IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 January 2023, accepted 11 February 2023, date of publication 27 February 2023, date of current version 8 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3249464

RESEARCH ARTICLE

Full-Length Row-Multiplier QC-LDPC Codes With Girth Eight and Short Circulant Sizes

JUHUA WANG[1], **JIANHUA ZHANG**[1], **QUAN ZHOU**[1], **AND LINTAO ZHANG**[2]
[1]China Academy of Space Technology (Xi'an), Xi'an 710100, China
[2]Department of Electrical Engineering, Tsinghua University, Beijing 100084, China

Corresponding author: Jianhua Zhang (zhangjhcast504@163.com)

This work was supported in part by the National Key Laboratory Foundation of China under Grant 6142411432107 and Grant 6142411204306.

ABSTRACT As a special case of a quasi-cyclic (QC) low-density parity-check (LDPC) code, a full-length row-multiplier (FLRM) QC-LDPC code is described by a compact exponent matrix based on two sequences of integers. The codes designed by a framework known as greatest-common-divisor (GCD) method, belong to a salient class of FLRM QC-LDPC codes, which can eliminate cycles of length up to six by carefully selecting a special sequence subject to a set of simple inequalities. However, the GCD method ensures the absence of these cycles only if circulant sizes are larger than a certain threshold. By combining the existing GCD method, novel sequences and a new analysis method (based on new lemmas of circulants and integers) for modulo equations, a group of novel FLRM QC-LDPC codes free of 4-cycles and 6-cycles are explicitly proposed for column weights from three to five in this paper, which possess circulant sizes much smaller than the forgoing threshold. Simulations show that the new FLRM QC-LDPC codes with shorter lengths perform almost the same as the existing FLRM QC-LDPC codes with longer lengths, and that the novel FLRM QC-LDPC codes noticeably outperform their counterparts with (nearly) identical lengths.

INDEX TERMS Cycle, greatest common divisor (GCD), low-density parity-check (LDPC) code, quasi-cyclic (QC).

I. INTRODUCTION

As is well known, performance of long low-density parity-check (LDPC) codes can approach theoretical limits by iterative decoding procedures. However, when code lengths are medium or small, it is necessary to skillfully design parity-check matrices (PCMs) to attain satisfactory performance. Eliminating short cycles is an effective way to obtain reasonably good PCMs for LDPC codes [1], [2], [3], [4], [5]. As an important category of LDPC codes, quasi-cyclic (QC) LDPC codes have attracted increasing attention in theoretical research [4], [6], [7] and engineering practice [8], due to their highly structured PCMs which greatly simplify the implementation complexity of encoders and decoders. The PCM of a QC-LDPC code is composed of circulants of the same size. Basically, there are two classes of methods to eliminate short cycles for QC-LDPC codes. One class is based on computer search (such as [9] and [10]), and the other class is based on explicit constructions via simple formulas (such as [11], [12], and [13]). Compared with methods relying upon computer search, the advantage of explicit constructions is that the acquisition of PCMs is extremely simple and does not require any computer search. In addition, simple tricks such as masking [3] and the Chinese remainder theorem (CRT) [14] can be easily combined with explicit constructions to enhance the randomness of PCMs and flexibility of code lengths, without deteriorating cycle characteristics.

This paper focuses on a class of QC-LDPC codes which are defined by two sequences of integers. One is an arithmetic sequence starting from zero with a common difference being one, and the other is carefully designed to guarantee the absence of short cycles. Such QC-LDPC codes are termed as full-length row-multiplier (FLRM) codes in [15]. Array codes [16] are a type of FLRM codes, but they only ensure the absence of cycles of length four. As a systematic and powerful approach to producing FLRM codes without cycles of length up to six, the greatest-common-divisor (GCD) method [17], [18] adopts a set of simple inequalities to select the second

The associate editor coordinating the review of this manuscript and approving it for publication was Zihuai Lin.

sequence. Several schemes [19], [20], [21], [22], [23], [24], [25], [26] which yield QC-LDPC code without cycles of length up to six, are obviously special cases of the GCD method. Moreover, the GCD method has found wide application in building other types of structured LDPC codes [27], [28], [29] which are different from the QC-LDPC codes merely based on circulant permutation matrices (CPMs). Nevertheless, the GCD method guarantees the absence of these cycles only if the size of CPMs is larger than a certain threshold.

By combining the existing GCD method and a novel analysis method for modulo equations, a series of novel FLRM QC-LDPC codes without cycles of length four and six are explicitly proposed in this paper. The prominent advantage of our new constructions lies in that the size of CPMs can be much smaller than the corresponding threshold determined by the existing GCD method. For example, for certain types of row weight L, the smallest threshold for column weight $J = 5$ provided by existing explicit methods is $(2L + 3)(L - 1)$ [12]. A new construction proposed in this paper (Theorem 7), by contrast, is able to offer a CPM size $((L+2)^2 - 1)$ about half of the foregoing threshold. Another advantage of most new constructions is that the resultant QC-LDPC codes noticeably outperform some existing counterparts. For example, a construction presented in this paper (Theorem 6) yields a $(480, 261)$ QC-LDPC code which outperforms the existing counterpart [17] ($(512, 276)$ QC-LDPC code) by 0.20 dB at the bit error rate (BER) of 10^{-5}. For another example, a novel construction in this paper (Theorem 8) combined with the masking skill, produces a $(1305, 580)$ QC-LDPC code which outperforms the masked array-based counterpart [16] ($(1341, 596)$ QC-LDPC code) by about 1.0 dB at the BER of 10^{-4}. At present, QC-LDPC codes have become an indispensable key technology in ground communication systems and satellite communication systems. The novel constructions proposed here for short QC-LDPC codes have the potential to be used for these communication systems.

The rest of the paper is organized as follows. Basic definitions and notations concerning FLRM QC-LDPC codes and the GCD method are introduced in Section II. New constructions for FLRM QC-LDPC codes without cycles of length up to six are proposed in Section III, Section IV and Section V, respectively. Performance of the novel codes are reported in Section VI. A byproduct pertaining to the smallest CPMs is presented in Section VII for FLRM QC-LDPC codes without cycles of length up to six. Finally, the conclusion is made in Section VIII.

II. PRELIMINARY

A (J, L)-regular LDPC code is the null space of a sparse PCM, in which each row has L nonzero elements and each column has J nonzero elements. A (J, L)-regular QC-LDPC code is a special LDPC code whose PCM is an array of circulants with the same size P. If all circulants in a PCM are circulant permutation matrices, the PCM of a QC-LDPC code can be uniquely described by a $J \times L$ exponent matrix $\mathbf{E}$ and the circulant size P [4]. Each element (say e) within $\mathbf{E}$ is a nonnegative integer smaller than P, and it stands for a specific CPM determined by e. To be specific, this CPM is a $P \times P$ square matrix, in which the only nonzero element (i.e., "1" for a binary code) in the first row is located in the e $(mod\ P)$-th column, and other row is generated by cyclicly shifting its previous row to the right by one position. In many cases, the actual code rate for a (J, L)-regular QC-LDPC code is slightly larger than the nominal (or designed) code rate $(L-J)/L$, due to a couple of inevitable redundant rows in its PCM.

The lengths of cycles for an LDPC code are even integers greater than or equal to four. For a QC-LDPC code, cycles of length $2l$ (denoted by "$2l$-cycles") can be efficiently detected via its exponent matrix as follows [4]. Firstly, use l horizontal lines and l vertical lines alternately to draw a closed polygon in a fixed (say counterclockwise) order in the exponent matrix. Secondly, take out the $2l$ elements within the exponent matrix which correspond to as many corners of this polygon in the same fixed order. Finally, utilize the plus sign and minus sign alternately to connect these elements. If the calculation result is zero modulo P, then there are $2l$-cycles within the PCM of the QC-LDPC code. Girth is the length of shortest cycles. Therefore, a QC-LDPC code free of 4-cycles and 6-cycles has girth at least eight.

This paper focuses on a class of QC-LDPC codes whose exponent matrices can be concisely expressed by $\mathbf{E}=\mathbf{S}_2^T \cdot \mathbf{S}_1$, where $\mathbf{S}_1 = [0, 1, \cdots, L-1]$, $\mathbf{S}_2$ is an increasing sequence composed of J integers, $[\alpha_0, \alpha_1, \cdots, \alpha_{J-1}]$, and T denotes transpose. The sequence $\mathbf{S}_2$ is also called a tuple with J entries. Such QC-LDPC codes are referred to as FLRM codes, because all integers from 0 to $L-1$ are used in $\mathbf{S}_1$ and each row of $\mathbf{E}$ is obtained by multiplying $\mathbf{S}_1$ by a corresponding integer in $\mathbf{S}_2$. It should be noted that, as $\mathbf{E}$ has a sub-matrix $[[0, \alpha_0, 2\alpha_0]^T, [0, \alpha_1, 2\alpha_1]^T]^T$, girth of an FLRM code is at most eight [12].

The recently proposed GCD method can ensure a girth-eight FLRM code, if $\mathbf{S}_2$ is in accord with a set of inequalities, $(\alpha_k - \alpha_i)/gcd(\alpha_k - \alpha_i, \alpha_j - \alpha_i) \geq L$ for any triple $(\alpha_i, \alpha_j, \alpha_k)$, where $0 \leq i < j < k \leq J-1$. Such a set of inequalities are called the GCD constraint.

Lemma 1 [17]: If $\mathbf{S}_2$ satisfies the GCD constraint, then it corresponds to an FLRM QC-LDPC code with girth eight for any circulant size larger than $(\alpha_{J-1} - \alpha_0)(L - 1)$.

On the other hand, the GCD constraint is also necessary for an FLRM code with girth eight.

Lemma 2 [15]: If $\mathbf{S}_2$ corresponds to a girth-eight FLRM QC-LDPC code for a certain circulant size, then $\mathbf{S}_2$ satisfies the GCD constraint.

According to Lemma 2, in order to design a girth-eight FLRM code, a sequence $\mathbf{S}_2$ which satisfies the GCD constraint must be selected. Besides, thanks to Lemma 1, if a qualified $\mathbf{S}_2$ has been found, then any circulant size larger than $(\alpha_{J-1} - \alpha_0)(L - 1)$ is able to produce a girth-eight FLRM code. This naturally raises a question: is it possible to obtain girth-eight FLRM codes with circulant sizes smaller than the threshold? If possible, is there any way to find them by explicit methods instead of random search procedures? In the following sections, this issue is explored for several small values of J.

For ease of the description of the main content in this paper, some useful properties and notations are introduced.

Lemma 3: Let a and b be two integers. Then $gcd(a, b) = gcd(a, b-a)$.

Lemma 4: Let a and b be two positive integers such that $b \geq 2a$. *Let i, j, and k be three distinct integers such that* $0 \leq i, j, k \leq L-1$. *Then* $|(i-j)a+(k-i)b| \leq -a+(L-1)b$.

Proof: Obviously, $(i-j)a+(k-i)b = (k-j)a+(k-i)(b-a)$. As $b-a \geq a$, it follows that $|(k-j)a+(k-i)(b-a)| \leq [(L-1)-1]a+[(L-1)-0](b-a) = -a+(L-1)b$. □

Lemma 5: For any given circulant size, the two sequences, $\mathbf{S}_2 = [\alpha_0, \alpha_1, \cdots, \alpha_{J-1}]$ *and* $\mathbf{S}_2' = [\alpha_{J-1}-\alpha_{J-1}, \alpha_{J-1}-\alpha_{J-2}, \cdots, \alpha_{J-1}-\alpha_0]$ *produce two equivalent FLRM QC-LDPC codes.*

Proof: For a circulant $\mathbf{C}$ defined by an exponent e, first flip its columns in the left-right direction and then flip all rows of the resultant matrix in the up-down direction. It is easy to understand that the final matrix is just a circulant $\mathbf{C}'$ defined by the exponent $e' = mod(-e, P)$. Therefore, taking the opposite number for each element within an exponent matrix merely corresponds to an equivalent PCM. Moreover, adding a constant to all elements in a column of an exponent matrix is equivalent to permuting P consecutive columns within a PCM. As a result, $\mathbf{S}_2$ and $\mathbf{S}_2'$ correspond to equivalent PCMs and hence equivalent codes. □

The flip operation in the proof of Lemma 5 is illustrated by $e = 2$ and $P = 5$. The circulant $\mathbf{C}$ defined by the exponent e is

$$\begin{pmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&0&0&0 \end{pmatrix}.$$

By flipping its columns in the left-right direction, the resultant matrix is obtained as

$$\begin{pmatrix} 0&0&1&0&0\\ 0&1&0&0&0\\ 1&0&0&0&0\\ 0&0&0&0&1\\ 0&0&0&1&0 \end{pmatrix}.$$

By flipping all rows of the above matrix in the up-down direction, the final matrix is obtained as

$$\begin{pmatrix} 0&0&0&1&0\\ 0&0&0&0&1\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0 \end{pmatrix},$$

which is just the circulant $\mathbf{C}'$ defined by the exponent $e' = mod(-e, P) = 3$.

Denote by "(r, s)-4-cycles" the cycles of length four located in the r-th and s-th rows of the exponent matrix. Denote by "(r, s, t)-6-cycles" the cycles of length six located in the r-th, s-th and t-th rows of the exponent matrix.

