Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 4099918, 11 pages
https://doi.org/10.1155/2021/4099918

Research Article

Design of Nonbinary LDPC Cycle Codes with Large Girth from Circulants and Finite Fields

Hengzhou Xu,[1,2] **Huaan Li**,[1] **Jixun Gao**,[3] **Guixiang Zhang**,[1] **Hai Zhu**,[1] **and Xiao-Dong Zhang**[2]

[1]*School of Network Engineering, Zhoukou Normal University, Zhoukou 466000, China*
[2]*School of Mathematical Sciences, Shanghai Jiao Tong University, Shanghai 200240, China*
[3]*School of Computer, Henan University of Engineering, Zhengzhou 451191, China*

Correspondence should be addressed to Hengzhou Xu; hzxu@zknu.edu.cn

Received 21 May 2021; Accepted 8 September 2021; Published 23 September 2021

Academic Editor: Miaowen Wen

In this paper, we study a class of nonbinary LDPC (NBLDPC) codes whose parity-check matrices have column weight 2, called NBLDPC cycle codes. We propose a design framework of $(2, \rho)$-regular binary quasi-cyclic (QC) LDPC codes and then construct NBLDPC cycle codes of large girth based on circulants and finite fields by randomly choosing the nonzero field elements in their parity-check matrices. For enlarging the girth values, our approach is twofold. First, we give an exhaustive search of circulants with column/row weight ρ and design a masking matrix with good cycle distribution based on the edge-node relation in undirected graphs. Second, according to the designed masking matrix, we construct the exponent matrix based on finite fields. The iterative decoding performances of the constructed codes on the additive white Gaussian noise (AWGN) channel are finally provided.

1. Introduction

Nonbinary low-density parity-check (NBLDPC) codes based on modulo arithmetics were first discovered by Gallager in 1960s [1] and redefined over finite fields GF (q) by Davey and MacKay in 1998 [2]. Similar to binary LDPC codes, NBLDPC codes also have the ability of approaching capacity when decoded with the iterative algorithms. Moreover, NBLDPC codes have much better performance than binary LDPC codes for the short and moderate code lengths. As much more low-complexity decoding algorithms were proposed [3–8], NBLDPC codes provide a promising coding scheme for 6G communications [9].

As shown in [10], NBLDPC codes over larger finite fields will have much better performance for a constant code length. However, when the finite field size is sufficiently large, the performance improvement is little. Moreover, when the finite field size is equal or greater than 64, the column weights of the parity-check matrices of good NBLDPC codes tend to 2. Since NBLDPC cycle codes perform well over various channels [11–13], it is worth studying NBLDPC codes over large finite fields whose parity-check matrices have column weight 2, referred to as NBLDPC cycle codes. As an important cycle codes, $(2, \rho)$-regular NBLDPC codes also perform well under iterative decoding; lots of methods for constructing such codes were proposed [14–17]. Among these works on the construction of NBLDPC codes, the codes can be mainly classified into two categories: the first one is constructed by means of computer search under the algorithms satisfying certain rules, and the other one is constructed based on combinatorial designs, graph theory, matrix theory, and finite fields [18]. Simulation results show that they all have good performance. For a given code rate and length, it is of great interest to study which one of them has the best error performance.

Cycle structure plays an important role in binary/nonbinary LDPC codes. Research results show that NBLDPC codes with large girth have good iterative performance [19]. In general, NBLDPC codes with large girth have large

Hamming minimum distance, and it can be ensured that NBLDPC codes have good performance in the waterfall and error-floor region. Hence, it is interesting to construct LDPC cycle codes with large girth.

In this paper, we focus on the construction of $(2, \rho)$-regular quasi-cyclic LDPC (QC-LDPC) codes with large girth. We first proposed the construction framework of $(2, \rho)$-regular QC-LDPC codes based on the edge-node relation in undirected graphs and transfer the construction of $(2, \rho)$-regular QC-LDPC codes into two main parts, i.e., circulants and exponent matrices. In the first part, we find circulants with good cycle distribution by performing an exhaustive search. In order to prune the search space of circulants, isomorphism theory of circulants is proposed. For the second part, we directly employ finite fields to construct exponent matrices of QC-LDPC codes. Here, the employed finite fields are divided two types, i.e., prime fields and finite fields of characteristic 2. Finally, numerical results to show the good performance of our proposed codes are provided.

The rest of this paper is organized as follows. Section 2 introduces the definitions of LDPC codes and their associated Tanner graphs. Section 3 presents the design framework of $(2, \rho)$-regular QC-LDPC codes. Design of NBLDPC cycle codes with large girth is proposed in Section 4, and numerical results are also provided in this section. Finally, Section 5 concludes this paper.

2. Preliminaries

2.1. LDPC Codes. A binary (γ, ρ)-regular LDPC code is generated by the null space of an $m \times n$ sparse parity-check matrix $\mathbf{H}$ over GF (2), and the matrix $\mathbf{H}$ has the following properties: (1) each column has γ 1's; (2) each row has ρ 1's; (3) $\gamma \ll m$ and $\rho \ll n$. If the sparse matrix $\mathbf{H}$ is over GF (q) for q being a prime power, then LDPC codes generated by such $\mathbf{H}$ are called nonbinary codes or q-ary codes. Binary LDPC codes are referred to as quasi-cyclic (QC) [20], if their parity-check matrices $\mathbf{H}$ have the following form

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}(p_{1,1}) & \mathbf{I}(p_{1,2}) & \mathbf{I}(p_{1,3}) & \cdots & \mathbf{I}(p_{1,\rho}) \\ \mathbf{I}(p_{2,1}) & \mathbf{I}(p_{2,2}) & \mathbf{I}(p_{2,3}) & \cdots & \mathbf{I}(p_{2,\rho}) \\ \mathbf{I}(p_{3,1}) & \mathbf{I}(p_{3,2}) & \mathbf{I}(p_{3,3}) & \cdots & \mathbf{I}(p_{3,\rho}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}(p_{\gamma,1}) & \mathbf{I}(p_{\gamma,2}) & \mathbf{I}(p_{\gamma,3}) & \cdots & \mathbf{I}(p_{\gamma,\rho}) \end{bmatrix}_{\gamma Q \times \rho Q}, \tag{1}$$

where for $1 \le i \le \gamma$, $1 \le j \le \rho$, $-1 \le p_{i,j} \le Q-1$, $\mathbf{I}(p_{i,j})$ is a $Q \times Q$ circulant permutation matrix (CPM) formed by cyclically shifting each row of a $Q \times Q$ identity matrix $\mathbf{I}$ to the right (or left) by $p_{i,j} (\mathrm{mod}\ Q)$ positions, and $\mathbf{I}(-1)$ is a zero matrix of size $Q \times Q$. Obviously, $\mathbf{I}(0)$ is an identity matrix of size $Q \times Q$. For example, if $Q = 4$, then

$$\begin{aligned} \mathbf{I}(0) &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \\ \mathbf{I}(1) &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \\ \mathbf{I}(2) &= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \\ \mathbf{I}(3) &= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \end{aligned} \tag{2}$$

