IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 30, 2020, accepted July 15, 2020, date of publication August 3, 2020, date of current version August 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3013838

Type-II QC-LDPC Codes From Multiplicative Subgroup of Prime Field

GUOHUA ZHANG[1], YULIN HU[2], (Senior Member, IEEE), DEFENG REN[1], YUANHUA LIU[1], AND YANG YANG[3]

[1]School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2]School of Electronic Information, Wuhan University, Wuhan 430072, China
[3]School of Information Engineering, Chang'an University, Xi'an 710064, China

Corresponding author: Yulin Hu (yulin.hu@ieee.org)

This work was supported in part by the National Natural Science Foundation of China under Grant 61471294.

ABSTRACT A quasi-cyclic (QC) low-density parity-check (LDPC) code is called type-II, if the maximum weight over all circulants appearing in the parity-check matrix has the value of two. On the basis of multiplicative subgroup analysis for the prime field, a novel algebraic approach for type-II QC-LDPC codes is proposed from Tanner's method. For column weight of four, the new type-II codes possess girth at least six and include a subset with very small circulant sizes almost attaining the theoretical lower bound. The new approach can yield type-II codes with two times smaller circulant sizes, in comparison with the state-of-the-art method. To enhance the flexibility of circulant sizes, a generalized Chinese-remainder-theorem (gCRT) method is proposed as well for type-II codes. Simulation results show that combining gCRT with the proposed short code yields compound type-II codes with a very promising decoding performance and flexible circulant sizes.

INDEX TERMS Circulant, girth, low-density parity-check (LDPC) codes, prime field, quasi-cyclic (QC).

I. INTRODUCTION

Recently, type-II quasi-cyclic (QC) low-density parity-check (LDPC) codes have attracted increasing attention [1]–[10], owing to the merit of commonly possessing larger upper bounds on distance [5], in comparison with traditional QC-LDPC codes [11]. On one hand, for column weight of four and small (even) row weight, type-II codes with the smallest circulant sizes (meeting the theoretical lower bound) have been reported via the computer-based search methods in [9] and [10]. On the other hand, type-II codes with small circulant sizes can also be explicitly constructed by a couple of algebraic methods, for example, [3], [6], [7], [10]. Among these studies, the state-of-the-art method (appendix B, [10]) can yield a class of type-II codes (with column weight of four) possessing circulant sizes only about two times larger than the theoretical lower bound.

In this article, a novel construction is designed for type-II QC-LDPC codes. In a special case, the new type-II codes possess circulant sizes which are much smaller than those of the existing algebraic methods; indeed, their circulant sizes are only marginally larger than the lower bound by one. To the best of our knowledge, this is the first algebraic construction capable of almost attaining the lower bound. To enhance the flexibility of circulant sizes, a generalized Chinese-remainder-theorem (gCRT) method is also proposed. As a byproduct, the rationales behind several conjectures and empirical rules on the girth of Tanner's method are disclosed as well.

The remainder of the paper is organized as follows. Basic notations and definitions are presented in Section II. New results on the girth of Tanner's method are put forward in Section III. In Section IV, novel type-II QC-LDPC codes are algebraically constructed on the basis of Tanner's method. Section V presents a generalized CRT method for enhancing the circulant-size flexibility of the new type-II QC-LDPC codes. Performance of the proposed type-II QC-LDPC codes and existing counterparts is compared in Section VI. Finally, Section VII concludes the whole work.

II. PRELIMINARY

An LDPC code is the null space of a sparse parity-check matrix (PCM). The PCM of a QC-LDPC code [5], [10], [12] is an $M \times N$ array of circulants with the same size of $P \times P$.

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

A weight-k *circulant* has k ones in its first row, where $0 \leq k \leq P$. In particular, a weight-0 circulant and a weight-1 circulant are called a zero matrix (ZM) and a circulant permutation matrix (CPM), respectively. If the maximum weight over all circulants is K ($K \geq 1$), then the PCM yields a type-K code. For instance, type-1 and type-2 can be also denoted by type-I and type-II, respectively. A type-I code without ZMs in its PCM is called *classical*.

For a weight-k circulant within the PCM of a type-K code, a K-tuple is formed by the k positions of ones (in the first row of the weight-k circulant) and $K - k$ ∞'s (i.e., using $K - k$ ∞'s to fill as many spare places). The components in the K-tuple are also called *exponents*. Therefore, a QC-LDPC code is associated with an $M \times N$ array of K-tuples. The K exponents for each K-tuple are randomly assigned to the K entries (in one-to-one correspondence) located in the same position of K matrices of size $M \times N$, leading to a total of K matrices, $\mathbf{E}_0, \mathbf{E}_1, \cdots, \mathbf{E}_{K-1}$, which are referred to as exponent matrices. Via the K exponent matrices and the circulant size P, the PCM can be uniquely described by $\sum_{i=0}^{K-1} f(\mathbf{E}_i, P)$, where the function f transforms a non-∞ exponent (say, e) within $\mathbf{E}_i$ to a specific $P \times P$ CPM (where '1' in the first row is located in the e-th column), and transforms ∞ to a $P \times P$ ZM.

A PCM with column (resp. row) weight J (resp. L) corresponds to a (J, L) code. A cycle of length $2l$ within a PCM is called a $2l$-cycle and the length of the shortest cycle is called girth. In this article, we denote girth at least g and exactly g by Gg^+ and Gg, respectively.

We finish this section by introducing two important results which are associated with the new contributions of this article. The first one is a lower bound on the circulant size for a $G6^+$ type-II $(2J', 2L')$ QC-LDPC code, as described by the following lemma.

Lemma 1: For a $G6^+$ type-II $(2J', 2L')$ QC-LDPC code whose PCM is composed of weight-2 circulants, the circulant size is greater than or equal to $4L'$ [9].

The other one is a well-known construction for classical QC-LDPC codes presented by R. M. Tanner [13], [14].

Tanner's method [13]: Let P be a prime number and denote by F_P the prime field with P elements. Let α and β be two nonzero (different) integers from F_P with orders of J and L, respectively. It is evident that $J|P - 1$ and $L|P - 1$. Define $\mathbf{E}_{tan}(i, r) = (\alpha^i \cdot \beta^r)_P$, where $0 \leq i \leq J - 1, 0 \leq r \leq L - 1$ and $(x)_P$ denotes x modulo P. The code associated with $\mathbf{E}_{tan}$ and P is called Tanner's (J, L) QC-LDPC code.

III. NEW RESULTS ON GIRTH OF TANNER's METHOD

Let P be a prime number. It is well known that for each positive integer K $(K|P-1)$, there are $\varphi(K)$ different elements with order K over the prime field F_P, where $\varphi(\cdot)$ is Euler's totient function. Therefore, for Tanner's method (where $J|P-1$ and $L|P-1$), at first glance there might exist as many as $\varphi(J) \cdot \varphi(L)$ different forms for $\mathbf{E}_{tan}$, one for each possible pair (α, β). However, we have the following result.

Lemma 2: Among all the $\varphi(J) \cdot \varphi(L)$ exponent matrices, where each of them is associated with a pair (α, β), there exists and only exists one inequivalent exponent matrix upon row and/or column permutations.