For a given exponent matrix, let LB_{ccs} be the lower bound on consecutive circulant sizes guaranteeing girth at least eight. That is to say, each circulant size greater than or equal to LB_{ccs} corresponds to a QC-LDPC code without 4-cycles and 6-cycles for the same exponent matrix. The value of LB_{ccs} can be readily calculated by Lemma 1 in [11].

Remark 1: The sequence $\mathbf{S}_2$ *involved in the following sections of this paper is based on a large number of randomly generated sequences and on the basis of trial and error. How to systematically obtain such sequences deserves further research. In addition, irregular QC-LDPC codes are more widely used in practice than regular ones. However, since regular QC-LDPC codes in many cases can serve as the basis of irregular counterparts, only regular QC-LDPC codes are considered in this paper. From the new constructions for regular QC-LDPC codes, irregular QC-LDPC counterparts can be produced via certain general tricks, such as column-splitting [15] and masking [3], [12]. How to generate irregular QC-LDPC codes based on the ideas of this paper but without resort to the tricks in question, is obviously an interesting problem worthy of further investigation.*

III. NEW CONSTRUCTIONS FOR J=3

According to Lemma 1, the existing tuple $[\alpha_0, \alpha_1, \alpha_2] = [0, 1, L]$ is able to guarantee a QC-LDPC code without 4-cycles and 6-cycles if the circulant size is greater than or equal to $L(L-1)+1$. In this section, it is analyzed whether this tuple ensures a code without 4-cycles and 6-cycles when the circulant size is smaller than $L(L-1)+1$. The answer to the question turns out to be in the negative, which prompts this article to try other options of $[\alpha_0, \alpha_1, \alpha_2]$. By changing the value of α_1, a new construction based on the tuple $[0, 2, L]$ is proposed to offer a noticeably smaller circulant size. Then, the new tuple $[0, 2, L]$ is extended to a general case $[0, \alpha_1, L]$ where α_1 is arbitrary chosen, which can provide a significantly smaller circulant size when α_1 is properly selected. Finally, by changing the value of α_2, another construction based on the tuple $[0, 1, \alpha_2]$ is presented, where α_2 takes different values greater than L according to the parity of L. Such a new construction can also provide a certain circulant size much smaller than $L(L-1)+1$.

A. NEW PROPERTY FOR EXISTING TUPLE [0,1,L]

Due to Lemma 1, only the tuples meeting GCD constraint need to be considered. For the existing tuple $[0, 1, L]$ which satisfies GCD constraint, the following theorem regarding the choice of circulant sizes is attained.

Theorem 1: $\mathbf{S}_2 = [0, 1, L]$ *corresponds to a girth-eight* $(3, L)$*-regular FLRM QC-LDPC code* if and only if *the circulant size is larger than* $L(L-1)$.

Proof: Due to Lemma 1, $\mathbf{S}_2$ yields a girth-eight FLRM QC-LDPC code for any $P \geq L(L-1)+1$. Therefore, it suffices to prove that $\mathbf{S}_2$ does not correspond to a girth-eight FLRM QC-LDPC code for any $P \leq L(L-1)$. The proof is given by contradiction. Assume there exists a certain $P \leq L(L-1)$ which ensures the absence of 4-cycles and 6-cycles.

(i): Let i and j be two column indexes such that $0 < i < j \leq L-1$. Then the 6-cycles governed by $[e(0,0)-e(2,0)]+[e(2,i)-e(1,i)]+[e(1,j)-e(0,j)] = 0\,(mod\ P)$ cannot occur, which means $(0-0)+(Li-i)+(j-0) \neq 0\,(mod\ P)$. Therefore,

$$P \notin \{iL+1, iL+2, \cdots, iL+(L-1-i)\} \tag{1}$$

for $1 \leq i \leq L-2$.

(ii) Let i and j be two column indexes such that $0 < j < i \leq L-1$. Then the 6-cycles governed by $[e(1,0)-e(2,0)]+[e(2,i)-e(0,i)]+[e(0,j)-e(1,j)] = 0\ (mod\ P)$ cannot appear, which indicates $Li - j \neq 0\ (mod\ P)$. Therefore,

$$P \notin \{iL-(i-1), \cdots, iL-1\} \tag{2}$$

for $2 \leq i \leq L-1$. By setting $i = i'+1$ in Eq. (2), it follows that

$$P \notin \{i'L+L-i', \cdots, i'L+L-1\} \tag{3}$$

for $1 \leq i' \leq L-2$. By combining Eq. (1) and Eq. (3), it follows that

$$\begin{aligned} P \notin \{&iL+1, \cdots, iL+L-(i+1), \\ &iL+L-i, \cdots, iL+L-1\} \end{aligned} \tag{4}$$

for $1 \leq i \leq L-2$. That is to say,

$$P \notin \{iL+1, \cdots, iL+L-1\} \tag{5}$$

for $1 \leq i \leq L-2$. Moreover, P cannot equal any element within $\mathbf{E}$, otherwise 4-cycles appear. Therefore, $P \notin \{1, 2, \cdots, L-1\}$ and $P \notin \{L, 2L, \cdots, (L-1)L\}$. Consequently, all values of P smaller than $(L-1)L+1$ are impossible, which contradicts the foregoing assumption. □

B. NEW CONSTRUCTION FROM TUPLE [0,2,L]

Next, whether the circulant size can be reduced for other settings is examined. It is easily verified that the tuple $[0, 2, L]$ satisfies GCD constraint when L is an odd number. With this setup, the circulant size can be reduced by $(L-3)$, as stated in the following theorem.

Theorem 2: Let $L \geq 5$ be an odd number. Then $\mathbf{S}_2 = [0, 2, L]$ corresponds to a $(3, L)$-regular FLRM QC-LDPC code with girth eight for the circulant size $P = L^2 - 2L + 4$.

Proof: Firstly, consider 4-cycles. Let i and j be two column indexes such that $0 < i < j \leq L-1$.

(i) (0, 1)-4-cycles can be expressed as $(0-2i)+(2j-0) = 0\ (mod\ P)$, which is equivalent to

$$2(j-i) = n(L^2-2L+4) \tag{6}$$

for a certain integer n. Since $0 < LHS \leq 2(L-1) < L^2 - 2L + 4$, Eq. (6) is impossible for any n.

(ii) (1, 2)-4-cycles can be denoted by $(2i-Li)+(Lj-2j) = 0\ (mod\ P)$, which reduces to

$$(L-2)(j-i) = n(L^2-2L+4) \tag{7}$$

for a certain integer n. As $0 < LHS \leq (L-2)(L-1) < L^2 - 2L + 4$, Eq. (7) cannot be true for any n.

(iii) (0, 2)-4-cycles can be represented by $(0-Li)+(Lj-0) = 0\ (mod\ P)$, which is equivalent to

$$L(j-i) = n(L^2-2L+4) \tag{8}$$

for a certain integer n. Because $0 < LHS \leq L(L-1) < 2(L^2-2L+4)$, Eq. (8) is possible only for $n = 1$. However, $n = 1$ means that 4 must be a multiple of L, which is impossible because L is odd.

Next, consider 6-cycles. Let i, j and k be three different column indexes such that $0 \leq i, j, k \leq L-1$. Then 6-cycles can be represented by $(0-2j)+(2i-Li)+(Lk-0) = 0\ (mod\ P)$, which is equivalent to

$$2(i-j)+L(k-i) = n(L^2-2L+4) \tag{9}$$

for some integer n. Thanks to Lemma 4, it follows that $|LHS| \leq -2 + L(L-1) = L^2 - L - 2 < 2(L^2-2L+4)$. Therefore, Eq. (9) is possible only for $n \in \{0, 1, -1\}$.

(i) If $n = 0$, Eq. (9) implies $L|2(i-j)$. As L is odd, it is clear that $L|(i-j)$, which is impossible.

(ii) If $n = 1$, Eq. (9) becomes

$$2(i-j)+L(k-i) = L^2-2L+4, \tag{10}$$

implying $L|[2(i-j)-4]$. Because L is odd, it is obvious that $L|(i-j-2)$, which is possible only for $i-j = 2$ or $i-j = -L+2$. When $i-j = 2$, Eq. (10) yields $k-i = L-2$ and hence $k-j = L$, which is impossible. When $i-j = -L+2$, Eq. (10) leads to $k-i = L$, which is also impossible.

(iii) Similarly, if $n = -1$, Eq. (9) becomes

$$2(i-j)+L(k-i) = -(L^2-2L+4), \tag{11}$$

indicating $L|[2(i-j)+4]$. As L is odd, it is clear that $L|(i-j+2)$, which is possible only for $i-j = L-2$ or $i-j = -2$. When $i-j = L-2$, Eq. (11) leads to $k-i = -L$, which is impossible. When $i-j = -2$, Eq. (11) yields $k-i = 2-L$ and hence $k-j = -L$, which is also impossible. □

Up to now, it has not been proved whether L^2-2L+4 is the smallest circulant size to guarantee girth eight. Nevertheless, it has been empirically verified that, for each odd L in the range $5 \leq L \leq 50$, the smallest P which enables $\mathbf{S}_2 = [0, 2, L]$ to generate a girth-eight code is exactly L^2-2L+4. Therefore, the following conjecture is likely to be true.

Conjecture 1: Let $\mathbf{S}_2 = [0, 2, L]$. The smallest P guaranteeing a girth-eight $(3, L)$-regular FLRM QC-LDPC code is $L^2 - 2L + 4$ for any odd $L \geq 5$.

Now, move one step toward Conjecture 1, and consider the circulant size one less than the above value. For L odd and $P = L^2-2L+3$, it is obvious that $e(2, L-1) = L(L-1) = L-3\ (mod\ P)$. Since $e(1, (L-3)/2)$ is also equal to $L-3$, there are 6-cycles in the three columns indexed by $(i, j, k) = (0, (L-3)/2, L-1)$.

In addition, it has been verified that for any odd L in the range $L = 5 \sim 50$, the LB_{ccs} for the exponent matrix in Theorem 2 (after modulo P) equals $L(L-1)+3$, which is marginally larger than the associated LB_{ccs} (i.e. $L(L-1)+1$) for the tuple $[0, 1, L]$ by only two.

C. NEW GENERALIZATION FROM TUPLE [0,α_1,L]

Two specific tuples of the form $[0, \alpha_1, L]$ with $\alpha_1 = 1$ and $\alpha_1 = 2$ have been analyzed, respectively, in the previous two subsections. For the general case, a salient feature is revealed in this subsection.

According to Lemma 5, the two tuples, $[0, \alpha_1, L]$ and $[0, L-\alpha_1, L]$, always lead to equivalent FLRM QC-LDPC codes. Therefore, it suffices to check α_1 in the range $1 \le \alpha_1 \le \lfloor L/2 \rfloor$. Our observations in this range are consistent with the following conjecture, much more general than Conjecture 1.

Conjecture 2: Let α_1 be an integer such that $1 \le \alpha_1 \le \lfloor L/2 \rfloor$ and $gcd(\alpha_1, L) = 1$. Then the smallest circulant size which enables $\mathbf{S}_2 = [0, \alpha_1, L]$ to yield a $(3, L)$-regular FLRM QC-LDPC code with girth eight is $P = L(L-\alpha_1)+\alpha_1^2$.

Remark 2: It has been verified that Conjecture 2 is true for each L in the range $4 \le L \le 50$ and each $\alpha_1 = 1 \sim \lfloor L/2 \rfloor$ satisfying $gcd(\alpha_1, L) = 1$. If Conjecture 2 is correct, then three properties follow immediately: (i) if $mod(L, 2) = 1$, then $[0, (L-1)/2, L]$ leads to a girth-eight FLRM code with the circulant size $P = (3L^2+1)/4$; (ii) if $mod(L, 4) = 0$, then $[0, L/2-1, L]$ produces a girth-eight FLRM code with $P = 3L^2/4+1$; and (iii) if $mod(L, 4) = 2$, then $[0, L/2-2, L]$ yields a girth-eight FLRM code with $P = 3L^2/4+4$.

D. NEW CONSTRUCTION FROM TUPLE [0,1,α_2>L]

In the previous three subsections, the scenarios (where α_2 is limited to L for the tuple $[0, \alpha_1, \alpha_2]$) have been considered. In this subsection, the case (where $\alpha_2 > L$ and α_1 is set to 1) is investigated.

Theorem 3: (i) If L is even, then $\mathbf{S}_2 = [0, 1, 3L/2]$ guarantees a girth-eight $(3, L)$-regular FLRM QC-LDPC code for $P = 3L^2/4+L/2$; (ii) If L is odd, then $\mathbf{S}_2 = [0, 1, (3L+1)/2]$ guarantees a girth-eight $(3, L)$-regular FLRM QC-LDPC code for $P = (3L^2+1)/4$.

Proof: Firstly, consider the first part of the theorem where L is even. The proofs of the absence of 4-cycles are similar to those in Theorem 2 and hence omitted. Let i, j and k be three different column indexes such that $0 \le i, j, k \le L-1$. Then the 6-cycles can be represented by $(0-j)+[i-(3L/2)i]+[(3L/2)k-0] = 0\,(mod\ P)$, which is equivalent to

$$(i-j)+(3L/2)(k-i) = n(3L^2/4+L/2) \tag{12}$$

for some integer n. By arranging terms, Eq. (12) becomes

$$(2i-j-k)+(3L/2+1)(k-i) = n[(3L/2+1)L/2]. \tag{13}$$

Therefore, $(3L/2+1)|(2i-j-k)$. Since $|2i-j-k| < 2L$, it is clear that $(2i-j-k) = 0$ or $\pm(3L/2+1)$.