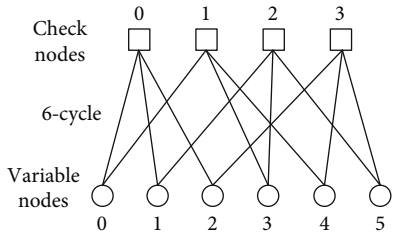
We can easily see that the positions of 1's of $\mathbf{H}$ in (1) are uniquely determined by the following matrix $\mathbf{P}$, called exponent matrix (or permutation shift matrix),

$$\mathbf{P} = \begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} & \cdots & p_{1,\rho} \\ p_{2,1} & p_{2,2} & p_{2,3} & \cdots & p_{2,\rho} \\ p_{3,1} & p_{3,2} & p_{3,3} & \cdots & p_{3,\rho} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{\gamma,1} & p_{\gamma,2} & p_{\gamma,3} & \cdots & p_{\gamma,\rho} \end{bmatrix}. \tag{3}$$

It is not hard to see that the correspondence between $\mathbf{P}$ and $\mathbf{H}$ is one-to-one. It is noticeable that the parameter Q is called *expansion factor* (or *lifting degree*) [21]. By replacing 1's in a CPM $\mathbf{I}(p_{i,j})$ of $\mathbf{H}$ in (1) with the same nonzero field element in finite field GF (q), the resulting code is nonbinary QC-LDPC codes [22].

2.2. Tanner Graph. Apart from the matrix representation, an LDPC code can be also described in a simple and intuitive way, i.e., a graphical model called Tanner graph [23]. In fact, the Tanner graph of an LDPC code with the parity-check matrix $\mathbf{H} = [h_{s,t}]$ is a bipartite graph in which the two classes of nodes are variable nodes (representing the code-bit nodes) and check nodes (representing the constraint nodes),

$$H_b = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad H_{nb} = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^1 & 0 & 0 & 0 \\ \alpha^1 & 0 & 0 & \alpha^2 & \alpha^1 & 0 \\ 0 & \alpha^2 & 0 & \alpha^0 & 0 & \alpha^0 \\ 0 & 0 & \alpha^0 & 0 & \alpha^2 & \alpha^1 \end{bmatrix}$$



(a) (b) (c)

Figure 1: Tanner graph of $\mathbf{H}_b$ (or $\mathbf{H}_{nb}$): (a) $\mathbf{H}_b$ over GF (2); (b) $\mathbf{H}_{nb}$ over GF (4); (c) Tanner graph.

respectively. An edge in a Tanner graph connects the check node s to the variable node t if and only if the row -s and column -t element $h_{s,t}$ in $\mathbf{H}$ is nonzero. A cycle in a Tanner graph is a sequence of the connected check nodes and variable nodes which start and end at the same node in the graph and contain no other nodes more than once. The cycle length is simply the number of the contained edges (or nodes), and the length of the shortest cycle is referred to as girth of the Tanner graph (or an LDPC code). As an example, Figure 1 shows the Tanner graph of $\mathbf{H}_b$ (or $\mathbf{H}_{nb}$) and an associate cycle of length 6 (6-cycle for short).

It is well-known that the iterative decoding algorithm converges to the optimal solution provided that the Tanner graph of an LDPC code is free of cycles [24]. In other words, short cycles, especially, the cycles of length 4, affect the decoding performance when decoded with the iterative algorithms based on belief propagation. In fact, there exist many cycles in an LDPC code with finite length. Hence, in order to avoid short cycles or obtain LDPC codes with large girth, many construction methods and techniques are proposed [25–33].

3. Design Framework of $(2, \rho)$-Regular Binary QC-LDPC Codes

3.1. Edge-Node Relation in Undirected Graphs. Let $G = (V, E)$ be an undirected graph, where V is a set of nodes and E is some subset of the pairs (called edges) $\{\{a, b\}: a, b \in V, a \neq b\}$. A cycle of $G = (V, E)$ has distinct nodes (or edges), and an edge in a cycle has two distinct nodes. If we treat the nodes and edges of $G = (V, E)$ as the check nodes and variable nodes, respectively, then a bipartite graph G_B can be obtained. Consider a cycle of length k (denoted by k -cycle for short) in $G = (V, E)$. This k-cycle will be turned into a $2k$-cycle in the above bipartite graph G_B. In other words, the girth of G_B is double that of $G = (V, E)$. Based on this process, we can construct bipartite graphs (or Tanner graphs) with large girth from an undirected graph. In order to make it clearly, we give an example.

Consider the following 4×4 matrix

$$B_{4\times4} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \quad (4)$$

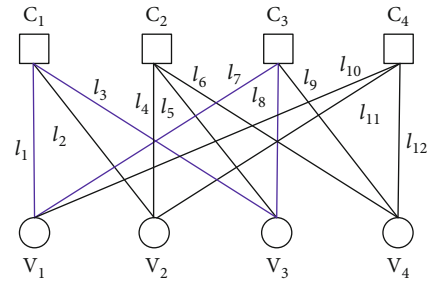


Figure 2: Tanner graph of $B_{4\times4}$.

It is easy to plot the Tanner graph of $B_{4\times4}$, given in Figure 2. By treating the nodes and edges of the Tanner graph in Figure 2 as the check nodes and variable nodes, respectively, we can construct a new bipartite graph, given in Figure 3. We can see from Figures 2 and 3 that a 4-cycle in the Tanner graph of $B_{4\times4}$ becomes a 8-cycle in the bipartite graph.

3.2. Construction Framework of $(2, \rho)$-Regular Binary QC-LDPC Codes. In this subsection, we will present the framework for constructing $(2, \rho)$-regular binary QC-LDPC codes by using the edge-node relation in an undirected graph in Section 3.1. In order to design $(2, \rho)$-regular codes, the node degree of $G = (V, E)$ should be ρ. Furthermore, to guarantee $(2, \rho)$-regular codes are quasi-cyclic, the incidence matrix of $G = (V, E)$ should possess quasi-cyclic structure. In conclusion, the incidence matrix of $G = (V, E)$ is (ρ, ρ)-regular and quasi-cyclic. Hence, in order to obtain $(2, \rho)$-regular binary QC-LDPC codes with large girth, we need to design a (ρ, ρ)-regular quasi-cyclic matrix with large girth. For convenience, this (ρ, ρ)-regular quasi-cyclic matrix is called base matrix. Next, we will give the construction framework.

First, we design a (ρ, ρ)-regular base matrix $\mathbf{B}$ of size $L \times L$. By employing the edge-node relation in Section 3.1, we can transfer the Tanner graph of $\mathbf{B}$ into a new bipartite graph, and the incidence matrix $\mathbf{B}_M$ of such a bipartite graph is obtained. It is obvious that $\mathbf{B}_M$ is a $(2, \rho)$-regular quasi-cyclic matrix of size $2L \times \rho L$. Second, we construct an exponent matrix $\mathbf{P}$ of size $2L \times \rho L$, and the corresponding expansion factor is Q. Third, we use $\mathbf{B}_M$ to mask the exponent matrix $\mathbf{P}$, and a $2L \times \rho L$ array $\mathbf{H}_M$ of $Q \times Q$ CPMs is constructed. The null space of $\mathbf{H}_M$ gives a $(2, \rho)$-regular binary QC-LDPC code of length ρLQ.