Proof: If α is an element with order J, then each element with order J is in the set $\{\alpha^0, \alpha^1, \cdots, \alpha^{J-1}\}$, which is a cyclic multiplicative subgroup of $F_P \setminus \{0\}$. Therefore, if α_1 and α_2 are of order J, then the vector $(\alpha_1^0, \alpha_1^1, \cdots, \alpha_1^{J-1})_P$ is a permutation of the one $(\alpha_2^0, \alpha_2^1, \cdots, \alpha_2^{J-1})_P$. Likewise, if β_1 and β_2 are of order L, then the vector $(\beta_1^0, \beta_1^1, \cdots, \beta_1^{L-1})_P$ is a permutation of the one $(\beta_2^0, \beta_2^1, \cdots, \beta_2^{L-1})_P$. As a result, the two resultant exponent matrices $\mathbf{E}_{tan}^{(1)}(i, r) = (\alpha_1^i \cdot \beta_1^r)_P$ and $\mathbf{E}_{tan}^{(2)}(i, r) = (\alpha_2^i \cdot \beta_1^r)_P$ are equivalent upon a certain row permutation, and the two ones $\mathbf{E}_{tan}^{(2)}(i, r) = (\alpha_2^i \cdot \beta_1^r)_P$ and $\mathbf{E}_{tan}^{(3)}(i, r) = (\alpha_2^i \cdot \beta_2^r)_P$ are equivalent upon a certain column permutation. Consequently, any two exponent matrices are equivalent upon row and/or column permutations. □

Example 1: Let $P = 37$, $J = 4$ and $L = 9$. Obviously, there are $\varphi(J) = 2$ elements ($\{6, 31\}$) of order $J = 4$, each of which can be chosen as α. Similarly, there are $\varphi(L) = 6$ elements ($\{7, 9, 12, 16, 33, 34\}$) of order $L = 9$, each of which can be chosen as β. We first choose $\alpha = 6$ and $\beta = 7$ to generate $\boldsymbol{E}_{tan}$.

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

Next, we choose $\alpha = 31$ and $\beta = 12$ to generate $\boldsymbol{E}_{tan}$.

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

It is easily verified that upon a row permutation (row indices from $(0, 1, 2, 3)$ to $(0, 3, 2, 1)$) and a column permutation (column indices from $(0, 1, \cdots, 8)$ to $(0, 5, 1, 6, 2, 7, 3, 8, 4)$), the second exponent matrix can be transformed into the first one. Therefore, the two exponent matrices are equivalent. Similarly, all other choices of α and β lead to exponent matrices equivalent to the first one. Consequently, there is only one inequivalent exponent matrix from Tanner's method for a feasible triple of (J, L, P).

Owing to Lemma 2, without loss of generality, α and β in Tanner's method can be set as $(x^{(P-1)/J})_P$ and $(x^{(P-1)/L})_P$, respectively, where x is a primitive element of F_P.

Lemma 3: If there are three pair-wisely shifted rows in the exponent matrix of a classical QC-LDPC code, i.e.,

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{L-1} \\ a_r & a_{mod(r+1,L)} & \cdots & a_{mod(r+L-1,L)} \\ a_s & a_{mod(s+1,L)} & \cdots & a_{mod(s+L-1,L)} \end{bmatrix}, \tag{3}$$

where $0 < r < s \leq L - 1$, then the associated PCM has 6-cycles regardless of the CPM size.

Proof: The $mod(L - s, L)$-th column of the middle row is $a_{mod(r-s,L)}$, and the same column of the last row is a_0.

Similarly, the $mod(r-s,L)$-th column of the first row is $a_{mod(r-s,L)}$, and the same column of the last row is a_r. Therefore, in the three columns (indexed by 0-th, $mod(L-s,L)$-th and $mod(r-s,L)$-th), there are 6-cycles described by $(a_0-a_r)+(a_{mod(r-s,L)}-a_0)+(a_r-a_{mod(r-s,L)})=0\,(mod\ P)$, regardless of P and the sequence $\{a_0,a_1,\cdots,a_{L-1}\}$. □

Lemma 4: For an even L ($L\geq 4$), there exist 8-cycles in the PCM of the codes from Tanner's method.

Proof: As $ord(\beta)=L$ and $2|L$, we have $(\beta^{L/2})_P=(-1)_P$. Select two rows (the i-th row and j-th row, $0\leq i<j\leq J-1$) from the exponent matrix. Then select four columns (the r-th, s-th, $(r+L/2)$-th and $(s+L/2)$-th columns, $0\leq r<s\leq L/2-1$) from the two rows. Owing to $(\beta^{L/2})_P=(-1)_P$, there is a pattern of 8-cycles associated with the selected rows and columns, which can be expressed as $[\mathbf{E}_{tan}(i,r)-\mathbf{E}_{tan}(j,r)]+[\mathbf{E}_{tan}(j,s+L/2)-\mathbf{E}_{tan}(i,s+L/2)]+[\mathbf{E}_{tan}(i,r+L/2)-\mathbf{E}_{tan}(j,r+L/2)]+[\mathbf{E}_{tan}(j,s)-\mathbf{E}_{tan}(i,s)]=0\,(mod\ P)$. □

Note that Lemma 4 is also applicable to any even J ($J\geq 4$). The proof is similar and omitted.

Lemma 5: If $J=ab$ and $L=ac$ hold, where $a\geq 3$ and $1\leq b\leq c$, then the girth of codes from Tanner's method is six.

Proof: Obviously, the girth of codes from Tanner's method is at least six. Now, we prove the existence of 6-cycles. Obviously, $x^{(P-1)/a}$ is an element with order a. From the exponent matrix, take the row whose first entry is in the set $\{x^{i(P-1)/a}|0\leq i\leq a-1\}$. There are in total a such rows. Next, from the selected rows, take the column whose first element is also in the set $\{x^{i(P-1)/a}|0\leq i\leq a-1\}$. There are in total a such columns. Thus, an $a\times a$ matrix is obtained. Performing row and column permutations yields an $a\times a$ circulant matrix (i.e., the $mod(i+1,a)$-th row can be obtained by cyclically shifting the i-th row to right by one position, $0\leq i\leq a-1$). Therefore, The proof is completed due to Lemma 3. □

Combining Lemma 4 and Lemma 5 (with $b=1$), we have proved an unsolved conjecture regarding the girth of Tanner's method.

Corollary 1: (Conj. 1, [15]): If $J|L$, then Tanner's (J,L) QC-LDPC codes have girth eight for $J=2$, and six for $J\geq 3$.

By setting $a=3$ and $b=2$, Lemma 5 implies a corollary, which justifies the empirical observation made in [15].

Corollary 2: Tanner's $(6,L)$ QC-LDPC codes have girth six when $mod(L,3)=0$.

On the basis of Lemma 4 together with Lemma 5, we have the following corollary, which provides the rationale behind the empirical results on the girth of Tanner's method in Tables 6–8 of [15].

Corollary 3: For a $G10^+$ Tanner's $(J>2,L)$ QC-LDPC code, J and L should be odd integers satisfying that $gcd(J,L)=1$.

For instance, besides each pair of two different primes, the two pairs, $(3,25)$ and $(5,9)$, are the two smallest ones with potential to guarantee $G10^+$ Tanner's QC-LDPC codes for a properly selected P. Actually, $P=64\cdot 3\cdot 25+1$ for $(3,25)$ and $P=36\cdot 5\cdot 9+1$ for $(5,9)$ really work.

IV. NEW TYPE-II QC-LDPC CODES DERIVED FROM TANNER's METHOD

A. NEW METHOD

Let $J\geq 4$ be even and $L>J/2$. Suppose that P is a prime number such that $J|P-1$ and $L|P-1$. Let α and β be two integers from the prime field F_P with orders of J and L, respectively. Define $\mathbf{E}_k(i,r)=(\alpha^{i+(k\cdot J)/2}\cdot\beta^r)_P$, where $k\in\{0,1\}$, $0\leq i\leq J/2-1$ and $0\leq r\leq L-1$.

Remark 1: The novel construction is motivated by Tanner's method [13]. To be specific, the two exponent matrices ($\mathbf{E}_0$ and $\mathbf{E}_1$) in the new construction are just the upper and lower parts, respectively, of the exponent matrix ($\mathbf{E}_{tan}$) in Tanner's method. It should be pointed out that Tanner's method is only applicable to classical QC-LDPC codes, while the new construction is designed for type-II QC-LDPC codes.