(i) If $(2i-j-k) = 0$, then Eq. (13) reduces to $(k-i) = n(L/2)$. Therefore, it follows that $k-j = nL$, which is impossible.

(ii) If $(2i-j-k) = 3L/2+1$, then Eq. (13) becomes $1+(k-i) = n(L/2)$. Thus, $i-j = (n+3)(L/2)$, which is possible only for $n = -2$ or $n = -4$. When $n = -2$, it is obvious that $(k-i) = -L-1$, which is impossible. When $n = -4$, it is obvious that $(k-i) = -2L-1$, which is also impossible.

(iii) If $(2i-j-k) = -(3L/2+1)$, then Eq. (13) reduces to $-1+(k-i) = n(L/2)$. It follows that $i-j = (n-3)(L/2)$, which is possible only for $n = 2$ or $n = 4$. When $n = 2$, it is clear that $(k-i) = L+1$, which is impossible. When $n = 4$, it is clear that $(k-i) = 2L+1$, which is also impossible.

Next, consider the second part of the theorem where L is odd. The proofs of the absence of 4-cycles are similar to those in Theorem 2 and hence omitted. The 6-cycles can be represented by $(0-j)+(i-\frac{3L+1}{2}i)+(\frac{3L+1}{2}k-0) = 0\,(mod\ P)$, which is equivalent to

$$(i-j)+\frac{3L+1}{2}(k-i) = n(3L^2+1)/4 \tag{14}$$

for some integer n. Because the LHS of Eq. (14) satisfies that $|LHS| \le -1+\frac{3L+1}{2}(L-1) < 2[3(L^2+1)/4]$, it is obvious that $n \in \{0, 1, -1\}$.

(i) If $n = 0$, Eq. (14) becomes $(i-j)+\frac{3L+1}{2}(k-i) = 0$, which leads to $\frac{3L+1}{2}|(i-j)$. It is impossible.

(ii) If $n = -1$, Eq. (14) turns into $(i-j)+\frac{3L+1}{2}(k-i) = -(3L^2+1)/4$, which is equivalent to

$$(i-j)-(L-1)/4+2(\frac{3L+1}{4})(k-i) = -L(3L+1)/4. \tag{15}$$

This equation can be expressed as

$$(i-j)-(L-1)/4 = z(3L+1)/4 \tag{16}$$

for some integer z. Since $|(i-j)-(L-1)/4| \le 5(L-1)/4$, it is clear that $z \in \{0, -1, 1\}$. If $z = 0$, Eq. (15) reduces to $(k-i) = -L/2$. It is impossible as L is odd. If $z = 1$, Eq. (16) becomes $(i-j) = (L-1)/4+(3L+1)/4 = L$, which is impossible. If $z = -1$, then Eq. (16) becomes $(i-j) = (L-1)/4-(3L+1)/4 = -(L+1)/2$. On the other hand, Eq. (15) yields $k-i = (1-L)/2$. Therefore, it follows that $k-j = -L$, which is impossible.

(iii) If $n = 1$, then Eq. (14) becomes $(i-j)+\frac{3L+1}{2}(k-i) = (3L^2+1)/4$, which is

$$(i-j)+(L-1)/4+2(\frac{3L+1}{4})(k-i) = L(3L+1)/4. \tag{17}$$

This equation can be rewritten as

$$(i-j)+(L-1)/4 = z(3L+1)/4, \tag{18}$$

where z is an integer. As LHS of Eq. (18) satisfies $|LHS| \le (L-1)+(L-1)/4 < 2[(3L+1)/4]$, it is obvious that $z \in \{0, -1, 1\}$. If $z = 0$, then Eq. (18) yields $(i-j) = -(L-1)/4$ and hence Eq. (17) reduces to $2(\frac{3L+1}{4})(k-i) = L(3L+1)/4$. Therefore, $(k-i) = L/2$. It is impossible

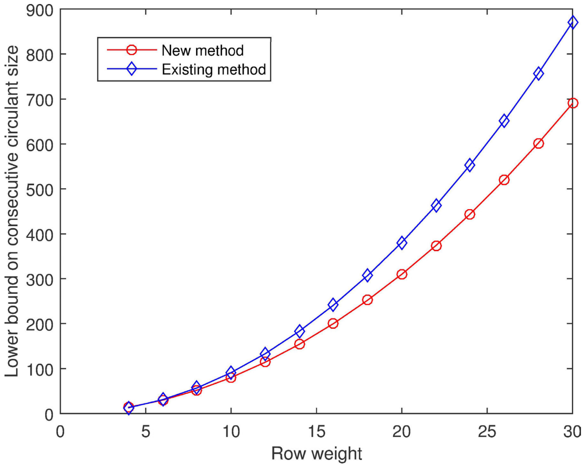

FIGURE 1. ***LB_{ccs}*** **comparison: new method (Theorem 3(i)) and existing method [17].**

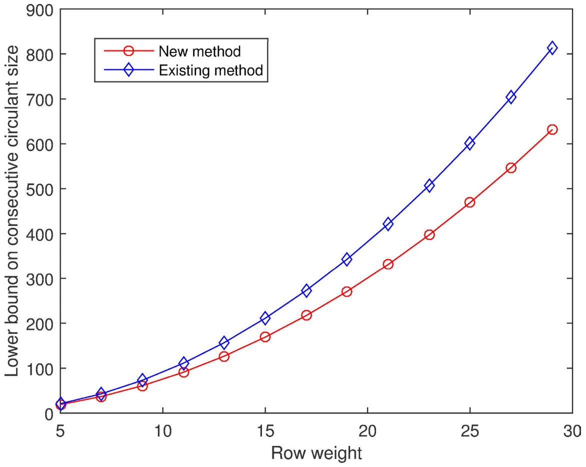

FIGURE 2. ***LB_{ccs}*** **comparison: new method (Theorem 3(ii)) and existing method [17].**

as L is odd. If $z = 1$, then Eq. (18) turns into $(i-j) = -(L-1)/4 + (3L+1)/4 = (L+1)/2$ and hence Eq. (17) reduces to $k - i = (L-1)/2$. As a result, $k - j = L$, which is impossible. If $z = -1$, then Eq. (18) becomes $(i-j) = -(L-1)/4 - (3L+1)/4 = -L$, which is impossible. □

The LB_{ccs} for the exponent matrix generated by Theorem 3 (i) (resp. Theorem 3 (ii)) (after modulo P) is compared with that for the exponent matrix generated by $[0, 1, L]^T \cdot [0, 1, \cdots, L-1]$ in Fig. 1 (resp. Fig. 2). It is observed that the new construction has a smaller LB_{ccs} and hence can offer more small circulant sizes guaranteeing girth-eight codes.

IV. NEW CONSTRUCTION FOR J=4

According to Lemma 1, the existing tuple $[0, 1, L, L+1]$ ensures a $(4, L)$-regular QC-LDPC code without 4-cycles and 6-cycles if the circulant size is greater than or equal to L^2. In this section, it is analyzed whether this tuple is feasible for girth-eight code with circulant sizes smaller than L^2. The answer to the question turns out to be in the negative. In an attempt to find tuples suitable for smaller circulant sizes, a novel tuple permitting larger entries is proposed, which includes the existing tuple $[0, 1, L, L+1]$ as a special case. On the one hand, it is proved that the novel method also works for the circulant size L^2. On the other hand, it is empirically found that the new method is suitable for circulant sizes smaller than L^2 for certain parameters, but no general rules are found. Instead, another new construction is presented based on the tuple $[0, L/2, L+1, 3L+1]$, which can provide much smaller circulant sizes when L can be divided by 8.

A. NEW PROPERTY FOR EXISTING TUPLE [0,1,L,L+1]

Theorem 4: $\boldsymbol{S}_2 = [0, 1, L, L+1]$ *corresponds to a girth-eight* $(4, L)$*-regular FLRM QC-LDPC code* if and only if *the circulant size* $P \geq L^2$.

Proof: Since the tuple $[0, 1, L, L+1]$ satisfies the GCD constraint, any circulant size $P \geq L^2$ can ensure a girth-eight QC-LDPC code. Moreover, owing to Theorem 1, any circulant size $P \leq L(L-1)$ corresponds to a QC-LDPC code with girth smaller than eight. Therefore, it suffices to consider the circulant size in the range $L(L-1)+1 \leq P \leq L^2 - 1$. For $1 \leq i \leq L-2$, the 6-cycles governed by $[e(0,i) - e(1,i)] + [e(1,0) - e(3,0)] + [e(3, L-1) - e(0, L-1)] = (L+1)(L-1) - i = 0\ (mod\ P)$ cannot occur. As a result, $P \notin \{L^2 - 1 - (L-2), L^2 - 1 - (L-1), \cdots, L^2 - 1 - 1\}$. Besides, it is obvious that $P \neq L^2 - 1$; otherwise, there exist 4-cycles expressed by $[e(0,0) - e(3,0)] + [e(3, L-1) - e(0, L-1)] = 0\ (mod\ L^2 - 1)$. □

B. NEW GENERALIZATION FROM TUPLE [0,x,yL,x+zL]

Theorem 5: Let x, y *and* z *be three integers (not necessarily distinct) such that* $gcd(x, L) = 1$, $gcd(y, L) = 1$ *and* $gcd(z, L) = 1$. *Then* $\boldsymbol{S}_2 = [0, x, yL, x+zL]$ *corresponds to a girth-eight* $(4, L)$*-regular FLRM QC-LDPC code for the circulant size* $P = L^2$.

Proof: Let i and j be two column indexes such that $0 \leq i < j \leq L-1$. There are six cases for 4-cycles.

(i) (0,1)-4-cycles: Such cycles can be expressed as $(0 - xi) + (xj - 0) = 0\ (mod\ P)$, which reduces to $x(j-i) = nL^2$ for a certain integer n. As $gcd(x, L) = 1$, it follows that $L|(j-i)$. Obviously, this is impossible.

(ii) (0,2)-4-cycles: The cycles can be represented by $[0 - (yL)i] + [(yL)j - 0] = 0\ (mod\ P)$, which is equivalent to $(yL)(j-i) = nL^2$ for a certain integer n. Because $gcd(y, L) = 1$, it is clear that $L|(j-i)$, which cannot hold true.

(iii) (0,3)-4-cycles: Such cycles can be denoted by $[0 - (x+zL)i] + [(x+zL)j - 0] = 0\ (mod\ P)$, which reduces to $(zL+x)(j-i) = nL^2$ for a certain integer n. Owing to Lemma 3 and $gcd(x, L) = 1$, it is clear that $gcd(zL+x, L) = 1$. Therefore, $L|(j-i)$, which is impossible.

(iv) (1,2)-4-cycles: The cycles can be expressed as $[xi - (yL)i] + [(yL)j - xj] = 0\ (mod\ P)$, which becomes $x(i-j) + yL(j-i) = nL^2$ for a certain integer n. Since $gcd(x, L) = 1$, it is obvious that $L|(i-j)$, which cannot hold true.

(v) (1,3)-4-cycles: Such cycles can be denoted by $[xi-(x+zL)i]+[(x+zL)j-xj]=0\ (mod\ P)$, which is equivalent to $zL(j-i)=nL^2$ for a certain integer n. As $gcd(z,L)=1$, it follows that $L|(j-i)$, which is impossible.

(vi) (2,3)-4-cycles: The cycles can be represented by $[(yL)i-(x+zL)i]+[(x+zL)j-(yL)j]=0\ (mod\ P)$, which reduces to $x(j-i)+L(z-y)(j-i)=nL^2$ for a certain integer n. As $gcd(x,L)=1$, it follows that $L|(j-i)$, which cannot hold true.

Let i, j and k be three different column indexes such that $0 \le i,j,k \le L-1$. There are four cases for 6-cycles.

(i) (0,1,2)-6-cycles: Such cycles can be denoted by $(0-xj)+[xi-(yL)i]+[(yL)k-0]=0\ (mod\ P)$, which is equivalent to $x(i-j)+yL(k-i)=nL^2$ for a certain integer n. As $gcd(x,L)=1$, it is clear that $L|(i-j)$. It is impossible.

(ii) (0,1,3)-6-cycles: The cycles can be described by $(0-xj)+[xi-(x+zL)i]+[(x+zL)k-0]=0\ (mod\ P)$, which is equivalent to $x(i-j)+(x+zL)(k-i)=nL^2$ for a certain integer n. By arranging terms, it becomes $x(k-j)+zL(k-i)=nL^2$. As $gcd(x,L)=1$, it is clear that $L|(k-j)$. Obviously, it is impossible.

(iii) (0,2,3)-6-cycles: Such cycles can be expressed as $[0-(yL)j]+[(yL)i-(x+zL)i]+[(x+zL)k-0]=0\ (mod\ P)$, which is equivalent to $(yL)(i-j)+(x+zL)(k-i)=nL^2$ for a certain integer n. It can be rewritten as $(yL)(i-j)+x(k-i)+(zL)(k-i)=nL^2$. As $gcd(x,L)=1$, it is obvious that $L|(k-i)$, which cannot hold true.