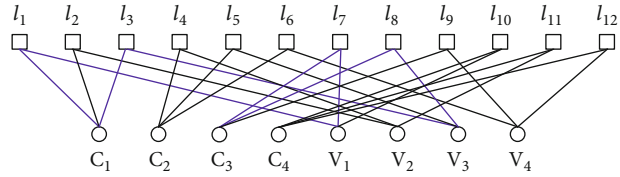


FIGURE 3: A new bipartite graph constructed from the Tanner graph of $B_{4\times4}$.

4. Design of Nonbinary LDPC Cycle Codes with Large Girth

In order to construct $(2, \rho)$-regular binary QC-LDPC codes with large girth, we only design a base matrix and a corresponding exponent matrix based on the construction framework in Section 3.2. By replacing the nonzero element in the parity-check matrices of binary QC-LDPC cycle codes with the nonzero field elements, nonbinary LDPC cycle codes can be obtained. In this paper, we do not optimize the nonzero field elements and adopt the optimized row elements in [34]. Next, we will provide the construction of the base matrices and exponent matrices.

4.1. Exhaustive Search of Circulants Based on Isomorphism Theory. In this paper, we employ the circulant as the base matrix. It can be seen from the construction framework in Section 3.2 that the size of the base matrix is not too large since the code lengths of NBLDPC codes are short or moderate. In the following, we will give the design of the circulants.

A circulant is a square matrix whose i-th row is generated by cyclically shifting the first row to the right (or left) by $(i-1)$ positions. Hence, the first row of a circulant is referred to as the generator of the circulant. For a circulant of size $L \times L$, each row (or column) is a rightward (or downward) cyclic-shift of its above (or left) row (or column), and the first row (or column) is the rightward (or downward) cyclic-shift of the last row (or column). Therefore, the rows and columns of a circulant have the same weight. It is clear that the row (or column) weight is associated with the row weight of the generator.

Consider a circulant C of size $L \times L$, and its generator is $G = (g_1, g_2, \cdots, g_L)$ where $g_i \in \{0, 1\}$ for $1 \le i \le L$. Let ρ be the number of the nonzero components of G. Hence, C is (ρ, ρ)-regular. We select the nonzero components from $g_1, g_2, \cdots, g_L$ and record their subscripts in a set S, called location set in this paper. Then, the location set S has ρ elements. Without loss of generality, the location set S is denoted by

$$S = \{s_1, s_2, \cdots, s_\rho\}, \tag{5}$$

where $1 \le s_i < s_j \le L$ for $1 \le i < j \le \rho$. It is obvious that the generator G and the location set S have a one-to-one correspondence. Based on the isomorphism theory of LDPC codes (or their parity-check matrices) in [16, 35, 36], we can directly give the isomorphism theory of the circulants as follows.

Theorem 1. *Let $S_1 = \{s_{1,1}, s_{1,2}, \cdots, s_{1,\rho}\}$ and $S_2 = \{s_{2,1}, s_{2,2}, \cdots, s_{2,\rho}\}$ be two location sets of the circulants C_1 and C_2 of size $L \times L$, respectively. Then, C_1 is isomorphic to C_2, denoted by $C_1 \cong C_2$, if S_2 is derived from S_1 with either of the following two methods.*

(1) For $r \in \{0, 1, \cdots, L-1\}$, the elements of S_2 are derived from these of S_1 by adding a constant r to the elements of S_1 modulo L, i.e., $s_{2,i} = s_{1,i} + r \pmod L$ for $1 \le i \le \rho$

(2) Suppose that r and L are coprime. The elements of S_2 are derived from these of S_1 using $s_{2,i} = r \cdot s_{1,i} \pmod L$ for $1 \le i \le \rho$

Note that in the calculation process, if the element in S_1 and S_2 equals 0, it actually equals L. Moreover, in the case (2) of Theorem 1, the number of r can be determined by a well-known function, called Euler's phi function, i.e.,

$$\phi(L) = L \prod_{r|L} \left(1 - \frac{1}{r}\right). \tag{6}$$

If $C_1 \cong C_2$, we say S_1 is isomorphic to S_2, denoted by $S_1 \cong S_2$.

In general, the size of the employed circulants in this paper is not large. Hence, we can make an exhaustive search of the circulants by using the computer. The search space of the location sets of the $L \times L$ circulants with row/column weight ρ is

$$\binom{L}{\rho} = \frac{L!}{(L-\rho)!\cdot\rho!}. \tag{7}$$

Based on the case (1) in Theorem 1, we can see that all the location sets of the $L \times L$ circulants have the following isomorphic form: $S = \{s_1 (= 1), s_2, \cdots, s_\rho\}$, where $2 \le s_i < s_j \le L$ for $2 \le i < j \le \rho$. Hence, the search space of such location sets S is

$$\binom{L-1}{\rho-1} = \frac{(L-1)!}{(L-\rho)!\cdot(\rho-1)!}. \tag{8}$$

That is, an exhaustive search of such location sets (or circulants) is feasible. Here, we do not provide the specific exhaustive search algorithm. Combined with the cycle-counting algorithms [37–39], the optimal $L \times L$ circulants with row/column weight ρ can be found. In this paper, the optimal ones are such circulants whose Tanner graphs have fewer short cycles and larger girths. In order to facilitate the readers, some optimal circulants are presented in Table 1.

4.2. Review of Finite Fields Based QC-LDPC Codes and Their Exponent Matrices. In this subsection, we will review the

Table 1: Some optimal $L \times L$ circulants with row/column weight ρ and location set S.

