IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 15, 2021, accepted February 4, 2021, date of publication February 11, 2021, date of current version February 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3058732

A Note on the Girth of (3, 19)-Regular Tanner's Quasi-Cyclic LDPC Codes

MANJIE ZHOU[1], HAI ZHU[1], HENGZHOU XU[1,2], BO ZHANG[3], AND KAIXUAN XIE[1]
[1]School of Network Engineering, Zhoukou Normal University, Zhoukou 466001, China
[2]School of Mathematical Sciences, Shanghai Jiao Tong University, Shanghai 200240, China
[3]Henan Provincial Research Center of Wisdom Education and Intelligent Technology Application Engineering Technology, Zhengzhou 451460, China

Corresponding authors: Hengzhou Xu (hzxu@zknu.edu.cn) and Kaixuan Xie (kaixuanxiezk@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61801527 and Grant 11971311, in part by the Tianyuan Special Funds of the National Natural Science Foundation of China under Grant 12026231 and Grant 12026230, in part by the Development Project of Henan Provincial Department of Science and Technology under Grant 212102310544, in part by the Natural Science Foundation of Henan under Grant 202300410523, and in part by the Open Research Fund of Henan Provincial Research Center of Wisdom Education and Intelligent Technology Application Engineering Technology under Grant 2019KFJJ008.

ABSTRACT In this article, we study the cycle structure of (3, 19)-regular Tanner's quasi-cyclic (QC) LDPC codes with code length $19p$, where p is a prime and $p \equiv 1 \pmod{57}$, and transform the conditions for the existence of cycles of lengths not more than 10 into polynomial equations in a 57th root of unity of the prime field $\mathbb{F}_p$. By employing the Euclidean division algorithm to check whether these equations have solutions over the prime field $\mathbb{F}_p$, the girth values of (3, 19)-regular Tanner's QC-LDPC codes of code length $19p$ are determined. In order to show the good performance of this class of QC-LDPC codes, numerical results are also provided.

INDEX TERMS QC-LDPC codes, Tanner graph, girth, prime field.

I. INTRODUCTION

Quasi-cyclic (QC) LDPC codes [1] are a class of well-known channel codes, and widely used in the communication and storage systems because of their excellent features: low-complexity encoding and decoding algorithms [2]–[5], good performance in the waterfall and error-floor regions [6]–[10], and easy implementations in hardware [11]–[13]. In general, the low-complexity algorithms for decoding LDPC codes are under the frame of iterative decoding. However, short cycles in the Tanner graph [14] of an LDPC code degrade the iterative decoding performance. Hence, constructing large girth LDPC codes and/or determining their girths is of interest in coding theory and graph theory [15], [16].

In 2001, Tanner presented a construction method to guarantee LDPC codes having large girths, and the proposed codes are regular [17]. For convenience, we call them (γ, ρ)-regular Tanner's QC-LDPC codes in this article. As pointed out in [1], the maximum girth value of fully-connected QC-LDPC codes is 12. It is clear that (γ, ρ)-regular Tanner's QC-LDPC codes are fully-connected, and then their possible maximum girth value is 12. However, for a specific Tanner's QC-LDPC code, its girth is unknown. In 2006, Kim *et al.* studied the girth of (3, 5)-regular Tanner's QC-LDPC codes of length $5p$ for p being a prime in the form of $(15i + 1)$ [18]. The results show that the girth of (3, 5)-regular Tanner's QC-LDPC codes is at least 8. In fact, there are one code with girth 8 (for $p = 31$), two codes with girth 10 (for $p = 61, 151$), and the remaining codes have girth 12 (for $p \neq 31, 61, 151$). In other words, most of (3, 5)-regular Tanner's QC-LDPC codes have the maximum girth value 12. This work is so encouraging, and then the girth distributions of the other families of (γ, ρ)-regular Tanner's QC-LDPC codes were studied, e.g., (3, 7)-regular codes [19], (3, 11)-regular codes [20], (3, 13)-regular codes [21], (3, 17)-regular codes [22], and (5, 11)-regular codes [23]. Similar conclusions were obtained: there are several Tanner's QC-LDPC codes with girths 6, 8, and 10, and the remaining codes achieve the maximum girth value 12. Recently, for finite code lengths, the girth distribution of (γ, ρ)-regular Tanner's QC-LDPC codes are analyzed in [24], where γ and ρ are positive integers greater than 2. However, the girth distribution of (γ, ρ)-regular Tanner's QC-LDPC codes is not given in the infinite code lengths. In addition, girth analysis of other classes of LDPC codes are given in [25]–[30], and some new constructions

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

of LDPC codes with large girth are also proposed [31]–[37].

In this article, we study the girth distribution of (3, 19)-regular Tanner's QC-LDPC codes with code length $19p$, where p is a prime in the form of $(57i + 1)$. We first analyze their cycle structure, and then transform the conditions for the existence of cycles of lengths 6, 8, and 10 into polynomial equations in a 57th root of unity of the prime field $\mathbb{F}_p$. By checking whether these equations have solutions over the prime field $\mathbb{F}_p$, the candidate prime values p are obtained. Then we derive the girth distribution of (3, 19)-regular Tanner's QC-LDPC codes by summarizing the obtained candidate values p. Finally, the iterative decoding performance of (3, 19)-regular Tanner's QC-LDPC codes over the AWGN channel are presented.

II. CYCLES IN (3, 19)-REGULAR TANNER'S QC-LDPC CODES

Let p be a prime number. It is clear that there exists a prime field of size p, denoted by $\mathbb{F}_p$. A (γ, ρ)-regular Tanner's QC-LDPC code of length $N = \rho p$ is given by the null space of the following parity-check matrix

$$\mathbf{H} = \left[\mathbf{I}(b^s a^t)\right] = \begin{bmatrix} \mathbf{I}(b^0a^0) & \mathbf{I}(b^0a^1) & \mathbf{I}(b^0a^2) & \cdots & \mathbf{I}(b^0a^{\rho-1}) \\ \mathbf{I}(b^1a^0) & \mathbf{I}(b^1a^1) & \mathbf{I}(b^1a^2) & \cdots & \mathbf{I}(b^1a^{\rho-1}) \\ \mathbf{I}(b^2a^0) & \mathbf{I}(b^2a^1) & \mathbf{I}(b^2a^2) & \cdots & \mathbf{I}(b^2a^{\rho-1}) \\ \vdots & \vdots & \ddots & \vdots & \\ \mathbf{I}(b^{\gamma-1}a^0) & \mathbf{I}(b^{\gamma-1}a^1) & \mathbf{I}(b^{\gamma-1}a^2) & \cdots & \mathbf{I}(b^{\gamma-1}a^{\rho-1}) \end{bmatrix}, \tag{1}$$