(iv) (1,2,3)-6-cycles: The cycles can be described by $[xj-(yL)j]+[(yL)i-(x+zL)i]+[(x+zL)k-xk]=0\ (mod\ P)$, which reduces to $x(j-k)+(yL)(i-j)+(x+zL)(k-i)=nL^2$ for a certain integer n. By arranging terms, it turns into $x(j-i)+(yL)(i-j)+(zL)(k-i)=nL^2$. Since $gcd(x,L)=1$, it is clear that $L|(j-i)$, which is impossible. □

Remark 3: By setting $(x,y,z)=(1,1,1)$, the sequence $\boldsymbol{S}_2$ becomes $[0,1,L,L+1]$, which is just an existing method. The new construction, however, is more general in the sense that it is able to yield a large number of girth-eight $(4,L)$-regular FLRM codes with the circulant size of L^2. In addition, it should be noted that for certain parameters, the circulant size can be smaller than L^2. For example, $(x,y,z)=(5,1,11)$ and $(x,y,z)=(9,13,7)$ are two tuples which ensure girth-eight FLRM codes with $P=60$ for $L=8$. For another example, $(x,y,z)=(4,15,21)$ and $(x,y,z)=(10,3,18)$ are two tuples which guarantee girth-eight FLRM codes with $P=111$ for $L=11$.

C. NEW CONSTRUCTION FROM TUPLE [0,L/2,L+1,3L+1]

According to Remark 3, the construction in Theorem 5 may, in very special cases, yields girth-eight FLRM codes with circulant sizes smaller than L^2, but no general rules have been found. Instead, a new tuple of $[\alpha_0,\cdots,\alpha_3]$ is sought out, which permits a smaller circulant size to produce girth-eight FLRM codes for each L satisfying $mod(L,8)=0$.

Theorem 6: If $mod(L,8)=0$, then $\boldsymbol{S}_2=[0,L/2,L+1,3L+1]$ corresponds to a girth-eight $(4,L)$-regular FLRM QC-LDPC code for the circulant size $P=L^2-L/2$.

Proof: Firstly, consider 4-cycles. Let i and j be two column indexes such that $0 \le i < j \le L-1$. There are six cases for 4-cycles.

(i) (0,1)-4-cycles can be expressed as $[0-(L/2)i]+[(L/2)j-0]=0\ (mod\ P)$, which is equivalent to

$$(L/2)(j-i)=n(L^2-L/2) \tag{19}$$

for a certain integer n. As $0 < LHS \le L(L-1)/2 < (L^2-L/2)$, Eq. (19) is impossible.

(ii) (0,2)-4-cycles can be denoted by $[0-(L+1)i]+[(L+1)j-0]=0\ (mod\ P)$, which reduces to

$$(L+1)(j-i)=n(L^2-L/2) \tag{20}$$

for a certain integer n. Because $0 < LHS \le (L+1)(L-1) < 2(L^2-L/2)$, Eq. (20) is possible only for $n=1$. When $n=1$, Eq. (20) becomes $(L+1)(j-i)=L^2-L/2$, where $LHS < RHS$ for the case $j-i \le L-2$ and $LHS > RHS$ for the case $j-i=L-1$. Therefore, Eq. (20) is impossible.

(iii) (0,3)-4-cycles can be represented by $[0-(3L+1)i]+[(3L+1)j-0]=0\ (mod\ P)$, which is equivalent to

$$(3L+1)(j-i)=n(L^2-L/2) \tag{21}$$

for a certain integer n. Since $0 < LHS \le (3L+1)(L-1) < 3(L^2-L/2)$, Eq. (21) is possible only for $n=1$ or $n=2$. (a) If $n=1$, then $(3L+1)(j-i)=(L/2)(2L-1)$. As $gcd(3L+1,L/2)=1$, it follows that $(L/2)|(j-i)$. The only possibility is $j-i=L/2$ and hence Eq. (21) becomes $3L+1=2L-1$, which is impossible. (b) If $n=2$, then $(3L+1)(j-i)=L(2L-1)$. As $gcd(3L+1,L)=1$, it is clear that $L|(j-i)$, which is also impossible.

(iv) (1,2)-4-cycles can be expressed as $[(L/2)i-(L+1)i]+[(L+1)j-(L/2)j]=0\ (mod\ P)$, which reduces to

$$(L/2+1)(j-i)=n(L^2-L/2) \tag{22}$$

for a certain integer n. However, Eq. (22) is impossible due to the relationship $0 < LHS \le (L/2+1)(L-1) < (L^2-L/2)$.

(v) (1,3)-4-cycles can be denoted by $[(L/2)i-(3L+1)i]+[(3L+1)j-(L/2)j]=0\ (mod\ P)$, which is equivalent to

$$(5L/2+1)(j-i)=n(L^2-L/2) \tag{23}$$

for a certain integer n. Because $0 < LHS \le (5L/2+1)(L-1) < 3(L^2-L/2)$, Eq. (23) is possible only for $n=1$ or $n=2$. (a) If $n=1$, then $(5L/2+1)(j-i)=(L/2)(2L-1)$. As $gcd(5L/2+1,L/2)=1$, it is clear that $j-i=L/2$ and hence $(5L/2+1)=2L-1$, which is impossible. (b) If $n=2$, then $(5L/2+1)(j-i)=(L/2)(4L-2)$. Similarly, because $gcd(5L/2+1,L/2)=1$, it is clear that $j-i=L/2$ and hence $5L/2+1=4L-2$, which is also impossible.

(vi) (2,3)-4-cycles can be expressed as $[(L+1)i-(3L+1)i]+[(3L+1)j-(L+1)j]=0\ (mod\ P)$, which reduces to

$$2L(j-i)=n(L^2-L/2) \tag{24}$$

for a certain integer n. As $0 < LHS \le 2L(L-1) < 2(L^2-L/2)$, Eq. (24) is possible only for $n=1$. However, $n=1$ leads to $2(j-i)=(L-1/2)$, which is impossible.

Next, consider 6-cycles. Let i, j and k be three different column indexes such that $0 \leq i, j, k \leq L-1$. There are four cases for 6-cycles.

(i) (0,1,2)-6-cycles can be represented by $[0-(L/2)j]+[(L/2)i-(L+1)i]+[(L+1)k-0)] = 0\,(mod\ P)$, which is equivalent to

$$(L/2)(i-j)+(L+1)(k-i) = n(L^2-L/2). \qquad (25)$$

If $n=0$, Eq. (25) becomes $(L/2)(i-j) = (L+1)(i-k)$. As $gcd(L/2, L+1) = 1$, it follows that $(L+1)|(i-j)$, which is impossible. If $n \neq 0$, $|RHS| \geq (L^2-L/2)$ but $|LHS| \leq (-1)L/2+(L+1)(L-1) = L^2-L/2-1$. Therefore, it is also impossible.

(ii) (0,1,3)-6-cycles can be denoted by $[0-(L/2)j]+[(L/2)i-(3L+1)i]+[(3L+1)k-0)] = 0\,(mod\ P)$, which is equivalent to $(L/2)(i-j)+(3L+1)(k-i) = n(L^2-L/2)$. By arranging terms, it turns into

$$(L/2)[i-j-n(2L-1)] = (3L+1)(i-k). \qquad (26)$$

Since $gcd(L/2, 3L+1) = 0$, it is clear that $i-k = L/2$ or $-L/2$. (a) If $i-k = L/2$, then $i-j = n(2L-1)+(3L+1)$. This is possible only when $n=-2$ and hence $i-j = -L+3$. However, this scenario implies $k-j = -L-L/2+3$, which is impossible. (b) If $i-k = -L/2$, then $i-j = n(2L-1)-(3L+1)$. This is possible only when $n=2$ and hence $i-j = L-3$. However, for this scenario it follows that $k-j = L+L/2-3$, which is also impossible.

(iii) (0,2,3)-6-cycles can be represented by $[0-(L+1)j]+[(L+1)i-(3L+1)i]+[(3L+1)k-0)] = 0\,(mod\ P)$, which is $(L+1)(i-j)+(3L+1)(k-i) = n(L^2-L/2)$. By arranging terms, it becomes

$$2(\frac{L}{2})(i-j)+6(\frac{L}{2})(k-i)+(k-j) = n(\frac{L}{2})(2L-1). \qquad (27)$$

Therefore, $k-j = L/2$ or $-L/2$. (a) If $k-j = L/2$, Eq. (27) reduces to $2(L/2)+4(k-i)+1 = n(2L-1)$. As $|LHS| \leq 5L-3 < 3(2L-1)$ and LHS is odd, it follows that $n \in \{-1, 1\}$. However, $n=1$ yields $k-i = (L-2)/4$, which is impossible as $8|L$. Similarly, $n=-1$ implies $k-i = -3L/4$ and hence $i-j = L/2+3L/4 > L-1$, which is impossible. (b) If $k-j = -L/2$, Eq. (27) becomes $2(-L/2)+4(k-i)+(-1) = n(2L-1)$. Because $|LHS| \leq 5L-3 < 3(2L-1)$ and LHS is odd, it is obvious that $n \in \{-1, 1\}$. However, $n=1$ leads to $k-i = 3L/4$ and hence $j-i = L/2+3L/4 > L-1$, which is impossible. Likewise, $n=-1$ yields $k-i = (2-L)/4$, which is also impossible.

(iv) (1,2,3)-6-cycles can be described by $[(L/2)j-(L+1)j]+[(L+1)i-(3L+1)i]+[(3L+1)k-(L/2)k] = 0\,(mod\ P)$, which is equivalent to $(L/2)(j-k)+(L+1)(i-j)+(3L+1)(k-i) = n(L^2-L/2)$ for a certain integer n. By arranging terms, it turns into

$$(\frac{L}{2})[(k-j)+4(k-i)]+(k-j) = n(\frac{L}{2})(2L-1). \qquad (28)$$

Therefore, $(k-j) = L/2$ or $k-j = -L/2$. (a) If $k-j = L/2$, Eq. (28) reduces to $(L/2)+4(k-i)+1 = n(2L-1)$. Since $|LHS| \leq 4L+L/2-3 < 3(2L-1)$ and LHS is odd, it follows that $n \in \{-1, 1\}$. However, $n=1$ means $k-i = (3L-4)/8$, which is impossible as $8|L$. Likewise, $n=-1$ leads to $k-i = -(5L)/8$ and hence $i-j = L/2+5L/8 > L-1$, which is impossible. (b) If $k-j = -L/2$, Eq. (28) reduces to $-(L/2)+4(k-i)-1 = n(2L-1)$. Because $|LHS| \leq 4L+L/2-3 < 3(2L-1)$ and LHS is odd, it is clear that $n \in \{-1, 1\}$. However, $n=1$ implies $k-i = (5L)/8$ and hence $j-i = L/2+5L/8 > L-1$, which is impossible. Similarly, $n=-1$ leads to $k-i = (4-3L)/8$, which is also impossible due to $8|L$. □

V. NEW CONSTRUCTION FOR J=5

In the literature, there are three existing tuples [12] which can explicitly produce $(5, L)$-regular QC-LDPC codes with girth eight for any circulant size greater than or equal to $\alpha_4(L-1)+1$, where α_4 stands for the last entry of the tuples. The three existing tuples are $[\alpha_0, \cdots, \alpha_4] = [0, 1, L+2, 2L+1, 2L+2]$, $[0, 1, L, L+1, 2L+3]$ and $[0, 2, L, 2L+1, 2L+2]$, respectively. In this section, whether these tuples are applicable to circulant sizes smaller than $\alpha_4(L-1)+1$ is explored. It turns out that the latter two tuples indeed work for certain types of L. For the rest scenarios where the latter two tuples are not applicable, two novel tuples are proposed to offer circulant sizes much smaller than $\alpha_4(L-1)+1$.

The five tuples are analyzed one by one in the following subsections V-A-V-E, respectively.

A. ON EXISTING TUPLE [0,1,L+2,2L+1,2L+2]

Regarding the first tuple $[0, 1, L+2, 2L+1, 2L+2]$, it has been empirically verified that for L in the range $L = 6 \sim 50$ such that $mod(L, 6) \notin \{1, 4\}$, girth cannot reach eight if the circulant size is smaller than $(2L+2)(L-1)+1$. Therefore, the following conjecture is likely to be true.

Conjecture 3: Let $L \geq 6$ be an integer satisfying $mod(L, 6) \notin \{1, 4\}$. For $\mathbf{S}_2 = [0, 1, L+2, 2L+1, 2L+2]$, the smallest circulant size ensuring a girth-eight FLRM QC-LDPC code is $(2L+2)(L-1)+1$.

B. NEW PROPERTY FOR EXISTING TUPLE [0,1,L,L+1,2L+3]

Now, consider the second tuple, $[0, 1, L, L+1, 2L+3]$. It turns out that a circulant size smaller than $(2L+3)(L-1)+1$ does exist.

Theorem 7: If $mod(L, 6) \in \{2, 4\}$, then $\mathbf{S}_2 = [0, 1, L, L+1, 2L+3]$ corresponds to a girth-eight $(5, L)$-regular FLRM QC-LDPC code for the circulant size $P = (L+2)^2-1$.

See appendix A for the proof of Theorem 7.

It has been verified that for L in the range $L = 8 \sim 50$ such that $mod(L, 6) \in \{2, 4\}$, girth cannot reach eight when the circulant size is smaller than $(L+2)^2-1$. Therefore, the following conjecture is likely to be true.

