

Short Regular Girth-8 QC-LDPC Codes From Exponent Matrices with Vertical Symmetry

Guohua Zhang*, Aijing Sun*, Ling Liu[†], and Yi Fang[‡]

*School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an, China, zhangghcast@163.com, sunaijing@xupt.edu.cn

[†]Guangzhou Institute of Technology, Xidian University, Guangzhou, China, liuling@xidian.edu.cn

[‡]School of Information Engineering, Guangdong University of Technology, Guangzhou, China, fangyi@gdut.edu.cn

Abstract

To address the challenge of constructing short girth-8 quasi-cyclic (QC) low-density parity-check (LDPC) codes, a novel construction framework based on vertical symmetry (VS) is proposed. Basic properties of the VS structure are presented. With the aid of these properties, existing explicit constructions for column weights from three to five which can be transformed into the VS structure are sorted out. Then two novel explicit constructions with the VS structure which guarantee short codes are presented for column weights of three and six. Moreover, an efficient search-based method is also proposed to find short codes with the VS structure. Compared with the state-of-the-art benchmarks, both the explicit constructions and the search-based method presented in this paper can provide shorter codes for most cases. Simulation results show that the new shorter codes can perform almost the same as or better than the longer existing counterparts. Thus, the new shorter codes can fit better with the low-latency requirement for modern communication systems.

I. INTRODUCTION

High-performance short codes have important applications in a variety of modern communication systems, including the future 6G system. A low-density parity-check (LDPC) code [1]–[3] with larger girth (being an even number at least four) typically provides a larger minimum distance and thus is likely to exhibit better performance [4]–[9]. A quasi-cyclic (QC) LDPC code is defined as the null space of a sparse parity-check matrix composed of circulants, and thus can be compactly described by its associated exponent matrix and the circulant size [2], [10], [11]. For the girth of 6, the problem of constructing short QC-LDPC codes has been partially solved by a couple of existing methods. By contrast, how to construct short girth-8 QC-LDPC codes has been a long-standing challenge for channel coding community [2]. In recent years, both explicit constructions (i.e. without using search) [12]–[14] and search-based methods [4], [15]–[17] for girth-8 codes with short lengths (or equivalently, small circulant sizes) have attracted increasing attention. In general, the smallest circulant sizes in the literature as far as we know are given by earliest-sequence (ES) method [18] ($J = 3$) and max-function method [19] ($J = 4$) for explicit constructions, and by horizontal symmetry (HS) [15] and integer-ring-sieve (IRS) methods [16] for search-based ones.

In this paper, we first present a new structure regarding exponent matrices, which is called vertical symmetry (VS) structure. An exponent matrix with the VS structure can be defined by $\mathbf{E}_{vs} = [\mathbf{E}_U^T, \mathbf{E}_D^T]^T$ if J is even, and $[\mathbf{0}^T, \mathbf{E}_U^T, \mathbf{E}_D^T]^T$ otherwise, where $\mathbf{E}_D = -\mathbf{E}_U$. Based on the VS structure, we then propose several new explicit and search-based methods, which are able to offer the current smallest circulant size for most cases of row weights. Moreover, simulations show that the proposed shorter codes perform as well as or even better than the existing benchmarks for longer lengths. Therefore, the novel short codes have potential to match better with low-latency requirement for modern communication systems.

II. EXPLICIT CONSTRUCTIONS FOR ODD COLUMN WEIGHTS

This section presents a basic property for VS exponent matrices with odd column weights, and then provides some explicit constructions for $J = 3$ and $J = 5$.

In this paper, only weight-1 circulant (i.e. cyclic permutation matrix, CPM) is considered. A $P \times P$ circulant associated with the respective element e within the $J \times L$ exponent matrix, is defined as a $P \times P$ identity matrix with all its rows being cyclically shifted to the right by $\text{mod}(e, P)$ positions. Consequently, the parity-check matrix of a (J, L) -regular QC-LDPC code is a $J \times L$ array of $P \times P$ circulants.

Lemma 1: Let $J \geq 3$ be odd. Suppose that the exponent matrix $\mathbf{E} = [\alpha_0, \alpha_1, \dots, \alpha_{J-1}]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$ satisfies the constraint $\alpha_i + \alpha_{J-1-i} = 2\alpha_{\frac{J-1}{2}}$ for each i in the range $0 \leq i < \frac{J-1}{2}$. Then $\mathbf{E}$ is equivalent to a VS exponent matrix: $\mathbf{E}_{vs} = [0, \mathbf{a}, -\mathbf{a}]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$, where $\mathbf{a} = [\alpha_{\frac{J+1}{2}} - \alpha_{\frac{J-1}{2}}, \alpha_{\frac{J+1}{2}+1} - \alpha_{\frac{J-1}{2}+1}, \dots, \alpha_{J-1} - \alpha_{\frac{J-1}{2}}]$.

Proof: See Appendix. □

Lemma 1 plays an important role in the following two subsections.

A. VS exponent matrices for $J = 3$

In this subsection, a type of VS exponent matrices for $J = 3$ is proposed, which contains three specific cases (two derived from existing sequences and one from a new sequence).

Let $J = 3$ and set $[\alpha_0, \alpha_1, \alpha_2] = [0, 1, 2]$. According to Lemma 1, $[0, 1, 2]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$ has an equivalent VS exponent matrix $\mathbf{E}_{vs} = [0, 1, -1]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$.

Theorem 1: Let $\{\beta_0, \beta_1, \dots, \beta_{L-1}\}$ be a sequence composed of L distinct (modulo P) integers such that (1) $2\beta_i \neq 2\beta_j \pmod{P}$, where $0 \leq i < j \leq L-1$; and (2) $2\beta_k \neq \beta_i + \beta_j \pmod{P}$, where i, j and k are different integers from 0 to $L-1$. Then $[0, 1, -1]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$ is a VS exponent matrix, which yields a girth-8 QC-LDPC code for the circulant size P .

Proof: See Appendix. □

In what follows, we consider three sequences which satisfy the inequality in Theorem 1. The first two sequences are existing ones in the literature, and the third is novel.

Definition 1 [20] [21]: If $\{s_0, s_1, \dots, s_{L-1}\}$ is a sequence of integers such that all pair-wise sums $(s_i + s_j, 0 \leq i < j \leq L-1)$ are distinct modulo P , then it is called a Sidon sequence over $\mathbf{Z}_P$, the integer ring of modulo P .

Corollary 1: Let $\{\beta_0, \beta_1, \dots, \beta_{L-1}\}$ be a Sidon sequence over $\mathbf{Z}_P$. Then $[0, 1, -1]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$ is a VS exponent matrix for a girth-8 QC-LDPC code with the circulant size P .

Since a Sidon sequence with L elements can possibly exist only if $P \geq L(L-1) + 1$, VS exponent matrices provided by Corollary 1 generally lead to large circulant sizes. To obtain short girth-8 codes with the VS structure, other sequences need to be examined. The earliest sequence (ES) belongs to such sequences allowing for girth-8 codes with short circulant sizes.

Definition 2 (ES) [18]: If n is even, set $s_{el}(n) = 3 \cdot s_{el}(n/2)$; otherwise, set $s_{el}(n) = s_{el}(n-1) + 1$, where $s_{el}(0) = 0$.

Corollary 2: Let $\{\beta_0, \beta_1, \dots, \beta_{L-1}\}$ consist of the first L entries of the ES. Then $[0, 1, -1]^T[\beta_0, \beta_1, \dots, \beta_{L-1}]$ is a VS exponent matrix for a girth-8 QC-LDPC code with the circulant size $P = 2 \cdot s_{el}(L-1) + 1$.