L	ρ	Location set S	L	ρ	Location set S	L	ρ	Location set S	L	ρ	Location set S
4	4	{0, 1, 2, 3}	5	5	{0, 1, 2, 3, 4}	6	6	{0, 1, 2, 3, 4, 5}	7	7	{0, 1, 2, 3, 4, 5, 6}
5	4	{0, 1, 2, 3}	6	5	{0, 1, 2, 3, 4}	7	6	{0, 1, 2, 3, 4, 5}	8	7	{0, 1, 2, 3, 4, 5, 6}
6	4	{0, 1, 2, 3}	7	5	{0, 1, 2, 3, 4}	8	6	{0, 1, 2, 3, 4, 5}	9	7	{0, 1, 2, 3, 4, 5, 6}
7	4	{0, 1, 2, 4}	8	5	{0, 1, 2, 3, 5}	9	6	{0, 1, 2, 3, 4, 6}	10	7	{0, 1, 2, 3, 4, 5, 7}
8	4	{0, 1, 2, 4}	9	5	{0, 1, 2, 3, 5}	10	6	{0, 1, 2, 3, 5, 6}	11	7	{0, 1, 2, 3, 4, 6, 7}
9	4	{0, 1, 2, 4}	10	5	{0, 1, 2, 3, 6}	11	6	{0, 1, 2, 4, 5, 7}	12	7	{0, 1, 2, 3, 4, 7, 9}
10	4	{0, 1, 2, 5}	11	5	{0, 1, 2, 4, 7}	12	6	{0, 1, 2, 3, 5, 8}	13	7	{0, 1, 2, 3, 4, 6, 9}
11	4	{0, 1, 2, 5}	12	5	{0, 1, 2, 4, 7}	13	6	{0, 1, 2, 3, 5, 9}	14	7	{0, 1, 2, 3, 5, 6, 9}
12	4	{0, 1, 3, 7}	13	5	{0, 1, 2, 4, 7}	14	6	{0, 1, 2, 3, 5, 9}	15	7	{0, 1, 2, 4, 5, 8, 10}
13	4	{0, 1, 3, 9}	14	5	{0, 1, 2, 4, 7}	15	6	{0, 1, 2, 3, 6, 10}	16	7	{0, 1, 2, 3, 5, 8, 12}
14	4	{0, 1, 4, 6}	15	5	{0, 1, 2, 4, 7}	16	6	{0, 1, 2, 3, 6, 10}	17	7	{0, 1, 2, 3, 5, 8, 12}
15	4	{0, 1, 3, 7}	16	5	{0, 1, 2, 5, 8}	17	6	{0, 1, 2, 3, 6, 10}	18	7	{0, 1, 2, 3, 5, 8, 12}
16	4	{0, 1, 3, 7}	17	5	{0, 1, 2, 4, 12}	18	6	{0, 1, 2, 4, 8, 13}	19	7	{0, 1, 2, 3, 5, 9, 14}
17	4	{0, 1, 3, 7}	18	5	{0, 1, 2, 5, 11}	19	6	{0, 1, 2, 4, 7, 11}	20	7	{0, 1, 2, 3, 6, 10, 15}
18	4	{0, 1, 3, 7}	19	5	{0, 1, 2, 6, 9}	20	6	{0, 1, 2, 4, 7, 12}	21	7	{0, 1, 2, 4, 8, 11, 16}
19	4	{0, 1, 3, 8}	20	5	{0, 1, 2, 5, 14}	21	6	{0, 1, 2, 4, 7, 12}	22	7	{0, 1, 2, 4, 6, 14, 17}
20	4	{0, 1, 3, 14}	21	5	{0, 1, 4, 14, 16}	22	6	{0, 1, 2, 4, 8, 13}	23	7	{0, 1, 2, 3, 8, 13, 17}
21	4	{0, 1, 3, 9}	22	5	{0, 1, 3, 7, 12}	23	6	{0, 1, 2, 4, 7, 15}	24	7	{0, 1, 2, 4, 7, 15, 19}
22	4	{0, 1, 3, 9}	23	5	{0, 1, 3, 8, 14}	24	6	{0, 1, 2, 4, 12, 19}	25	7	{0, 1, 2, 4, 7, 12, 16}
23	4	{0, 1, 3, 10}	24	5	{0, 1, 3, 11, 20}	25	6	{0, 1, 2, 4, 9, 15}	26	7	{0, 1, 2, 4, 7, 13, 18}
24	4	{0, 1, 3, 10}	25	5	{0, 1, 3, 15, 21}	26	6	{0, 1, 2, 5, 9, 15}	27	7	{0, 1, 2, 4, 7, 12, 21}
25	4	{0, 1, 3, 10}	26	5	{0, 1, 3, 7, 12}	27	6	{0, 1, 2, 5, 13, 22}	28	7	{0, 1, 2, 4, 7, 17, 21}
26	4	{0, 1, 3, 11}	27	5	{0, 1, 3, 7, 18}	28	6	{0, 1, 4, 15, 20, 22}	29	7	{0, 1, 2, 4, 7, 12, 16}
27	4	{0, 1, 4, 10}	28	5	{0, 1, 3, 13, 24}	29	6	{0, 1, 2, 4, 18, 23}	30	7	{0, 1, 2, 4, 7, 15, 25}
28	4	{0, 1, 3, 12}	29	5	{0, 1, 3, 7, 19}	30	6	{0, 1, 2, 5, 14, 24}	30	5	{0, 1, 3, 12, 25}

finite field based method for constructing QC-LDPC codes, and provide two classes of exponent matrices of these QC-LDPC codes [18].

4.2.1. A General Construction of QC-LDPC Codes Based on Finite Fields of Characteristic 2. Let GF (q) be a finite field with $q = 2^t$ with $t \geq 2$, and let α be a primitive element of GF (q). For each nonzero element α^i with $0 \leq i \leq q-2$, we define the location vector $v(\alpha^i)$ as a $(q-1)$-tuple over GF (2),

$$v(\alpha^i) = (v_1, v_2, \cdots, v_{q-1}), \tag{9}$$

whose components correspond to the nonzero elements $\alpha_0, \alpha_1, \cdots, \alpha_{q-2}$ of GF (q), where the i-th component v_i is set to 1 and all the other $(q-2)$ components are 0. Hence, based on the nonzero element α^i of GF (q), we can uniquely form a $(q-1) \times (q-1)$ square matrix $M(\alpha^i)$ whose j-th row is obtained by cyclically shifting every component of the $(q-1)$-ary location vector $v(\alpha^i)(j-1)$ places to the right (or left) for $0 \leq i \leq q-2, 1 \leq j \leq q-1$. The resulting square matrix $M(\alpha^i)$ is a CPM, and it is also referred to as the $(q-1)$-fold matrix dispersion (or expansion) of the nonzero field element α^i over GF (2) [18].

Consider a $\gamma \times \rho$ matrix $\mathbf{P}$ over GF (q),

$$P = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_\gamma \end{bmatrix} = \begin{bmatrix} p_{1,2} & p_{1,3} & \cdots & p_{1,\rho} \\ p_{2,2} & p_{2,3} & \cdots & p_{2,\rho} \\ p_{3,2} & p_{3,3} & \cdots & p_{3,\rho} \\ \vdots & \vdots & \ddots & \vdots \\ p_{\gamma,2} & p_{\gamma,3} & \cdots & p_{\gamma,\rho} \end{bmatrix}, \tag{10}$$

whose rows satisfy the following two constraints: (1) for $1 \leq i < \gamma, 0 \leq k, l \leq q-2$ and $k \neq l$, $\alpha^k p_i$ and $\alpha^l p_i$ have at most one position where both of them have the same element of GF (q) (i.e., they differ in at least $(\rho-1)$ positions); (2) for $1 \leq i, j < \gamma, i \neq j$, and $0 \leq k, l \leq q-2$,$\alpha^k p_i$ and $\alpha^l p_j$ differ in at least $(\rho-1)$ positions. These constraints are called α-multiplied row constraints in [18]. By replacing each of its entry $p_{i,j}$ with the binary matrix $M(p_{i,j})$, we obtain a $\gamma \times \rho$ array $H_{\gamma,\rho}$ of $(q-1) \times (q-1)$ CPMs. Then, the null space of $H_{\gamma,\rho}$ gives a binary (γ, ρ)-regular QC-LDPC code. Moreover, the α-multiplied row constraints ensure the Tanner graph of this code free of cycle of length 4. Hence, the constructed QC-LDPC codes have girth at least 6.

Table 2: The nonzero field elements in the parity-check matrix of the proposed 64-ary (496,248) LDPC cycle code in Example 1.