Lemma 6: $\boldsymbol{E}_1(i,r)=(-\boldsymbol{E}_0(i,r))_P$.

Proof: It is obvious owing to $(\alpha^{J/2})_P=(-1)_P$. □

By Lemma 6, it is obvious that $\mathbf{E}_0(i,r)\neq\mathbf{E}_1(i,r)$; therefore, the construction yields a type-II QC-LDPC code whose PCM is composed of weight-2 circulants.

Example 2: Set $J=4$, $L=7$ and $P=29$. Obviously, $J|P-1$ and $L|P-1$. Choose $\alpha=12$ and $\beta=7$ such that $ord(\alpha)=J=4$ and $ord(\beta)=L=7$. According to the new construction, we have two exponent matrices, $\boldsymbol{E}_0$ and $\boldsymbol{E}_1$, as follows.

$$\begin{bmatrix}\alpha^0\beta^0 & \alpha^0\beta^1 & \cdots & \alpha^0\beta^6\\ \alpha^1\beta^0 & \alpha^1\beta^1 & \cdots & \alpha^1\beta^6\end{bmatrix}\tag{4}$$

and

$$\begin{bmatrix}\alpha^2\beta^0 & \alpha^2\beta^1 & \cdots & \alpha^2\beta^6\\ \alpha^3\beta^0 & \alpha^3\beta^1 & \cdots & \alpha^3\beta^6\end{bmatrix},\tag{5}$$

which are

$$\begin{bmatrix}1 & 7 & 20 & 24 & 23 & 16 & 25\\ 12 & 26 & 8 & 27 & 15 & 18 & 10\end{bmatrix}$$

and

$$\begin{bmatrix}28 & 22 & 9 & 5 & 6 & 13 & 4\\ 17 & 3 & 21 & 2 & 14 & 11 & 19\end{bmatrix},$$

respectively. Obviously, $\boldsymbol{E}_0(i,r)+\boldsymbol{E}_1(i,r)=0\ (mod\ P)$ for any i and r $(0\leq i\leq 1, 0\leq r\leq 6)$, as expected by Lemma 6. It is readily verified that the two exponent matrices correspond to a $G6^+$ type-II $(4,14)$ QC-LDPC code with circulant size of 29, which almost attains the lower bound (28) in Lemma 1.

Remark 2: (i) Due to Lemma 6, the index of the row (in $\mathbf{E}_0$) with the entry $(\alpha^i)_P$ is the same as that of the row (in $\mathbf{E}_1$) with the entry $(-\alpha^i)_P$, where $0\leq i\leq J/2-1$. Combining this observation with Lemma 2, it is evident that our method also yields only one inequivalent exponent matrix upon row and/or column permutations. (ii) If L is even, then there always exist two 2-tuples, i.e., $(1,(-1)_P)$ and $((-1)_P,1)$, which are associated with the first row and the two columns

(0-th and $L/2$-th columns) of the two exponent matrices. As the two 2-tuples lead to 4-cycles, L must be an odd integer if $G6^+$ type-II QC-LDPC codes are required.

Example 3: Set $J = 4$, $L = 6$ and $P = 73$. Obviously, $J|P-1$ and $L|P-1$. Choose $\alpha = 27$ and $\beta = 9$ such that $ord(\alpha) = J = 4$ and $ord(\beta) = L = 6$. According to the new construction, we have two exponent matrices, $\mathbf{E}_0$ and $\mathbf{E}_1$, as follows.

$$\begin{bmatrix} 1^* & 9 & 8 & 72^* & 64 & 65 \\ 27 & 24 & 70 & 46 & 49 & 3 \end{bmatrix} \tag{6}$$

and

$$\begin{bmatrix} 72^* & 64 & 65 & 1^* & 9 & 8 \\ 46 & 49 & 3 & 27 & 24 & 70 \end{bmatrix}. \tag{7}$$

It is observed that there are two 2-tuples, $(1, 72)$ and $(72, 1)$, corresponding to the first row and the two columns (0-th and 3-th columns) of the two exponent matrices, which lead to 4-cycles described by $(1-72)+(72-1) = 0\,(mod\ P)$ regardless of P. Therefore, to ensure girth at least six, L should be odd in our new construction.

Remark 3: 4-cycles for a type-II $(2J', 2L')$ QC-LDPC code can be identified by the following steps: (i) for each 4-tuple of (i, j, r, s) $(0 \le i < j \le J'-1, 0 \le r < s \le L'-1)$, select two row ($i$-th and j-th rows) and two columns (r-th and s-th columns) from the two exponent matrices, $\mathbf{E}_0$ and $\mathbf{E}_1$; (ii) identify all patterns of 4-cycles associated with the two resultant 2×2 matrices. In step (ii), all patterns of 4-cycles are summarized in Table 1, according to [10]. The exponent corresponds to the i'-th row and r'-th column is denoted by $\{e_0(i', r'), e_1(i', r')\}$, where $0 \le i', r' \le 1$. In Table 1, for the case of $c(n)$ $(0 \le n \le 15)$, the inequality avoiding 4-cycles can be expressed by $e_{n_0}(0, 0) - e_{n_1}(1, 0) + e_{n_2}(1, 1) - e_{n_3}(0, 1) \neq 0\ (mod\ P)$, where (n_3, n_2, n_1, n_0) is the binary form of n. For example, the binary form of 3 is $(0, 0, 1, 1)$.

TABLE 1. Inequalities avoiding 4-cycles for any type-II QC-LDPC code.

no.	inequality
(a0)	$2(e_0(0,0) - e_1(0,0)) \neq 0\ (mod\ P)$
(a1)	$2(e_0(0,1) - e_1(0,1)) \neq 0\ (mod\ P)$
(a2)	$2(e_0(1,0) - e_1(1,0)) \neq 0\ (mod\ P)$
(a3)	$2(e_0(1,1) - e_1(1,1)) \neq 0\ (mod\ P)$
(b0)	$e_0(0,0) - e_1(0,0) + e_0(0,1) - e_1(0,1) \neq 0\ (mod\ P)$
(b1)	$e_1(0,0) - e_0(0,0) + e_0(0,1) - e_1(0,1) \neq 0\ (mod\ P)$
(b2)	$e_0(1,0) - e_1(1,0) + e_0(1,1) - e_1(1,1) \neq 0\ (mod\ P)$
(b3)	$e_1(1,0) - e_0(1,0) + e_0(1,1) - e_1(1,1) \neq 0\ (mod\ P)$
(b4)	$e_0(0,0) - e_1(0,0) + e_0(1,0) - e_1(1,0) \neq 0\ (mod\ P)$
(b5)	$e_1(0,0) - e_0(0,0) + e_0(1,0) - e_1(1,0) \neq 0\ (mod\ P)$
(b6)	$e_0(0,1) - e_1(0,1) + e_0(1,1) - e_1(1,1) \neq 0\ (mod\ P)$
(b7)	$e_1(0,1) - e_0(0,1) + e_0(1,1) - e_1(1,1) \neq 0\ (mod\ P)$
(c0)	$e_0(0,0) - e_0(1,0) + e_0(1,1) - e_0(0,1) \neq 0\ (mod\ P)$
(c1)	$e_1(0,0) - e_0(1,0) + e_0(1,1) - e_0(0,1) \neq 0\ (mod\ P)$
(c2)	$e_0(0,0) - e_1(1,0) + e_0(1,1) - e_0(0,1) \neq 0\ (mod\ P)$
$\vdots$	$\vdots$
(c15)	$e_1(0,0) - e_1(1,0) + e_1(1,1) - e_1(0,1) \neq 0\ (mod\ P)$

B. CASE OF J=4

Let L be an odd integer. As $gcd(J, L) = 1$, P can be expressed as $4mL + 1$, where $m \ge 1$ is an integer.