where $0 \le s \le \gamma - 1$, $0 \le t \le \rho - 1$, b and a are nonzero elements of $\mathbb{F}_p$ with orders γ and ρ, respectively. There are two points to note about the matrix $\mathbf{H}$: 1) The value of $(b^s a^t)$ is computed modulo p; 2) $\mathbf{I}(b^s a^t)$ stands for a $p \times p$ circulant permutation matrix (CPM) created by cyclically shifting each row of an identity matrix $\mathbf{I}$ of size $p \times p$ to the right $(b^s a^t)$ positions. Furthermore, let $p = \gamma \cdot \rho \cdot i + 1$, and then there exists a primitive $(\gamma\rho)$-th root of unity in the prime field $\mathbb{F}_p$, denoted by θ. It is easy to see that the orders of θ^γ and θ^ρ are ρ and γ, respectively. Assume that $a = \theta^\gamma$ and $b = \theta^\rho$. Hence, the matrix $\mathbf{H}$ in (1) becomes

$$\mathbf{H} = \left[\mathbf{I}(\theta^{\rho \cdot s + \gamma \cdot t})\right]$$

with $0 \le s \le \gamma - 1$ and $0 \le t \le \rho - 1$.

In this article, we study the (3, 19)-regular Tanner's QC-LDPC codes. Hence, $\gamma = 3$, $\rho = 19$, and the prime $p \equiv 1 \pmod{57}$. Let P_{57} be the set of the primes p, i.e., $p \in P_{57} = \{229, 457, 571, 1483, 1597, \ldots\}$. In the following, the mentioned primes p are in P_{57}. Assume that θ is a primitive 57th root of unity in the prime field $\mathbb{F}_p$. Hence, the parity-check matrix of a (3, 19)-regular Tanner's QC-LDPC code of length $19p$ is given by

$$\mathbf{H} = \left[\mathbf{I}\left(\theta^{19s+3t}\right)\right], \tag{2}$$

where $0 \le s \le 2$ and $0 \le t \le 18$.

As presented in [1], a cycle of length $2i$, denoted by $2i$-cycle for short, in the Tanner graph of $\mathbf{H}$ in (1) is expressed as an ordered sequence of CPMs:

$$\mathbf{I}(b^{s_0}a^{t_0}), \mathbf{I}(b^{s_1}a^{t_0}), \mathbf{I}(b^{s_1}a^{t_1}), \ldots, \mathbf{I}(b^{s_0}a^{t_{i-1}}), \mathbf{I}(b^{s_0}a^{t_0})$$

with for $0 \le k \le i - 1$, $s_k \neq s_{k+1}$, $t_k \neq t_{k+1}$, $s_i = s_0$, and $t_i = t_0$. The positions of these ordered CPMs can be simplified as

$$(s_0, t_0) : (s_1, t_1) : \ldots : (s_{i-2}, t_{i-2}) : (s_{i-1}, t_{i-1}) :, \tag{3}$$

where the colon between (s_k, t_k) and (s_{k+1}, t_{k+1}) is the CPM $\mathbf{I}(b^{s_{k+1}}a^{t_k})$, and (s_k, t_k) stands for the CPM $\mathbf{I}(b^{s_k}a^{t_k})$. For simplicity, the $2i$-cycle determined by (3) is said to be of type $(s_0, s_1, s_2, \ldots, s_{i-1})$. The sufficient and necessary condition for the existence of such a $2i$-cycle is presented in [1], and further improved in [8]. Assume that the girth is g. For $g \le 2i \le (2g - 2)$, the sufficient and necessary condition for the existence of a $2i$-cycle determined by (3) is

$$\sum_{k=0}^{i-1} (b^{s_k}a^{t_k} - b^{s_{k+1}}a^{t_k}) \equiv 0 \pmod{p}, \tag{4}$$

where for $0 \le k \le i - 1$, $s_k \neq s_{k+1}$, $t_k \neq t_{k+1}$, $s_i = s_0$, and $t_i = t_0$. Since $a = \theta^3$ and $b = \theta^{19}$, equation (4) can be written as follows.

$$\sum_{k=0}^{i-1} (\theta^{19s_k} - \theta^{19s_{k+1}})\,\theta^{3t_k} = 0 \pmod{p}.$$

Following the definition in [18], the above equation is referred to as *basic equation* in the remaining paper. Without loss of generality, let $t_0 = 0$. Based on the equivalence relation of types in [18], we provide the equivalence relation among cycles in (3, 19)-regular Tanner's QC-LDPC codes as follows.

Definition 1: Type $(s_0, s_1, \ldots, s_{i-1})$ is equivalent to type $(s_0^*, s_1^*, \ldots, s_{i-1}^*)$ in (3, 19)-regular Tanner's QC-LDPC codes if one of the following conditions is satisfied:

1) There is an integer $a \in \{0, 1, 2\}$ such that $s_j = s_j^* + a \pmod{3}$ for all $j \in \{0, 1, \ldots, i - 1\}$.
2) There is an integer $a \in \{1, 2\}$ such that $s_j = a \cdot s_j^* \pmod{3}$ for all $j \in \{0, 1, \ldots, i - 1\}$.
3) There is an integer $a \in \{0, 1, \ldots, i - 1\}$ such that $s_j = s_{j+a}^*$ for all $j \in \{0, 1, \ldots, i - 1\}$.
4) There is an integer $a \in \{0, 1, \ldots, i - 1\}$ such that $s_j = s_{i-1-j+a}^*$ for all $j \in \{0, 1, \ldots, i - 1\}$.

Note that the addition and subtraction operations in the subscript of s are performed under modulo i.

Based on the type equivalence relation in **Definition 1**, cycles of lengths 4, 6, 8, and 10 can be divided into the following five classes of types.

1) 4-cycles: All types are equivalent to the unique class $(1, 2)$.
2) 6-cycles: All types are equivalent to the unique class $(1, 2, 0)$.
3) 8-cycles: All types are classified into the following two classes, i.e., $(1, 2, 1, 2)$ and $(1, 2, 1, 0)$.

TABLE 1. All cases in class $(1, 2, 0)$.