Conjecture 4: Let $L \geq 8$ be an integer satisfying $mod(L, 6) \in \{2, 4\}$. For $\mathbf{S}_2 = [0, 1, L, L+1, 2L+3]$, the smallest circulant size guaranteeing a girth-eight FLRM QC-LDPC code is $(L+2)^2-1$.

The LB_{ccs} for the exponent matrix in Theorem 7 (after modulo P) is compared with that for the original

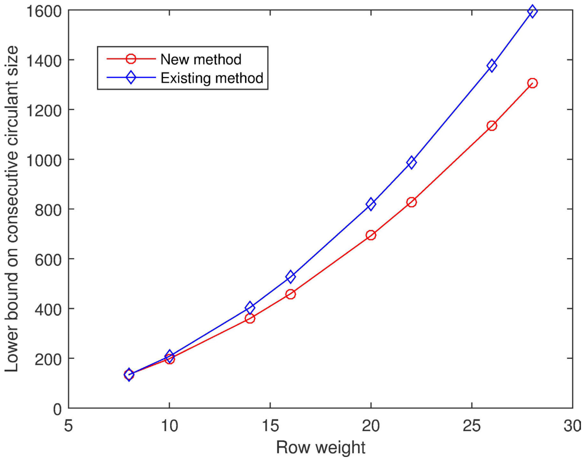

FIGURE 3. LB_{ccs} **comparison: new method (Theorem 7) and existing method [12].**

exponent matrix [12] generated by $[0, 1, L, L+1, 2L+3]^T \cdot [0, 1, \cdots, L-1]$ in Fig. 3. It is observed that the novel method provides a smaller LB_{ccs}, which enables more small circulant sizes to produce girth-eight codes.

C. NEW PROPERTY FOR EXISTING TUPLE [0,2,L,2L+1,2L+2]

Finally, consider the third tuple, $[0, 2, L, 2L+1, 2L+2]$. It turns out that a circulant size smaller than $(2L+2)(L-1)+1$ does exist.

Theorem 8: If $mod(L, 6) \in \{1, 3\}$, then $\mathbf{S}_2 = [0, 2, L, 2L+1, 2L+2]$ corresponds to a girth-eight $(5, L)$-regular FLRM QC-LDPC code for $P = 2L(L-1)+1$.

See appendix B for the proof of Theorem 8.

It is possible to further reduce the circulant size. It has been verified that for L in the range $19 \leq L \leq 100$ satisfying $mod(L, 6) \in \{1, 3\}$, the sequence $\mathbf{S}_2 = [0, 2, L, 2L+1, 2L+2]$ corresponds to a girth-eight $(5, L)$-regular FLRM QC-LDPC code for $P = 2L(L-3)+3$.

Up to now, two tuples have been found, which guarantee girth-eight FLRM codes with circulant sizes smaller than $\alpha_4(L-1)+1$ for $mod(L, 6) \in \{2, 4\}$ and $mod(L, 6) \in \{1, 3\}$, respectively. In regard to the non-applicable scenarios $(mod(L, 6) \in \{0, 5\})$, two novel tuples applicable to the case $mod(L, 6) = 0$ and the case $mod(L, 6) = 5$, respectively, are empirically conceived in the following two subsections.

D. NEW CONSTRUCTION FROM TUPLE [0,1,L+1,L+2,3L]

Conjecture 5: If $mod(L, 6) = 0$, then $\mathbf{S}_2 = [0, 1, L+1, L+2, 3L]$ corresponds to a girth-eight $(5, L)$-regular FLRM QC-LDPC code for $P = L^2 + 14L - 3$.

The validity of Conjecture 5 has been verified for $6 \leq L \leq 100$ such that $mod(L, 6) = 0$. Although Conjecture 5 would probably be proved by taking full advantage of the skills used in the proof of Theorem 7, it is not proved here and is left as an open problem.

For certain choices of L, the circulant size can be chosen even smaller. For L in the range $6 \leq L < 54$ such that $mod(L, 6) = 0$, it has been verified that $[0, 1, L+1, L+2, 3L]$ corresponds to a girth-eight $(5, L)$-regular FLRM QC-LDPC code for $P = L^2 + 10L - 3$; however, for $L = 54$, such a circulant size leads to girth smaller than eight.

E. NEW CONSTRUCTION FROM TUPLE [0,2,L+2,L+8,3L+8]

The validity of the following conjecture has been verified for $5 \leq L \leq 100$ such that $mod(L, 6) = 5$.

Conjecture 6: If $mod(L, 6) = 5$, then $\mathbf{S}_2 = [0, 2, L+2, L+8, 3L+8]$ corresponds to a girth-eight $(5, L)$-regular FLRM QC-LDPC code for $P = L^2 + 8L + 16$.

If $mod(L, 12) = 5$, the circulant size can be chosen even smaller. The correctness of the following conjecture has been verified for $5 \leq L \leq 100$ such that $mod(L, 12) = 5$.

Conjecture 7: If $mod(L, 12) = 5$, then $\mathbf{S}_2 = [0, 2, L+2, L+8, 3L+8]$ corresponds to a girth-eight $(5, L)$-regular FLRM QC-LDPC code for $P = L^2 + 8L + 12$.

It is probable to prove Conjecture 6 and Conjecture 7 by taking full advantage of the skills employed in the proof of Theorem 7; however, they are not proved here and are left as open problems.

The new constructions (which have been proved in this paper) for girth-eight FLRM QC-LDPC codes are summarized in Table. 1. Besides, a set of conjectures raised in this paper regarding girth-eight FLRM QC-LDPC codes are listed in Table. 2.

TABLE 1. **Summary of novel constructions.**

J	$\mathbf{S}_2$	circulant size	note (Theorem)
3	$[0, 2, L]$	$L^2 - 2L + 4$	L odd (Th. 2)
3	$[0, 1, 3L/2]$	$3L^2/4 + L/2$	L even (Th. 3i)
3	$[0, 1, (3L+1)/2]$	$(3L^2+1)/4$	L odd (Th. 3ii)
4	$[0, x, yL, x+zL]$	L^2	x, y, z coprime to L (Th. 5)
4	$[0, L/2, L+1, 3L+1]$	$L^2 - L/2$	$mod(L, 8) = 0$ (Th. 6)
5	$[0, 1, L, L+1, 2L+3]$	$L^2 + 4L + 3$	$mod(L, 6) \in \{2, 4\}$ (Th. 7)
5	$[0, 2, L, 2L+1, 2L+2]$	$2L^2 - 2L + 1$	$mod(L, 6) \in \{1, 3\}$ (Th. 8)

TABLE 2. **Summary of main conjectures.**

J	$\mathbf{S}_2$	circulant size	note (Conjecture)
3	$[0, \alpha_1, L]$	$L^2 - \alpha_1 L + \alpha_1^2$	$gcd(\alpha_1, L) = 1$ (Conj. 2)
5	$[0, 1, L+1, L+2, 3L]$	$L^2 + 14L - 3$	$mod(L, 6) = 0$ (Conj. 5)
5	$[0, 2, L+2, L+8, 3L+8]$	$L^2 + 8L + 16$	$mod(L, 6) = 5$ (Conj. 6)
5	$[0, 2, L+2, L+8, 3L+8]$	$L^2 + 8L + 12$	$mod(L, 12) = 5$ (Conj. 7)

VI. PERFORMANCE SIMULATIONS

In this section, a set of novel girth-eight FLRM QC-LDPC codes or their derived codes are compared with existing counterparts, in terms of the bit/block error rate. The BPSK modulation, AWGN channel and sum-product-algorithm (SPA) decoding are used in our simulations. With the increase of iterations for SPA, decoding performance gradually improves. However, when the number of iterations exceeds a certain integer (such as 100), performance improvement is negligible. This paper adopts the convention in some existing papers, and set the number of iterations to 50.

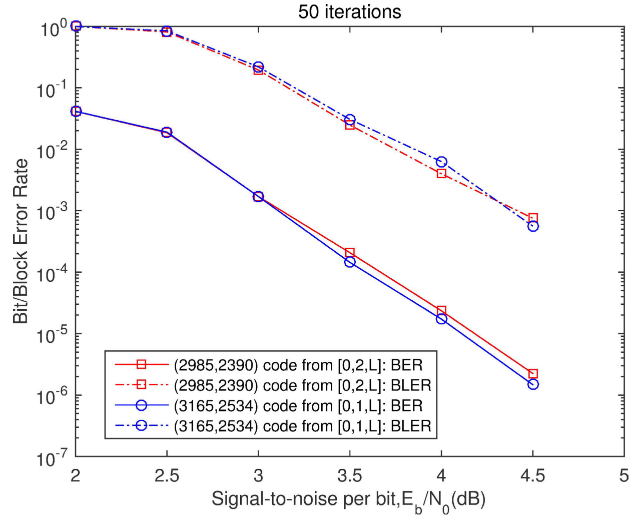

FIGURE 4. Performance comparison of $(3, L)$-regular FLRM QC-LDPC codes: new code generated by $[0, 2, L]$ (in Theorem 2) and existing code obtained by $[0, 1, L]$ [17], where $L = 15$.

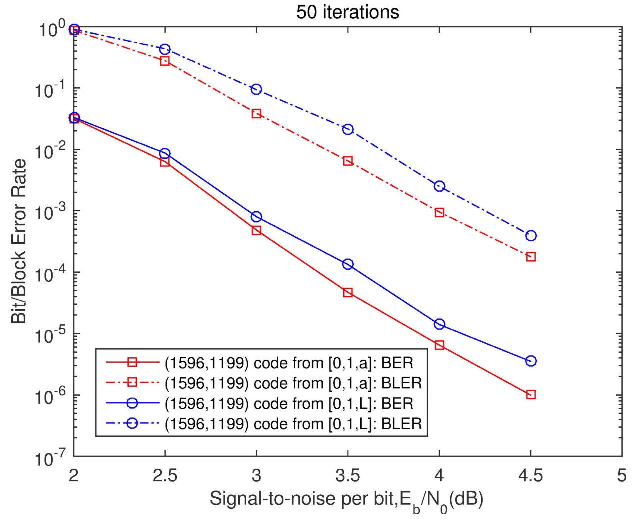

FIGURE 5. Performance comparison of $(3, L)$-regular QC-LDPC codes: new code generated by $[0, 1, a]$ (in Theorem 3(i)) and existing code obtained by $[0, 1, L]$ [17], where $L = 12$ and $a = 3L/2$.

Example 1: For $L = 15$, two $(3, L)$-regular FLRM QC-LDPC codes are constructed with girth eight. According to Theorem 2, the first code is generated based on the new tuple $[0, 2, L]$ and a circulant size $P = L^2 - 2L + 4 = 199$. The second one is obtained by the existing tuple $[0, 1, L]$ [17] with a circulant size $P = L(L - 1) + 1 = 211$. Although the new code is 180 bits shorter than its counterpart, it is observed in Fig. 4 that they perform almost the same.

Example 2: For $L = 12$, set $\boldsymbol{E}= [0, 1, 3L/2]^T \cdot [0, 1, \cdots , L - 1]$ and $P_0 = 3L^2/4 + L/2 = 114$ according to Theorem 3(i). Let $\boldsymbol{E}$'$=$ mod$(\boldsymbol{E}, P_0)$. Then select another circulant size $P = 133$ to produce a $(3, 12)$-reguar QC-LDPC code based on $\boldsymbol{E}$'. For comparison, another code is obtained by the existing tuple $[0, 1, L]$ [17] and the same circulant size $P = 133$. It is noticed in Fig. 5 that the new code performs noticeably better than the existing one.

For $L = 9$, two $(3, L)$-regular girth-eight QC-LDPC codes are constructed as follows. The first code is generated by the existing tuple $[0, 1, L]$ [17] with a circulant size $P = L(L - 1) + 1 = 73$. According to Theorem 3(ii), let $\boldsymbol{E}= [0, 1, (3L + 1)/2]^T \cdot [0, 1, \cdots , L - 1]$ and $P_0 = (3L^2 + 1)/4 = 61$. Set $\boldsymbol{E}$'$=$ mod$(\boldsymbol{E}, P_0)$. Then the second code is obtained from $\boldsymbol{E}$' and the same circulant size $P = 73$. It is observed in Fig. 6 that the novel code markedly outperforms its counterpart.

As can be seen from the two new codes in this example, circulant sizes different from those in Theorem 3 can be chosen to construct girth-eight QC-LDPC codes, as long as they are not smaller than the associated LB_{ccs} for $\boldsymbol{E}$'.

Example 3: For $L = 12$, two $(4, L)$-regular FLRM QC-LDPC codes are constructed with girth eight. According to Theorem 5, the first code is generated based on the novel tuple $[0, 1, 5L, 1 + 7L]$ and a circulant size $P = L^2 = 144$. The second one is obtained by the existing tuple $[0, 1, L, L + 1]$ [17] with the same circulant size $P = 144$. It is observed in Fig. 7 that they perform more or less the same.