Generally speaking, as far as explicit constructions for column weight of three are concerned, the ES has held the best record in providing the shortest circulant size (i.e. P in Corollary 2) since its invention in 2004. A thought-provoking question, therefore, is whether there exists a way to go beyond the unrivaled ES. In our search for exponent matrices by using a Two-Direction column-scanning greedy strategy, a magical sequence (called TD for short) is discovered. Through careful analysis, we realize that the TD is inextricably linked with the ES, and can be compactly defined via the latter.

Definition 3 (TD): Let $s_{td}(n) = (-1)^{n+1}[6 \cdot s_{el}(\lfloor \frac{n}{4} \rfloor) + \text{mod}(n, 4)]$ for each $n \geq 0$.

Let $\{\beta_0, \beta_1, \dots, \beta_{L-1}\}$ be a sequence consisting of the first L entries of a TD sequence, i.e., $\beta_i = s_{td}(i)$ for $0 \leq i \leq L-1$. Define the value of $P(L)$ by an iterative manner: $P(L) = 3 \cdot P(L/2)$ for an even $L \geq 4$ and $P(L) = 3 \cdot P(\frac{L+1}{2}) + \text{mod}(L, 4) - 5$ for an odd $L \geq 3$, where $P(2) = 3$.

Conjecture 1: Let $\{\beta_0, \beta_1, \dots, \beta_{L-1}\}$ be a sequence consisting of the first L entries of the TD. For the circulant size $P(L)$, the VS exponent matrix $[0, 1, -1]^T[\beta_0, \beta_1, \dots, \beta_{L-1}]$ generates a girth-8 QC-LDPC code.

The validity of Conjecture 1 has been verified for each L in the range of $3 \leq L \leq 500$. As shown in Fig. 1, for the vast majority of cases the TD offers a smaller circulant size than ES, and for the rest cases the former provides the same circulant size as ES.

Besides the single circulant size of $P(L)$, many circulant sizes larger than $2 \cdot s_{el}(L-1)$ also allow girth-8 codes.

Conjecture 2: The exponent matrix also leads to a $(3, L)$ -regular girth-8 QC-LDPC code for any *odd* circulant size $P \geq P_x$, where $P_x = 2 \cdot s_{el}(L-1) + 1$.

For each L in the range $3 \leq L \leq 100$, Conjecture 2 has been verified for each odd circulant size P in the range of $P_x \leq P < 2 \cdot P_x$. This indicates that for a general row weight, the new method not only provides the smallest circulant size to the best of our knowledge, in the sense of explicit constructions, but also allows for rather flexible circulant sizes.

B. VS exponent matrices for $J \geq 5$

Let $\beta_i = f_J(i)$ for $0 \leq i \leq L-1$, where the function $f_J(i)$ is defined by the base-expansion method in Section IV of [23]. Then $\mathbf{E} = [0, 1, \dots, J-1]^T[\beta_0, \beta_1, \dots, \beta_{L-1}]$ corresponds to a girth-8 (J, L) -regular QC-LDPC code for each circulant size larger than $f_J(L-1) \cdot (J-1)$, according to the proof of Construction 5 in [23]. Since $\alpha_i + \alpha_{J-1-i} = 2\alpha_{\frac{J-1}{2}} = J-1$ for each i in the range $0 \leq i < \frac{J-1}{2}$, the constraint in Lemma 1

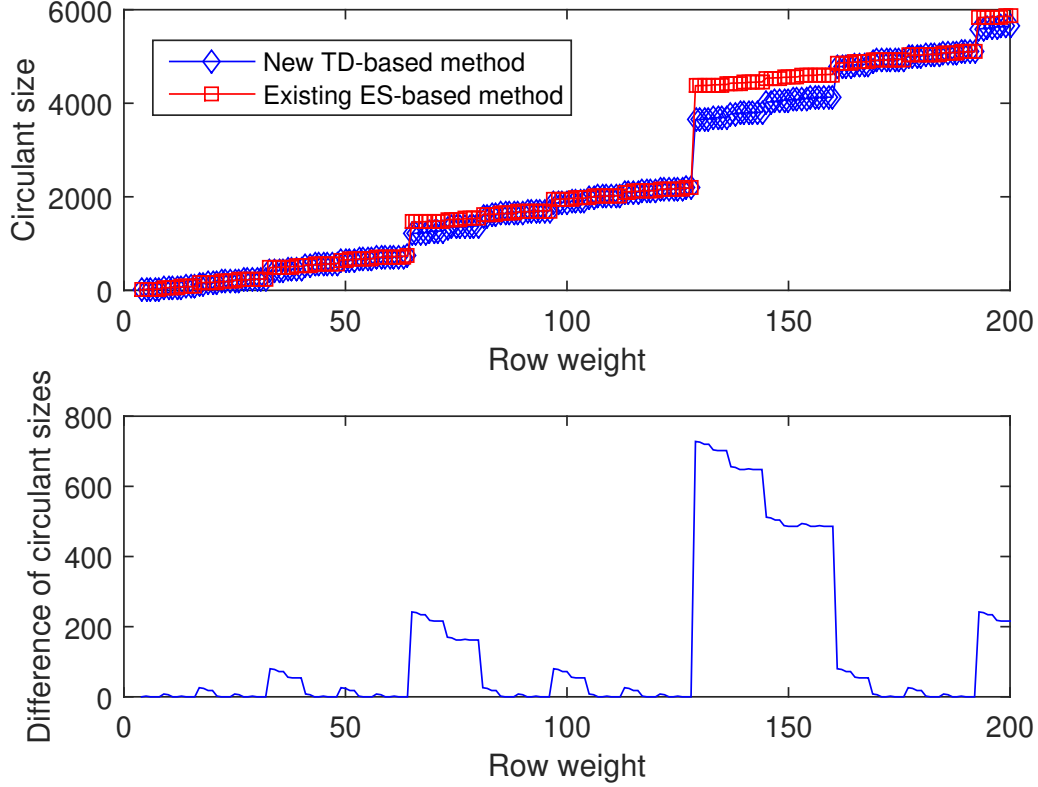


Fig. 1. Circulant size comparison of two explicit VS methods for $J = 3$: the proposed TD-based method and existing ES-based method.

holds. Therefore, according to Lemma 1, $\mathbf{E}$ has an equivalent VS form $\mathbf{E}_{vs} = [\mathbf{0}, \mathbf{a}, -\mathbf{a}]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$, where $\mathbf{a} = [1, 2, \dots, (J-1)/2]$.

Although VS exponent matrices with odd values of J can be generated without search via the base-expansion method [23] and Lemma 1, their circulant sizes are generally not small. As for an odd $J \geq 5$, we have not yet found an effective way to explicitly construct VS exponent matrices with the smallest possible circulant sizes, but this issue clearly deserves further investigation.

III. EXPLICIT CONSTRUCTIONS FOR EVEN COLUMN WEIGHTS

This section presents a basic property for VS matrices with even column weights, and then provides some explicit constructions for $J = 4$ and $J = 6$.

Lemma 2: Let $J \geq 4$ be even. If an exponent matrix $\mathbf{E} = [\alpha_0, \alpha_1, \dots, \alpha_{J-1}]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$ satisfies $\alpha_i + \alpha_{J-1-i} = 2x$ for each i ($0 \leq i \leq J/2 - 1$), where x is a constant, then $\mathbf{E}$ is equivalent to a VS exponent matrix $\mathbf{E}_{vs} = [\mathbf{a}, -\mathbf{a}]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$, where $\mathbf{a} = [\alpha_{J/2} - x, \dots, \alpha_{J-1} - x]$.

