Research Article

Construction of Quasi-Cyclic LDPC Codes Based on Fundamental Theorem of Arithmetic

Hai Zhu ¹, Liqun Pu,² Hengzhou Xu ¹, and Bo Zhang¹

¹School of Network Engineering, Zhoukou Normal University, Zhoukou, China

²School of Mathematics and Statistics, Zhengzhou University, Zhengzhou, China

Correspondence should be addressed to Hai Zhu; zhu_sea@163.com and Hengzhou Xu; hzzxu@zknz.edu.cn

Received 23 November 2017; Revised 5 February 2018; Accepted 7 March 2018; Published 15 April 2018

Academic Editor: Qin Huang

Copyright © 2018 Hai Zhu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Quasi-cyclic (QC) LDPC codes play an important role in 5G communications and have been chosen as the standard codes for 5G *enhanced mobile broadband* (eMBB) data channel. In this paper, we study the construction of QC LDPC codes based on an arbitrary given expansion factor (or lifting degree). First, we analyze the cycle structure of QC LDPC codes and give the necessary and sufficient condition for the existence of short cycles. Based on the fundamental theorem of arithmetic in number theory, we divide the integer factorization into three cases and present three classes of QC LDPC codes accordingly. Furthermore, a general construction method of QC LDPC codes with girth of at least 6 is proposed. Numerical results show that the constructed QC LDPC codes perform well over the AWGN channel when decoded with the iterative algorithms.

1. Introduction

Low-density parity-check (LDPC) codes [1] are a class of modern channel coding. Because of the advantages of approaching the Shannon capacity and the iterative decoding algorithms with lower complexity, LDPC codes have been attracting great interests of the industries and academia. For various specific communication systems [2–4], LDPC codes have been well designed and chosen as their standard codes. As an important scenario of 5G communications, the *enhanced mobile broadband* (eMBB) data channel had adopted the LDPC coding scheme [5], and LDPC codes have recently been determined after several rounds of discussions [6–12]. However, the other two scenarios of 5G communications, that is, *ultrareliable and low latency communications* (URLLC) and *massive machine-type-communication* (mMTC), have no candidate channel coding at present. The promising coding techniques for 5G communication systems are turbo codes, binary/nonbinary LDPC codes, spatially coupled (SC) LDPC codes [13], block Markov superposition transmission (BMST) [14], and polar codes. The encoding/decoding complexity, performance, spectral efficiency, and robustness comparisons among them can be found in [15]. Recently, some low-complexity decoding algorithms

of these modern channel codes have been proposed [16, 17]. These significant works can facilitate and accelerate the applications of these modern coding techniques in 5G communications. According to the definition and description of URLLC and mMTC provided by ITU-R [18], these two scenarios require low latency and high reliability. That is, short data package communication which has no visible error floor down to block error rate (BLER) of 10^{-5} should be considered. Research results [19] show that LDPC codes have good performance in the waterfall and error-floor region. Moreover, LDPC codes have good robust property [15, 20] and then their good performance can be also obtained over various channels. Hence, LDPC coding still has a strong competitiveness in the applications of URLLC and mMTC.

LDPC codes can be divided into two major classes: (1) random-like codes constructed by means of computer search under the efficient algorithms [21, 22] and (2) structured codes constructed based on algebraic tools, combinatorial structures, and graphs, such as finite geometries [23], finite fields [24], balanced incomplete block designs (BIBDs) [20], resolvable group divisible designs (RGDDs) [25], and protographs [26, 27]. Research results show that well designed algebraic-based LDPC codes have no error floor at the bit error rate (BER) down to 10^{-15} [28]. To

facilitate implementation, LDPC codes usually have some special structures, such as diagonal structure and quasi-cyclic (QC) structure. In general, quasi-cyclic (QC) LDPC codes [29] have advantages of encoding and decoding with low complexity [30, 31], easy hardware implementation [32], and good iterative performance [33], and then they have attracted comprehensive attention.

In order to support lots of data packets with various lengths in the eMBB scenario of 5G communications, the designed 5G LDPC codes are chosen as rate-compatible (RC) QC LDPC codes. Notice that the number of expansion factors (or lifting degrees) of 5G QC LDPC codes is not much. On the other hand, some encoding algorithms [34] are only suitable for QC LDPC codes with certain expansion factor (or lifting degree). Furthermore, the encoding and decoding of QC LDPC codes with expansion factors (or lifting degrees) being the power of two can be easily implemented by linear shift registers. Hence, it is interesting to construct QC LDPC codes from an arbitrary given expansion factor (or lifting degree).

In this paper, we focus on the construction of QC LDPC codes from given expansion factors (or lifting degrees). We first introduce the fundamental theorem of arithmetic in number theory and divide the integer factorization into three categories. By analyzing the cycle structure of QC LDPC codes, we present three classes of QC LDPC codes based on three families of integers. Furthermore, a general construction of QC LDPC codes with girth of at least 6 based on the fundamental theorem of arithmetic is proposed. Finally, in order to show the good performance of our constructed QC LDPC codes, numerical simulation results are provided.

The rest of this paper is organized as follows. Section 2 introduces the fundamentals of number theory, the definitions, basic concepts, and cycle structure of QC LDPC codes. Section 3 presents three classes of QC LDPC codes and a general construction method. Numerical results are also provided in this section. Finally, Section 4 concludes this paper.

2. Preliminaries

2.1. Fundamentals of Number Theory

Theorem 1. Every composite number, which is greater than one, factors uniquely as a product of prime numbers.