	All cases (i, j)	Modified basic equation	Reduced form	Candidate prime values p
1	(i, i)	$1 + \theta^{3i+19} + \theta^{6i-19}$	$1 + u + u^2$	None
2	$(i, 2i)$	$1 + \theta^{3i+19} + \theta^{9i-19}$	$1 + u + u^{41}$	4447
3	$(i, 3i)$	$1 + \theta^{3i+19} + \theta^{12i-19}$	$1 + u + u^{23}$	6841
4	$(i, 4i)$	$1 + \theta^{3i+19} + \theta^{15i-19}$	$1 + u + u^5$	6841
5	$(i, 5i)$	$1 + \theta^{3i+19} + \theta^{18i-19}$	$1 + u + u^{44}$	6841
6	$(i, 6i)$	$1 + \theta^{3i+19} + \theta^{21i-19}$	$1 + u + u^{26}$	4447
7	$(i, 7i)$	$1 + \theta^{3i+19} + \theta^{24i-19}$	$1 + u + u^8$	None
8	$(i, 8i)$	$1 + \theta^{3i+19} + \theta^{27i-19}$	$1 + u + u^{47}$	4447
9	$(i, 9i)$	$1 + \theta^{3i+19} + \theta^{30i-19}$	$1 + u + u^{29}$	None
10*	$(i, -i)$	None	None	None
11	$(i, -2i)$	$1 + \theta^{3i+19} + \theta^{54i-19}$	$1 + u + u^{56}$	None
12	$(i, -3i)$	$1 + \theta^{3i+19} + \theta^{51i-19}$	$1 + u + u^{17}$	4447
13	$(i, -4i)$	$1 + \theta^{3i+19} + \theta^{48i-19}$	$1 + u + u^{35}$	6841
14	$(i, -5i)$	$1 + \theta^{3i+19} + \theta^{45i-19}$	$1 + u + u^{53}$	6841
15	$(i, -6i)$	$1 + \theta^{3i+19} + \theta^{42i-19}$	$1 + u + u^{14}$	6841
16	$(i, -7i)$	$1 + \theta^{3i+19} + \theta^{39i-19}$	$1 + u + u^{32}$	4447
17	$(i, -8i)$	$1 + \theta^{3i+19} + \theta^{36i-19}$	$1 + u + u^{50}$	None
18	$(i, -9i)$	$1 + \theta^{3i+19} + \theta^{33i-19}$	$1 + u + u^{11}$	4447

4) 10-cycles: All types are equivalent to the unique class $(1, 2, 0, 1, 2)$.

III. GIRTH ANALYSIS OF (3, 19)-REGULAR TANNER'S QC-LDPC CODES

Let $i = t_1 - t_0 \pmod{19}$, $j = t_2 - t_1 \pmod{19}$, $k = t_3 - t_2 \pmod{19}$, and $l = t_4 - t_3 \pmod{19}$. Since $t_k \neq t_{k+1}$ for $0 \leq k \leq 3$, then the integer variables i, j, k, and l are not equal to zero, and they are greater than -10 and less than 10. According to the classified five equivalent classes, we check whether the sufficient and necessary conditions for the existence of the corresponding cycles are satisfied, and the candidate prime values p can be obtained. Next, we analyze the five equivalent classes one by one.

A. CLASS $(1, 2)$

Based on the type equivalence relation in **Definition 1**, all 4-cycles have the unique class $(1, 2)$. The corresponding positions in (3) are $(1, 0) : (2, i) :$ with $i \neq 0 \pmod{19}$. Furthermore, the basic equation can be written as

$$\sum_{k=0}^{1} (\theta^{19s_k} - \theta^{19s_{k+1}})\,\theta^{3t_k} = \theta^{19}(1-\theta^{19})(1-\theta^{3i}) = 0 \pmod{p}.$$

Since θ is a primitive 57th root of unity, we have $\theta^{19} \neq 0, \theta^{19} \neq 1$, and $\theta^{3i} \neq 1$, where $-9 \leq i \leq 9$ and $i \neq 0$. Therefore, the above equation is not satisfied, and then there are no 4-cycles in (3, 19)-regular Tanner's QC-LDPC codes.

B. CLASS $(1, 2, 0)$

Based on the type equivalence relation in **Definition 1**, all 6-cycles have the unique class $(1, 2, 0)$. Its corresponding positions in (3) are $(1, 0) : (2, i) : (0, i + j) :$, where $i + j \neq 0 \pmod{19}$. The basic equation can be written as

$$\sum_{k=0}^{2} (\theta^{19s_k} - \theta^{19s_{k+1}})\,\theta^{3t_k} = \theta^{19}(1-\theta^{19})(1+\theta^{3i+19}+\theta^{3(i+j)-19}) = 0 \pmod{p}.$$

Since $\theta^{19} \neq 0$ and $\theta^{19} \neq 1$, the basic equation becomes

$$1 + \theta^{3i+19} + \theta^{3(i+j)-19} = 0 \pmod{p}. \tag{5}$$

Following [18]–[22], the above modified equation is called *modified basic equation* in this article. Therefore, there is a 6-cycle if and only if equation (5) holds for some possible pairs (i, j). According to the existence of 6-cycles, equation $i + j \neq 0 \pmod{19}$ is satisfied. In this case, the pair (i, j) is invalid, and the other pairs are valid. Next, we will consider all valid cases. Assume that i is a variable. Thus we can employ the variable i to represent j. In order to facilitate the understanding, all pairs (i, j) are recorded in Table 1. The superscript "$*''$ of the index number indicates that the corresponding pair (i, j) is invalid.

1) THE CASE OF (i, i)

Based on Table 1, we can see that the modified basic equation is

$$1 + \theta^{3i+19} + \theta^{6i-19} = 1 + \theta^{3i+19} + \left(\theta^{3i+19}\right)^2.$$

Since i is greater than -10 and less than 10,

$$\left(\theta^{3i+19}\right)^3 = \theta^{9i+57} = \theta^{9i} \neq 1,$$

and then

$$\left(\theta^{3i+19}\right)^3 - 1 = \left(\theta^{3i+19} - 1\right)\left(\left(\theta^{3i+19}\right)^2 + \theta^{3i+19} + 1\right) \neq 0.$$