Row index	Nonzero field elements				Row index	Nonzero field elements				Row index	Nonzero field elements			
1	37	9	22	0	2	7	0	18	44	3	0	37	9	19
4	0	37	19	9	5	7	18	44	0	6	7	18	0	44
7	7	18	44	0	8	0	18	44	7	9	19	9	0	37
10	0	18	44	7	11	0	9	37	22	12	18	44	7	0
13	9	19	37	0	14	18	0	7	44	15	22	37	0	9
16	0	44	7	18	17	9	19	0	37	18	37	22	0	9
19	44	18	7	0	20	9	37	22	0	21	19	37	9	0
22	0	22	37	9	23	44	7	0	18	24	0	7	44	18
25	9	37	0	22	26	19	9	37	0	27	22	37	0	9
28	9	22	37	0	29	9	37	22	0	30	37	9	22	0
31	37	9	22	0	32	22	9	37	0	33	7	18	44	0
34	37	0	9	22	35	0	37	22	9	36	7	44	0	18
37	0	44	7	18	38	9	0	37	19	39	37	9	22	0
40	0	9	19	37	41	44	7	18	0	42	37	19	9	0
43	9	37	0	19	44	37	9	22	0	45	0	9	19	37
46	19	9	37	0	47	0	19	37	9	48	18	0	44	7
49	0	19	9	37	50	22	37	9	0	51	37	0	9	22
52	18	7	0	44	53	0	9	37	22	54	44	7	0	18
55	7	0	44	18	56	9	0	37	22	57	9	19	37	0
58	22	9	37	0	59	9	19	37	0	60	0	44	18	7
61	18	7	0	44	62	9	37	0	19	63	22	0	9	37
64	7	0	18	44	65	18	44	0	7	66	19	37	9	0
67	9	37	22	0	68	18	7	0	44	69	0	9	22	37
70	37	22	0	9	71	18	7	44	0	72	7	0	18	44
73	0	22	37	9	74	7	0	44	18	75	9	0	19	37
76	37	0	9	19	77	9	37	0	22	78	0	37	9	22
79	37	9	0	22	70	9	0	37	19	81	7	44	18	0
82	0	44	18	7	83	9	37	22	0	84	44	0	7	18
85	9	22	37	0	86	9	19	37	0	87	22	9	0	37
88	0	18	7	44	89	9	37	22	0	90	18	0	7	44
91	37	22	9	0	92	0	22	37	9	93	37	0	9	22
94	9	22	37	0	95	44	0	7	18	96	0	9	19	37
97	7	44	18	0	98	9	19	37	0	99	7	44	18	0
100	37	22	0	9	101	0	22	9	37	102	22	0	37	9
103	44	0	7	18	104	22	9	0	37	105	22	0	37	9
106	44	7	18	0	107	37	19	0	9	108	0	9	37	22
109	9	37	19	0	110	44	18	0	7	111	37	22	9	0
112	7	0	18	44	113	0	18	44	7	114	37	22	0	9
115	0	9	37	19	116	7	18	0	44	117	9	0	22	37
118	0	37	19	9	119	0	9	22	37	120	19	37	9	0
121	37	0	22	9	122	37	0	9	22	123	0	7	44	18
124	19	37	0	9	125	7	44	18	0	126	7	44	0	18
127	9	37	22	0	128	44	18	0	7	129	7	18	0	44
130	0	37	22	9	131	7	0	44	18	132	0	37	9	22
133	0	44	18	7	134	44	18	7	0	135	9	37	0	22
136	9	37	19	0	137	0	9	37	22	138	18	44	7	0
142	0	18	7	44	143	44	18	0	7	144	9	37	0	19
145	0	18	7	44	146	18	0	7	44	147	19	9	37	0

Table 2: Continued.

Row index	Nonzero field elements				Row index	Nonzero field elements				Row index	Nonzero field elements			
148	44	18	0	7	149	37	0	19	9	150	19	0	9	37
151	0	37	22	9	152	7	18	44	0	153	44	0	7	18
154	0	37	9	22	155	18	0	7	44	156	44	7	0	18
157	0	37	9	19	158	22	37	9	0	159	7	18	44	0
160	0	37	9	19	161	0	18	7	44	162	0	37	9	22
163	7	18	44	0	164	37	22	9	0	165	0	9	37	22
166	0	37	19	9	167	18	44	7	0	168	9	0	22	37
169	0	37	9	19	170	44	0	18	7	171	9	0	19	37
172	9	0	37	19	173	9	37	19	0	174	44	7	18	0
175	19	0	37	9	176	0	22	9	37	177	9	0	37	19
178	0	18	7	44	179	0	18	44	7	180	37	0	9	22
181	9	37	0	22	182	0	37	22	9	183	37	0	22	9
184	0	9	22	37	185	9	19	37	0	186	44	7	18	0
187	19	9	0	37	188	37	0	9	22	189	18	44	7	0
190	22	37	9	0	191	37	19	0	9	192	37	9	19	0
193	0	37	19	9	194	22	0	37	9	195	7	0	18	44
196	37	19	0	9	197	9	37	22	0	198	22	9	0	37
199	44	18	0	7	200	22	37	9	0	201	7	18	0	44
202	0	19	9	37	203	0	44	18	7	204	9	0	19	37
205	7	18	0	44	206	37	19	0	9	207	7	44	18	0
208	44	0	18	7	209	19	37	0	9	210	44	18	0	7
211	19	37	0	9	212	18	0	7	44	213	37	9	22	0
214	0	9	37	22	215	22	37	0	9	216	19	37	9	0
217	7	44	18	0	218	44	0	7	18	219	44	0	7	18
220	37	0	19	9	221	22	9	0	37	222	44	18	7	0
223	19	9	37	0	224	18	0	44	7	225	37	22	9	0
226	22	9	37	0	227	19	37	9	0	228	18	44	7	0
229	9	19	37	0	230	18	44	7	0	231	18	7	0	44
232	44	7	18	0	233	44	18	0	7	234	37	22	9	0
235	22	9	37	0	236	22	9	0	37	237	44	0	18	7
238	0	37	22	9	239	37	22	0	9	240	37	19	0	9
241	0	18	7	44	242	19	37	0	9	243	22	9	0	37
244	44	7	18	0	245	9	37	19	0	246	37	22	0	9
247	44	7	18	0	248	19	9	0	37					

According to the definition in Section 2, we can see that the above $\gamma \times \rho$ matrix $\mathbf{P}$ is the exponent matrix, and the associate expansion factor is $(q-1)$. A framework for constructing such matrix $\mathbf{P}$ based on two arbitrary subsets of a finite field was proposed in [40]. Let η be a nonzero element in GF (q) and α be a primitive element. For $1 \le \gamma, \rho \le q$, let $T_1 = \{\alpha^{i_1}, \alpha^{i_2}, \cdots, \alpha^{i_\gamma}\}$ and $T_2 = \{\alpha^{j_1}, \alpha^{j_2}, \cdots, \alpha^{j_\rho}\}$ be two arbitrary subsets of elements in GF (q) with i_k and j_l in the set $\{-\infty, 0, 1, 2, \cdots, q-2\}$, $i_1 < i_2 < \cdots < i_\gamma$, and $j_1 < j_2 < \cdots < j_\rho$. The $\gamma \times \rho$ matrix $\mathbf{P}$ can be formed by

$$P(\eta) = \left[\eta\alpha^{i_k} + \alpha^{j_l}\right]_{1 \le k \le \gamma, 1 \le l \le \rho}. \tag{11}$$

Under this framework, some well-known constructions of QC-LDPC codes based on finite fields and combinatorial designs are special cases [14, 41, 42]. For example, when $T_1 = T_2 = \mathrm{GF}(q)$, $P(\eta)$ is a Latin square over GF (q) [43].