This theorem is the well-known fundamental theorem of arithmetic in number theory, and it had been proved by Gauss and Clarke [36]. This theorem is also called the unique factorization theorem. That is, every integer greater than one is either prime itself or the product of the prime numbers and this product is unique, up to the order of the factors. For example, $1400 = 14 \times 100 = 2 \times 7 \times 2 \times 2 \times 5 \times 5 = 2^3 \times 5^2 \times 7$. This theorem is twofold: first, 1400 can be written as a product of the primes, and second, no matter how this is done, there will always be three 2s, two 5s, one 7, and no other primes in this product. Hence, for a given integer $L \geq 2$, L can be represented by the unique product; that is,

$$L = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}, \quad (1)$$

where $p_1, p_2, \dots, p_k$ are prime numbers.

The following three lemmas and one theorem are useful for constructing QC LDPC codes with girth of at least 6.

Lemma 2. Let p be a prime, and let e_1 and e_2 be two positive integers. If a and b are two integers for $1 \leq a \leq p^{e_1} - 1$ and $1 \leq b \leq p^{e_2} - 1$, then $ab \not\equiv 0 \pmod{p^{e_1+e_2}}$.

Proof. Since a and b are two integers with $1 \leq a \leq p^{e_1} - 1$ and $1 \leq b \leq p^{e_2} - 1$, then

$$1 = 1 \times 1 \leq a \times b \leq (p^{e_1} - 1)(p^{e_2} - 1) < p^{e_1+e_2}. \quad (2)$$

That is, $ab \not\equiv 0 \pmod{p^{e_1+e_2}}$. $\square$

Lemma 3. Let p_1 and p_2 be two different primes, and let e_1 and e_2 be two positive integers. If a and b are two integers for $1 \leq a \leq p_1^{e_1} - 1$ and $1 \leq b \leq p_2^{e_2} - 1$, then $ab \not\equiv 0 \pmod{p_1^{e_1} p_2^{e_2}}$.

Proof. Since a and b are two integers with $1 \leq a \leq p_1^{e_1} - 1$ and $1 \leq b \leq p_2^{e_2} - 1$, then

$$1 \leq a \times b \leq (p_1^{e_1} - 1)(p_2^{e_2} - 1) < p_1^{e_1} p_2^{e_2}. \quad (3)$$

That is, $ab \not\equiv 0 \pmod{p_1^{e_1} p_2^{e_2}}$. $\square$

Lemma 4. Let $L = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be a positive integer where $p_1, p_2, \dots, p_k$ are k different primes and $e_1, e_2, \dots, e_k$ are k positive integers. If $a = p_i^{e_i}$ and $b = p_j^{e_j}$ with $1 \leq i, j \leq k$ and $i \neq j$, then $ab \not\equiv 0 \pmod{L}$.

Proof. Since $a = p_i^{e_i}$ and $b = p_j^{e_j}$ with $1 \leq i, j \leq k$ and $i \neq j$, then

$$1 \leq a \times b \leq p_i^{e_i} p_j^{e_j} < p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = L. \quad (4)$$

That is, $ab \not\equiv 0 \pmod{L}$. $\square$

Theorem 5. Let L be a positive integer. If a and b are two positive integers and $ab < L$, then $ab \not\equiv 0 \pmod{L}$.

Proof. Since a and b are two positive integers and $ab < L$, then

$$1 \leq ab < L. \quad (5)$$

That is, $ab \not\equiv 0 \pmod{L}$. $\square$

2.2. QC LDPC Codes and Their Associated Tanner Graphs. A (γ, ρ) -regular quasi-cyclic (QC) LDPC code [29] of length ρL can be completely specified by the null space of the following matrix over $\text{GF}(2)$:

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}(p_{0,0}) & \mathbf{I}(p_{0,1}) & \cdots & \mathbf{I}(p_{0,\rho-1}) \\ \mathbf{I}(p_{1,0}) & \mathbf{I}(p_{1,1}) & \cdots & \mathbf{I}(p_{1,\rho-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}(p_{\gamma-1,0}) & \mathbf{I}(p_{\gamma-1,1}) & \cdots & \mathbf{I}(p_{\gamma-1,\rho-1}) \end{bmatrix}, \quad (6)$$

where, for $0 \leq i \leq \gamma - 1$ and $0 \leq j \leq \rho - 1$, $\mathbf{I}(p_{i,j})$ is an $L \times L$ circulant permutation matrix (CPM) with a one at column- $(r + p_{i,j}) \pmod{L}$ for row- r , $0 \leq r \leq L - 1$, and zero elsewhere.

FIGURE 1: Tanner graph of $\mathbf{H}$.

It is clear that $\mathbf{I}(0)$ represents the $L \times L$ identity matrix. Notice that the parameter L is referred to as the *expansion factor* (or *lifting degree*) [37]. It can be easily observed that the positions of nonzero elements in $\mathbf{H}$ are uniquely determined by the following matrix, called *permutation shift matrix* or *exponent matrix*:

$$\mathbf{P} = \begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,\rho-1} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,\rho-1} \\ \vdots & \vdots & \ddots & \vdots \\ p_{\gamma-1,0} & p_{\gamma-1,1} & \cdots & p_{\gamma-1,\rho-1} \end{bmatrix}. \quad (7)$$

That is, there is a one-to-one correspondence between $\mathbf{P}$ and $\mathbf{H}$.