Lemma 7: If r and s are two integers, $0 \le r < s \le L-1$, then we have (i) $\alpha \neq (-1)_P$; (ii) $(\beta^{s-r})_P \neq (-1)_P$; (iii) $(\alpha \pm \beta^{s-r})_P \neq 0$; and (iv): $(\alpha\beta^{s-r})_P \neq (\pm 1)_P$.

Proof: (i) $\alpha = (-1)_P$ leads to $(\alpha^2)_P = 1$, which contradicts the premise that $ord(\alpha) = 4$. (ii) If $(\beta^{s-r})_P = (-1)_P$, then $(x^{4m(s-r)})_P = (-1)_P$, which implies $4m(s-r) = (P-1)/2\ (mod\ P-1)$; however, it is impossible as L is odd. (iii) Supposing $(\alpha + \beta^{s-r})_P = 0$, then $(x^{Lm})_P = (x^{4m(s-r)+(P-1)/2})_P$, indicating $Lm = 4m(s-r) + (P-1)/2\ (mod\ P-1)$. This is impossible as $mod(L, 4) \neq 0$. Next, if $(\alpha - \beta^{s-r})_P = 0$, then $(x^{Lm})_P = (x^{4m(s-r)})_P$, which implies $Lm = 4m(s-r)\ (mod\ P-1)$, again impossible due to $mod(L, 4) \neq 0$. Therefore, we have $(\alpha \pm \beta^{s-r})_P \neq 0$. (iv) If $(\alpha\beta^{s-r})_P = 1$, then we have $Lm + 4m(s-r) = 0\ (mod\ P-1)$. It is impossible as $mod(L, 4) \neq 0$. Next, $(\alpha\beta^{s-r})_P = (-1)_P$ means $Lm + 4m(s-r) = (P-1)/2\ (mod\ P-1)$; however, it cannot hold owing to $mod(L, 4) \neq 0$. As a result, we conclude that $(\alpha\beta^{s-r})_P \neq (\pm 1)_P$. □

Combining the new method and Lemma 7 yield the first main contribution of this article.

Theorem 1: Let $J = 4$ and L be an odd integer. Suppose that P is a prime number such that $P = 4mL + 1$, where $m \ge 1$ is an integer. Let α and β be two integers from the prime field F_P with orders of $J = 4$ and L, respectively. Define $\mathbf{E}_k(i, r) = (\alpha^{i+(k \cdot J)/2} \cdot \beta^r)_P$, where $k \in \{0, 1\}$, $i \in \{0, 1\}$ and $0 \le r \le L-1$. Then the two exponent matrices, $\mathbf{E}_0$ and $\mathbf{E}_1$, correspond to a $G6^+$ type-II $(4, 2L)$ QC-LDPC code with circulant size $P = 4mL + 1$.

Proof: According to [10], 4-cycles for a type-II $(4, 2L)$ QC-LDPC code can be classified into three categories: within one, two or four circulants. We consider them one by one. In the following, each expression governing a possible pattern of 4-cycles is transformed into a product of factors, and hence it cannot equal zero modulo P due to the related items in Lemma 7, or due to the orders of α and β.

(1) Within a circulant. There are two cases: a circulant in the first row or second row. (1.1) In the first row: the circulant in r-th column can be denoted by its exponent, $(\alpha^0\beta^r, \alpha^2\beta^r)$. Then we have $2(\alpha^0\beta^r - \alpha^2\beta^r) = 2(1-\alpha^2)\beta^r$. (1.2) In the second row: the circulant in r-th column can be denoted by $(\alpha^1\beta^r, \alpha^3\beta^r)$. Similar to (1.1), we have $2(\alpha^1\beta^r - \alpha^3\beta^r) = 2\alpha(1-\alpha^2)\beta^r$.

(2) Within two circulants. There are three cases: two circulants in the first row, in the second row, or in a column. (2.1) In the first row $(r < s)$: denote the two circulants by their exponents, $(\alpha^0\beta^r, \alpha^2\beta^r)$, $(\alpha^0\beta^s, \alpha^2\beta^s)$. There are two subcases, which can be uniformly expressed as $(-1)^a(\alpha^0\beta^r - \alpha^2\beta^r) + (\alpha^0\beta^s - \alpha^2\beta^s) = 2\beta^r[\beta^{s-r} + (-1)^a]$, where a is an integer in $\{0, 1\}$. (2.2) In the second row $(r < s)$: the two circulants can be expressed by $(\alpha^1\beta^r, \alpha^3\beta^r)$, $(\alpha^1\beta^s, \alpha^3\beta^s)$. Similar to (2.1), there are also two subcases, which can be uniformly denoted by $(-1)^a(\alpha^1\beta^r - \alpha^3\beta^r) + (\alpha^1\beta^s - \alpha^3\beta^s) = 2\alpha\beta^r[\beta^{s-r} + (-1)^a]$. (2.3) In a column: the two circulants can be denoted by $(\alpha^0\beta^r, \alpha^2\beta^r)$, $(\alpha^1\beta^r, \alpha^3\beta^r)$. Again, there are two subcases which can be uniformly represented by $(-1)^a(\alpha^0\beta^r - \alpha^2\beta^r) + (\alpha^1\beta^r - \alpha^3\beta^r) = 2[\alpha + (-1)^a]\beta^r$.

(3) Within four circulants. Denote the four circulants by their exponents, $(\alpha^0\beta^r, \alpha^2\beta^r)$, $(\alpha^1\beta^r, \alpha^3\beta^r)$, $(\alpha^0\beta^s, \alpha^2\beta^s)$ and $(\alpha^1\beta^s, \alpha^3\beta^s)$. There are 16 cases, which can be represented by c(0) to c(15) in Table 2. □

TABLE 2. **16 cases of 4-cycles within four circulants for the new type-II (4, 2*L*) QC-LDPC codes, where each factor form is not zero modulo *P*, owing to the related items in Lemma 7.**