4.2.2. Construction of QC-LDPC Codes Based on Prime Fields. Let p be a prime. Consider a $p \times p$ matrix

$$P = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,p} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ p_{p,1} & p_{p,2} & \cdots & p_{p,p} \end{bmatrix}, \tag{12}$$

where $p_{i,j} = (i-1) \cdot (j-1) (\mathrm{mod}\ p)$ for $1 \le i \le p$ and $1 \le j \le p$. We select a $\gamma \times \rho$ submatrix from P and replace its elements $p_{s,t}$ with the CPMs $\mathbf{I}(p_{s,t})$ for $1 \le s \le \gamma$ and $1 \le t \le \rho$. The

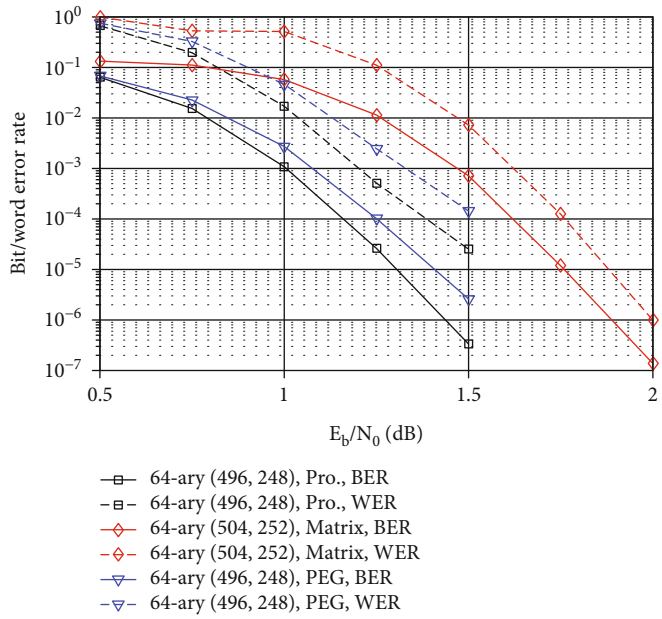


Figure 4: The error performances of the proposed (496,248) LDPC cycle code over GF (64), the comparable (504,252) irregular QC-LDPC code over GF (64) constructed from finite field GF (64) in [15], and (2,4)-regular (496,248) LDPC code over GF (64) constructed based on the progressive edge-growth (PEG) algorithm in [46]. The transmissions on the BPSK modulated AWGN channel are assumed.

following $\gamma \times \rho$ array $H(P_{\gamma\times\rho})$ of $p \times p$ CPMs over GF (2) is obtained.

$$H\left(P_{\gamma\times\rho}\right) = \left[I\left(p_{s,t}\right)\right]_{1\le s\le\gamma, 1\le t\le\rho}. \tag{13}$$

Actually, the null space of $H(P_{\gamma\times\rho})$ gives a (γ, ρ)-regular QC-LDPC code of length $p\rho$ with girth at least 6. Notice that the exponent matrix of this code is $P_{\gamma\times\rho}$ and the expansion factor is p. How to select good γ rows and ρ columns of CPMs from P in (12) can be found in [44, 45].

4.3. Nonbinary LDPC Cycle Codes and Numerical Results. Combined with Sections 3.2, 4.1, and 4.2, we can easily construct a binary QC-LDPC cycle code. Based on the replacement of the nonzero elements in finite fields, nonbinary LDPC cycle codes can be constructed. In order to show the advantages of our proposed construction methods, we next provide some examples.

Table 3: The nonzero field elements in the corresponding CPMs of the parity-check matrices $H_{\mathrm{M},256}(P_{8\times16,2})$ in Example 2.

Row index	Nonzero field elements			
1	0	182	8	172
2	173	0	182	8
3	40	167	0	127
4	40	127	0	169
5	40	169	0	128
6	172	8	182	0
7	8	172	182	0
8	40	169	128	0

Example 1. Consider the all-one matrix (or circulant) of size 4×4. It is clear that there is only one such circulant for $\rho = 4$ and $L = 4$. The following 8×16 matrix $B_{8\times16}$ can be obtained based on the construction framework in Section 3.2.

$$7ptB_{8\times16} = \begin{bmatrix} 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0 \\ 0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \end{bmatrix}. \tag{14}$$

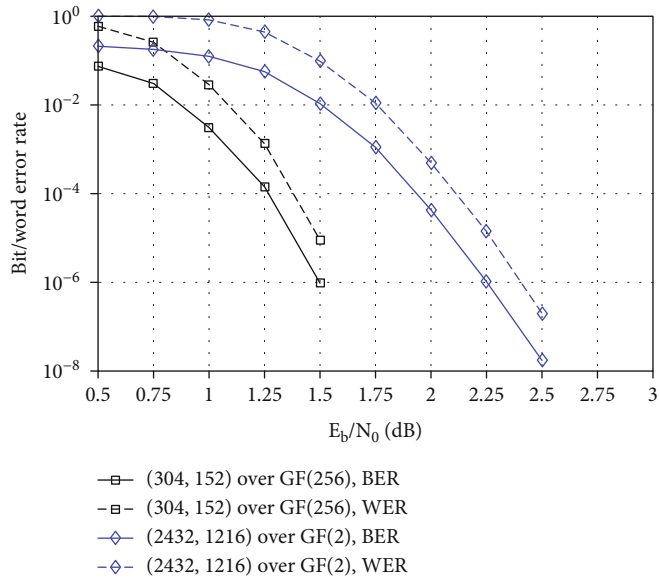


Figure 5: The error performances of the constructed (304,152) QC-LDPC cycle code over GF (256) and the comparable (2432,1216) LDPC code over GF (2) constructed based on the progressive edge-growth (PEG) algorithm in [46]. The transmissions on the BPSK modulated AWGN channel are assumed.