An LDPC code is commonly described by a bipartite graph known as Tanner graph [38] in coding theory. Tanner graph of $\mathbf{H}$, denoted by $\mathcal{G}(V, C)$, consists of a set V of variable nodes (containing pL code symbols of a code word) and a set C of check nodes (containing γL local check-sum constraints on the code symbols). An edge in $\mathcal{G}(V, C)$ connects the variable node i to the check node j if and only if the element at column- i and row- j of $\mathbf{H}$ is nonzero. A cycle is formed by a sequence of vertices (or edges) in $\mathcal{G}(V, C)$ which starts and ends at the same vertex (or edge) and contains other vertices (or edges) not more than once. The cycle of length k is denoted as k -cycle for short and the length of the shortest cycle is called the girth of $\mathcal{G}(V, C)$ (or an LDPC code). As an example, Figure 1 shows the Tanner graph of $\mathbf{H}$ and an associate 6-cycle.

In graph theory, the biadjacency matrix $\mathbf{A} = [a_{ij}]$ of a bipartite graph $\mathcal{G}(U, V)$ can be constructed as follows. The rows of $\mathbf{A}$ are labeled by the $|U|$ vertices in U and the columns are labeled by $|V|$ vertices in V . The element a_{ij} at the row labeled by the vertex $i \in U$ and the column labeled by the vertex $j \in V$ is 1 if and only if there exists an edge between the vertices i and j and otherwise 0. Actually, for an LDPC code given by the null space of $\mathbf{H}$, $\mathbf{H}$ is the biadjacency matrix of its relevant Tanner graph $\mathcal{G}(V, C)$.

Moreover, isomorphism theory of QC LDPC codes was proposed in [39–41] based on the isomorphism of graphs in graph theory. According to the isomorphism of QC LDPC

codes, the parity-check matrix in (6) can be simplified as the following matrix:

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}(0) & \mathbf{I}(0) & \cdots & \mathbf{I}(0) \\ \mathbf{I}(0) & \mathbf{I}(p_{1,1}) & \cdots & \mathbf{I}(p_{1,\rho-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}(0) & \mathbf{I}(p_{\gamma-1,1}) & \cdots & \mathbf{I}(p_{\gamma-1,\rho-1}) \end{bmatrix}. \quad (8)$$

That is, $p_{i,0} = p_{0,j} = 0$ for $0 \leq i \leq \gamma - 1$, $0 \leq j \leq \rho - 1$. Equivalently, its exponent matrix is

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & p_{1,1} & \cdots & p_{1,\rho-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & p_{\gamma-1,1} & \cdots & p_{\gamma-1,\rho-1} \end{bmatrix}. \quad (9)$$

That is why the elements in the first row and first column of the exponent matrix $\mathbf{P}$ are usually set to 0 in the research process [29, 42]. Hence, we only consider such $\mathbf{H}$ and $\mathbf{P}$ in the following discussions.

2.3. Cycle Structure of QC LDPC Codes. Consider a QC LDPC code $\mathcal{C}$ given by the null space of $\mathbf{H}$ in (8). It can be seen from [29] that a cycle in the Tanner graph of $\mathcal{C}$ is associated with a family of the ordered CPMs in $\mathbf{H}$. As shown in [29], a $2i$ -cycle in the Tanner graph of the code $\mathcal{C}$ (or $\mathbf{H}$) is represented by an ordered sequence of CPMs

$$\mathbf{I}(p_{j_0,k_0}), \mathbf{I}(p_{j_1,k_0}), \mathbf{I}(p_{j_1,k_1}), \mathbf{I}(p_{j_2,k_1}), \mathbf{I}(p_{j_2,k_2}), \dots, \mathbf{I}(p_{j_{i-1},k_{i-1}}), \mathbf{I}(p_{j_0,k_0}), \quad (10)$$

where $j_i = j_0$, $k_i = k_0$, $0 \leq j_m \leq \gamma - 1$, $j_{m-1} \neq j_m$, $0 \leq k_m \leq \rho - 1$, and $k_{m-1} \neq k_m$ for $1 \leq m \leq i$. The above sequence can be simplified as

$$\mathbf{I}(p_{j_0,k_0}), \mathbf{I}(p_{j_1,k_1}), \mathbf{I}(p_{j_2,k_2}), \dots, \mathbf{I}(p_{j_{i-1},k_{i-1}}). \quad (11)$$

It can be seen that such a $2i$ -cycle corresponds to the elements $p_{j_0,k_0}, p_{j_1,k_1}, p_{j_2,k_2}, \dots, p_{j_{i-1},k_{i-1}}$ in the exponent matrix $\mathbf{P}$. Furthermore, short cycles of QC LDPC codes can be determined by the elements of $\mathbf{P}$ [39, 40].

FIGURE 2: The structure of $2i$ -cycle and nonexistence of the $4i$ -cycle.

Let g be the girth of the code $\mathcal{C}$. It can be seen from [43] that, for $g \leq 2i \leq 2g-2$, the necessary and sufficient condition for the existence of a $2i$ -cycle in the Tanner graph of the code $\mathcal{C}$ (or $\mathbf{H}$) can be generalized as follows:

$$\sum_{m=0}^{i-1} (p_{j_m, k_m} - p_{j_{m+1}, k_{m+1}}) = 0 \pmod{L} \quad (12)$$

with $j_0 = j_i$, $k_0 = k_i$, $k_m \neq k_{m+1}$, and $j_m \neq j_{m+1}$. Note that (12) is not the sufficient condition for the existence of a $2i$ -cycle in the Tanner graph of the code $\mathcal{C}$ (or $\mathbf{H}$) for $2i \geq 2g$, but it is the necessary condition. Here we give a counterexample. Consider a $2i$ -cycle ($i \geq g$) whose cycle structure is given in Figure 2. Clearly, (12) is satisfied. Let $p_{j_m, k_m} = p_{j_{m+1}, k_{m+1}}$ for $0 \leq m \leq i-1$, and $j_0 = j_{2i}$, $k_0 = k_{2i}$, $k_m \neq k_{m+1}$, $j_m \neq j_{m+1}$. According to (12), we have

