 (2018), 1528–1531.

[21] A. Sakzad, M.-R. Sadeghi and D. Panario, Codes with girth 8 Tanner graph representation, *Designs, Codes and Cryptography*, 57 (2010), 71–81.

[22] S. Song, B. Zhou, S. Lin and K. Abdel-Ghaffar, A unified approach to the construction of binary and nonbinary Quasi-cyclic LDPC codes based on finite field, *IEEE Trans. Commun.*, 57 (2009), 84–93.
[23] M. H Tadayon, T. Aliroza and B. Massino, Efficient search of compact QC-LDPC and SC-LDPC convolutional codes with large girth, IEEE Commun. Letters, 22 (2018), 1156–1159.

[24] X. F. Tao, Y. F. Li, Y. H. Lin and Z. Q. Hu On the construction of LDPC codes free of small trapping sets by controlling cycles, IEEE Commun. Letters, 22 (2018), 9–12.

[25] A. Tasdighi, A. H. Banihashemi and M. R. Sadeghi, Efficient search of girth-optimal QC-LDPC codes, IEEE Trans. Inf. Theory, 62 (2016), 1552–1564.

[26] J. D. 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, 59 (2013), 2293–2314.

[27] Y. G. Wang, J. S. Yedidia and S. C. Draper, Construction of high-girth QC-LDPC codes, 2008 5th Int. Symp. Turbo Codes and related Topics, (2008), 180–185.

[28] G. Zhang, R. Sun and X. Wang, Explicit construction of girth-eight QC-LDPC codes and its application in CRT methods, J. Commun., 33 (2012), 171–176.

[29] L. Zhang, S. Lin, K. Abdel Ghaflar, Z. Ding and B. Zhou Quasi-Cyclic LDPC codes on cyclic subgroups of finite fields, IEEE Trans. Commun., 59 (2011), 2330–2336.

[30] L. Zhang, S. Lin, K. Abdel Ghaflar and B. Zhou, Circulant arrays: Rank analysis and construction of Quasi-Cyclic LDPC codes, IEEE Int. Symp. Inf. Theory (ISIT), (2010), 814–818.

Received December 2018; revised August 2019.

E-mail address: famirzade@gmail.com
E-mail address: msadeghi@aut.ac.ir
E-mail address: daniel@math.carleton.ca