no.	original form	factor form
(c0)	$(\alpha^0\beta^r - \alpha\beta^r) + (\alpha\beta^s - \alpha^0\beta^s)$	$(1-\alpha)\beta^r(1-\beta^{s-r})$
(c1)	$(\alpha^2\beta^r - \alpha\beta^r) + (\alpha\beta^s - \alpha^0\beta^s)$	$(\alpha-1)\beta^r(\alpha+\beta^{s-r})$
(c2)	$(\alpha^0\beta^r - \alpha^3\beta^r) + (\alpha\beta^s - \alpha^0\beta^s)$	$(1+\alpha)\beta^r(1+\alpha\beta^{s-r})$
(c3)	$(\alpha^2\beta^r - \alpha^3\beta^r) + (\alpha\beta^s - \alpha^0\beta^s)$	$(\alpha-1)\beta^r(1+\beta^{s-r})$
(c4)	$(\alpha^0\beta^r - \alpha\beta^r) + (\alpha^3\beta^s - \alpha^0\beta^s)$	$-(1+\alpha)\beta^r(\alpha+\beta^{s-r})$
(c5)	$(\alpha^2\beta^r - \alpha\beta^r) + (\alpha^3\beta^s - \alpha^0\beta^s)$	$-(1+\alpha)\beta^r(1+\beta^{s-r})$
(c6)	$(\alpha^0\beta^r - \alpha^3\beta^r) + (\alpha^3\beta^s - \alpha^0\beta^s)$	$(1+\alpha)\beta^r(1-\beta^{s-r})$
(c7)	$(\alpha^2\beta^r - \alpha^3\beta^r) + (\alpha^3\beta^s - \alpha^0\beta^s)$	$(1+\alpha)\beta^r(\alpha-\beta^{s-r})$
(c8)	$(\alpha^0\beta^r - \alpha\beta^r) + (\alpha\beta^s - \alpha^2\beta^s)$	$(1+\alpha)\beta^r(\beta^{s-r}-\alpha)$
(c9)	$(\alpha^2\beta^r - \alpha\beta^r) + (\alpha\beta^s - \alpha^2\beta^s)$	$(1+\alpha)\beta^r(\beta^{s-r}-1)$
(c10)	$(\alpha^0\beta^r - \alpha^3\beta^r) + (\alpha\beta^s - \alpha^2\beta^s)$	$(1+\alpha)\beta^r(1+\beta^{s-r})$
(c11)	$(\alpha^2\beta^r - \alpha^3\beta^r) + (\alpha\beta^s - \alpha^2\beta^s)$	$(1+\alpha)\beta^r(\alpha+\beta^{s-r})$
(c12)	$(\alpha^0\beta^r - \alpha\beta^r) + (\alpha^3\beta^s - \alpha^2\beta^s)$	$(1-\alpha)\beta^r(1+\beta^{s-r})$
(c13)	$(\alpha^2\beta^r - \alpha\beta^r) + (\alpha^3\beta^s - \alpha^2\beta^s)$	$-(1+\alpha)\beta^r(1+\alpha\beta^{s-r})$
(c14)	$(\alpha^0\beta^r - \alpha^3\beta^r) + (\alpha^3\beta^s - \alpha^2\beta^s)$	$(1+\alpha)\beta^r(1-\alpha\beta^{s-r})$
(c15)	$(\alpha^2\beta^r - \alpha^3\beta^r) + (\alpha^3\beta^s - \alpha^2\beta^s)$	$(1-\alpha)\beta^r(\beta^{s-r}-1)$

By replacing L with $2n+1$, the constraint of $P = 4mL+1$ being a prime number becomes that $P = (8m)n + (4m+1)$ should be a prime number. Owing to $gcd(8m, 4m+1) = 1$, it immediately follows Dirichlet's theorem [16] that there are infinitely many primes with the form $(8m)n + (4m+1)$ for each fixed m.

Lemma 8: (Dirichlet's theorem) [16]: For any two integers a and b satisfying $a > 0$ and $gcd(a, b) = 1$, there exist infinitely many primes with the form $an + b$.

Summarizing the above analysis, we have the following key corollary.

Corollary 4: For each fixed $m \geq 1$, there exist infinitely many choices of L such that $G6^+$ type-II $(4, 2L)$ QC-LDPC codes exist with circulant size $4mL + 1$.

By setting $m = 1$ in our method, it turns out that we have explicitly presented a class of $G6^+$ type-II $(4, 2L)$ QC-LDPC codes with almost the smallest circulant sizes (i.e., larger than the lower bound by one), for infinitely many choices of L. Compared with several existing methods, the new construction ($J = 4$, $m = 1$) has the following merits. First, although the two search-based random methods [9], [10] (algorithm 1, therein) provide the smallest circulant sizes meeting the lower bound, it is generally difficult to yield type-II QC-LDPC codes for a relatively large L. Second, for all permissible choices of L in our method, the circulant sizes for the new method are much smaller than those of the method in [10] (Appendix B, therein). Finally, by combining truncation with our construction, $G6^+$ type-II $(4, 2L)$ QC-LDPC codes for any L can be readily constructed with small circulant sizes. For instance, for $L = 16$, the first 16 columns of the exponent matrix for $L' = 25$ can be utilized to generate a $G6^+$ type-II $(4, 2L)$ QC-LDPC code with circulant size of $4L' + 1 = 101$, which is still much smaller than the counterpart (i.e., $8L = 128$) of the method in [10]. In this way, it can be promptly verified that compared with state-of-the-art algebraic approach in [10], the method we proposed can yield a much smaller circulant size for any $L \geq 3$, as depicted in Fig. 1.

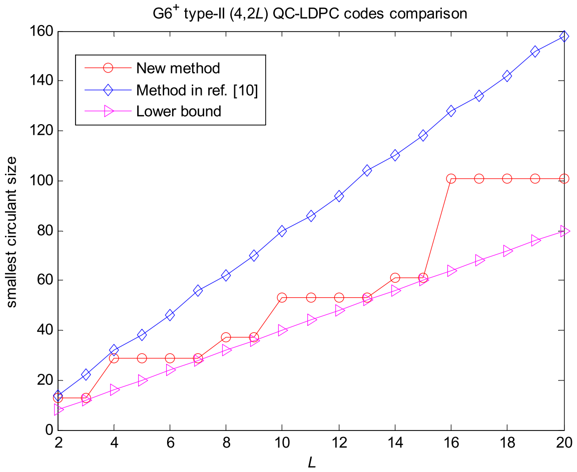


FIGURE 1. ***G6*$^+$ type-II (4, 2*L*) QC-LDPC codes comparison: the smallest circulant sizes for new and existing methods.**

Remark 4: Actually, the curve labeled as "New method" is obtained by combining two classes of L's. The first class of L's is directly permissible for our new method, and the corresponding smallest circulant sizes almost coincide with the lower bound (only larger by one). For the second class of L's (i.e., the rest choices of L's), the corresponding smallest circulant sizes are calculated by combining truncation with our new method. For this reason, the curve of the proposed new method is not smooth, and the size is not strictly monotonic with L. On the other hand, if we only consider the first class of L's, the curve will be smooth and strictly monotonic with L.

C. CASE OF $J \geq 6$

Unlike the case of $J = 4$, an odd integer L for the scenario of $J \geq 6$ does not necessarily lead to a $G6^+$ type-II $(J, 2L)$ QC-LDPC code. For example, the triple ($J = 6, L = 9, P = 37$) is not a qualified choice to guarantee a $G6^+$ type-II $(J, 2L)$ code with circulant size P. Nevertheless, using a program capable of identifying all types of 4-cycles described in Table 1, we find many feasible triples of (J, L, P) which yield $G6^+$ type-II $(J, 2L)$ codes with circulant size P. For $6 \leq J \leq 12$, $J/2 < L \leq 12$ and $J + 1 \leq P \leq 1000$, all such triples are listed in Table 3.

Interestingly, by checking a relatively large L, many $G6^+$ type-II $(J, 2L)$ QC-LDPC codes are found with almost the smallest circulant size (i.e., $4L + 1$), just the same as the case of $J = 4$. For example, such pairs of (J, L) are $(6, 27), (6, 45), (6, 57), (6, 69), \cdots;$ $(10, 25), (10, 45), \cdots;$ $(14, 175), (14, 273), \cdots; (18, 135), (18, 189), \cdots$. Since the pair (J, L) corresponds to a type-II $(2J', 2L')$ code where $J' = J/2$ and $L' = L$, the above observation implies that

TABLE 3. New type-II (J, 2L) QC-LDPC codes without 4-cycles.

J	L	P
6	5	{31,151,181,211,241,271,331,421,541,571,601,631,661,691,751,811,991}
6	7	{43,127,211,337,379,421,463,631,673,757,883,967}
6	9	{73,109,127,163,181,199,271,307,379,397,433,487,523,541,577,613,631, 739,757,811,829,883,919,937,991}
6	11	{199,331,397,463,727,859,991}
8	5	{41,241,281,401,521,601,641,761,881}
8	7	{113,281,337,449,617,673,953}
8	9	{73,433,577,937}
8	11	{89,353,617,881}
10	7	{211,281,421,491,631,701,911}
10	9	{181,271,541,631,811,991}
10	11	{331,661,881,991}
12	7	{337,421,673,757}
12	9	{109,181,397,433,541,577,613,757,829,937}
12	11	{397}

the lower bound in Lemma 1 is very tight not only for the case of $J' = 2$ but also for many (if not all) values of J'.