$$\begin{aligned} \sum_{n=0}^{2i-1} (p_{j_n, k_n} - p_{j_{n+1}, k_{n+1}}) &= 2 \sum_{m=0}^{i-1} (p_{j_m, k_m} - p_{j_{m+1}, k_{m+1}}) \\ &= 0 \pmod{L}, \end{aligned} \quad (13)$$

where $j_0 = j_i = j_{2i}$, $k_0 = k_i = k_{2i}$, $k_n \neq k_{n+1}$, $j_n \neq j_{n+1}$, for $0 \leq n \leq 2i-1$. That is, the ordered elements $p_{j_0, k_0}, p_{j_1, k_0}, p_{j_1, k_1}, \dots, p_{j_0, k_{2i-1}}$ (i.e., $p_{j_0, k_0}, p_{j_1, k_0}, p_{j_1, k_1}, \dots, p_{j_0, k_{i-1}}, p_{j_0, k_0}, p_{j_1, k_0}, p_{j_1, k_1}, \dots, p_{j_0, k_{2i-1}}$) make (12) hold, but they do not determine a $4i$ -cycle. A visual representation is depicted in Figure 2. Therefore, (4) in [29] and (3) in [39] are not applicable to the cycles with lengths larger than $2g-2$.

3. Construction of Quasi-Cyclic LDPC Codes with Girth of at Least 6

Based on the aforementioned, there exists a one-to-one correspondence between the exponent matrix $\mathbf{P}$ and the parity-check matrix $\mathbf{H}$ of a QC LDPC code. Hence, construction of a QC LDPC code is equivalent to the design of its exponent matrix $\mathbf{P}$. In this section, we present three classes of QC LDPC codes with girth of at least 6 and then give a general construction of QC LDPC codes with girth of at least 6 based on an arbitrary integer.

First, we design the exponent matrix $\mathbf{P}$ in (9) as follows:

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & p_{1,1} & \cdots & p_{1,\rho-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & p_{\gamma-1,1} & \cdots & p_{\gamma-1,\rho-1} \end{bmatrix}, \quad (14)$$

where $p_{i,j} = i \times j \pmod{L}$ for $1 \leq i \leq \gamma-1$, $1 \leq j \leq \rho-1$. Second, we replace the 0s and $p_{i,j}$ in the designed exponent matrix $\mathbf{P}$ with CPMs $\mathbf{I}(0)$ and $\mathbf{I}(p_{i,j})$ of the same size $L \times L$, respectively, and then obtain a $\gamma \times \rho$ array $\mathbf{H}$ of $L \times L$ CPMs. This array is a $\gamma L \times \rho L$ matrix over $\text{GF}(2)$ with column and row weights γ and ρ , respectively. The null space of this matrix gives a (γ, ρ) -regular QC LDPC code.

Remark 6. As shown in [44], girth and short cycles play an important role in the design of LDPC codes. If the above constructed (γ, ρ) -regular QC LDPC code does not have good iterative performance, we can replace some CPMs in the above array $\mathbf{H}$ with zero matrices (ZMs) of the same size to reduce the number of short cycles and possibly enlarge the girth value. This replacement is called masking. On the other hand, if the lengths of the desired QC LDPC codes are shorter than ρL or they require much higher code rates, then we can take a $\gamma' \times \rho'$ subarray of the designed array $\mathbf{H}$, where $\gamma' \leq \gamma$ and $\rho' \leq \rho$. Notice that this subarray can be obtained from the following two steps: (1) Choose the first γ' row-CPMs of the designed array $\mathbf{H}$; (2) select ρ' column-CPMs from ρ column-CPMs of the designed array $\mathbf{H}$. In this paper, both the masking technique and the selection method in [43] are employed to construct (or further optimize) QC LDPC codes.

3.1. Three Classes of QC LDPC Codes with Girth of at Least 6. Based on (12), we can see that Tanner graph of the designed array $\mathbf{H}$ contains a 4-cycle if and only if the following equation is satisfied:

$$\begin{aligned} \sum_{m=0}^1 (p_{j_m, k_m} - p_{j_{m+1}, k_{m+1}}) &= (j_0 - j_1)(k_0 - k_1) \\ &= 0 \pmod{L}, \end{aligned} \quad (15)$$

where $j_0 \neq j_1$ and $k_0 \neq k_1$. It can be observed that the existence of 4-cycles in the Tanner graph of the designed array $\mathbf{H}$ is related to L . According to the fundamental theorem of arithmetic, the values of L can be divided into three categories and three classes of QC LDPC codes with girth of at least 6 are proposed. Notice that all numerical simulations in the following examples, *binary phase shift keying* (BPSK), *additive white Gaussian noise* (AWGN) channel, and the *sum-product algorithm* (SPA), are assumed.

3.1.1. The Case of $L = p^e$. Let $L = p^e$, where p is a prime and e is a positive integer, and let $e = e_1 + e_2$, where e_1, e_2 are two positive integers and $e_1 \leq e_2$. Consider $\gamma = p^{e_1}$ and $\rho = p^{e_2}$. Since $1 \leq j_0, j_1 \leq p^{e_1} - 1$, $1 \leq k_0, k_1 \leq p^{e_2} - 1$, $j_0 \neq j_1$, and $k_0 \neq k_1$, then $1 \leq j_0 - j_1 \leq p^{e_1} - 1$ and $1 \leq k_0 - k_1 \leq p^{e_2} - 1$, where the calculation is taken modulo p^{e_1} and modulo p^{e_2} , respectively. Hence, (15) is not satisfied

according to Lemma 2. That is, Tanner graph of the designed array $\mathbf{H}$ has no 4-cycles and then the constructed QC LDPC codes have girth of at least 6.