Proof: Lemma 2 can be similarly proved as Lemma 1. □

Lemma 2 has a crucial role in the following two subsections.

A. VS exponent matrices for $J = 4$

In this subsection, a type of VS exponent matrices for $J = 4$ is proposed, from which three specific cases are generated by combining Lemma 2 and certain existing constructions (based on greatest common divisor (GCD) [22]–[25], disjoint difference sets (DDS) [26] and max function [19]).

Let $e(i, r)$ be the entry in the i -th row and r -th column of a $J \times L$ matrix $\mathbf{E}$, where $0 \leq i \leq J - 1$ and $0 \leq r \leq L - 1$. Then $\mathbf{E}$ can be expressed as $\mathbf{E} = [e(i, r)]$ for brevity.

Lemma 3: Suppose that $\mathbf{E} = [e(i, r)]$ is a $4 \times L$ exponent matrix satisfying $e(0, r) = 0$ and $e(3, r) = e(1, r) + e(2, r)$ for each r ($0 \leq r \leq L - 1$). Then $\mathbf{E}$ can be equivalently transformed into a VS matrix $\mathbf{E}_{vs}$:

$$\begin{bmatrix} a(0) & a(1) & \cdots & a(L-1) \\ b(0) & b(1) & \cdots & b(L-1) \\ -a(0) & -a(1) & \cdots & -a(L-1) \\ -b(0) & -b(1) & \cdots & -b(L-1) \end{bmatrix} \quad (1)$$

for the following two cases: (i) $e(1, r) + e(2, r)$ being even for each r ($0 \leq r \leq L - 1$): in this case, set $a(r) = -[e(1, r) + e(2, r)]/2$ and $b(r) = [e(1, r) - e(2, r)]/2$. (ii) P being odd: in this case, if $e(1, r) + e(2, r)$ is even, set $a(r) = -[e(1, r) + e(2, r)]/2$ and $b(r) = [e(1, r) - e(2, r)]/2$; otherwise, set $a(r) = -[P + e(1, r) + e(2, r)]/2$ and $b(r) = [e(1, r) - e(2, r) - P]/2$.

Proof: See Appendix. □

The case 1 in Lemma 3 is illustrated by two examples. The first one is an explicit construction based on GCD, while the second is based on random search.

Example 1 (GCD): Let $J = 4$ and L be odd. Set $\mathbf{E} = [0, 1, L, L + 1]^T [0, 1, \dots, L - 1]$ [22]. Then its VS form is $\mathbf{E}_{vs} = [\mathbf{a}, -\mathbf{a}]^T [0, 1, \dots, L - 1]$, where $\mathbf{a} = [(L - 1)/2, (L + 1)/2]$. The VS matrix corresponds to a $(4, L)$ -regular girth-8 QC-LDPC code for any circulant size $P \geq L^2$.

Example 2: Set $P = 38$ and $L = 8$. Generate the exponent matrix $\mathbf{E}$ according to Lemma 3, where the middle two rows are $[e(1, 0), e(1, 1), \dots, e(1, L - 1)] = [7, 10, 20, 11, 29, 2, 35, 12]$ and $[e(2, 0), e(2, 1), \dots, e(2, L - 1)] = [1, 10, 22, 3, 15, 16, 19, 28]$, respectively. Then, thanks to Lemma 3 (case 1), it is easily seen that $\mathbf{E}$ is equivalent to the following VS exponent matrix:

$$\begin{bmatrix} 34 & 28 & 17 & 31 & 16 & 29 & 11 & 18 \\ 3 & 0 & 37 & 4 & 7 & 31 & 8 & 30 \\ -34 & -28 & -17 & -31 & -16 & -29 & -11 & -18 \\ -3 & 0 & -37 & -4 & -7 & -31 & -8 & -30 \end{bmatrix}, \quad (2)$$

which corresponds to a $(4, 8)$ -regular girth-8 code with the circulant size of 38. The length of this code is shorter than the shortest one [15] in the literature as far as we know.

To illustrate the case 2 in Lemma 3, we first use an example based on DDS [26], and then present an explicit construction which is a modification of the max-function method [19].

Example 3 (DDS): Set $P = 131$ and $L = 8$. Then the two sets, $\mathbf{d}_1 = [0, 31, 37, 55, 56, 83, 97, 99]$ and $\mathbf{d}_2 = [0, 12, 17, 21, 47, 50, 57, 70]$ form a $(P, L, 2)$ -DDS over $\mathbf{Z}_P$. Due to Lemma 3 (case 2), a VS exponent matrix can be obtained as follows:

$$\begin{bmatrix} 0 & 44 & 104 & 93 & 14 & 130 & 54 & 112 \\ 0 & 75 & 10 & 17 & 70 & 82 & 20 & 80 \\ 0 & -44 & -104 & -93 & -14 & -130 & -54 & -112 \\ 0 & -75 & -10 & -17 & -70 & -82 & -20 & -80 \end{bmatrix}, \quad (3)$$

which corresponds to a $(4, 8)$ -regular girth-8 code with the circulant size of 131.

Since a $(P, L, 2)$ -DDS over $\mathbf{Z}_P$ possibly exists only if $P \geq 2L(L-1)+1$ [26], the circulant size ($\geq 2L(L-1)+1$) in Example 3 is much larger than that ($\geq L^2$) in Example 1. Circulant sizes noticeably smaller than that in Example 1, are redolent of our earlier construction for $J = 4$ based on max function [19], which is considered as a scheme able to provide by far the smallest circulant sizes in an explicit manner [15]. The max-function method can be slightly modified to attain VS girth-8 codes for each odd circulant size larger than approximately $3L^2/4$, where L can be arbitrarily chosen.

Corollary 3 (max-function): Let $\mathbf{E} = [e(i, r)]$ be a $4 \times L$ exponent matrix. Set $e(0, r) = 0$, $e(1, r) = r$ and $e(3, r) = e(2, r) + e(1, r)$ for $0 \leq r \leq L-1$, where $e(2, 0) = 0$ and $e(2, r+1) = e(2, r) + \max(r+2, L-r)$ for $0 \leq r \leq L-2$. For each odd $P \geq \lceil 3 \cdot L^2/4 \rceil + L-1$, there exists a VS exponent matrix $\mathbf{E}_{vs}$ which corresponds to a $(4, L)$ -regular girth-8 QC-LDPC code for the circulant size P .

Proof: See Appendix. $\square$

In summary, the circulant sizes available from Example 1 (GCD, L odd) and Example 3 (DDS, P odd) are approximately linear with L^2 and $2L^2$, respectively, while that from Corollary 3 (max-function, P odd) is merely with $3L^2/4$. Clearly, explicit constructions suitable for even P noticeably smaller than L^2 , remain unsolved and deserve further research.

B. VS exponent matrices for $J = 6$

In this subsection, new VS exponent matrices with small circulant sizes are proposed for $J = 6$.

Theorem 2: The VS exponent matrix $\mathbf{E}_{vs} = [\mathbf{a}, -\mathbf{a}]^T[0, 1, \dots, L-1]$ corresponds to a $(6, L)$ -regular girth-8 QC-LDPC code for the circulant size P , where $\mathbf{a}$ and P can be separately determined for four cases: (i) if $\text{mod}(L, 6) \in \{0, 2\}$, set $\mathbf{a} = [2, L+1, L+3]$ and $P = (L+2)^2+3$; (ii) if $\text{mod}(L, 6) \in \{1, 3\}$, choose $\mathbf{a} = [2, L, L+2]$ and $P = (L+1)^2+3$; (iii) if $\text{mod}(L, 6) = 4$, set $\mathbf{a} = [2, L+3, L+5]$ and $P = (L+1)(L+5)$; (iv) if $\text{mod}(L, 6) = 5$, choose $\mathbf{a} = [2, L+2, L+4]$ and $P = L(L+4)$.