TABLE 2. **Representation of u^s.**

u^s	θ^t	u^s	θ^t	u^s	θ^t
u	θ^{3i+19}	u^2	θ^{6i-19}	u^3	θ^{9i}
u^4	θ^{12i+19}	u^5	θ^{15i-19}	u^6	θ^{18i}
u^7	θ^{21i+19}	u^8	θ^{24i-19}	u^9	θ^{27i}
u^{10}	θ^{30i+19}	u^{11}	θ^{33i-19}	u^{12}	θ^{36i}
u^{13}	θ^{39i+19}	u^{14}	θ^{42i-19}	u^{15}	θ^{45i}
u^{16}	θ^{48i+19}	u^{17}	θ^{51i-19}	u^{18}	θ^{54i}
u^{19}	θ^{19}	u^{20}	θ^{3i-19}	u^{21}	θ^{6i}
u^{22}	θ^{9i+19}	u^{23}	θ^{12i-19}	u^{24}	θ^{15i}
u^{25}	θ^{18i+19}	u^{26}	θ^{21i-19}	u^{27}	θ^{24i}
u^{28}	θ^{27i+19}	u^{29}	θ^{30i-19}	u^{30}	θ^{33i}
u^{31}	θ^{36i+19}	u^{32}	θ^{39i-19}	u^{33}	θ^{42i}
u^{34}	θ^{45i+19}	u^{35}	θ^{48i-19}	u^{36}	θ^{51i}
u^{37}	θ^{54i+19}	u^{38}	θ^{-19}	u^{39}	θ^{3i}
u^{40}	θ^{6i+19}	u^{41}	θ^{9i-19}	u^{42}	θ^{12i}
u^{43}	θ^{15i+19}	u^{44}	θ^{18i-19}	u^{45}	θ^{21i}
u^{46}	θ^{24i+19}	u^{47}	θ^{27i-19}	u^{48}	θ^{30i}
u^{49}	θ^{33i+19}	u^{50}	θ^{36i-19}	u^{51}	θ^{39i}
u^{52}	θ^{42i+19}	u^{53}	θ^{45i-19}	u^{54}	θ^{48i}
u^{55}	θ^{51i+19}	u^{56}	θ^{54i-19}	u^{57}	$\theta^0\ (=1)$

Hence,

$$\left(\theta^{3i+19}\right)^2 + \theta^{3i+19} + 1 \neq 0.$$

Therefore, the modified basic equation has no solution in $\mathbb{F}_p$ for case (i, i).

2) THE CASE OF $(i, 2i)$

Let $u = \theta^{3i+19}$, and the values of u^s can be represented by the powers of θ for $1 \leq s \leq 57$, as shown in Table 2. Based on Tables 1 and 2, the modified basic equation in this case becomes

$$u^{41} + u + 1 = 0 \pmod{p}.$$

$u^{57} - 1$ can be factorized as follows.

$u^{57} - 1 = (u-1)(u^{18} + u^{17} + u^{16} + u^{15} + u^{14} + u^{13} + u^{12} + u^{11} + u^{10} + u^9 + u^8 + u^7 + u^6 + u^5 + u^4 + u^3 + u^2 + u + 1)(u^2 + u + 1)(u^{36} - u^{35} + u^{33} - u^{32} + u^{30} - u^{29} + u^{27} - u^{26} + u^{24} - u^{23} + u^{21} - u^{20} + u^{18} - u^{16} + u^{15} - u^{13} + u^{12} - u^{10} + u^9 - u^7 + u^6 - u^4 + u^3 - u + 1)$.

Since u is a primitive 57th root of unity in $\mathbb{F}_p$, then

$$\begin{aligned} &u^{36} - u^{35} + u^{33} - u^{32} + u^{30} - u^{29} + u^{27} - u^{26} + u^{24} \\ &\quad - u^{23} + u^{21} - u^{20} + u^{18} - u^{16} + u^{15} - u^{13} + u^{12} - u^{10} \\ &\quad + u^9 - u^7 + u^6 - u^4 + u^3 - u + 1 = 0 \pmod{p}. \end{aligned} \tag{6}$$

Furthermore, the modified basic equation $u^{41} + u + 1$ can be factorized into $u^{41} + u + 1 = (u^2 + u + 1)(u^{39} - u^{38} + u^{36} - u^{35} + u^{33} - u^{32} + u^{30} - u^{29} + u^{27} - u^{26} + u^{24} - u^{23} + u^{21} - u^{20} + u^{18} - u^{17} + u^{15} - u^{14} + u^{12} - u^{11} + u^9 - u^8 + u^6 - u^5 + u^3 - u^2 + 1)$. Since $u^3 \neq 1 \pmod{p}$, then $u^2 + u + 1 \neq 0$. Thus, $u^{41} + u + 1$ can be simplified as $u^{39} - u^{38} + u^{36} - u^{35} + u^{33} - u^{32} + u^{30} - u^{29} + u^{27} - u^{26} + u^{24} - u^{23} + u^{21} - u^{20} + u^{18} - u^{17} + u^{15} - u^{14} + u^{12} - u^{11} + u^9 - u^8 + u^6 - u^5 + u^3 - u^2 + 1$, and this equation is called the *reduced form* of $u^{41} + u + 1$. By applying the Euclidean division algorithm to this reduced form and equation (6), the remainder polynomials are given as follows.
$-u^{20} + u^{19} - u^{17} + u^{16} - u^{14} + u^{13} - u^{11} + u^{10} - u^8 + u^7 - u^5 + u^4 - u^2 + 1$, $u^{15} - u^{13} + u^{12} - u^{10} + u^9 - u^7 + u^6 - u^4 + u^3 - u + 1$, $-u^{14} + u^{13} - u^{11} + u^{10} - u^8 + u^7 - u^5 + u^4 + u^3 - 3u^2 + 2u$, $u^4 - u^3 - u^2 + u + 1$, $5u^3 - 6u^2 - 9u - 6$, $(26/25)u^2 + (64/25)u + 31/25$, $(10175/338)u + 2675/169$, $751543/4141225$.
It is clear that the remainder $751543/4141225$ equals zero in $\mathbb{F}_{4447}$, and it is a nonzero element in $\mathbb{F}_p$ for $p \in P_{57} \backslash \{4447\}$. The remaining remainder polynomials over $\mathbb{F}_p$ do not equal zero for $p \in P_{4447}$. Therefore, the basic equation has no solution in $\mathbb{F}_p$ apart from $p = 4447$.

3) THE REMAINING CASES OF (i, j)

The remaining valid cases of (i, j) are $(i, 3i)$, $(i, 4i)$, $(i, 5i)$, $(i, 6i)$, $(i, 7i)$, $(i, 8i)$, $(i, 9i)$, $(i, -2i)$, $(i, -3i)$, $(i, -4i)$, $(i, -5i)$, $(i, -6i)$, $(i, -7i)$, $(i, -8i)$, and $(i, -9i)$. Similar to the case of $(i, 2i)$, we can accordingly obtain their modified basic equations, reduced forms, and candidate prime values p. Combined with the cases of (i, i), $(i, 2i)$, we record them in Table 1.

Based on the results in Table 1, we can conclude that for $p = 4447, 6841$, the (3, 19)-regular Tanner's QC-LDPC code of length $19p$ has girth 6, and then the girth of the other codes is at least 8.