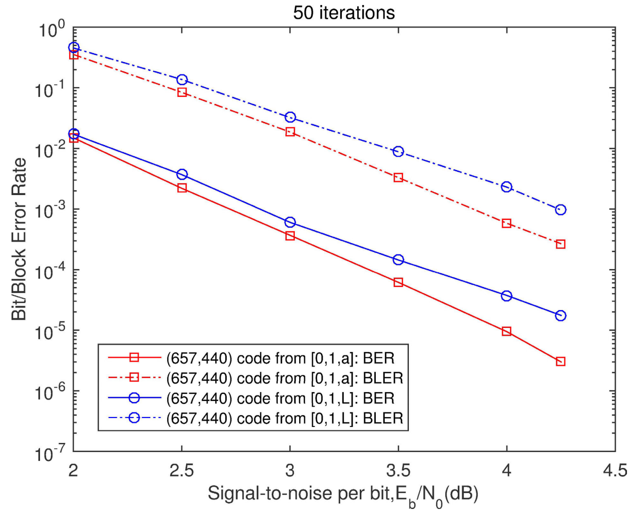

FIGURE 6. Performance comparison of $(3, L)$-regular QC-LDPC codes: new code generated by $[0, 1, a]$ (in Theorem 3(ii)) and existing code obtained by $[0, 1, L]$ [17], where $L = 9$ and $a = (3L + 1)/2$.

The advantage of Theorem 5 is that, via this theorem, many nonequivalent girth-eight $(4, L)$-regular codes with the same length can be easily found, so better girth-eight codes can be further picked out from these candidates by utilizing certain advanced skills.

For $L = 8$, two $(4, L)$-regular FLRM QC-LDPC codes are constructed with girth eight. According to Theorem 6, the first code is generated based on the new tuple $[0, L/2, L + 1, 3L+1]$ and a circulant size $P = L^2-L/2 = 60$. The second one is obtained by the existing tuple $[0, 1, L, L+1]$ [17] with a circulant size $P = L^2 = 64$. Although the novel code is sightly shorter than its counterpart, it is observed in Fig. 8 that the new FLRM code noticeably outperforms the existing FLRM code.

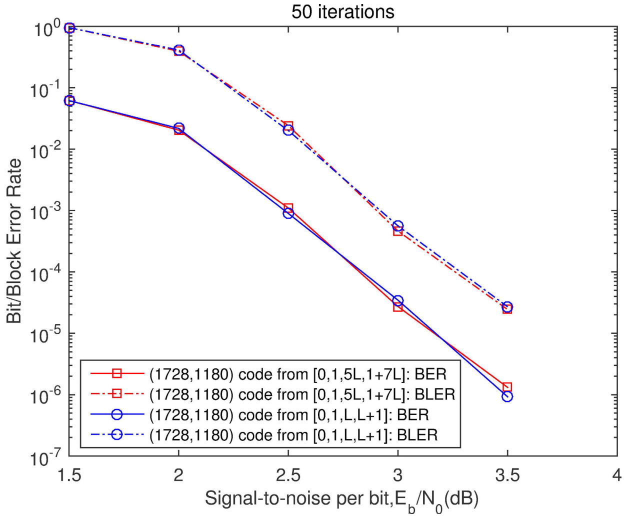

FIGURE 7. **Performance comparison of $(4, L)$-regular FLRM QC-LDPC codes: new code generated by $[0, 1, 5L, 1 + 7L]$ (in Theorem 5) and existing code obtained by $[0, 1, L, L + 1]$ [17], where $L = 12$.**

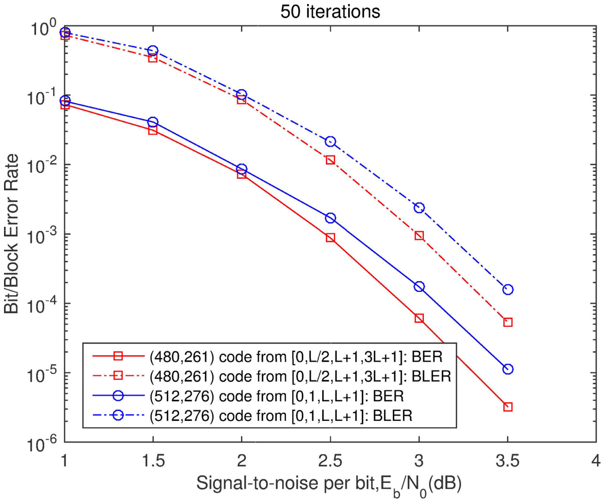

FIGURE 8. **Performance comparison of $(4, L)$-regular FLRM QC-LDPC codes: new code generated by $[0, L/2, L + 1, 3L + 1]$ (in Theorem 6) and existing code obtained by $[0, 1, L, L + 1]$ [17], where $L = 8$.**

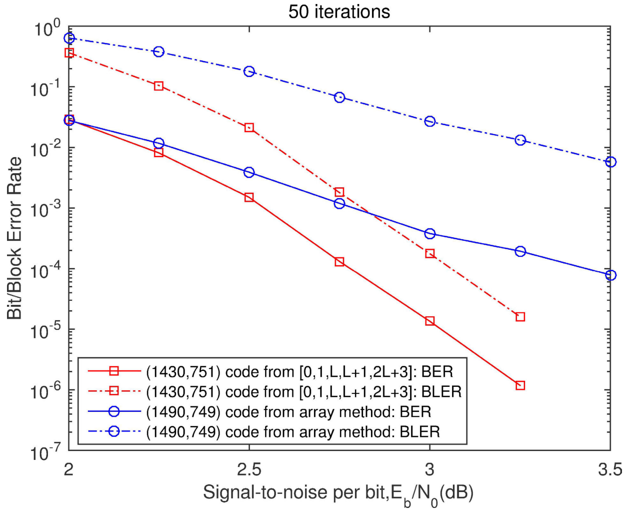

FIGURE 9. **Performance comparison of $(5, L)$-regular FLRM QC-LDPC codes: new code generated by $[0, 1, L, L + 1, 2L + 3]$ (in Theorem 7) and array code generated by $[0, 1, 2, 3, 4]$ [16], where $L = 10$.**

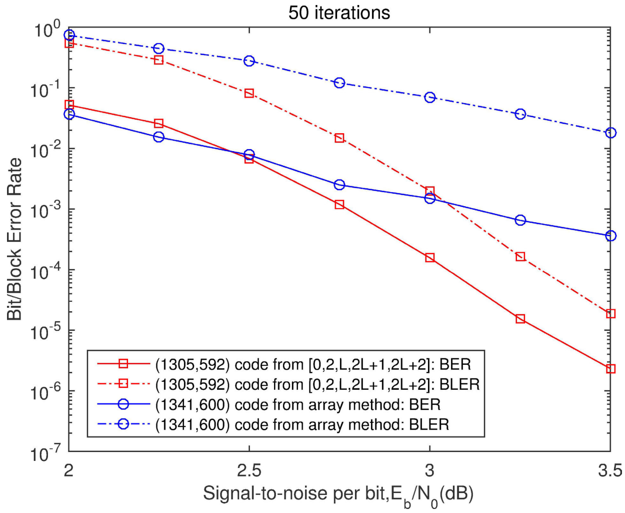

FIGURE 10. **Performance comparison of $(5, L)$-regular FLRM QC-LDPC codes: new code generated by $[0, 2, L, 2L + 1, 2L + 2]$ (in Theorem 8) and array code generated by $[0, 1, 2, 3, 4]$ [16], where $L = 9$.**

Example 4: Let $L = 10$. According to Theorem 7, a new $(5, L)$-regular FLRM QC-LDPC code is constructed with girth eight, which is generated from the tuple $[0, 1, L, L + 1, 2L + 3]$ with a new circulant size $P = (L + 2)^2 - 1 = 143$. By setting $L = 9$, a novel girth-eight $(5, L)$-regular FLRM QC-LDPC code is constructed via Theorem 8 from the tuple $[0, 2, L, 2L + 1, 2L + 2]$ with a new circulant size $P = 2L(L - 1) + 1 = 145$. Because there are no existing girth-eight FLRM codes which are explicitly constructed with comparable circulant sizes in the literature, two array-based FLRM QC-LDPC codes [16] with similar prime circulant sizes ($P = 149$ for both $L = 10$ and $L = 9$) are adopted as counterparts of the two new codes. The exponent matrices for the array-based codes are both $[0, 1, \cdots, 4]^T \cdot [0, 1, \cdots, L - 1]$. It should be noted that array-based codes only ensure girth six. It is observed in Fig. 9 and Fig. 10 that the new girth-eight FLRM codes significantly outperform the array-based counterparts.

Nevertheless, performance of the new $(5, L)$-regular codes is far from satisfactory, probably because the corresponding decoding thresholds for such row/column weights are relatively large. To improve performance, a binary 5×9 masking matrix (defined by Eq. (7) in [12]) is applied to the exponent matrices of the new code and array-based code with $L = 9$. As is well known [12], each zero within the masking matrix implies that a corresponding $P \times P$ CPM within the PCM of a QC-LDPC code is replaced by a $P \times P$ zero matrix. By comparing Fig. 10 and Fig. 11, it is observed that the two masked codes both noticeably outperform their respective unmasked versions, and that the masked new code

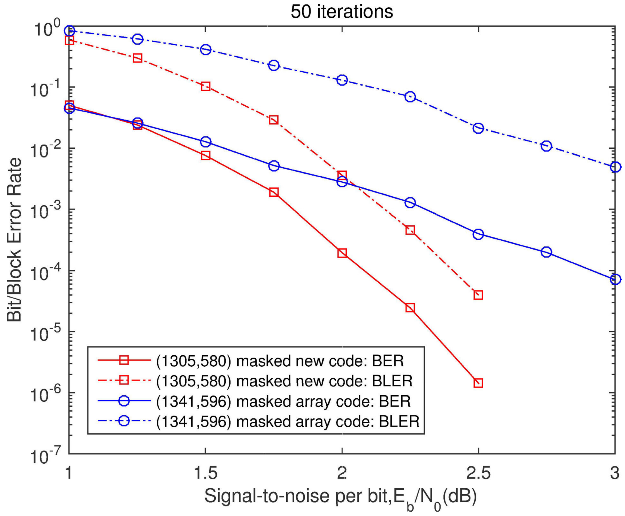

FIGURE 11. Performance comparison of the masked QC-LDPC codes corresponding to the new QC-LDPC code and array-based QC-LDPC code in Fig. 10, with the masking matrix defined by Eq. (7) in [12].

TABLE 3. Comparison of the minimum circulant size (P_{min}) for a randomly generated novel tuple and that [29] for the tuple with the smallest α_{J-1} [15], where $J = 5$.

L	new $\mathbf{S}_2$	new P_{min}	P_{min} [29]
5	$[0, 5, 6, 14, 16]$	39	49
6	$[0, 5, 6, 11, 19]$	59	63
7	$[0, 1, 7, 8, 18]$	59	67
8	$[0, 3, 8, 22, 26]$	93	111
9*	$[0, 1, 9, 10, 23]$	103	103
10*	$[0, 1, 10, 11, 23]$	143	143
11	$[0, 4, 11, 37, 43]$	143	165
12	$[0, 1, 12, 17, 31]$	173	221
13	$[0, 2, 13, 15, 38]$	195	199
14	$[0, 1, 14, 15, 31]$	255	285
15	$[0, 1, 15, 16, 58]$	323	368
16	$[0, 1, 16, 17, 35]$	323	407
17*	$[0, 1, 17, 18, 38]$	357	357
18	$[0, 1, 18, 25, 47]$	403	529
19	$[0, 1, 19, 20, 42]$	437	595
20	$[0, 1, 20, 21, 43]$	483	525

still performs significantly better than the masked array-based code. The desirable performance indicates that, the novel girth-eight FLRM QC-LDPC codes with large column weights can be well combined with masking matrices to produce good QC-LDPC codes.

VII. A BYPRODUCT: COMPARISON OF MINIMUM CIRCULANT SIZES FOR TUPLES FOUND BY TWO DIFFERENT SCHEMES

As a byproduct of this paper, a set of tuples for $J = 5$ which satisfy the GCD constraint have been randomly generated. Different from those tuples found in [15] which possess the smallest α_{J-1}, the new tuples are allowed to take much larger α_{J-1}. In our setting, α_{J-1} is limited to be at most $4L$. For each L in the range $5 \leq L \leq 20$, the tuple randomly found (not necessarily conducting exhaustive search) and the associated minimum circulant size are listed in Table 3. It is noticed that for most cases the new minimum circulant size is remarkably smaller than the one computed in [29] based on the tuple found in [15]. For the three cases where $L \in \{9, 10, 17\}$, the minimum circulant size found here is exactly equal to that in [29].

For small or moderate values of L, via optimizing search space (such as Algorithm 1 in [15]), it is possible to conduct exhaustive search in a reasonably short time, so as to find tuples with the smallest circulant sizes (among all tuples subject to $\alpha_{J-1} \leq 4L$). However, the design of an efficient method based on exhaustive search is outside the scope of the paper.

VIII. CONCLUSION

New properties, constructions and conjectures are put forward for FLRM QC-LDPC codes with girth eight. The contributions of this paper can be summarized as four aspects.

(i) It has been proved that, for girth-eight FLRM codes, the two existing tuples, $[0, 1, L]$ and $[0, 1, L, L+1]$, cannot offer circulant sizes smaller than their LB_{ccs} bounds.