Example 7. Consider $L = 256 = 2^8$. Let $\gamma = 2^2$ and $\rho = 2^6$. According to (14), we can obtain the exponent matrix $\mathbf{P}$ of size 4×64 . By employing the method in [43], we select the first 4 rows and the 2nd, 16th, 19th, 35th, 50th, 55th, 62nd, and 63rd columns of $\mathbf{P}$ and construct a 4×8 array $\mathbf{H}$ of 256×256 CPMs by replacing the elements of the selected submatrix with the corresponding CPMs. By using the matrix

$$\mathbf{M}_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \quad (16)$$

to mask $\mathbf{H}$, a 1024×2048 matrix with column and row weights 3 and 6, respectively, is obtained. This matrix gives a $(3, 6)$ -regular $(2048, 1024)$ QC LDPC code. The bit error rates (BERs) of this code decoded by the SPA (5, 10, 20, and 50 iterations) are shown in Figure 3. Also shown in Figure 3 is the performance of the $(3, 6)$ -regular $(2048, 1024)$ algebraic QC LDPC code constructed based on finite field $\text{GF}(p^s)$ [35]. This comparable code is constructed from the prime field $\text{GF}(257)$ and then the CPM size of its parity-check matrix is 256×256 . Notice that the exponent matrix and masking matrix of this comparable code are

$$\mathbf{P}_1 = \begin{bmatrix} 179 & 75 & 202 & 52 & 116 & 24 & 15 & 176 \\ 23 & 179 & 75 & 202 & 52 & 116 & 24 & 15 \\ 25 & 23 & 179 & 75 & 202 & 52 & 116 & 24 \\ 162 & 25 & 23 & 179 & 75 & 202 & 52 & 116 \end{bmatrix}, \quad (17)$$

$$\mathbf{M}_{4 \times 8} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

respectively. It can be observed that these two codes have similar performance when decoded using the SPA with various iterations. It is well known that algebraic-based LDPC codes have fast decoding convergence [19, 45, 46]. That is, the SPA decoding of the proposed LDPC code also converges fast, as shown in Figure 3. We can see that the performance gap between 20 and 50 iterations is less than 0.15 dB at the BER of 10^{-6} , and the gap is also less than 0.25 dB at the BER of 10^{-7} ; hence this code achieves a fast rate of decoding convergence.

3.1.2. The Case of $L = p_1^{e_1} p_2^{e_2}$. Let $L = p_1^{e_1} p_2^{e_2}$, where p_1, p_2 are two different prime numbers and e_1, e_2 are two positive integers. Assume $\gamma = \min\{p_1^{e_1}, p_2^{e_2}\}$ and $\rho = \max\{p_1^{e_1}, p_2^{e_2}\}$. Without loss of generality, $p_1^{e_1} < p_2^{e_2}$ is assumed. Since $1 \leq j_0, j_1 \leq p_1^{e_1} - 1$, $1 \leq k_0, k_1 \leq p_2^{e_2} - 1$, $j_0 \neq j_1$, and $k_0 \neq k_1$, then $1 \leq j_0 - j_1 \leq p_1^{e_1} - 1$ and $1 \leq k_0 - k_1 \leq p_2^{e_2} - 1$, where the calculation is taken modulo $p_1^{e_1}$ and modulo $p_2^{e_2}$, respectively. Hence, (15) is not satisfied according to Lemma 3. That is, Tanner graph of the designed array $\mathbf{H}$ does not contain 4-cycles and the girth of the constructed QC LDPC codes is at least 6.

FIGURE 3: The bit error performance of the proposed $(3, 6)$ -regular $(2048, 1024)$ QC LDPC code and the comparable $(3, 6)$ -regular $(2048, 1024)$ algebraic QC LDPC code [19] in Example 7. The decoding algorithm is the SPA with 5, 10, 20, and 50 iterations.

Example 8. Consider $L = 72 = 2^3 \times 3^2 = 4 \times 18$. Since $12 < 18$, let $\gamma = 2^2$ and $\rho = 18$. According to (14), we can obtain the exponent matrix $\mathbf{P}$ of size 4×18 . By employing the method in [43], we select the first 4 rows and the 1st, 2nd, 3rd, 4th, 5th, 6th, 12th, 13th, 15th, 16th, 17th, and 18th columns of $\mathbf{P}$ and construct a 4×12 array $\mathbf{H}$ of 72×72 CPMs by replacing the elements of the selected submatrix with the corresponding CPMs. By using the matrix

$$\mathbf{M}_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \quad (18)$$

to mask $\mathbf{H}$, a 288×864 matrix with column and row weights 3 and 9, respectively, is obtained. This matrix gives a $(3, 9)$ -regular $(864, 576)$ QC LDPC code. The bit/word error rates (BERs/WERs) of this code decoded by the SPA with 50 iterations are shown in Figure 4. Also shown in Figure 4 is the performance of the $(3, 9)$ -regular $(864, 576)$ algebraic QC LDPC code constructed from the finite field $\text{GF}(73)$ [35]. The exponent and masking matrices of this algebraic QC LDPC code are

$$\mathbf{P}_2 = \begin{bmatrix} 49 & 41 & 21 & 40 & 29 & 71 & 39 & 3 & 58 & 61 & 65 & 52 \\ 23 & 49 & 41 & 21 & 40 & 29 & 71 & 39 & 3 & 58 & 61 & 65 \\ 24 & 23 & 49 & 41 & 21 & 40 & 29 & 71 & 39 & 3 & 58 & 61 \\ 57 & 24 & 23 & 49 & 41 & 21 & 40 & 29 & 71 & 39 & 3 & 58 \end{bmatrix},$$

TABLE 1: The cycle distributions of two (864, 576) QC LDPC codes in Example 8.