C. *CLASS* (1, 2, 1, 2)

The equivalent class (1, 2, 1, 2) corresponds to a series of 8-cycles whose positions in (3) are $(1, 0) : (2, i) : (1, i+j) : (2, i+j+k) :$ for $i + j + k \neq 0 \pmod{19}$. Hence, the basic equation can be rewritten as follows.

$$\begin{aligned} \sum_{k=0}^{3} &(\theta^{19 s_k} - \theta^{19 s_{k+1}})\, \theta^{3 t_k} \\ &= \theta^{19}(1 - \theta^{19})(1 - \theta^{3i} + \theta^{3(i+j)} - \theta^{3(i+j+k)}) \\ &= 0 \pmod{p}. \end{aligned}$$

Since $\theta^{19} \neq 0$ and $\theta^{19} \neq 1$, the modified basic equation is

$$1 - \theta^{3i} + \theta^{3(i+j)} - \theta^{3(i+j+k)} = 0 \pmod{p}. \tag{7}$$

Let $v = \theta^{3i}$, and y^s can be easily obtained for $1 \leq s \leq 19$, as shown in Table 3. It is clear that v is a primitive 19th root of unity in $\mathbb{F}_p$ for $p \in P_{57}$. Since

$$\begin{aligned} v^{19} - 1 = (v-1)(&v^{18} + v^{17} + v^{16} + v^{15} + v^{14} \\ &+ v^{13} + v^{12} + v^{11} + v^{10} + v^9 + v^8 + v^7 \\ &+ v^6 + v^5 + v^4 + v^3 + v^2 + v + 1) \end{aligned}$$

and $y \neq 1$, we can obtain

$$\begin{aligned} v^{18} &+ v^{17} + v^{16} + v^{15} + v^{14} + v^{13} + v^{12} + v^{11} \\ &+ v^{10} + v^9 + v^8 + v^7 + v^6 + v^5 + v^4 + v^3 \\ &+ v^2 + v + 1 = 0 \pmod{p}. \end{aligned} \tag{8}$$

TABLE 3. Representation of v^s.

v^s	θ^t	v^s	θ^t	v^s	θ^t	v^s	θ^t
v	θ^{3i}	v^2	θ^{6i}	v^3	θ^{9i}	v^4	θ^{12i}
v^5	θ^{15i}	v^6	θ^{18i}	v^7	θ^{21i}	v^8	θ^{24i}
v^9	θ^{27i}	v^{10}	θ^{30i}	v^{11}	θ^{33i}	v^{12}	θ^{36i}
v^{13}	θ^{39i}	v^{14}	θ^{42i}	v^{15}	θ^{45i}	v^{16}	θ^{48i}
v^{17}	θ^{51i}	v^{18}	θ^{54i}	v^{19}	$\theta^{57i}\ (=1)$		

TABLE 4. All invalid cases (i, j, k) for 8-cycles.

$(i, -9i, 8i)$	$(i, -8i, 7i)$	$(i, -7i, 6i)$	$(i, -6i, 5i)$
$(i, -5i, 4i)$	$(i, -3i, 2i)$	$(i, -2i, i)$	$(i, i, -2i)$
$(i, 2i, -3i)$	$(i, 3i, -4i)$	$(i, 5i, -6i)$	$(i, 6i, -7i)$
$(i, 7i, -8i)$	$(i, 8i, -9i)$	$(i, 9i, 9i)$	$(i, 4i, -5i)$
$(i, -4i, 3i)$			

Similar to class $(1, 2, 0)$, we list all invalid cases (i, j, k) in Table 4 for $i+j+k = 0\ (\bmod\ 19)$, and the other cases are valid. According to equation (7), we can obtain the modified basic equation and the reduced form corresponding to each valid case. By applying the Euclidean division algorithm to the reduced form of the modified basic equation and equation (8), and then checking whether the remainder is equal to zero over $\mathbb{F}_p$ for $p \in P_{57}$, the candidate value p is obtained.

D. CLASS (1, 2, 1, 0)

The 8-cycles also have the other equivalent class, i.e., class $(1, 2, 1, 0)$, and the corresponding positions in (3) are $(0, 0) : (1, i) : (0, i+j) : (2, i+j+k) :$ for $i+j+k \neq 0\ (\bmod\ 19)$. The basic equation can be rewritten as follows.

$$\begin{aligned}\sum_{k=0}^{3} (\theta^{19s_k} - \theta^{19s_{k+1}})\,\theta^{3t_k} &= \theta^{19}(1-\theta^{19})(1-\theta^{3i}-\theta^{3(i+j)-19}+\theta^{3(i+j+k)-19}) \\ &= 0\ (\bmod\ p).\end{aligned}$$

Since $\theta^{19} \neq 0$ and $\theta^{19} \neq 1$, the modified basic equation is given by

$$1-\theta^{3i}-\theta^{3(i+j)-19}+\theta^{3(i+j+k)-19} = 0\ (\bmod\ p). \tag{9}$$

Set $u = \theta^{3i+19}$. For $1 \leq s \leq 57$, u^s is recorded in Table 2. Just like class $(1, 2, 1, 2)$, there are 17 invalid cases (see Table 4) and 307 valid cases, and the candidate values p can be also obtained for each valid case. Note that the equation which is employed to apply the Euclidean division algorithm to the reduced form of the modified basic equation is equation (6).

According to the conclusion in Subsection III-B, we summarize all obtained candidate values p, and (3, 19)-regular Tanner's QC-LDPC codes with girth 8 are found. That is, (3, 19)-regular Tanner's QC-LDPC codes of length $19p$ have girth 8 for $p \in G_8$, where $G_8 = \{229, 457, 571, 1483, 1597, 2053, 2281, 3079, 3307, 4219, 4561, 5701, 7411, 7753, 9349, 9463, 11059, 15619, 16759, 17443, 18583, 27361, 29983, 30553, 32833, 40813, 46171, 48337, 53923, 56431, 56659, 62701, 78889, 85159, 90403, 101347, 125287, 130873, 174763, 177841, 187987, 196879, 202693, 204517, 213523, 234499, 355909, 371299, 372667, 425107, 611839, 741457, 947341, 1462507, 1521673, 4370761, 5414089, 5468923, 83498959, 186833917\}$.