(ii) For girth-eight $(3, L)$-regular FLRM codes, three new tuples ($[0, 2, L]$, $[0, 1, 3L/2]$ and $[0, 1, (3L + 1)/2]$) have been proposed, which can provide some circulant sizes smaller than their LB_{ccs} bounds for certain types of L. The circulant sizes for the latter two tuples are asymptotically half of their corresponding LB_{ccs} bounds. With regard to girth-eight $(4, L)$-regular FLRM code, a novel tuple $[0, L/2, L + 1, 3L + 1]$ has been presented, which offers a circulant size about one third of its LB_{ccs} bound for a certain type of L. Besides, a new tuple has been put forward, which includes the existing tuple $[0, 1, L, L + 1]$ as a special case and provides the circulant size L^2 regardless of the LB_{ccs} bounds. As for girth-eight $(5, L)$-regular FLRM codes, it has been discovered that the two existing tuples, $[0, 1, L, L + 1, 2L + 3]$ and $[0, 2, L, 2L+1, 2L+2]$ can offer some circulant sizes smaller than their LB_{ccs} bounds for certain types of L. The circulant size for the former is asymptotically half of its corresponding LB_{ccs} bound.

(iii) A couple of conjectures (Conjectures 1 and 2 for two new tuples with $J = 3$, and Conjectures 3 and 4 for two existing tuples with $J = 5$) have been raised on the smallest circulant sizes guaranteeing girth-eight FLRM codes. Moreover, for $J = 5$, several conjectures (Conjectures 5 $\sim$ 7 for two novel tuples) have been proposed on certain circulant sizes asymptotically one third of the respective LB_{ccs} bounds.

(iv) The new constructions in this paper reveal an interesting fact: if a small circulant size is required, the last entry in a tuple does not have to choose the smallest possible value. By adopting the same idea, a simple random search has been employed to achieve the current smallest circulant sizes for girth-eight FLRM codes with $J = 5$.

In the near future, the following work pertaining to girth-eight FLRM QC-LDPC codes deserves further research: (i) proving the conjectures raised in this paper or providing counterexamples; (ii) designing tuples which further decrease circulant sizes for J up to five, and tuples suitable for small circulant sizes for J larger than five; and (iii) exploring how to eliminate small trapping sets [30] or absorbing sets [31] for the novel girth-eight FLRM QC-LDPC codes.

APPENDIX A

Proof of Theorem 7.

Proof: Firstly, consider 4-cycles. There are ten cases for 4-cycles. The 4-cycles which occur in any two rows of the first four rows are impossible due to GCD constraint. Therefore, only the rest four cases where the last row is involved need to be considered. Let i and j be two column indexes such that $0 \leq i < j \leq L-1$.

(i) (0,4)-4-cycles can be denoted by $[0-(2L+3)i]+[(2L+3)j-0] = 0 \ (mod\ P)$, which reduces to

$$(2L+3)(j-i) = n[(L+2)^2-1] \tag{29}$$

for a certain integer n. As $0 < LHS < (2L+3)(L-1) < 2[(L+2)^2-1]$, Eq. (29) is possible only for $n=1$. When $n=1$, Eq. (29) reduces to $2(L+2)(j-i)-(L+2)^2 = i-j-1$. As a result, $(L+2)|(i-j-1)$, which is impossible.

(ii) (1,4)-4-cycles can be represented by $[i-(2L+3)i]+[(2L+3)j-j] = 0 \ (mod\ P)$, which is equivalent to

$$(2L+2)(j-i) = n[(L+2)^2-1] = n(L+3)(L+1) \tag{30}$$

for a certain integer n. Eq. (30) reduces to $2(j-i) = n(L+3)$. As L is even, $gcd(2, L+3) = 1$. Therefore, it follows that $(L+3)|(j-i)$, which is impossible.

(iii) (2,4)-4-cycles can be described as $[Li-(2L+3)i]+[(2L+3)j-Lj] = 0 \ (mod\ P)$, which turns into

$$(L+3)(j-i) = n(L+3)(L+1) \tag{31}$$

for a certain integer n. Therefore, $(L+1)|(j-i)$, which is impossible.

(iv) (3,4)-4-cycles can be denoted by $[(L+1)i-(2L+3)i]+[(2L+3)j-(L+1)j] = 0 \ (mod\ P)$, which is equivalent to

$$(L+1)(j-i)+(j-i) = n(L+3)(L+1) \tag{32}$$

for a certain integer n. As a result, $(L+1)|(j-i)$, which is impossible.

Next, consider 6-cycles. There are ten cases for 6-cycles. The 6-cycles which occur within any three rows of the first four rows are impossible due to GCD constraint. Therefore, only the rest six cases where the last row is involved need to be considered. Let i, j and k be three different column indexes such that $0 \leq i, j, k \leq L-1$.

(i) (0,1,4)-6-cycles can be described by $(0-j)+[i-(2L+3)i]+[(2L+3)k-0] = 0 \ (mod\ P)$, which is equivalent to

$$(i-j)+(2L+3)(k-i) = n[(L+2)^2-1] \tag{33}$$

for a certain integer n. Eq. (33) reduces to $(k-j)+2(L+1)(k-i) = n(L+3)(L+1)$. Therefore, $(L+1)|(k-j)$, which is impossible.

(ii) (0,2,4)-6-cycles can be denoted by $(0-Lj)+[Li-(2L+3)i]+[(2L+3)k-0] = 0 \ (mod\ P)$, which is equivalent to

$$L(i-j)+(2L+3)(k-i) = n[(L+2)^2-1] \tag{34}$$

for a certain integer n. By arranging terms, Eq. (34) becomes $L(k-j)+(L+3)(k-i) = n(L+3)(L+1)$. As $gcd(L, 3) = 1$, it is clear that $gcd(L, L+3) = 1$ and hence $(L+3)|(k-j)$, which is impossible.

(iii) (0,3,4)-6-cycles can be expressed as $[0-(L+1)j]+[(L+1)i-(2L+3)i]+[(2L+3)k-0] = 0 \ (mod\ P)$, which is equivalent to

$$(L+1)(i-j)+(2L+3)(k-i) = n[(L+2)^2-1] \tag{35}$$

for a certain integer n. Eq. (35) can be rewritten as $(L+1)(i-j)+2(L+1)(k-i)+(k-i) = n(L+3)(L+1)$. Therefore, $(L+1)|(k-i)$, which is impossible.

(iv) (1,2,4)-6-cycles can be described by $(j-Lj)+[Li-(2L+3)i]+[(2L+3)k-k] = 0 \ (mod\ P)$, which reduces to

$$(L+3)(k-i)+(L-1)(k-j) = n(L+3)(L+1) \tag{36}$$

for a certain integer n. As L is even, $gcd(L-1, L+3) = gcd(L-1, 4) = 1$. Therefore, it follows that $(L+3)|(k-j)$, which is impossible.

(v) (1,3,4)-6-cycles can be represented by $[j-(L+1)j]+[(L+1)i-(2L+3)i]+[(2L+3)k-k] = 0 \ (mod\ P)$, which is equivalent to

$$(L+1)(i-j)+2(L+1)(k-i)+(j-i) = n(L+3)(L+1) \tag{37}$$

for a certain integer n. Therefore, $(L+1)|(j-i)$, which is impossible.

(vi) (2,3,4)-6-cycles are associated with the tuple $(L, L+1, 2L+3)$. Therefore, such cycles cannot occur for a circulant size larger than $[(2L+3)-L](L-1) = (L+3)(L-1)$, due to Lemma 1. □

APPENDIX B

Proof of Theorem 8.

Proof: Firstly, consider 4-cycles. The 4-cycles which occur within any two rows of the first three rows are impossible due to GCD constraint. Therefore, only the rest seven cases related to the last two rows need to be considered. Let i and j be two column indexes such that $0 \leq i < j \leq L-1$.

(i) (0,3)-4-cycles can be denoted by $[0-(2L+1)i]+[(2L+1)j-0] = 0 \ (mod\ P)$, which is equivalent to

$$(2L+1)(j-i) = n[2L(L-1)+1] \tag{38}$$

for a certain integer n. Since $0 < (2L+1)(j-i) \leq (2L+1)(L-1) < 2[2L(L-1)+1]$, Eq. (38) is possible only for $n=1$. In this case, $(2L+1)(j-i) = 2L(L-1)+1$, which is $2L(j-i)+(j-i-1) = 2L(L-1)$, indicating that $2L|(j-i-1)$. This is possible only for $j-i=1$; however, this means $2L = 2L(L-1)$, which is impossible.

(ii) (1,3)-4-cycles can be represented by $[2i-(2L+1)i]+[(2L+1)j-2j] = 0 \ (mod\ P)$, which reduces to

$$(2L-1)(j-i) = n[2L(L-1)+1] \tag{39}$$

for a certain integer n. As $0 < (2L-1)(j-i) \leq (2L-1)(L-1) < 2L(L-1)+1$. Eq. (39) is impossible.

(iii) (2,3)-4-cycles can be expressed by $[Li-(2L+1)i]+[(2L+1)j-Lj]=0\ (mod\ P)$, which is equivalent to

$$(L+1)(j-i)=n[2L(L-1)+1] \tag{40}$$

for a certain integer n. Because $0<(L+1)(j-i)\leq(L+1)(L-1)<2L(L-1)+1$. Eq. (40) is impossible.

(iv) (0,4)-4-cycles can be denoted by $[0-(2L+2)i]+[(2L+2)j-0]=0\ (mod\ P)$, which reduces to

$$(2L+2)(j-i)=n[2L(L-1)+1] \tag{41}$$

for a certain integer n. Because $0<(2L+2)(j-i)\leq(2L+2)(L-1)<2[2L(L-1)+1]$, Eq. (41) is possible only for $n=1$. In this case, $(2L+2)(j-i)=2L(L-1)+1$, which can be rewritten as $2L(j-i)+2(j-i)-1=2L(L-1)$. As a result, $2L|2(j-i)-1$, which is impossible because $0<2(j-i)-1<2L$.

(v) (1,4)-4-cycles can be represented by $[2i-(2L+2)i]+[(2L+2)j-2j]=0\ (mod\ P)$, which is equivalent to

$$(2L)(j-i)=n[2L(L-1)+1] \tag{42}$$

for a certain integer n. As $0<(2L)(j-i)\leq(2L)(L-1)<2L(L-1)+1$, Eq. (42) is impossible.

(vi) (2,4)-4-cycles can be denoted by $[Li-(2L+2)i]+[(2L+2)j-Lj]=0\ (mod\ P)$, which reduces to

$$(L+2)(j-i)=n[2L(L-1)+1] \tag{43}$$

for a certain integer n. Since $0<(L+2)(j-i)\leq(L+2)(L-1)<2L(L-1)+1$, Eq. (43) is impossible.

(vii) (3,4)-4-cycles can be described by $[(2L+1)i-(2L+2)i]+[(2L+2)j-(2L+1)j]=0\ (mod\ P)$, which is equivalent to

$$j-i=n[2L(L-1)+1] \tag{44}$$

for a certain integer n. As $0<j-i\leq L-1<2L(L-1)+1$, Eq. (44) is impossible.

Next, consider 6-cycles. There are a total of ten types of 6-cycles. Let i,j and k be three different column indexes such that $0\leq i,j,k\leq L-1$.

(i) (0,1,2)-6-cycles correspond to the tuple $[0,2,L]$. Therefore, according to Lemma 1, such cycles cannot exist for a circulant size larger than $L(L-1)$.

(ii) (0,1,3)-6-cycles can be described by $(0-2j)+[2i-(2L+1)i]+[(2L+1)k-0]=0\ (mod\ P)$, which is equivalent to

$$2(i-j)+(2L+1)(k-i)=n[2L(L-1)+1] \tag{45}$$

for a certain integer n. Because $|LHS|\leq(2L+1)(L-1)-2<2[2L(L-1)+1]$, it is clear that $n\in\{0,1,-1\}$. (a) If $n=0$, Eq. (45) becomes $2(i-j)+(2L+1)(k-i)=0$. Therefore, $2L+1|(i-j)$, which is impossible. (b) If $n=1$, Eq. (45) reduces to $2(i-j)+(2L+1)(k-i)=2L(L-1)+1$, which is $2L(k-i)+k+i-2j-1=2L(L-1)$. Thus, $2L|(k+i-2j-1)$. As $|(k+i-2j-1)|<2L$, it is possible only for $(k+i-2j-1)=0$. In this case, $2L(k-i)=2L(L-1)$, which implies $k-i=L-1$. Therefore, it follows that $j-i=L/2-1$, which is impossible because L is odd. (c) If $n=-1$, Eq. (45) reduces to $2(i-j)+(2L+1)(k-i)=-[2L(L-1)+1]$, which is equal to $2L(k-i)+k+i-2j+1=-2L(L-1)$. Thus, $2L|(k+i-2j+1)$. Since $|(k+i-2j+1)|<2L$, it is possible only for $(k+i-2j+1)=0$. In this case, $2L(k-i)=-2L(L-1)$, indicating $i-k=L-1$. As a result, $i-j=L/2-1$, which is impossible due to an odd L.