Code	4-cycles	6-cycles	8-cycles	10-cycles	12-cycles
Proposed code	0	288	12852	110736	1514772
Algebraic code [35]	0	360	8316	109800	1402308

FIGURE 4: The error performance of the proposed (3,9)-regular (864,576) QC LDPC code and the comparable (3,9)-regular (864,576) algebraic QC LDPC code constructed based on finite field GF (73) [35] in Example 8.

$$\mathbf{M}_{4 \times 12} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad (19)$$

respectively. Notice that the CPM size of this algebraic code is 72×72 . It can be observed that these two codes also have similar performance. Moreover, the cycle distributions of these two codes are given in Table 1. We can see that although the proposed code has fewer shortest cycles than the algebraic QC LDPC code, the proposed code has much more cycles of length 8 than the algebraic QC LDPC code. That is why the proposed code does not perform better than the algebraic QC LDPC code in the high-SNR region.

3.1.3. The Case of $L = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Let $L = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where $p_1, p_2, \dots, p_k$ are k different prime numbers and $e_1, e_2, \dots, e_k$ are k positive integers. Without loss of generality, we assume $p_i^{e_i} < p_j^{e_j}$, where $1 \leq i, j \leq k$, and $i \neq j$. Consider $\gamma = p_i^{e_i}$ and $\rho = p_j^{e_j}$. Since $1 \leq j_0, j_1 \leq p_i^{e_i} - 1$, $1 \leq k_0, k_1 \leq p_j^{e_j} - 1$, $j_0 \neq j_1$, and $k_0 \neq k_1$, then $1 \leq j_0 - j_1 \leq p_i^{e_i} - 1$ and $1 \leq k_0 - k_1 \leq p_j^{e_j} - 1$, where the calculation is taken modulo $p_i^{e_i}$ and modulo $p_j^{e_j}$, respectively. Hence, (15) is not satisfied

according to Lemma 4. That is, Tanner graph of the designed array $\mathbf{H}$ does not have 4-cycles and the constructed QC LDPC codes have girth of at least 6.

Example 9. Consider $L = 105 = 3 \times 5 \times 7$. Since $10 < 21$, let $\gamma = 5$ and $\rho = 21$. According to (14), we can obtain the exponent matrix $\mathbf{P}$ of size 5×21 . By employing the method in [43], we select the first 5 rows and the 1st, 2nd, 3rd, 6th, 7th, 13th, 16th, 17th, 20th, and 21st columns of $\mathbf{P}$ and construct a 5×10 array $\mathbf{H}$ of 105×105 CPMs by replacing the elements of the selected submatrix with the corresponding CPMs. By using the matrix

$$\mathbf{M}_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \quad (20)$$

to mask $\mathbf{H}$, a 525×1050 matrix with column and row weights 3 and 6, respectively, is obtained. This matrix gives a (3,6)-regular (1050, 525) QC LDPC code of girth 8. For comparison, we simultaneously present the simulation for the (3,6)-regular (1050, 525) LDPC code constructed based on the progressive edge-growth (PEG) algorithm [22]. The bit/word error rates (BERs/WERs) of these two codes decoded with the SPA (50 iterations) are shown in Figure 5. It can be seen that although these two codes have similar performance in the waterfall region, the proposed code performs better than the PEG-LDPC code in the high-SNR region.

3.2. A General Construction of QC LDPC Codes from an Arbitrary Positive Integer. For a given positive integer L , we in general find out two positive integers a and b such that $ab \leq L$ and $a, b \geq 3$. Assume $a \leq b$. Consider $\gamma = a$ and $\rho = b$, where $1 \leq i, j \leq k$, and $i \neq j$. Since $1 \leq j_0, j_1 \leq a - 1$, $1 \leq k_0, k_1 \leq b - 1$, $j_0 \neq j_1$, and $k_0 \neq k_1$, then $1 \leq j_0 - j_1 \leq a - 1$ and $1 \leq k_0 - k_1 \leq b - 1$, where the calculation is taken modulo a and modulo b , respectively. Hence, (15) is not satisfied according to Theorem 5. That is, Tanner graph of the designed array $\mathbf{H}$ does not have 4-cycles and the constructed QC LDPC codes have girth of at least 6.