E. CLASS (1, 2, 0, 1, 2)

All 10-cycles have the unique equivalent class (1, 2, 0, 1, 2), and the corresponding positions in (3) are $(0, 0) : (1, i) : (2, i + j) : (0, i + j + k) : (1, i + j + k + l) :$, where $i+j+k+l \neq 0\ (\bmod\ 19)$. The basic equation can be rewritten as follows.

$$\begin{aligned}\sum_{k=0}^{4} (\theta^{19s_k} - \theta^{19s_{k+1}})\,\theta^{3t_k} &= \theta^{19}(1-\theta^{19})\cdot \\ &\quad (1+\theta^{3i+19}+\theta^{3(i+j)-19}+\theta^{3(i+j+k)}-\theta^{3(i+j+k+l)}) \\ &= 0\ (\bmod\ p).\end{aligned}$$

Since $\theta^{19} \neq 0$ and $\theta^{19} \neq 1$, the modified basic equation is

$$\begin{aligned}1+\theta^{3i+19}+\theta^{3(i+j)-19}+\theta^{3(i+j+k)}-\theta^{3(i+j+k+l)} \\ = 0\ (\bmod\ p).\end{aligned} \tag{10}$$

Similar to class $(1, 2, 0)$, class $(1, 2, 1, 2)$, and class $(1, 2, 1, 0)$, 307 invalid cases of (i, j, k, l) with $i+j+k+l = 0\ (\bmod\ 19)$ are first found, and the remaining 5525 cases of (i, j, k, l) are valid. Second, based on equation (10), we can obtain the modified basic equation and the reduced equation for each valid case. Third, we apply the Euclidean division algorithm to the reduced form of the modified basic equation and equation (6), and then check whether the resulting remainder is equal to zero over $\mathbb{F}_p$ for $p \in P_{57}$, the candidate value p is obtained from within. Finally, by summarizing the obtaining candidate values p and combining with the conclusions in Subsections III-B and III-D, we can find all (3, 19)-regular Tanner's QC-LDPC codes with length $19p$ and girth 10. In order to save space, the invalid and valid cases of (i, j, k, l), and their associated modified basic equations and reduced forms are omitted, we here only give the obtained results. That is, the girth of (3, 19)-regular Tanner's QC-LDPC codes of length $19p$ is 10 for $p \in G_{10}$, where $G_{10} = \{2851, 3877, 4789, \dots\}$ and the element number in G_{10} is 831. In order to facilitate the reader to view and retrieve, G_{10} is given in Appendix A.

IV. NUMERICAL RESULTS

In order to show the performance of (3, 19)-regular Tanner's QC-LDPC codes, numerical simulation results of some codes are provided in this section. Notice that the transmission is over the AWGN channel with BPSK modulation and the employed decoding algorithm is the sum-product algorithm (SPA).

Consider $p = 457, 571, 1483, 2053, 2281$. By suitably selecting the primitive elements, we can construct the five prime fields $\mathbb{F}_p$. Based on the parity-check matrix $\mathbf{H}$ in (2) and the primitive 57th root of unity in $\mathbb{F}_p$, we can obtain five (3, 19)-regular Tanner's QC-LDPC codes of lengths $8683 (= 19 \times 457)$, $10849 (= 19 \times 571)$, 28177

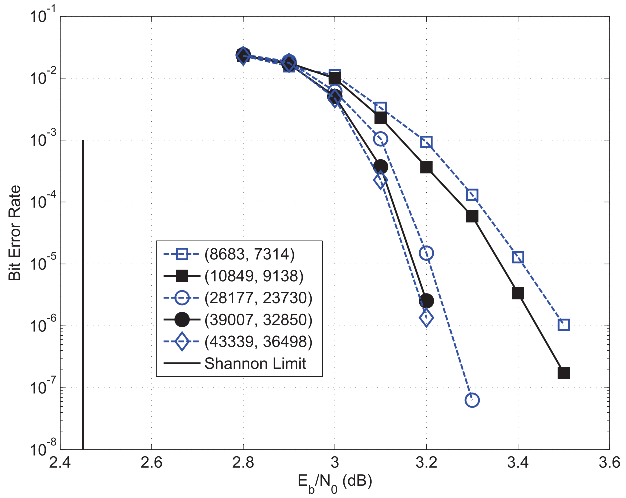

FIGURE 1. **The error performance of Tanner's QC-LDPC (8683, 7314), (10849, 9138), (28177, 23730), (39007, 32850), and (43339, 36498) codes.**

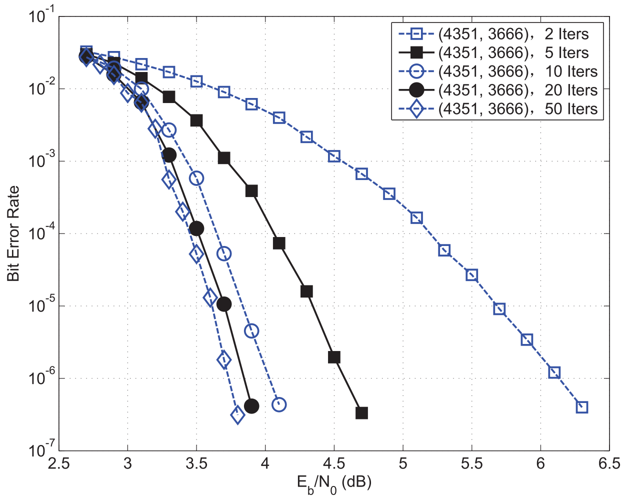

FIGURE 2. **The rate of decoding convergence of the Tanner's QC-LDPC (4351, 3666) code.**

$(= 19 \times 1483)$, $39007(= 19\times 2053)$, and 43339 $(= 19\times 2281)$. Their corresponding exponent matrices $\mathbf{P}_{457}$, $\mathbf{P}_{571}$, $\mathbf{P}_{1483}$, $\mathbf{P}_{2053}$, and $\mathbf{P}_{2281}$ are given in Appendix B. Their parity-check matrices have two redundant rows, and they are Tanner's QC-LDPC (8683, 7314), (10849, 9138), (28177, 23730), (39007, 32850), and (43339, 36498) codes. Notice that the girth of these five codes is 8. The bit error performance of these codes decoded with the SPA are shown in Figure 1. The maximum number of iterations is 50. We can see that, at the bit error rates (BERs) of 10^{-6}, the (3, 19)-regular Tanner's QC-LDPC codes of lengths 8683, 10849, 28177, 39007, and 43339 perform about 1.05 dB, 1.0 dB, 0.8 dB, 0.75 dB, and 0.7 dB from the Shannon limit, respectively. It can be seen that, when the length is greater than 40000 bits, the (3, 19)-regular Tanner's QC-LDPC codes perform about 0.7 dB away from the Shannon limit at the BER of 10^{-6}, and the performance gap will become smaller with the increase of the code length.

Consider $p = 229$. According to the parity-check matrix $\mathbf{H}$ in (2) and the primitive 57th root of unity in $\mathbb{F}_{229}$, we can obtain the (3, 19)-regular Tanner's QC-LDPC (4351, 3666) code which corresponding exponent matrix $\mathbf{P}_{229}$ is given in Appendix B. The girth of this code is 8, and its parity-check matrix also has two redundant rows. Moreover, the BER performance of the (3, 19)-regular Tanner's QC-LDPC (4351, 3666) code is shown in Figure 2. The employed decoding algorithm is the SPA with 2, 5, 10, 20, and 50 iterations. We can see that this code converges fast. At BER$=10^{-6}$, the performance gap between 10 iterations and 50 iterations is less than 0.3 dB while the performance gap between 20 and 50 iterations is about 0.1 dB. That is, the decoding performance is good enough when the iteration number is 20. Besides, no error floor is observed down to BER $\approx 3\times 10^{-7}$.