Based on the prime field GF (31), we can construct an 8×16 array $H(P_{8\times16,1})$ of 31×31 CPMs in the form of (13) by choosing the 8 rows and 16 columns from the exponent matrix P in equation (12). The indices of the chosen 8 rows and 16 columns from P are {3, 4, 5, 10, 15, 17, 24, 28} and {1, 4, 5, 6, 7, 8, 9, 10, 11, 15, 16, 19, 26, 28, 29, 30}, respectively. The row and column selection method is based on the proposed method in [45]. By employing $B_{8\times16}$ to mask $H(P_{8\times16,1})$, we can obtain an array $H_{\mathrm{M}}(P_{8\times16,1})$ of 31×31 CPMs. By replacing the 1's of each row in $H_{\mathrm{M}}(P_{8\times16,1})$ with nonzero elements of GF (64) in the corresponding rows of Table 2, a $(2, 4)$-regular matrix $H_{\mathrm{M},64}(P_{8\times16,1})$ over GF (64) is obtained. Note that the numbers in Table 2 are the power numbers of α, where α is a primitive element of GF (64) created by using the primitive polynomial $p(x) = 1 + x + x^6$. The null space of $H_{\mathrm{M},64}(P_{8\times16})$ gives a $(2, 4)$-regular (496,248) LDPC cycle code over GF (64). The girth of this code is 16, and the number of 16-cycles is 775. For comparison, we reconstruct the irregular (504,252) QC-LDPC code over GF (64) based on finite field GF (64) and the masking matrix $B_{\mathrm{mask}}(4, 8)$ in [15]. The average column and row weights in the parity-check matrix of (504,252) QC-LDPC code over GF (64) are 2.5 and 5, respectively. Moreover, we also design a comparable (2,4)-regular (496,248) LDPC code over GF (64) based on the progressive edge-growth (PEG) algorithm in [46], called PEG-LDPC code. Note that the nonzero elements of the parity-check matrix of the (2,4)-regular (496,248) PEG-LDPC code over GF (64) are randomly chosen. When decoded with the fast-Fourier-transform (FFT) based Q-ary sum-product algorithm (QSPA) with 50 iterations, the bit/word error rates (BERs/WERs) of these three nonbinary LDPC codes are shown in Figure 4. In the simulations, the transmissions on the BPSK modulated AWGN channel are assumed. We can see that at the BER of 2×10^{-6}, the proposed nonbinary (496,248) LDPC cycle code outperforms the (504,252) QC-LDPC code over GF (64) and the (2,4)-regular (496,248) PEG-LDPC code over GF (64) about 0.45 dB and 0.1 dB, respectively.

In the above example, we can see that the constructed nonbinary LDPC cycle code is not quasi-cyclic because of the randomly chosen nonzero field elements in its parity-check matrix. Hence, we next show the performances of the proposed nonbinary QC-LDPC cycle codes.

Example 2. Consider the prime field GF (19), we can easily construct an 8×16 matrix $P_{8\times16,2}$ over GF (19) based on the exponent matrix P in equation (12) and the construction framework in Section 3.2. The indices of the chosen 8 rows and 16 columns from P are {1, 2, 4, 5, 7, 8, 14, 15} and {1, 2, 3, 4, 5, 6, 7, 9, 10, 13, 14, 15, 16, 17, 18, 19}, respectively. The row and column selection method is also based on the proposed method in [45]. By dispersing each entry of $P_{8\times16,2}$ into the corresponding CPMs of size 19×19, an 8×16 array $H(P_{8\times16,2})$ of 19×19 CPMs is obtained. By employing $B_{8\times16}$ in equation (14) to mask the array $H(P_{8\times16,2})$, we can construct an array $H_M(P_{8\times16,2})$ of 19×19 CPMs. By replacing the 1's of each CPM in $H_M(P_{8\times16,2})$ with the same nonzero element of GF (256) in the corresponding row of Table 3, a (2,4)-regular matrix $H_{M,256}(P_{8\times16,2})$ over GF (256) is obtained. It is noticeable that the numbers in Table 3 are the power numbers of α, where α is a primitive element of GF (256) created by using the primitive polynomial $p(x) = 1 + x^2 + x^3 + x^4 + x^8$. The null space of $H_{M,256}(P_{8\times16,2})$ gives a (2,4)-regular (304,152) LDPC cycle code over GF (256). The girth of this code is 16, and the number of 16-cycles is 969. Since the nonzero field elements of a

CPM in $H_{M,256}(P_{8\times16,2})$ are the same, and the resulting (304,152) LDPC cycle code over GF (256) is quasi-cyclic.

For comparison, we construct the (3,6)-regular (2432, 1216) LDPC code over GF (2) based on the progressive edge-growth (PEG) algorithm in [46]. The error performances of these two LDPC codes are shown in Figure 5. In the simulations, the employed decoding algorithms of the constructed (304,152) QC-LDPC cycle code over GF (256) and the (2432,1216) LDPC code over GF (2) are the QSPA (50 iterations) and the sum-product algorithm (SPA) with 50 iterations, respectively. The transmissions on the BPSK modulated AWGN channel are assumed. We can see that the constructed (304,152) QC-LDPC cycle code over GF (256) can outperform the (2432,1216) LDPC code over GF (2) about 0.75 dB at the BER of 10^{-6}.

5. Conclusion

This paper proposed a design framework of binary QC-LDPC cycle codes and constructed nonbinary LDPC (NBLDPC) cycle codes based on circulants and finite fields. The presented construction method consists of three parts. First, the masking matrices are designed based on circulants and the point-line relation in graph theory. Second, the exponent matrices of binary QC-LDPC cycle codes are constructed from finite fields and the designed masking matrices. Third, by replacing 1's in the parity-check matrices of binary QC-LDPC cycle codes with the nonzero field elements, NBLDPC cycle codes are obtained. Numerical results show that the constructed NBLDPC cycle codes have good iterative decoding performance.

Data Availability

The data used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants 61801527 and 11971311, the TianYuan Special Funds of the National Natural Science Foundation of China under Grants 12026230 and 12026231, and the Development Project of Henan Provincial Department of Science and Technology under Grants 212102310544 and 212102310551.

References

[1] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.

[2] M. Davey and D. MacKay, "Low-density parity check codes over GF(q)," *IEEE Communications Letters*, vol. 2, no. 6, pp. 165–167, 1998.

[3] S. Wang, Q. Huang, and Z. Wang, "Symbol flipping decoding algorithms based on prediction for non-binary LDPC codes," *IEEE Transactions on Communications*, vol. 65, no. 5, pp. 1913–1924, 2017.

[4] Q. Huang, L. Song, and Z. Wang, "Set message-passing decoding algorithms for regular non-binary LDPC codes," *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5110–5122, 2017.

[5] B. Dai, R. Liu, C. Gao, and Z. Mei, "Symbol flipping algorithm with self-adjustment strategy for LDPC codes over GF(q)," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7189–7193, 2019.

[6] Z. Liu, R. Liu, and L. Zhao, "GPU-based non-binary LDPC decoder with weighted bit-reliability based algorithm," *China Communications*, vol. 17, no. 5, pp. 78–88, 2020.

[7] S. Song, J. Tian, J. Lin, and Z. Wang, "An improved reliability-based decoding algorithm for NB-LDPC codes," *IEEE Communications Letters*, vol. 25, no. 4, pp. 1153–1157, 2021.

[8] V. B. Wijekoon, E. Viterbo, and Y. Hong, "Decoding of NB-LDPC codes over subfields," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 716–727, 2021.

[9] S. Chen, Y. C. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, requirements, and technology trend of 6G: how to tackle the challenges of system coverage, capacity, user data-rate and movement speed," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 218–228, 2020.

[10] X. Y. Hu and E. Eleftheriou, "Binary representation of cycle Tanner-graph GF(2^b) codes," in *2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577)*, pp. 528–532, Paris, France, June 2004.

[11] H. Song, J. Liu, and B. V. K. VijayaKumar, "Large girth cycle codes for partial response channels," *IEEE Transactions on Magnetics*, vol. 40, no. 4, pp. 3084–3086, 2004.