Proof: See Appendix. $\square$

From Fig. 2, it is clear that the circulant sizes offered by the new girth-8 codes in Theorem 3 are much shorter than existing benchmarks for almost all values of row weight.

IV. SEARCH-BASED METHOD

In Section II and III, VS exponent matrices are proposed via pure formulae without search procedure. In this section, we consider how to obtain VS exponent matrices with the aid of simple but efficient search procedure. To

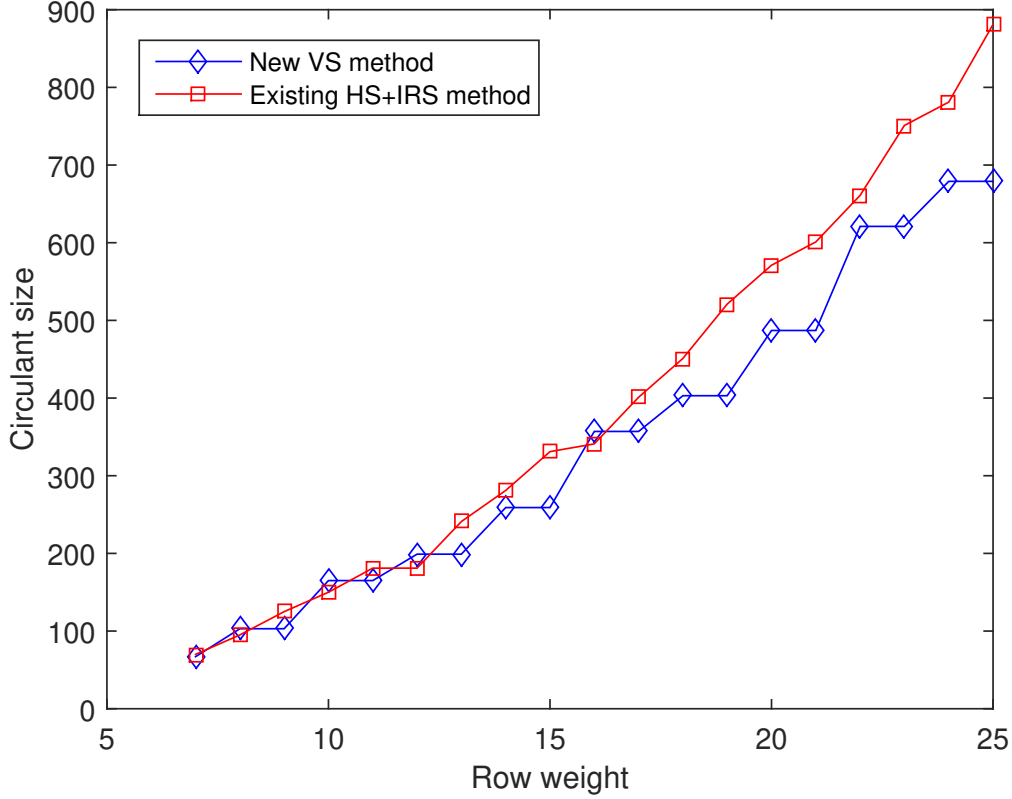


Fig. 2. Circulant size comparison for $J = 6$: the proposed explicit VS method and existing random (HS+IRS) method.

be specific, we only consider a type of VS exponent matrices, the upper part of which can be expressed as the product of two sequences: $\{\alpha_0, \alpha_1, \dots, \alpha_{\lfloor \frac{J-2}{2} \rfloor}\}$ and $\{\beta^0, \beta^1, \dots, \beta^{L-1}\}$. Set $J_0 = \lfloor \frac{J-2}{2} \rfloor$. Define $\mathbf{E}_U = [\alpha_i \cdot \beta^r]$ for $0 \leq i \leq J_0$ and $0 \leq r \leq L-1$.

A. Governing equations for 4-cycles

Let r and s be two indexes such that $0 \leq r < s \leq L-1$.

(1) If a 4-cycle exists in the upper (or lower) part of the exponent matrix, then such a cycle can be represented by $(\alpha_i - \alpha_j)(\beta^r - \beta^s) = 0 \pmod{P}$, where $0 \leq i < j \leq J_0$. (2) If a 4-cycle occurs cross the upper and lower parts of the exponent matrix, then this cycle can be denoted by $(\alpha_i + \alpha_j)(\beta^r - \beta^s) = 0 \pmod{P}$, where $0 \leq i \leq j \leq J_0$. (3) For a 4-cycle in the all-zero row and the upper (or lower) part, it can be expressed as $\alpha_i(\beta^r - \beta^s) = 0 \pmod{P}$, where $0 \leq i \leq J_0$.

B. Governing equations for 6-cycles

Let r, s and t be different indexes in the range $0 \leq r, s, t \leq L-1$. (1) If a 6-cycle exists in the upper (or lower) part of the exponent matrix, then such a cycle can be represented by $(\alpha_i - \alpha_j) \cdot \beta^s + (\alpha_j - \alpha_k) \cdot \beta^r + (\alpha_k - \alpha_i) \cdot \beta^t = 0 \pmod{P}$, where $0 \leq i < j < k \leq J_0$.

(2a) If a 6-cycle occurs in two rows in the upper part and one row in the lower part of the exponent matrix, then this cycle can be expressed by $(\alpha_i - \alpha_j) \cdot \beta^s + (\alpha_j + \alpha_k) \cdot \beta^r - (\alpha_k + \alpha_i) \cdot \beta^t = 0 \pmod{P}$ where $0 \leq i < j \leq J_0$ and $0 \leq k \leq J_0$. (2b) If a 6-cycle exists in one row in the upper part and two rows in the lower part of the exponent matrix, then this cycle can be denoted by $(\alpha_i + \alpha_j) \cdot \beta^s + (\alpha_k - \alpha_j) \cdot \beta^r - (\alpha_k + \alpha_i) \cdot \beta^t = 0 \pmod{P}$ where $0 \leq i \leq J_0$ and $0 \leq j < k \leq J_0$.

(3a) If a 6-cycle occurs in the all-zero row and the upper (or lower) part of the exponent matrix, then such a cycle can be represented by $\alpha_i(\beta^r - \beta^s) + \alpha_j(\beta^t - \beta^r) = 0 \pmod{P}$, where $0 \leq i < j \leq J_0$. (3b) If a 6-cycle exists in the all-zero row, the upper part, and the lower part of the exponent matrix, then this cycle can be expressed as $\alpha_i(\beta^r - \beta^s) - \alpha_j(\beta^t - \beta^r) = 0 \pmod{P}$, where $0 \leq i, j \leq J_0$.

C. Search algorithm

To reduce search space, α_0 is set to 1. Consequently, huge search space due to $L \lfloor J \rfloor / 2$ values is significantly reduced to very small space merely involving $\lfloor J \rfloor / 2$ values. For example, when $J = 4$ and $J = 5$, it suffices to search for only two values (α_1 and β) to generate a (J, L) -regular QC-LDPC code without cycles of four and six. For another example, when $J = 6$ and $J = 7$, only three values (α_1 , α_2 and β) are enough to define the new QC-LDPC codes. The results of this search method (by avoiding all 4-cycles and 6-cycles described in Subsection B) are listed in Tables II~IV. Compared with the state-of-the-art benchmarks (HS and IRS methods), the new search method can provide shorter codes for most values of L (especially for $J = 5$ and $J = 6$).