V. CONCLUSION

In this article, we obtained the girth value g of (3, 19)-regular Tanner's QC-LDPC codes of length $19p$, $p \in P_{57}$ (P_{57} is a set of the primes with form $57s+1$), i.e.,

$$g = \begin{cases} 6, & if\ p \in G_6; \\ 8, & if\ p \in G_8; \\ 10, & if\ p \in G_{10}; \\ 12, & if\ p \in P_{57} \setminus (G_6 \cup G_8 \cup G_{10}); \end{cases}$$

where $G_6 = \{4447, 6841\}$, G_8 and G_{10} is given in Appendix A. Notice that the cardinalities of the sets G_8 and G_{10} are 60 and 831, respectively. That is, there are 2 codes of girth 6, 60 codes of girth 8, 831 codes of girth 10, and the remaining codes have girth 12, such as for $p = 21661, 23143, 25309, 27817, \ldots$. Furthermore, numerical simulation results show that (3, 19)-regular Tanner's QC-LDPC codes have good iterative decoding performance and low error floor.

APPENDIX. A

In the following, we provide two prime sets G_8 and G_{10} for (3, 19)-regular Tanner's QC-LDPC codes with girths 8 and 10. When p takes values in the set G_8, the girth of (3, 19)-regular Tanner's QC-LDPC code with code length $19p$ is 8, and the girth is 10 while p is in the set G_{10}.

G_8={229, 457, 571, 1483, 1597, 2053, 2281, 3079, 3307, 4219, 4561, 5701, 7411, 7753, 9349, 9463, 11059, 15619, 16759, 17443, 18583, 27361, 29983, 30553, 32833, 40813, 46171, 48337, 53923, 56431, 56659, 62701, 78889, 85159, 90403, 101347, 125287, 130873, 174763, 177841, 187987, 196879, 202693, 204517, 213523, 234499, 355909, 371299, 372667, 425107, 611839, 741457, 947341, 1462507, 1521673, 4370761, 5414089, 5468923, 83498959, 186833917}.