Example 10. Consider $L = 127 > 4 \times 31$, and let $\gamma = 4$, $\rho = 31$. According to (14), we can obtain the exponent matrix $\mathbf{P}$ of size 4×31 . By employing the method in [43], we select the first 4 rows and the 1st, 2nd, 6th, 7th, 22nd, 26th, 29th, and 31st columns of $\mathbf{P}$ and construct a 4×8 array $\mathbf{H}$ of 127×127 CPMs by replacing the elements of the selected submatrix with the

FIGURE 5: The error performance of the proposed (3,6)-regular (1050, 525) QC LDPC code and the comparable (3,6)-regular (1050, 525) QC LDPC code constructed based on the PEG algorithm [22] in Example 9.

corresponding CPMs. By using the method in [43], we design a masking matrix, that is,

$$\mathbf{M}_4 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}; \quad (21)$$

to mask $\mathbf{H}$, a 508×1016 matrix with column and row weights 3 and 6, respectively, is obtained. This matrix gives a (3,6)-regular (1016, 508) QC LDPC code of girth 8. For comparison, we also construct a (3,6)-regular (1016, 508) QC LDPC code based on the partial geometry [28]. Note that the exponent matrix of this code is

$$\mathbf{P}_3 = \begin{bmatrix} 2 & 83 & 33 & 46 & 36 & 94 & 42 & 86 \\ 109 & 15 & 84 & 94 & 57 & 43 & 3 & 115 \\ 112 & 76 & 70 & 36 & 111 & 57 & 66 & 117 \\ 31 & 80 & 67 & 78 & 50 & 60 & 16 & 63 \end{bmatrix}, \quad (22)$$

and the masking matrix is also $\mathbf{M}_{4 \times 8}$ in Example 7. The bit/word error performance of these two codes decoded by the SPA with 50 iterations is shown in Figure 6. It can be seen that these two codes have similar performance. We can also observe from Figure 6 that, for the proposed QC LDPC code, there are no error floors in the BER curves down to $\text{BER} = 2.27 \times 10^{-7}$ and in the WER curves down to $\text{WER} = 3.5 \times 10^{-6}$.

4. Conclusion

In this paper, based on the fundamental theorem of arithmetic, we presented a method for constructing QC LDPC codes with girth of at least 6 from an arbitrary integer. According to the integer factorization, we divided the integers

FIGURE 6: The bit error performance of the proposed (3,6)-regular (1016, 508) QC LDPC code and the comparable (3,6)-regular (1016, 508) QC LDPC code constructed from partial geometry [28] in Example 10.

into three categories and then constructed three classes of QC LDPC codes. Furthermore, a general construction of QC LDPC codes with girth of at least 6 was proposed. Numerical results show that the constructed QC LDPC codes have good performance over the AWGN channel and converge fast under iterative decoding. In other words, for an arbitrary integer $L(\geq 6)$, we can easily construct QC LDPC codes whose parity-check matrices consist of several CPMs and/or zero matrices of size $L \times L$, and the proposed method ensured that the resultant QC LDPC codes have girth of at least 6. Moreover, the proposed QC LDPC codes perform as well as the algebraic QC LDPC codes.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61103143, the Joint Funds of the National Natural Science Foundation of China under Grant U1504601, the Key Scientific and Technological Project of Henan under Grants 162102310589, 172102310124, and 182102310867, the Key Scientific Research Projects of Henan Educational Committee under Grant 18B510022, and the School-Based Program of Zhoukou Normal University under Grant ZKNUB2201705.

References

- [1] R. G. Gallager, "Low-Density Parity-Check Codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.