Example 4: Set $J = 10$, $L = 25$ and $P = 101$. Obviously, $J|P-1$ and $L|P-1$. Choose $\alpha = 6$ and $\beta = 5$ such that $ord(\alpha) = J$ and $ord(\beta) = L$ hold. The novel construction yields two exponent matrices, $\mathbf{E}_0$ and $\mathbf{E}_1$, as follows.

$$\begin{bmatrix} 1 & 5 & 25 & 24 & 19 & \cdots & 84 & 16 & 80 & 97 & 81 \\ 6 & 30 & 49 & 43 & 13 & \cdots & 100 & 96 & 76 & 77 & 82 \\ 36 & 79 & 92 & 56 & 78 & \cdots & 95 & 71 & 52 & 58 & 88 \\ 14 & 70 & 47 & 33 & 64 & \cdots & 65 & 22 & 9 & 45 & 23 \\ 84 & 16 & 80 & 97 & 81 & \cdots & 87 & 31 & 54 & 68 & 37 \end{bmatrix} \tag{8}$$

and

$$\begin{bmatrix} 100 & 96 & 76 & 77 & 82 & \cdots & 17 & 85 & 21 & 4 & 20 \\ 95 & 71 & 52 & 58 & 88 & \cdots & 1 & 5 & 25 & 24 & 19 \\ 65 & 22 & 9 & 45 & 23 & \cdots & 6 & 30 & 49 & 43 & 13 \\ 87 & 31 & 54 & 68 & 37 & \cdots & 36 & 79 & 92 & 56 & 78 \\ 17 & 85 & 21 & 4 & 20 & \cdots & 14 & 70 & 47 & 33 & 64 \end{bmatrix} \tag{9}$$

It is readily verified that the two exponent matrices correspond to a $G6^+$ type-II (10, 50) QC-LDPC code with circulant size of 101, which almost attains the lower bound (100) in Lemma 1.

V. GENERALIZED CRT METHOD FOR ENHANCING CIRCULANT-SIZE FLEXIBILITY

As described in the previous sections, the proposed construction can enable novel $G6^+$ type-II (4, 2L) QC-LDPC codes to possess almost the smallest circulant size P, where P is a prime number in the form of $4L+1$. In this section, we present a method for enhancing the circulant-size flexibility of the new type-II QC-LDPC codes.

It is well known that the Chinese remainder theorem (CRT) method [17], [18] is a very effective technique to construct a long QC-LDPC code from two short component QC-LDPC codes, which can guarantee that the girth of the long code is not less than the larger girth of the two short ones. However, the original form of the CRT is only applicable to type-I QC-LDPC codes. In this section, we generalize the CRT method to the type-K ($K \geq 1$) case. The nearly shortest type-II code we proposed is utilized as one component code in the generalized CRT (gCRT) method, while the other component code can be randomly generated. Simulations show that via combining the gCRT procedure with our new short codes, type-II codes with a variety of circulant sizes can be obtained with promising decoding performance.

gCRT: Let P_a and P_b be two coprime circulant sizes, i.e., $gcd(P_a, P_b) = 1$. Suppose that $\mathbf{U}_k$ $(0 \leq k \leq K-1)$ and $\mathbf{V}_k$ $(0 \leq k \leq K-1)$ are $2K$ exponent matrices that satisfy the following conditions. (i): they are all of size $J \times L$; and (ii) the first K exponent matrices are associated with P_a and the last K ones associated with P_b. Let $B_0, B_1, \cdots, B_{K-1}$ and A be $K+1$ positive integers such that $gcd(B_k, P_b) = 1$ $(0 \leq k \leq K-1)$ and $gcd(A, P_a) = 1$. From the $2K$ exponent matrices, we define K compound exponent matrices as $\mathbf{Z}_k(i,r) = A \cdot P_b \cdot \mathbf{U}_k(i,r) + B_k \cdot P_a \cdot \mathbf{V}_k(i,r)$ $(mod\ P_a \cdot P_b)$, where $0 \leq k \leq K-1$, $0 \leq i \leq J-1$, and $0 \leq r \leq L-1$.

Regarding the gCRT method, we have the following theorem, which is the second main contribution of this article.

Theorem 2: If the K exponent matrices $\mathbf{U}_k$ $(0 \leq k \leq K-1)$ correspond to a Gg type-K (JK, LK) QC-LDPC code with circulant size P_a, then the K compound matrices $\mathbf{Z}_k$ $(0 \leq k \leq K-1)$ yield a Gg$^+$ type-K (JK, LK) QC-LDPC code with circulant size $P_a \cdot P_b$.

Proof: (i) First, we prove that for any given pair (i, r) the K exponents $\mathbf{Z}_k(i,r)$ $(0 \leq k \leq K-1)$ are distinct. Assume that there exist two identical exponents (say $\mathbf{Z}_k(i,r)$ and $\mathbf{Z}_{k'}(i,r)$). Then $A \cdot P_b \cdot \mathbf{U}_k(i,r) + B_k \cdot P_a \cdot \mathbf{V}_k(i,r) = A \cdot P_b \cdot \mathbf{U}_{k'}(i,r) + B_{k'} \cdot P_a \cdot \mathbf{V}_{k'}(i,r)$ $(mod\ P_a \cdot P_b)$. Rearranging terms and taking modulo P_a on both sides, we have $A \cdot P_b \cdot [\mathbf{U}_k(i,r) - \mathbf{U}_{k'}(i,r)] = 0$ $(mod\ P_a)$, which is impossible as $\mathbf{U}_k(i,r) \neq \mathbf{U}_{k'}(i,r)$, $gcd(A, P_a) = 1$ and $gcd(P_b, P_a) = 1$. Therefore, the K matrices, $\mathbf{Z}_k$ $(0 \leq k \leq K-1)$, lead to a type-K (KJ, KL) QC-LDPC codes.

(ii) Next, we prove the nondecreasing girth property. Assume there is a cycle of length $2l$ $(2l < g)$ associated with the K exponent matrices, $\mathbf{Z}_k$ $(0 \leq k \leq K-1)$. Then such a cycle can be expressed by an ordered series of $2l$ exponents, $\mathbf{Z}_{k_0}(i_0, r_0)$, $\mathbf{Z}_{k_1}(i_1, r_0)$, $\cdots$, $\mathbf{Z}_{k_{2l-2}}(i_{l-1}, r_{l-1})$, $\mathbf{Z}_{k_{2l-1}}(i_l, r_{l-r})$, where $i_l = i_0$. Thus, we have $\sum_{n=0}^{l-1}[\mathbf{Z}_{k_{2n}}(i_n, r_n) - \mathbf{Z}_{k_{2n+1}}(i_{n+1}, r_n)] = 0$ mod $(P_a \cdot P_b)$ [10], where (i) $i_n = i_{n+1}$ and $k_{2n} = k_{2n+1}$ cannot hold simultaneously; and (ii) $r_n = r_{n+1}$ and $k_{2n+1} = k_{2n+2}$ cannot hold simultaneously ($r_l \triangleq r_0$ and $k_{2l} \triangleq k_0$). Consequently, we have $A \cdot P_b \cdot \sum_{n=0}^{l-1}[\mathbf{U}_{k_{2n}}(i_n, r_n) - \mathbf{U}_{k_{2n+1}}(i_{n+1}, r_n)] + P_a \cdot \sum_{n=0}^{l-1}[B_{k_{2n}} \cdot \mathbf{V}_{k_{2n}}(i_n, r_n) - B_{k_{2n+1}} \cdot \mathbf{V}_{k_{2n+1}}(i_{n+1}, r_n)] = 0$ $(mod\ P_a \cdot P_b)$. Taking modulo P_a on both sides, we have $A \cdot P_b \cdot \sum_{n=0}^{l-1}[\mathbf{U}_{k_{2n}}(i_n, r_n) - \mathbf{U}_{k_{2n+1}}(i_{n+1}, r_n)] = 0$ $(mod\ P_a)$. It reduces to $\sum_{n=0}^{l-1}[\mathbf{U}_{k_{2n}}(i_n, r_n) - \mathbf{U}_{k_{2n+1}}(i_{n+1}, r_n)] = 0$ $(mod\ P_a)$, owing to $gcd(A, P_a) = 1$ and $gcd(P_b, P_a) = 1$. However, this expression means a cycle with length at most $2l$ $(2l < g)$ associated with the K exponent matrices, $\mathbf{U}_k$ $(0 \leq k \leq K-1)$, contradicting the premise that the K matrices with circulant size P_a correspond to girth g. □