[12] Ronghui Peng and Rong-Rong Chen, "Application of nonbinary LDPC cycle codes to MIMO channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2020–2026, 2008.

[13] X. Liu, F. Xiong, Z. Zhou, Y. Yin, and L. Zhang, "Construction of QC LDPC cycle codes over GF(q) based on cycle entropy and applications on patterned media storage," *IEEE Transactions on Magnetics*, vol. 51, no. 11, pp. 1–5, 2015.

[14] Shumei Song, Bo Zhou, Shu Lin, and K. Abdel-Ghaffar, "A unified approach to the construction of binary and nonbinary quasi-cyclic LDPC codes based on finite fields," *IEEE Transactions on Communications*, vol. 57, no. 1, pp. 84–93, 2009.

[15] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "A matrix-theoretic approach to the construction of non-binary quasi-cyclic LDPC codes," *IEEE Transactions on Communications*, vol. 63, no. 4, pp. 1057–1068, 2015.

[16] H. Xu, C. Chen, M. Zhu, B. Bai, and B. Zhang, "Nonbinary LDPC cycle codes: efficient search, design, and code optimization," *Science China Information Sciences*, vol. 61, no. 8, pp. 089303:1–089303:3, 2018.

[17] H. Xu, H. Li, M. Xu, D. Feng, and H. Zhu, "Two classes of QC-LDPC cycle codes approaching Gallager lower bound," *Science China Information Sciences*, vol. 62, no. 10, pp. 209305:1–209305:3, 2019.

[18] W. E. Ryan and S. Lin, *Channel Codes: Classical and Modern*, Cambridge Univ. Press, New York, USA, 2009.

[19] C. Chen, B. Bai, G. Shi, X. Wang, and X. Jiao, "Nonbinary LDPC codes on cages: structural property and code

optimization," *IEEE Transactions on Communications*, vol. 63, no. 2, pp. 364–375, 2015.

[20] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1788–1793, 2004.

[21] J. Li, K. Liu, S. Lin, K. Abdel-Ghaffar, and R. E. Ryan, "An unnoticed strong connection between algebraic-based and protograph-based LDPC codes, part I: binary case and interpretation," in *2015 Information Theory and Applications Workshop (ITA)*, pp. 36–50, San Diego, CA, USA, February 2015.

[22] S. Zhao and X. Ma, "Construction of high-performance array-based non-binary LDPC codes with moderate rates," *IEEE Communications Letters*, vol. 20, no. 1, pp. 13–16, 2016.

[23] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.

[24] R. J. McEliece, D. J. C. MacKay, and Jung-Fu Cheng, "Turbo decoding as an instance of Pearl's 'belief propagation' algorithm," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 2, pp. 140–152, 1998.

[25] X. Jiang, X. G. Xia, and M. H. Lee, "Efficient progressive edge-growth algorithm based on Chinese remainder theorem," *IEEE Transactions on Communications*, vol. 62, no. 2, pp. 442–451, 2014.

[26] Q. Diao, J. Li, S. Lin, and I. Blake, "New classes of partial geometries and their associated LDPC codes," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 2947–2965, 2016.

[27] X. Jiang, H. Hai, H. M. Wang, and M. H. Lee, "Constructing large girth QC protograph LDPC codes based on PSD-PEG algorithm," *IEEE Access*, vol. 5, pp. 13489–13500, 2017.

[28] X. Qin, C. Yang, Z. Zheng, and Z. Wang, "Optimization of QC-LDPC codes by edge exchange method based on ACE," *IEEE Photonics Technology Letters*, vol. 31, no. 17, pp. 1401–1404, 2019.

[29] 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.

[30] G. Wu, Y. Lv, and J. He, "Design of high-rate LDPC codes based on matroid theory," *IEEE Communications Letters*, vol. 23, no. 12, pp. 2146–2149, 2019.

[31] X. Tao, Y. Xin, B. Wang, and L. Chang, "Layered construction of quasi-cyclic LDPC codes," *IEEE Communications Letters*, vol. 24, no. 5, pp. 946–950, 2020.

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

[33] A. Dehghan and A. H. Banihashemi, "On finding bipartite graphs with a small number of short cycles and large girth," *IEEE Transactions on Information Theory*, vol. 66, no. 10, pp. 6024–6036, 2020.

[34] C. Poulliat, M. Fossorier, and D. Declercq, "Design of regular $(2, d_c)$-LDPC codes over GF(q) using their binary images," *IEEE Transactions on Communications*, vol. 56, no. 10, pp. 1626–1635, 2008.

[35] A. Tasdighi, A. H. Banihashemi, and M. R. Sadeghi, "Efficient search of girth-optimal QC-LDPC codes," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 1552–1564, 2016.

[36] H. Xu, B. Bai, M. Zhu, B. Zhang, and Y. Zhang, "Construction of short-block nonbinary LDPC codes based on cyclic codes," *China Communications*, vol. 14, no. 8, pp. 1–9, 2017.

[37] M. Karimi and A. H. Banihashemi, "Counting short cycles of quasi cyclic protograph LDPC codes," *IEEE Communications Letters*, vol. 16, no. 3, pp. 400–403, 2012.

[38] M. Karimi and A. H. Banihashemi, "Message-passing algorithms for counting short cycles in a graph," *IEEE Transactions on Communications*, vol. 61, no. 2, pp. 485–495, 2013.

[39] A. Dehghan and A. H. Banihashemi, "On computing the number of short cycles in bipartite graphs using the spectrum of the directed edge matrix," *IEEE Transactions on Information Theory*, vol. 66, no. 10, pp. 6037–6047, 2020.

[40] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Algebraic quasi-cyclic LDPC codes: construction, low error-floor, large girth and a reduced-complexity decoding scheme," *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 2626–2637, 2014.

[41] J. Kang, Q. Huang, L. Zhang, B. Zhou, and S. Lin, "Quasi-cyclic LDPC codes: an algebraic construction," *IEEE Transactions on Communications*, vol. 58, no. 5, pp. 1383–1396, 2010.

[42] L. Zhang, S. Lin, K. Abdel-Ghaffar, Z. Ding, and B. Zhou, "Quasi-cyclic LDPC codes on cyclic subgroups of finite fields," *IEEE Transactions on Communications*, vol. 59, no. 9, pp. 2330–2336, 2011.

[43] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. F. Blake, "Quasi-cyclic LDPC codes: an algebraic construction, rank analysis, and codes on Latin squares," *IEEE Transactions on Communications*, vol. 58, no. 11, pp. 3126–3139, 2010.

[44] H. Xu, D. Feng, R. Luo, and B. Bai, "Construction of quasi-cyclic LDPC codes via masking with successive cycle elimination," *IEEE Communications Letters*, vol. 20, no. 12, pp. 2370–2373, 2016.

[45] H. Zhu, B. Zhang, M. Xu, H. Li, and H. Xu, "Array based quasi-cyclic LDPC codes and their tight lower bounds on the lifting degree," *Physical Communication*, vol. 36, p. 100765, 2019.

[46] Xiao-Yu Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 386–398, 2005.