Moreover, the following example shows that by using a random search without the constraint of $\mathbf{E}_U = [\alpha_i \cdot \beta^r]$, the VS structure we proposed can provide the current smallest circulant sizes for $J = 4$ and small values of L .

Example 4: Let $J = 4$. Then the following two $\mathbf{E}_U$'s lead to a VS girth-8 $(4, 5)$ -regular code with $P = 21$ and a VS girth-8 $(4, 7)$ -regular code with $P = 29$, respectively.

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 8 \\ 0 & 8 & 3 & 7 & 10 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 & 4 & 9 & 25 & 26 \\ 0 & 2 & 12 & 9 & 11 & 19 & 14 \end{bmatrix}.$$

V. PERFORMANCE SIMULATIONS

In this section, three new VS codes are compared with existing benchmarks in terms of bit-error rate (BER) and block-error rate (BLER). Assume the BPSK modulation, AWGN channel and sum-product-algorithm (SPA) decoding. (1) for $J = 3$ and $L = 9$, the new TD-based VS code is compared with existing ES-based code; (2) for $J = 6$ and $L = 11$, the new code (generated by Theorem 2 (iv)) is compared with the two codes from IRS-search method [16] and HS-search method [15]; (3) for $J = 6$ and $L = 12$, the new search-based code is compared with the code from IRS-search method [16]. From Fig. 3~5, it is observed that the new shorter VS codes perform almost the same as or better than the longer counterparts. Also shown in Fig. 5 is the noticeably improved performance of a masked $(3, 6)$ -regular code, which is generated by combining the new VS code with a masking matrix (from $\mathbf{g}_1 = [1, 0, 0, 0, 1, 1]$ and $\mathbf{g}_2 = [0, 1, 0, 0, 1, 1]$ via the manner described in Example 2 (code 1) of [24]).

TABLE I
CIRCULANT SIZE COMPARISON FOR $J = 4$: NEW SEARCH METHOD AND THE STATE-OF-THE-ART SEARCH METHOD [15] (NA: NOT AVAILABLE).

L	P_{new}	$[\alpha_1, \beta]$	P_{HS} [15]
5	29	[12,5]	23
6	37	[3,11]	24
7	43	[12,4]	30
8	53	[23,3]	39
9	61	[24,3]	48
10	61	[24,3]	57
11	89	[4,2]	67
12	91	[31,19]	80
13	131	[17,39]	98
14	137	[37,16]	112
15	137	[37,16]	130
16	137	[37,16]	150
17	137	[37,16]	170
18	181	[72,101]	190
19	199	[74,124]	205
20	199	[74,124]	220
21	199	[74,124]	NA
22	277	[4,16]	NA
23	277	[4,16]	NA
24	313	[25,19]	NA
25	313	[25,19]	350

VI. CONCLUSION

A new structure called vertical symmetry (VS) for exponent matrices of QC-LDPC codes is proposed to construct short codes without cycles of length four and six. Properties, explicit constructions and search-based methods regarding the novel structure are investigated. While the VS-based QC-LDPC codes have shorter lengths for most row weights, their performances are identical to or even superior to the existing benchmarks for longer lengths.

ACKNOWLEDGMENT

This work was supported in part by the NSF of China under Grant 62322106, and the Guangdong Basic and Applied Basic Research Foundation under Grant 2022B1515020086.

REFERENCES

- [1] R. M. Tanner, D. Sridhara, and T. E. Fuja, "A class of group-structured LDPC codes," in *Proc. Int. Symp. Commun. Theory and Applications*, pp. 1-5, Ambleside, U.K., Jul. 2001.
- [2] 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.
- [3] L. Song, S. Yu, and Q. Huang, "Low-density parity-check codes: highway to channel capacity," *China Commun.*, vol. 20, no. 2, pp. 235-256, Feb. 2023.

TABLE II
CIRCULANT SIZE COMPARISON FOR $J = 5$: NEW SEARCH METHOD AND AND THE STATE-OF-THE-ART SEARCH METHOD [15].

L	P_{new}	$[\alpha_1, \beta]$	P_{HS} [15]
6	49	[6,19]	35
7	71	[2,20]	53
8	73	[27,2]	64
9	73	[27,2]	81
10	89	[34,2]	99
11	89	[34,2]	121
12	137	[37,9]	142
13	185	[43,113]	165
14	211	[28,12]	190
15	217	[100,122]	225
16	233	[89,3]	250
17	233	[89,3]	280
18	233	[89,5]	320
19	289	[38,57]	360
20	289	[38,57]	400
21	313	[25,19]	NA
22	313	[25,19]	NA
23	313	[25,19]	NA
24	313	[25,19]	NA
25	313	[25,19]	590

- [4] I. Kim and H.-Y. Song, "A simple construction for QC-LDPC codes of short lengths with girth at least 8," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1462-1465, Jeju, Korea(South), 21-23 Oct. 2020.
- [5] I. Kim, T. Kojima, and H.-Y. Song, "Some short-length girth-8 QC-LDPC codes from primes of the form $t^2 + 1$," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1211-1215, Jun. 2022.
- [6] I. Kim and H.-Y. Song, "A construction for girth-8 QC-LDPC codes using Golomb rulers," *Electron. Lett.*, vol. 58, no. 15, pp. 582-584, Jul. 2022.
- [7] A. Gómez-Fonseca, R. Smarandache, and D. G. M. Mitchell, "A low complexity PEG-like algorithm to construct quasi-cyclic LDPC codes," in *12th International Symposium on Topics in Coding (ISTC)*, pp. 1-5, Brest, France, 04-08 Sept. 2023.
- [8] H. Chimal-Dzul and A. Gómez-Fonseca, "Using partial orthomorphisms to construct short quasi-cyclic LDPC codes with girth at least 6," in *2023 12th International Symposium on Topics in Coding (ISTC)*, pp. 1-5, Brest, France, 04-08 Sept. 2023.
- [9] A. Gómez-Fonseca, R. Smarandache, and D. G. M. Mitchell, "An efficient strategy to count cycles in the Tanner graph of quasi-cyclic LDPC codes," *IEEE J. Sel. Area. Inf. Theory*, vol. 4, pp. 499-513, Sept. 2023.
- [10] F. Amirzade, M.-R. Sadeghi, and D. Panario, "Construction of protograph-based LDPC codes with chordless short cycles," *IEEE Trans. Inf. Theory*, vol. 70, no. 1, pp. 51-74, Jan. 2024.
- [11] H. Li, H. Xu, C. Chen, and B. Bai, "Efficient construction of quasi-cyclic LDPC codes with multiple lifting sizes," *IEEE Commun. Lett.*, vol. 28, no. 4, pp. 754-758, Apr. 2024.
- [12] Y. Zhang and X. Da, "Construction of girth-eight QC-LDPC codes from arithmetic progression sequence with large column weight," *Electron. Lett.*, vol. 51, no. 16, pp. 1257-1259, Aug. 2015.
- [13] 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.

TABLE III
CIRCULANT SIZE COMPARISON FOR $J = 6$: NEW SEARCH METHOD AND THE STATE-OF-THE-ART SEARCH METHODS [15], [16].