By setting $K = 1$, the above gCRT immediately reduces to CRT [17], [18] which is only applicable to type-I QC-LDPC codes. We note that for $K = 3$ the girth of the type-K code from gCRT cannot exceed six [19], as there exists one or more weight-3 circulants within the PCM of a type-K code.

VI. EXAMPLES AND SIMULATIONS

In this section, several new type-II codes are compared with existing counterparts in terms of bit error rate (BER) and block error rate (BLER) performance. Binary phase shift keying (BPSK) transmission over an additive white Gaussian noise (AWGN) channel, and iterative decoding using the sum-product algorithm (SPA) are assumed.

Example 5: *Let $J = 4$, $L = 7$ and $P = 29$. Generate two exponent matrices $\boldsymbol{E}_0$ and $\boldsymbol{E}_1$, according to the new method in Sect. A, IV. The first five columns of them yield a type-II $(4, 10)$ QC-LDPC code, which is used as the first component code ($P_a = 29$) in gCRT, while the second code is randomly generated with $P_b = 13$. Thus, a type-II $(4, 10)$ QC-LDPC code with length $5 \cdot P_a \cdot P_b = 1885$ is obtained by using the setting of $A = 23$, $B_0 = 8$ and $B_1 = 12$. For comparison, a type-II $(4, 10)$ counterpart with circulant size 381 [6] is constructed by the cyclic difference set (CDS). We notice that in Fig. 2 the two codes perform almost identically, while the former possesses a more flexible circulant size, due to the nearly shortest length of the first component code in gCRT.*

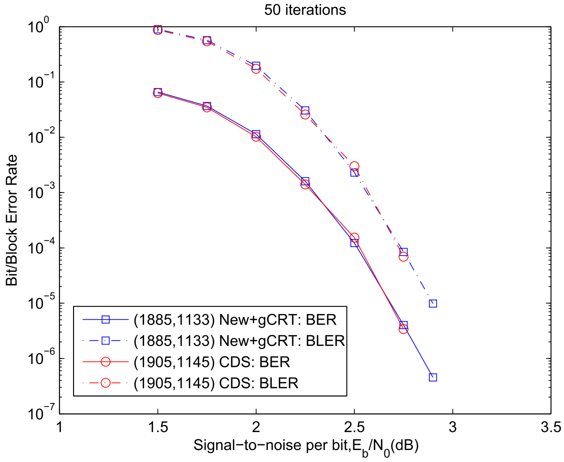


FIGURE 2. **Performance comparison of type-II (4, 10) QC-LDPC codes without 4-cycles: new+gCRT and CDS methods.**

Example 6: *Use the same matrices $\boldsymbol{E}_0$ and $\boldsymbol{E}_1$ as in Example 5. They yield a type-II $(4, 14)$ QC-LDPC code (C_0) with length $7 \cdot 29 = 203$. With the setup ($P_a = 29$, $P_b = 8, A = 23, B_0 = 3, B_1 = 5$), combining C_0 and a random code yields a type-II $(4, 14)$ QC-LDPC code with length $L \cdot P_a \cdot P_b = 1624$. Similarly, by utilizing C_0 and a randomly generated code, another type-II $(4, 14)$ QC-LDPC code with length 3248 can also be obtained with the setup ($P_a = 29, P_b = 16, A = 23, B_0 = 3, B_1 = 5$). For comparison, two random type-II $(4, 14)$ QC-LDPC codes without 4-cycles are generated. We see in Fig. 3 that the two new compound codes perform almost as well as the their random counterparts. Compared with codes from the random construction, the advantage of the new compound codes lies in that the girth can be guaranteed to be at least six without computer search, thanks to the first algebraically constructed short G6$^+$ component code.*

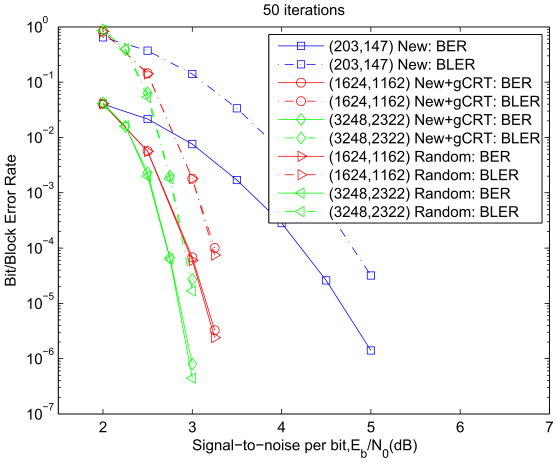


FIGURE 3. **Performance comparison of type-II (4, 14) QC-LDPC codes without 4-cycles: new+gCRT and random methods.**

Example 7: *In this example, we compare the performance of the new type-II QC-LDPC code and its type-I counterpart. The two exponent matrices in Example 4 are used to generate a new type-II $(10, 50)$ QC-LDPC code with circulant size of 101. The method based on two arbitrary sets of a finite field [20] (denoted by TAS) is utilized to yield the type-I counterpart. Use the prime field GF(53), and choose 2 as the primitive element. Select two set $\{6, 7, 8, 18, 21, 24, 26, 41, 45, 46\}$ and $\{0, 1, \cdots, 49\}$. According to the TAS method, the two sets lead to a type-I QC-LDPC code, whose PCM is a 10×50 array of circulants with size of 52. Except for 9 ZMs, all the circulants are CPMs. We see in Fig. 4 that the two QC-LDPC codes perform almost identically, although the new code has a shorter length. Besides, since the novel type-II code possesses a much larger circulant size (101) than its type-I counterpart (52), its complexity in terms of encoder implementation is much lower when a two-stage encoder scheme [2] is applied.*

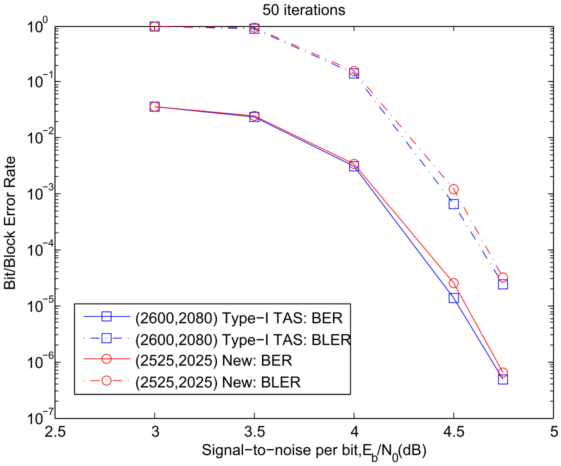


FIGURE 4. **Performance comparison of QC-LDPC codes without 4-cycles: new (type-II) and TAS (type-I) methods.**

VII. CONCLUSION

New results on the girth of Tanner's method are proved, which solve a couple of conjectures and empirical rules recently raised regarding Tanner's method. Inspired by Tanner's method, a novel class of type-II QC-LDPC codes with girth at least six is proposed, which can yield a subset with nearly the shortest circulant sizes. Moreover, a generalized CRT method is presented to enhance the flexibility of circulant sizes or equivalently the code lengths for type-II QC-LDPC codes. The compound type-II code obtained by combining gCRT with the new short code performs almost the same as the existing algebraically constructed counterpart, while possessing a more flexible circulant size.