(iii) (0,1,4)-6-cycles can be described by $(0-2j)+[2i-(2L+2)i]+[(2L+2)k-0]=0\ (mod\ P)$, which is equivalent to

$$2(i-j)+(2L+2)(k-i)=n[2L(L-1)+1] \tag{46}$$

for a certain integer n. By arranging terms, Eq. (46) becomes $2(k-j)+(2L)(k-i)=n[2L(L-1)+1]$. Since $|LHS|\leq 2L(L-1)+2(L-2)<2[2L(L-1)+1]$, it follows that $n\in\{0,1,-1\}$. (a) If $n=0$, Eq. (46) reduces to $2(k-j)+(2L)(k-i)=0$. Therefore, $L|k-j$, which is impossible. (b) If $n=1$, Eq. (46) becomes $[2(k-j)-1]+(2L)(k-i)=2L(L-1)$. As a result, $2L|[2(k-j)-1]$, which is impossible as $2(k-j)-1$ is odd. (c) If $n=-1$, Eq. (46) turns into $[2(k-j)+1]+(2L)(k-i)=-2L(L-1)$. Therefore, $2L|[2(k-j)+1]$, which is impossible because $2(k-j)+1$ is odd.

(iv) (0,2,3)-6-cycles can be described by $(0-Lj)+[Li-(2L+1)i]+[(2L+1)k-0]=0\ (mod\ P)$, which is equivalent to

$$L(i-j)+(2L+1)(k-i)=n[2L(L-1)+1] \tag{47}$$

for a certain integer n. Since $|LHS|\leq(2L+1)(L-1)+L(0-1)<2L(L-1)+1$, it is clear that $n=0$. In this case, Eq. (47) becomes $L(i-j)+(2L+1)(k-i)=0$, which is $L(i-j)+(2L)(k-i)+(k-i)=0$. Thus, $L|(k-i)$, which is impossible.

(v) (0,2,4)-6-cycles can be described by $(0-Lj)+[Li-(2L+2)i]+[(2L+2)k-0]=0\ (mod\ P)$, equivalent to

$$L(i-j)+(2L+2)(k-i)=n[2L(L-1)+1] \tag{48}$$

for a certain integer n. Because $|LHS|\leq(2L+2)(L-1)+L(0-1)=2L^2-L-2<2[2L(L-1)+1]$, it follows that $n\in\{0,1,-1\}$.

(a) If $n=0$, Eq. (48) reduces to $L(i-j)+(2L+2)(k-i)=0$. Since $gcd(2L+2,L)=gcd(2,L)=1$, it is obvious that $L|(k-i)$, which is impossible.

(b) If $n=1$, Eq. (48) becomes $L(i-j)+(2L+2)(k-i)=2L(L-1)+1$, which can be rewritten as $L(i-j)+(2L)(k-i)+2(k-i)-1=2L(L-1)$, showing $L|[2(k-i)-1]$. Because $0<|2(k-i)-1|<2L$, it is clear that $2(k-i)-1\in\{L,-L\}$. If $2(k-i)-1=L$, then $(k-i)=(L+1)/2$ and hence $i-j=L-4$. Therefore, when $L\geq 7$, it follows that $k-j=(L+1)/2+L-4\geq L$, which is impossible. If $2(k-i)-1=-L$, then $(k-i)=(1-L)/2$ and hence $(i-j)=3L-2$, which is impossible.

(c) If $n=-1$, Eq. (48) turns into $L(i-j)+(2L+2)(k-i)=-[2L(L-1)+1]$, which is $L(i-j)+(2L)(k-i)+2(k-i)+1=-2L(L-1)$, showing $L|2(k-i)+1$. Because $0<|2(k-i)+1|<2L$, it is clear that $2(k-i)+1\in\{L,-L\}$.

If $2(k-i)+1=L$, then $(k-i)=(L-1)/2$ and hence $(i-j)=-(3L-2)$, which is impossible. If $2(k-i)+1=-L$, then $(k-i)=-(L+1)/2$ and hence $(i-j)=-(L-4)$. Therefore, it follows that $k-j=-[(L+1)/2+L-4]$. When $L\geq 7$, it is obvious that $k-j\leq -L$, which is impossible.

(vi) (0,3,4)-6-cycles can be described by $[0-(2L+1)j]+[(2L+1)i-(2L+2)i]+[(2L+2)k-0]=0\,(mod\ P)$, which is equivalent to

$$(2L+1)(i-j)+(2L+2)(k-i)=n[2L(L-1)+1] \tag{49}$$

for a certain integer n. By arranging terms, Eq. (49) becomes $(2L+1)(k-j)+(k-i)=n[2L(L-1)+1]$. As $|LHS|\leq(2L+1)(L-1)+(L-2)<2[2L(L-1)+1]$, it is clear that $n\in\{0,1,-1\}$.

(a) If $n=0$, Eq. (49) reduces to $(2L+1)(k-j)+(k-i)=0$ and hence $2L+1|k-i$, which is impossible.

(b) If $n=1$, Eq. (49) becomes $(2L+1)(k-j)+(k-i)=2L(L-1)+1$, which is equivalent to $2L(k-j)+(2k-i-j-1)=2L(L-1)$. Therefore, $2L|(2k-i-j-1)$. As $|2k-i-j-1|\leq 2L-2<2L$, it is obvious that $2k-i-j-1=0$ and hence $k-j=L-1$. It is possible only for $k=L-1$ and $j=0$; however, for this case it follows that $i=2L-3$, which is impossible.

(c) If $n=-1$, Eq. (49) turns into $(2L+1)(k-j)+(k-i)=-[2L(L-1)+1]$, which can be expressed as $2L(k-j)+(2k-i-j+1)=-2L(L-1)$. Therefore, $2L|(2k-i-j+1)$. As $|2k-i-j+1|\leq 2L-2$, it follows that $2k-i-j+1=0$ and hence $k-j=1-L$. It is possible only for $k=0$ and $j=L-1$; however, for this case, $i=2-L$, which is impossible.

(vii) (1,2,3)-6-cycles correspond to the tuple $[2,L,2L+1]$. Therefore, thanks to Lemma 1, such cycles are impossible for a circulant size larger than $(2L-1)(L-1)$.

(viii) (1,2,4)-6-cycles are associated with the tuple $[2,L,2L+2]$. As a result, these cycles cannot occur for a circulant size larger than $2L(L-1)$, owing to Lemma 1.

(ix) (1,3,4)-6-cycles correspond to the tuple $[2,2L+1,2L+2]$. Therefore, according to Lemma 1, such cycles are impossible for a circulant size larger than $2L(L-1)$.

(x) (2,3,4)-6-cycles are associated with the tuple $[L,2L+1,2L+2]$. Thus, these cycles cannot exist for a circulant size larger than $(L+2)(L-1)$, thanks to Lemma 1. □

REFERENCES

[1] L. Zhang and J. Wang, "Construction of QC-LDPC codes from Sidon sequence using permutation and segmentation," *IEEE Commun. Lett.*, vol. 26, no. 8, pp. 1710–1714, Aug. 2022.

[2] J. Wang, G. Zhang, and Q. Zhou, "Coset-based QC-LDPC codes without small cycles," *Electron. Lett.*, vol. 50, no. 22, pp. 1597–1598, 2014.

[3] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar, "Construction of regular and irregular LDPC codes: Geometry decomposition and masking," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 121–134, Jan. 2007.

[4] 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.

[5] B. Vasic, K. Pedagani, and M. Ivkovic, "High-rate girth-eight low-density parity-check codes on rectangular integer lattices," *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1248–1252, Aug. 2004.

[6] G. 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.

[7] G. Zhang, Y. Hu, D. Ren, Y. Liu, and Y. Yang, "Type-II QC-LDPC codes from multiplicative subgroup of prime field," *IEEE Access*, vol. 8, pp. 142459–142467, 2020.

[8] J. Wang, S. Yuan, Y. Zhou, and G. Zhang, "Codec implementation of QC-LDPC code in CCSDS near-Earth standard," in *Proc. 5th Int. Conf. Comput. Commun. Syst. (ICCCS)*, May 2020, pp. 575–579.

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

[10] F. Abedi and M. Gholami, "On the construction of multitype quasi-cyclic low-density parity-check codes with different girth and length," *IEEE Access*, vol. 9, pp. 59725–59740, 2021.

[11] G. Zhang, R. Sun, and X. Wang, "Several explicit constructions for (3, L) QC-LDPC codes with girth at least eight," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1822–1825, Sep. 2013.

[12] J. Zhang and G. Zhang, "Deterministic girth-eight QC-LDPC codes with large column weight," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 656–659, Apr. 2014.

[13] M. Zhou, H. Zhu, H. Xu, B. Zhang, and K. Xie, "A note on the girth of (3,19)-regular Tanner's quasi-cyclic LDPC codes," *IEEE Access*, vol. 9, pp. 28582–28590, 2021.

[14] Y. Liu, X. Wang, R. Chen, and Y. He, "Generalized combining method for design of quasi-cyclic LDPC codes," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 392–394, May 2008.

[15] G. Zhang, Y. Hu, Y. Fang, and D. Ren, "Relation between GCD constraint and full-length row-multiplier QC-LDPC codes with girth eight," *IEEE Commun. Lett.*, vol. 25, no. 9, pp. 2820–2823, Sep. 2021.

[16] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc. 2nd Int. Symp. Turbo Codes Rel. Topics*, Sep. 2000, pp. 553–556.

[17] G. Zhang, "Construction of girth-eight QC-LDPC codes from greatest common divisor," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 369–372, Feb. 2013.

[18] G. Zhang, Y. Fang, and Y. Liu, "Automatic verification of GCD constraint for construction of girth-eight QC-LDPC codes," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1453–1456, Sep. 2019.

[19] K. Liu, Z. Fei, and J. Kuang, "Novel algebraic constructions of nonbinary structured LDPC codes over finite fields," in *Proc. IEEE 68th Veh. Technol. Conf.*, Sep. 2008, pp. 1–5.

[20] K. Liu, Z. Fei, and J. Kuang, "Three algebraic methods for constructing nonbinary LDPC codes based on finite fields," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2008, pp. 1–5.

[21] G. He, X. Li, Q. Li, Z. Zhou, and D. Zheng, "Regular quasi-cyclic low density parity check codes with girth 8 from elementary number theory," *China Commun.*, vol. 9, no. 4, pp. 80–88, Apr. 2012.

[22] J. Zhang, C. Li, and J. Bao, "A construction method of QC-LDPC codes without short cycles," in *Proc. 4th Int. Conf. Multimedia Inf. Netw. Secur.*, Nov. 2012, pp. 138–141.

[23] G. Zhang, Z. Liu, and M. Wang, "Simplification and extension of a class of girth-eight QC-LDPC codes," *Space Electron. Technol.*, vol. 12, no. 4, pp. 30–34, 2015.

[24] M. Majdzade and M. Gholami, "A class of column-weight-3 quasi-cyclic low-density parity-check codes from greatest common divisor," in *Proc. 6th Int. Conf. Combinatorics, Cryptograph, Comput. Sci. Compputing*, Nov. 2021, pp. 546–548.

[25] M. Majdzade and M. Gholami, "On the class of high-rate QC-LDPC codes with girth 8 from sequences satisfied in GCD condition," *IEEE Commun. Lett.*, vol. 24, no. 7, pp. 1391–1394, Jul. 2020.

[26] M. Majdzade, M. Gholami, and G. Raeisi, "(7, K) girth-8 QC-LDPC codes with an explicit construction," *J. Algebr. Syst.*, vol. 9, no. 2, pp. 229–239, 2022.

[27] R. Wang, Y. Li, H. Zhao, L. Qin, and H. Zhang, "Construction of girth-eight quasi-cyclic low-density parity-check codes with low encoding complexity," *IET Commun.*, vol. 10, no. 2, pp. 148–153, 2016.

[28] M. Gholami and M. Alinia, "Explicit APM-LDPC codes with girths 6, 8, and 10," *IEEE Signal Process. Lett.*, vol. 24, no. 6, pp. 741–745, Jun. 2017.

[29] K. Zhu and H. Yang, "Constructing girth eight GC-LDPC codes based on the GCD FLRM matrix with a new lower bound," *Sensors*, vol. 22, p. 7335, pp. 1–15, 2022.

[30] 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.

[31] 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.

JUHUA WANG received the B.Sc. degree in applied electronics from Yantai Normal University, China, in 1998, and the M.Sc. degree in communication and information systems from the China Academy of Space Technology (Xi'an), Xi'an, China, in 2001. Since 2001, she has been with the China Academy of Space Technology (Xi'an), where she is currently a Senior Engineer. Her research interests include error correcting codes (particularly, construction and codec hardware implementation for LDPC codes) and image compression.

JIANHUA ZHANG is currently a Research Fellow with the China Academy of Space Technology (Xi'an), Xi'an, China, where he is also the Director of the Institute of Space Data Transmission and Processing. His current research interests include satellite communications, laser communications, software-defined radio systems, and space networking.

QUAN ZHOU received the bachelor's degree in communication engineering from the Institute of Northwest Telecommunications Engineering (now named Xidian University), China, in 1986, and the master's and Ph.D. degrees in communication and information systems from Xidian University, in 1989 and 1992, respectively. Since 1992, he has been with the China Academy of Space Technology (Xi'an), Xi'an, China, where he was an Engineer, from 1992 to 1994, and a Senior Engineer (Associate Professor), from 1994 to 1998, and has been a Research Fellow (Full Professor) and a Ph.D. Supervisor, since 1998. His research interests include data transmission, channel coding, satellite communication, and image processing.

LINTAO ZHANG is currently pursuing the degree with the Department of Electrical Engineering, Tsinghua University, Beijing, China. Her research interests include electrical automation and applied electronic technology, and channel coding (particularly, construction and simulation of LDPC codes).