L	P_{new}	$[\alpha_1, \alpha_2, \beta]$	P_{HS} [15]	P_{IRS} [16]
7	97	[35,36,43]	70	101
8	109	[8,37,16]	95	121
9	109	[8,37,16]	125	151
10	143	[11,12,28]	150	181
11	169	[26,64,46]	182	181
12	169	[65,77,19]	218	181
13	271	[47,110,30]	254	241
14	289	[16,68,5]	296	281
15	289	[34,135,99]	337	331
16	289	[34,135,99]	380	341
17	361	[18,133,33]	429	401
18	361	[38,75,33]	478	451
19	451	[7,147,46]	530	521
20	451	[7,147,46]	584	571
21	529	[22,46,28]	NA	601
22	529	[22,46,28]	NA	661
23	599	[35,267,18]	NA	751
24	601	[45,189,2]	NA	781
25	601	[45,189,2]	NA	881

- [14] J. Wang, J. Zhang, Q. Zhou, and L. Zhang, "Full-length row-multiplier QC-LDPC codes with girth eight and short circulant sizes," *IEEE Access*, vol. 11, pp. 22250-22265, Mar. 2023.
- [15] 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.
- [16] A. Tasdighi and E. Boutillon, "Integer ring sieve for constructing compact QC-LDPC codes with girths 8, 10, and 12," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 35-46, Jan. 2022.
- [17] A. Kharin, A. Dryakhlov, E. Mirokhin, K. Zaverkin, A. Ovinnikov, and E. Likhobabin, "An approach to the generation of regular QC-LDPC codes with girth 8," in *Proc. 9th Medit. Conf. Embedded Comput. (MECO)*, pp. 1-4, Budva, Montenegro, 08-11 Jun. 2020.
- [18] 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.
- [19] G. Zhang, R. Sun, and X. Wang, "Explicit construction of girth-eight QC-LDPC codes and its application in CRT method," *J. Commun.*, vol. 33, no. 3, pp. 171-176, Mar. 2012. (in Chinese).
- [20] 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.
- [21] 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.
- [22] G. Zhang, R. Sun, and X. Wang, "Construction of girth-eight QC-LDPC codes from greatest common divisor," *IEEE Commun. Lett.*, vol. 17, no. 2, pp. 369-372, Feb. 2013.
- [23] 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.
- [24] 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, Sept. 2019.
- [25] G. Zhang, H. Liu, M. Lou, and Y. Fang, "Constructions of girth-eight QC-LDPC codes with dual-diagonal structure based on GCD

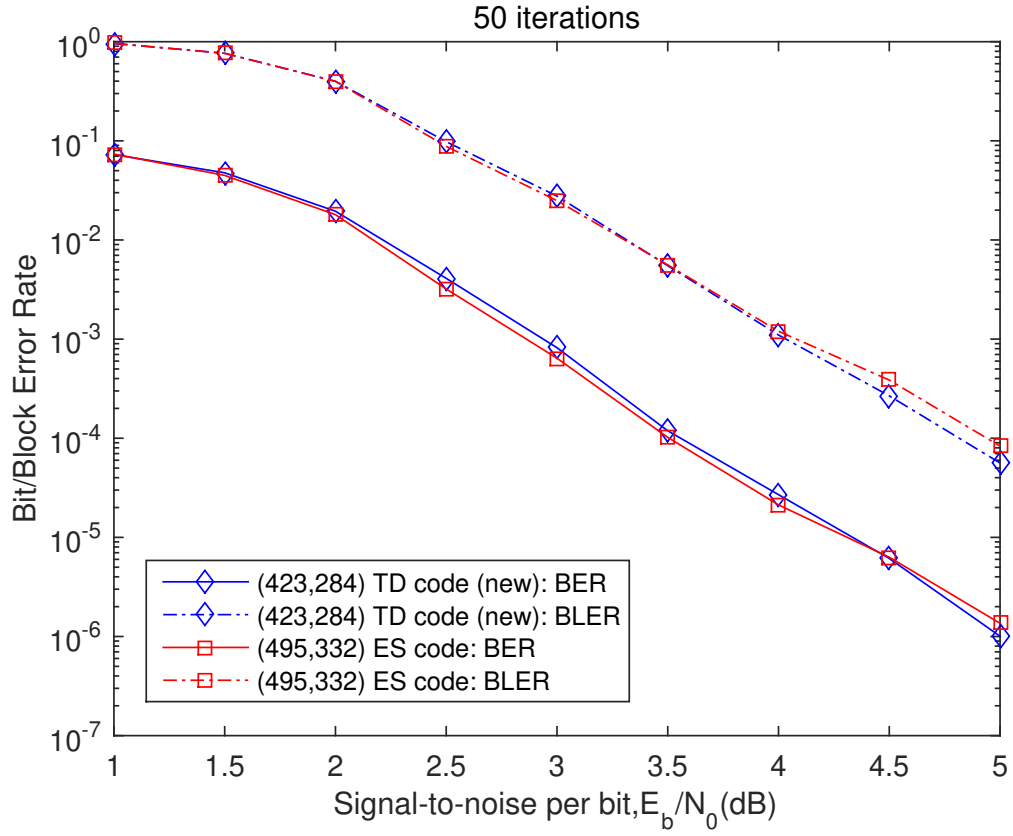


Fig. 3. Performance comparison of (3,9)-regular girth-8 VS codes: derived from existing ES and new TD methods.

framework,” in *2023 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 269-274, Hangzhou, China, 02-04 Nov. 2023.

- [26] G. Zhang, M. Ni, Y. Hu, and Y. Yang, “Quasi-cyclic LDPC codes with girth at least eight based on disjoint difference sets,” *IEEE Commun. Lett.*, vol. 27, no. 1, pp. 55-59, Jan. 2023.

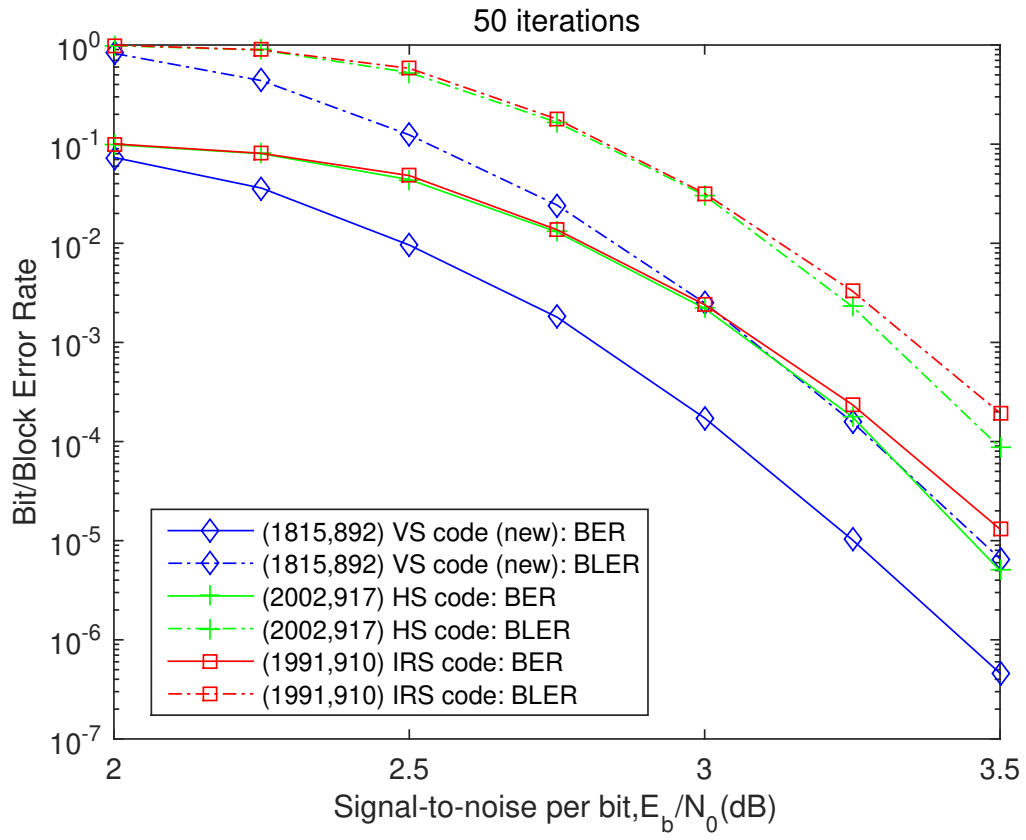


Fig. 4. Performance comparison of (6, 11)-regular girth-8 codes: new VS code ($L = 11$ in Theorem 2 (iv)) and existing HS and IRS codes.