- [2] IEEE Standard, "Air Interface for Fixed Broadband Wireless Access Systems," IEEE Standard P802.16e/D1, 2005.
- [3] European Telecommunications Standards Institute, *Digital Video Broadcasting (DVB)*, European Telecommunications Standards Institute, Sophia Antipolis, France, 2009.
- [4] CCSDS, "Short Block Length LDPC Codes for TC Synchronization and Channel Coding," CCSDS 231.1-O-1, 2015.
- [5] 3GPP, "Document 3GPP chairman's notes 3GPP TSG RAN WG1 meeting 87," 2016, <https://www.3gpp.org>.
- [6] 3GPP, "Document 3GPP chairman's notes 3GPP TSG RAN WG1 meeting AH NR1," 2017, <https://www.3gpp.org>.
- [7] 3GPP, "Document 3GPP chairman's notes 3GPP TSG RAN WG1 meeting 88," 2017, <https://www.3gpp.org>.
- [8] 3GPP, "Document 3GPP chairman's notes 3GPP TSG RAN WG1 meeting 88bis," 2017, <https://www.3gpp.org>.
- [9] 3GPP, "Document 3GPP chairman's notes 3GPP TSG RAN WG1 meeting 89," 2017, <https://www.3gpp.org>.
- [10] 3GPP, "Document 3GPP chairman's notes 3GPP TSG RAN WG1 meeting AH NR2," 2017, <https://www.3gpp.org>.
- [11] 3GPP, "Document 3GPP R1-1711982 3GPP TSG RAN WG1 meeting AH NR2," 2017, <https://www.3gpp.org>.
- [12] 3GPP, "Document 3GPP R1-1712254 3GPP TSG RAN WG1 meeting 90," 2017, <https://www.3gpp.org>.
- [13] M. Zhang, Z. Wang, Q. Huang, and S. Wang, "Time-Invariant Quasi-Cyclic Spatially Coupled LDPC Codes Based on Packings," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 4936–4945, 2016.
- [14] X. Ma, K. Huang, and B. Bai, "Systematic block Markov superposition transmission of repetition codes," *IEEE Transactions on Information Theory*, vol. 64, no. 3, pp. 1604–1620, 2018.
- [15] B. Bai, "Nonbinary LDPC coding for 5G communication systems," in *Proceedings of the 10th International Conference on Information, Communications and Signal Processing (ICICS'15)*, pp. 2–4, Singapore, 2015.
- [16] 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.
- [17] Q. Huang, L. Song, and Z. Wang, "Set Message-Passing Decoding Algorithms for Regular Non-Binary LDPC Codes," *IEEE Transactions on Communications*, 2017.
- [18] 3GPP, "Study on scenarios and requirements for next generation access technologies," Technical Report (TR) 38.913, 2016.
- [19] W. Ryan and S. Lin, *Channel Codes: Classical and Modern*, Cambridge University Press, New York, NY, USA, 2009.
- [20] L. Lan, Y. Y. Tai, S. Lin, B. Memari, and B. Honary, "New constructions of quasi-cyclic LDPC codes based on special classes of BIBD's for the AWGN and binary erasure channels," *IEEE Transactions on Communications*, vol. 56, no. 1, pp. 39–48, 2008.
- [21] T. Tian, C. Jones, J. D. Villasenor, and R. D. Wesel, "Construction of irregular LDPC codes with low error floors," in *Proceedings of the International Conference on Communications (ICC'03)*, pp. 3125–3129, 2003.
- [22] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 51, no. 1, pp. 386–398, 2005.
- [23] Q. Diao, Y. Y. Tai, S. Lin, and K. Abdel-Ghaffar, "LDPC codes on partial geometries: construction, trapping set structure, and puncturing," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 59, no. 12, pp. 7898–7914, 2013.
- [24] S. Song, B. Zhou, S. Lin, and K. Abdel-Ghaffar, "A unified approach to the construction of binary and nonbinary quasi-cyclic LDPC codes based on finite fields," *IEEE Transactions on Communications*, vol. 57, no. 1, pp. 84–93, 2009.
- [25] H. Xu, D. Feng, C. Sun, and B. Bai, "Construction of LDPC codes based on resolvable group divisible designs," in *Proceedings of the International Workshop on High Mobility Wireless Communications (HMWC'15)*, pp. 111–115, 2015.
- [26] D. Divsalar, S. Dolinar, C. R. Jones, and K. Andrews, "Capacity-approaching protograph codes," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 6, pp. 876–888, 2009.
- [27] D. G. Mitchell, R. Smarandache, and J. Costello, "Quasi-cyclic LDPC codes based on pre-lifted protographs," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 60, no. 10, pp. 5856–5874, 2014.
- [28] Q. Diao, J. Li, S. Lin, and I. F. Blake, "New classes of partial geometries and their associated LDPC codes," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 62, no. 6, pp. 2947–2965, 2016.
- [29] M. P. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 50, no. 8, pp. 1788–1793, 2004.
- [30] Z. Li, L. Chen, L. Zeng, S. Lin, and W. H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," *IEEE Transactions on Communications*, vol. 54, no. 1, pp. 71–81, 2006.
- [31] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Decoding of quasi-cyclic LDPC codes with section-wise cyclic structure," in *Proceedings of the IEEE Information Theory and Applications Workshop (ITA'14)*, pp. 1–10, Calif, USA, 2014.
- [32] F. Cai, X. Zhang, D. Declercq, S. K. Planjery, and B. Vasic, "Finite alphabet iterative decoders for LDPC codes: optimization, architecture and analysis," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 5, pp. 1366–1375, 2014.
- [33] H. Liu, Q. Huang, G. Deng, and J. Chen, "Quasi-cyclic representation and vector representation of RS-LDPC Codes," *IEEE Transactions on Communications*, vol. 63, no. 4, pp. 1033–1042, 2015.
- [34] Q. Huang, L. Tang, S. He, Z. Xiong, and Z. Wang, "Low-complexity encoding of quasi-cyclic codes based on Galois Fourier transform," *IEEE Transactions on Communications*, vol. 62, no. 6, pp. 1757–1767, 2014.
- [35] 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.
- [36] C. F. Gauss and A. A. Clarke, *Disquisitiones arithmeticae (Second, corrected edition)*, Springer, New York, NY, USA, 1966.
- [37] J. Li, K. Liu, S. Lin, K. Abdel-Ghaffar, and W. E. Ryan, "An unnoticed strong connection between algebraic-based and protograph-based LDPC codes, Part I: Binary case and interpretation," in *Proceedings of the Information Theory and Applications Workshop (ITA'15)*, pp. 36–45, San Diego, Calif, USA, 2015.
- [38] R. M. Tanner, "A recursive approach to low complexity codes," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.
- [39] A. Tasdighi, A. H. Banihashemi, and M.-R. Sadeghi, "Efficient search of girth-optimal QC-LDPC codes," *Institute of Electrical*

- and Electronics Engineers Transactions on Information Theory*, vol. 62, no. 4, pp. 1552–1564, 2016.
- [40] C. Sun, H. Xu, D. Feng, and B. Bai, “(3, L) quasi-cyclic LDPC codes: Simplified exhaustive search and designs,” in *Proceedings of the 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC’16)*, pp. 271–275, Brest, France, 2016.
 - [41] H. Xu, C. Chen, M. Zhu, B. M. Bai, and B. Zhang, “Nonbinary LDPC cycle codes: Efficient search, design, and code optimization,” *Science China Information Sciences*, <http://engine.scichina.com/doi/10.1007/s11432-017-9271-6>.
 - [42] 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.
 - [43] 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.
 - [44] H. Xu and B. Bai, “Superposition Construction of Q-Ary LDPC Codes by Jointly Optimizing Girth and Number of Shortest Cycles,” *IEEE Communications Letters*, vol. 20, no. 7, pp. 1285–1288, 2016.
 - [45] Q. Huang, K. Liu, and Z. Wang, “Low-density arrays of circulant matrices: Rank and row-redundancy, and QC-LDPC codes,” in *Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT 2012*, pp. 3073–3077, USA, July 2012.
 - [46] H. Xu, D. Feng, C. Sun, and B. Bai, “Algebraic-based nonbinary ldpc codes with flexible field orders and code rates,” *China Communications*, vol. 14, no. 4, pp. 111–119, 2017.