Since type-II QC-LDPC codes permit not only weight-1/weight-0 circulant but also weight-2 circulant, they are more flexible than their type-I counterparts in terms of row/column weight optimization, decoding threshold optimization and distance optimization. Thus, compared with type-I QC-LDPC codes, type-II QC-LDPC codes more likely achieve a better performance in certain application scenarios. For instance, in the near-Earth satellite communication standard of CCSDS, a type-II QC-LDPC code designed by Shu Lin's group has been adopted. The combination of type-II QC-LDPC codes with several existing techniques (such as spatially-coupled method and cycle/absorbing set analysis) is a promising direction for the possible future developments of such type-II QC-LDPC codes.

REFERENCES

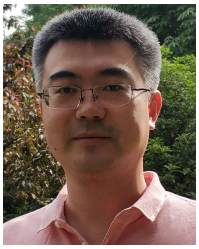
[1] R. Smarandache and P. O. Vontobel, "On regular quasi-cyclic LDPC codes from binomials," in *Proc. Int. Symp. Inf. Theory*, Chicago, IL, USA, Jun./Jul. 2004, p. 274.
[2] Z. Li, L. Chen, L. Zeng, S. Lin, and W. H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," *IEEE Trans. Commun.*, vol. 54, no. 1, pp. 71–81, Jan. 2006.
[3] K. Lally, "Explicit construction of type-II QC LDPC codes with girth at least 6," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2371–2375.
[4] M. Fujisawa and S. Sakata, "A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. 90, no. 5, pp. 1055–1061, May 2007.
[5] R. Smarandache and P. O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto- and tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.
[6] L. Zhang, B. Li, and L. Cheng, "Construction of type-II QC LDPC codes based on perfect cyclic difference set," *Chin. J. Electron.*, vol. 24, no. 1, pp. 146–151, Jan. 2015.
[7] G. Zhang, "Type-II quasi-cyclic low-density parity-check codes from Sidon sequences," *Electron. Lett.*, vol. 52, no. 5, pp. 367–369, Mar. 2016.
[8] S. Vafi and N. R. Majid, "Half rate quasi cyclic low density parity check codes based on combinatorial designs," *J. Comput. Commun.*, vol. 4, no. 12, pp. 39–49, 2016.
[9] M.-R. Sadeghi and F. Amirzade, "Analytical lower bound on the lifting degree of multiple-edge QC-LDPC codes with girth 6," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1528–1531, Aug. 2018.
[10] 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.
[11] 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.
[12] Y. Fang, P. Chen, G. Cai, F. C. M. Lau, S. C. Liew, and G. Han, "Outage-limit-approaching channel coding for future wireless communications: Root-protograph low-density parity-check codes," *IEEE Veh. Technol. Mag.*, vol. 14, no. 2, pp. 85–93, Jun. 2019.
[13] R. M. Tanner, D. Sridhara, and T. E. Fuja, "A class of group-structured LDPC codes," in *Proc. Int. Symp. Commun. Theory Appl.*, Ambleside, U.K., Jul. 2001, pp. 365–370.
[14] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, "On the girth of tanner (3, 5) quasi-cyclic LDPC codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1739–1744, Apr. 2006.
[15] H. Xu, H. Li, B. Bai, M. Zhu, and B. Zhang, "Tanner (J, L) quasi-cyclic LDPC codes: Girth analysis and derived codes," *IEEE Access*, vol. 7, pp. 944–957, 2019.
[16] P. Ribenboim, *Classical Theory of Algebraic Numbers*. New York, NY, USA: Springer-Verlag, 2001, p. 523.
[17] S. Myung and K. Yang, "A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem," *IEEE Commun. Lett.*, vol. 9, no. 9, pp. 823–825, Sep. 2005.
[18] 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.
[19] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "Design of multiple-edge protographs for QC LDPC codes avoiding short inevitable cycles," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4598–4614, Jul. 2013.
[20] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Quasi-cyclic LDPC codes on two arbitrary sets of a finite field," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jun. 2014, pp. 2454–2458.

GUOHUA ZHANG received the B.Sc. degree in electronics and information system from Shandong University, China, in 1999, the M.Sc.Eng. degree in communication and information system from the China Academy of Space Technology, Xi'an, China, in 2002, and the Ph.D. degree in communication and information system from Xidian University, China, in 2010. From July 2002 to May 2019, he was with the China Academy of Space Technology. In 2016, he was a Visiting Scholar with the Institute for Theoretical Information Technology, RWTH Aachen University, Aachen, Germany. He is currently a Professor with the School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications, China. His research interests include information and coding theory (especially LDPC codes) and sequence design. During his master's degree, he discovered a type of sequence (later named Weil sequence), which has now been adopted in the L1C signal design for the Global Navigation Satellite System of USA and the BeiDou Navigation Satellite System of China.

YULIN HU (Senior Member, IEEE) received the M.Sc. degree in EE from USTC, China, in 2011, and the Ph.D. degree (Hons.) in EE from RWTH Aachen University. He successfully defended his dissertation of a joint Ph.D. program supervised by Prof. Anke Schmeink at RWTH Aachen University and Prof. James Gross at the KTH Royal Institute of Technology, in December 2015. He was a Postdoctoral Research Fellow with RWTH Aachen University, from January 2016 to December 2016. Since 2017, he has been working as a Senior Researcher and the Project Lead of the ISEK Research Group, RWTH Aachen University. From May 2017 to July 2017, he was a Visiting Scholar with Prof. M. Cenk Gursoy in Syracuse University, USA. His research interests include information theory and optimal design of wireless communication systems. He has been invited to contribute submissions to multiple conferences. He has served as a TPC Member of many conferences and was an Organizer of special session-10 in the IEEE ISWCS 2018. He was a recipient of the IFIP/IEEE Wireless Days Student Travel Awards, in 2012. He received the Best Paper Awards at the IEEE ISWCS 2017 and the IEEE PIMRC 2017. He is serving as an Editor for *Physical Communication* (Elsevier) and the *EURASIP Journal on Wireless Communications and Networking* and the Lead Editor of Urllc-LoPIoT special issue in *Physical Communication*.

DEFENG REN received the B.S. degree in information security and the Ph.D. degree in communication and information systems from Xidian University, Xi'an, China, in 2008 and 2013, respectively. From November 2013 to January 2019, he was with the China Academy of Space Technology, Xi'an. Since March 2019, he has been with the School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an. He is currently a Senior Engineer. His research interests include multicarrier modulation, channel coding, cooperative spectrum sensing, and satellite communications.

YUANHUA LIU received the B.Sc. degree in communication engineering and the Ph.D. degree in communication and information system from Xidian University, China, in 2005 and 2010, respectively. She is currently an Associate Professor with the School of Communications and Information Engineering, Xi'an University of Posts and Telecommunications, China. Her research interests include information theory and coding theory.



YANG YANG received the B.Sc. degree in communication engineering and the Ph.D. degree in communication and information system from Xidian University, China, in 2004 and 2012, respectively. He is currently a Faculty Member with the School of Information Engineering, Chang'an University, China. His research interests include information theory, channel coding, and joint source-channel coding.