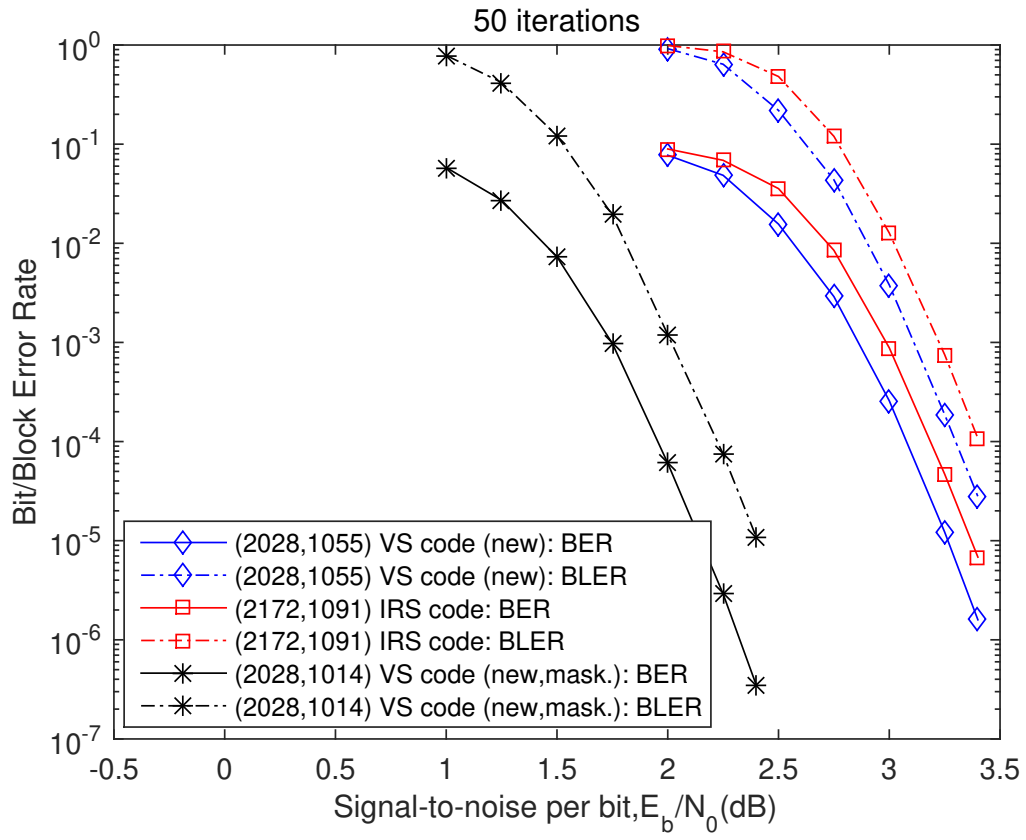


Fig. 5. Performance comparison of (6, 12)-regular girth-8 codes: new VS code ($L = 12$ in Table III) and existing IRS code.

APPENDIX A
PROOF OF LEMMA 1

Proof: Clearly, after subtracting $\alpha_{\frac{J-1}{2}} \cdot \beta_i$ from each element within the i -th column of this matrix, the resultant matrix is equivalent to the original matrix. Perform this operation in turn for all columns, and the final matrix becomes $[\alpha_0 - \alpha_{\frac{J-1}{2}}, \alpha_1 - \alpha_{\frac{J-1}{2}}, \dots, \alpha_{J-1} - \alpha_{\frac{J-1}{2}}]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$. Since $\alpha_i + \alpha_{J-1-i} = 2\alpha_{\frac{J-1}{2}}$, we have $\alpha_i - \alpha_{\frac{J-1}{2}} = -(\alpha_{J-1-i} - \alpha_{\frac{J-1}{2}})$. As a result, rearranging rows leads to the VS exponent matrix $\mathbf{E}_{vs} = [0, \mathbf{a}, -\mathbf{a}]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$. $\square$

APPENDIX B
PROOF OF THEOREM 1

Proof: Thanks to Lemma 1, it suffices to prove that $[0, 1, 2]^T [\beta_0, \beta_1, \dots, \beta_{L-1}]$ leads to a QC-LDPC code free of 4-cycles and 6-cycles for the circulant size P . First, consider 4-cycles. Case (1): If there exist 4-cycles associated with the first two rows of the exponent matrix, then such cycles can be expressed as $(0 - \beta_i) + (\beta_j - 0) = 0 \pmod{P}$, where $0 \leq i < j \leq L-1$. It reduces to $\beta_i = \beta_j \pmod{P}$, which is impossible due to Condition (i) in the theorem. Case (2): If there are 4-cycles in the first and last rows of the exponent matrix, then they can be denoted by $(0 - 2\beta_i) + (2\beta_j - 0) = 0 \pmod{P}$, where $0 \leq i < j \leq L-1$. It becomes $2\beta_i = 2\beta_j \pmod{P}$, which is impossible due to Condition (i) in the theorem. Case (3): The nonexistence of 4-cycles associated with the last two rows of the exponent matrix can be similarly proved as in Case (1).

Next, consider 6-cycles. Let i, j and k be three different indexes from 0 to $L-1$. If there exist 6-cycles in three rows of the exponent matrix, then without loss of generality they can be expressed as $(0 - \beta_j + \beta_i - 2\beta_i + 2\beta_k - 0) = 0 \pmod{P}$, equivalent to $2\beta_k = \beta_i + \beta_j \pmod{P}$. It is impossible owing to Condition (2) in the theorem.

Finally, the exponent matrix is not associated with 4-cycles but has a sub-matrix $[0, 1, 2]^T [\beta_i, \beta_j]$, where $0 \leq i < j \leq L-1$. Therefore, 8-cycles exist [23]. $\square$

APPENDIX C
PROOF OF LEMMA 3

Proof: (i) case 1: Subtracting $[e(1, r) + e(2, r)]/2$ from each element within the r -th column results in an equivalent exponent matrix. The r -th column becomes $[a(r), b(r), -b(r), -a(r)]^T$. Swapping the last two rows yields the final VS exponent matrix. (ii) case 2: If $e(1, r) + e(2, r)$ is even, subtract $[e(1, r) + e(2, r)]/2$ from each element within the r -th column; otherwise, subtract $[P + e(1, r) + e(2, r)]/2$. The r -th column becomes $[a(r), b(r), -b(r), -a(r)]^T$. Swapping the last two rows yields the final VS exponent matrix. $\square$

APPENDIX D
PROOF OF COROLLARY 3

Proof: On the one hand, according to Theorem 1 in [19], the exponent matrix $\mathbf{E}$ leads a girth-8 QC-LDPC code for each circulant size $P \geq \lceil 3L^2/4 \rceil + L - 1$. On the other hand, according to Lemma 3(ii), a VS exponent matrix $\mathbf{E}_{vs}$ can be generated from $\mathbf{E}$ as long as the circulant size P is odd. Therefore, $\mathbf{E}_{vs}$ corresponds to a girth-8 QC-LDPC code for each odd circulant size $P \geq \lceil 3L^2/4 \rceil + L - 1$. $\square$

APPENDIX E

PROOF OF THEOREM 2

The following two properties and three transformations are useful in the proof of our new construction.

p.0: For a triple of integers $(0, a, b)$ such that $0 < a < b$ and $b/\gcd(b, a) \geq L$, the matrix $[0, a, b]^T \cdot [0, 1, \dots, L-1]$ has no 6-cycles for any circulant size $P \geq b(L-1) + 1$.

p.1: For a triple of integers $(0, a, b)$ such that $\gcd(a, c) = c$ and $\gcd(b, c) = 1$, the matrix $[0, a, b]^T \cdot [0, 1, \dots, L-1]$ has no 6-cycles for any circulant size P satisfying $\gcd(P, c) = c$.

Shifting ('S'): For any circulant size, the two exponent matrices, $[a_0, a_1, \dots, a_i]^T \cdot [0, 1, \dots, L-1]$ and $[a_0 - a_0, a_1 - a_0, \dots, a_i - a_0]^T \cdot [0, 1, \dots, L-1]$ have the same cycle distribution.

Reversion ('R') : For any circulant size, the two exponent matrices, $[a_0, a_1, \dots, a_i]^T \cdot [0, 1, \dots, L-1]$ and $[a_i - a_i, a_i - a_{i-1}, \dots, a_i - a_0]^T \cdot [0, 1, \dots, L-1]$ have the same cycle distribution.

Division ('D'): For any circulant size P and any positive integer d such that $\gcd(d, P) = 1$, the two exponent matrices, $[d \cdot a_0, d \cdot a_1, \dots, d \cdot a_i]^T \cdot [0, 1, \dots, L-1]$ and $[a_0, a_1, \dots, a_i]^T \cdot [0, 1, \dots, L-1]$ have the same cycle distribution. This transformation with the parameter d is denoted by 'd'.

Proof: We only prove the case (iii), i.e. $\text{mod}(L, 6) = 4$; the other cases can be similarly proved. It is equivalent to proving that $[0, 2, L+3, L+7, 2L+8, 2L+10]^T \cdot [0, 1, \dots, L-1]$ corresponds to a girth-8 QC-LDPC code for the circulant size of $P = (L+1)(L+5)$. First, consider 4-cycles. There are 15 cases. The three cases, expressed as $(0, 2)$, $(0, L+3)$ and $(0, L+7)$, directly guarantee the absence of 4-cycles for $P = (L+5)(L+1)$. According to Transformation 'D', the two cases, $(0, 2L+8)$, $(0, 2L+10)$, are turned into $(0, L+4)$ and $(0, L+5)$, respectively; By utilizing first Transformation 'S' and then 'D', the two cases, $(2, 2L+8)$ and $(2, 2L+10)$, are reduced to $(0, L+3)$ and $(0, L+4)$, respectively. Therefore, 4-cycles are also impossible for the four cases. For each of the rest 8 cases, it is reduced to the form $(0, x)$ via 'S', where $2 \leq x \leq L+7$. As a result, these 8 cases also exclude 4-cycles.

Now, we consider 6-cycles. There are 20 cases for 6-cycles, as listed in Table IV. The reason why 6-cycles for each case cannot exist is explained in the last column of Table IV. For example, Case 12 means that the original triple $[2, L+3, 2L+8]$ can be reduced to $[0, L+1, 2L+6]$ via 'S', and further to $[0, L+5, 2L+6]$ via 'R'. Accordingly, the original matrix $[2, L+3, 2L+8]^T \cdot [0, 1, \dots, L-1]$ is reduced to $[0, L+1, 2L+6]^T \cdot [0, 1, \dots, L-1]$, and further to $[0, L+5, 2L+6]^T \cdot [0, 1, \dots, L-1]$. By choosing $a = L+5$, $b = 2L+6$ and $c = L+5$, we now check whether a, b, c and $P = (L+1)(L+5)$ satisfy all the conditions in Property p.1. Since $\text{mod}(L, 6) = 4$, it follows that $\gcd(L+1, 2) = 1$ and hence $\gcd(b, c) = \gcd(L+1, 4) = 1$. Moreover, it is obvious that $\gcd(P, c) = c$ and $\gcd(a, c) = c$. Therefore, thanks to Property p.1, the matrix $[0, L+5, 2L+6]^T \cdot [0, 1, \dots, L-1]$ are not associated with 6-cycles for the circulant size $P = (L+1)(L+5)$. Other 19 cases in this table can be similarly analyzed. $\square$

TABLE IV
REASONS FOR THE NONEXISTENCE OF 6-CYCLES ASSOCIATED WITH EACH COMBINATION OF THREE ROWS WITHIN THE EXPONENT
MATRIX. THE NOTATION $a \sim b$ MEANS $\text{gcd}(a, b) = 1$

#	Original triple	Reduced form	Reason
1	$[0, 2, L + 3]$	-	L even, p.0
2	$[0, 2, L + 7]$	-	L even, p.0
3	$[0, 2, 2L + 8]$	$(/2)[0, 1, L + 4]$	P odd, p.0
4	$[0, 2, 2L + 10]$	$(/2)[0, 1, L + 5]$	P odd, p.0
5	$[0, L + 3, L + 7]$	$(R)[0, 4, L + 7]$	L even, p.0
6	$[0, L + 3, 2L + 8]$	$(R)[0, L + 5, 2L + 8]$	$L + 1 \sim 2$, p.1
7	$[0, L + 3, 2L + 10]$	-	$L + 1 \sim 2$, p.1
8	$[0, L + 7, 2L + 8]$	$(R)[0, L + 1, 2L + 8]$	$L + 1 \sim 6$, p.1
9	$[0, L + 7, 2L + 10]$	$(R)[0, L + 3, 2L + 10]$	same as #7
10	$[0, 2L + 8, 2L + 10]$	$(R)[0, 2, 2L + 10]$ $(/2)[0, 1, L + 5]$	same as #4
11	$[2, L + 3, L + 7]$	$(S)[0, L + 1, L + 5]$ $(R)[0, 4, L + 5]$	L even, p.0
12	$[2, L + 3, 2L + 8]$	$(S)[0, L + 1, 2L + 6]$ $(R)[0, L + 5, 2L + 6]$	$L + 1 \sim 2$, p.1
13	$[2, L + 3, 2L + 10]$	$(S)[0, L + 1, 2L + 8]$	same as #8
14	$[2, L + 7, 2L + 8]$	$(S)[0, L + 5, 2L + 6]$	same as #12
15	$[2, L + 7, 2L + 10]$	$(S)[0, L + 5, 2L + 8]$	same as #6
16	$[2, 2L + 8, 2L + 10]$	$(S)[0, 2L + 6, 2L + 8]$ $(R)[0, 2, 2L + 8]$ $(/2)[0, 1, L + 4]$	same as #3
17	$[L + 3, L + 7, 2L + 8]$	$(S)[0, 4, L + 5]$	same as #11
18	$[L + 3, L + 7, 2L + 10]$	$(S)[0, 4, L + 7]$	same as #5
19	$[L + 3, 2L + 8, 2L + 10]$	$(S)[0, L + 5, L + 7]$ $(R)[0, 2, L + 7]$	same as #2
20	$[L + 7, 2L + 8, 2L + 10]$	$(S)[0, L + 1, L + 3]$ $(R)[0, 2, L + 3]$	same as #1