G_{10} = {2851, 3877, 4789, 4903, 6043, 6271, 7069, 7297, 7639, 7867, 8209, 8779, 8893, 9007, 10831, 11173, 11287, 11743, 11971, 12541, 13339, 13567, 13681, 14251, 14479, 14593, 14821, 15277, 15391, 15733, 16189, 16417, 16987, 18013, 18127, 19267, 19381, 19609, 20407, 20521, 20749, 21319, 21433, 22003, 22573, 23029, 23371, 23599, 23827, 24169, 24967, 25423, 25537, 26107, 26449, 28387, 28729, 28843, 29527, 29641, 30781, 31123, 32377, 32491, 33289, 33403, 35569, 35797, 35911, 37963, 39901, 40129, 40357, 40471, 40927, 41269, 42181, 42409, 42751, 42979, 43777, 43891, 45259, 45943, 47881, 49363, 49477, 50047, 51871, 53239, 53353, 54151, 54949, 55291, 59167, 59509, 61333, 62131, 62929, 63841, 65437, 66463, 66919, 67033, 67261, 67489, 69427, 70111, 71479, 71707, 72733, 73189, 73417, 74101, 75013, 75583, 76039, 77863, 79231, 79801, 80599, 81853, 81967, 82651, 83221, 83791, 86413, 87211, 87553, 89833, 92683, 93253, 95419, 95989, 96331, 97813, 98041, 98269, 98953, 99409, 101119, 101917, 102259, 103171, 103399, 104311, 105337, 111493, 111949, 113089, 114229, 114343, 114571, 114799, 116167, 120157, 121867, 123121, 126199, 127681, 130531, 131101, 131671, 131899, 132241, 133153, 133723, 135661, 137143, 138283, 138967, 139537, 141931, 144667, 145009, 145807, 146719, 147289, 148429, 152989, 154927, 155383, 157321, 158803, 160969, 162907, 164617, 166669, 169063, 175333, 175447, 180463, 182059, 186619, 187189, 192091, 195511, 196081, 200869, 201667, 204859, 206341, 207481, 212383, 215689, 217969, 225493, 227089, 236209, 239857, 248293, 253423, 254791, 261061, 262543, 263911, 268813, 269041, 273943, 278617, 280327, 283519, 285457, 290359, 290473, 292069, 292867, 293893, 314299, 326611, 328777, 333451, 334363, 335047, 336643, 346903, 347359, 347929, 357733, 358987, 362863, 363889, 371869, 373693, 378823, 391021, 408691, 410629, 413251, 417811, 436621, 447451, 451669, 455431, 471391, 476863, 477091, 488833, 505819, 507757, 523489, 529531, 539107, 544123, 547087, 549481, 556093, 557803, 563047, 576613, 577867, 594511, 621301, 623353, 624721, 632473, 646609, 653563, 662797, 665761, 669181, 690271, 711133, 718087, 718999, 723901, 735529, 738379, 754111, 764143, 768589, 770527, 781129, 782497, 794923, 807463, 820459, 822739, 825361, 830719, 851239, 856369, 857053, 868909, 870049, 882019, 885553, 905161, 919183, 921919, 954979, 956119, 975157, 976411, 976639, 978349, 985531, 988951, 993283, 1006279, 1012321, 1051423, 1051879, 1062367, 1073881, 1085509, 1120849, 1142737, 1151629, 1155619, 1159153, 1181611, 1197799, 1200307, 1212847, 1217179, 1217977, 1222537, 1232683, 1253089, 1261639, 1263463, 1279081, 1290823, 1294129, 1296409, 1306213, 1317271, 1333231, 1334371, 1366747, 1430131, 1442899, 1453957, 1459771, 1466383, 1509133, 1517569, 1535923, 1562371, 1571149, 1575481, 1603183, 1615837, 1627123, 1627237, 1650379, 1652089, 1662007, 1687657, 1729153, 1738273, 1751041, 1767229, 1787179, 1806901, 1827307, 1854781, 1866751, 1947691, 1984057, 2043907, 2083693, 2094523, 2112079, 2112193, 2137159, 2147989, 2176831, 2192791, 2202253, 2203849, 2214907, 2282281, 2285587, 2308387, 2343157, 2343613, 2376559, 2386591, 2396509, 2426947, 2437663, 2453053, 2462401, 2477791, 2489647, 2507773, 2544253, 2548813, 2550181, 2583127, 2654149, 2672617, 2698609, 2707843, 2716849, 2748769, 2755153, 2883061, 2925583, 2937667, 2940517, 2948839, 3037189, 3048247, 3053719, 3077203, 3118243, 3139447, 3203857, 3227683, 3227911, 3304291, 3309307, 3377821, 3394693, 3410881, 3412477, 3450781, 3460243, 3469363, 3471301, 3534799, 3584047, 3593509, 3615967, 3663277, 3837469, 3851149, 3905527, 3921601, 3972103, 3986467, 4034689, 4058401, 4139341, 4142989, 4171261, 4217203, 4247071, 4273519, 4333027, 4348189, 4396981, 4434259, 4502317, 4625779, 4670923, 4765543, 4799401, 4922179, 4944409, 4966411, 5132053, 5233171, 5267599, 5289373, 5319697, 5505061, 5572663, 5625673, 5627269, 5681647, 5844781, 5891293, 5908393, 5918083, 5928229, 6097633, 6122029, 6238651, 6345127, 6370207, 6446131, 6456733, 6633433, 6642553, 6678691, 6744583, 6806257, 7003933, 7034143, 7290643, 7335787, 7397119, 7549537, 7594453, 7621927, 7687021, 7809913, 7854487, 7931893, 8047717, 8060257, 8150773, 8164567, 8227381, 8280619, 8283697, 8552623, 8764321, 8907391, 8967241, 9056389, 9277549, 9391663, 9511933, 9771967, 9853933, 9867841, 9954823, 9988339, 10151017, 10280293, 10560619, 10701637, 10750429, 10906267, 10932829, 10980253, 10992337, 11159233, 11330119, 11419153, 11426449, 11556409, 11577499, 11580691, 11674171, 11991433, 12022441, 12192073, 12398413, 12575341, 12819643, 12833893, 12901951, 13018801, 13070557, 13089367, 13098601, 13750567, 13772683, 13882009, 14212267, 14317603, 14318971, 14454631, 14593141, 14763457, 15382933, 15434233, 15461707, 15469687, 15604093, 16143997, 16426831, 16555309, 16875877, 17021911, 17163841, 17465827, 17612659, 18346021, 18370873, 18554527, 18788683, 18798487, 18929473, 19688029, 20124763, 20312863, 20491957, 20530603, 20872603, 20924131, 21114853, 21382981, 21830317, 22070857, 22135723, 22534153, 22537573, 22598677, 22644733, 22866463, 23244373, 24273679, 24366247, 24482527, 24631069, 24730249, 25184311, 27011389, 27938437, 27971497, 28079683, 28816693, 30118687, 30132709, 30532507, 30615727, 30632713, 30674323, 30807589, 31357297, 31436983, 31837807, 33538003, 33694183, 34535047, 35863603, 36255421, 36448651, 36915367, 37356433, 37543393, 38336833, 38376391, 38389843, 38806171, 39871501, 40758763, 41173837, 41841763, 41971723, 42178177, 44439937, 45493069, 45509143, 45804973, 46062043, 46761433, 46833937, 47277283, 47751751, 48554881, 49740139, 51616921, 52139611, 53385859, 53970793, 55712029, 56137933, 58836769, 59119033, 59928433, 60572077, 60581767, 60744331, 61390939, 63649393, 66635167, 66636649, 69055387, 69063937, 73674553, 74227339, 74326519, 74831767, 75116653, 75188131, 76954789, 77069929, 78557287, 79211989, 81448441, 82324987, 83235847, 88370179, 89867683, 89905531, 92425843, 94793737, 95310043, 96739831, 102104671, 102215023, 103481449, 105767377, 105770227, 106599919, 107337271, 114075697, 114165871, 119827567, 120027067, 121782097, 127707361, 129569779, 130587913, 131956483, 137177683, 140941279, 145457503, 146041297, 146354227, 147551113, 160761091, 160997527, 162074257, 166400557, 169276777, 171099751, 178411027, 190106857, 193370677, 199050043, 207951391, 224704261, 251155111, 263743789, 264776857, 267067231, 278669581, 285449959, 303089407, 329689027, 360244219, 360709681, 379546129, 389655649, 397640209, 399876889, 409464859, 427385773, 438131641, 467012971, 472909963, 505984327, 515498539, 520840921, 563507929, 584072161, 654366613, 685422721, 695514913, 741595651, 793654663, 815581423, 848595823, 886508347, 958608103, 1031171041, 1197785233, 1375661143, 1384107061, 1398772591, 1413220723, 1608792511, 1610170201, 1911696667, 1932003487, 1952618791, 2086293367, 2102593543, 2110568413, 2116392673, 2190842653, 2194202119, 2591182609, 2947907191, 2978078317, 3296776603, 3349895701, 3464814313, 3747773941, 3821158477, 4169297263, 4266148927, 4976533999, 5175371203, 5456052541, 5856580141, 6145260061, 6719885041, 6878418343, 7253547313, 7370232697, 7749316441, 8084888437, 8211281263, 8560648627, 8873039863, 10253112691, 13706511157, 14603640427, 16530893191, 16720906339, 17162646307, 19765641823, 19860064489, 20418086851, 21191481433, 21285505441, 24803650549, 28471886917, 34430733151, 52511112289, 56338228291, 58815132511, 68207417977, 73503597829, 74397607147, 78449716627, 86907724669, 133002769213, 147552166273, 345171707773, 382919621131}.

APPENDIX. B

In Section IV, we construct six (3, 19)-regular Tanner's QC-LDPC codes of lengths 4351 (= 19 × 229), 8683 (= 19 × 457), 10849 (= 19 × 571), 28177 (= 19 × 1483), 39007 (= 19 × 2053), and 43339 (= 19 × 2281). Notice that the selected primitive 57th unity roots are 6 in $\mathbb{F}_{229}$, 13 in $\mathbb{F}_{457}$, 3 in $\mathbb{F}_{571}$, 2 in $\mathbb{F}_{1483}$, 2 in $\mathbb{F}_{2053}$, and 7 in $\mathbb{F}_{2281}$. Their corresponding exponent matrices $\mathbf{P}_{229}$, $\mathbf{P}_{457}$, $\mathbf{P}_{571}$, $\mathbf{P}_{1483}$, $\mathbf{P}_{2053}$, and $\mathbf{P}_{2281}$ are given as follows.

$$\mathbf{P}_{229} = \left[\begin{matrix} 1 & 216 & 169 & 93 & 165 & 145 & 176 & 2 & 203 \\ 140 & 12 & 73 & 196 & 200 & 148 & 137 & 51 & 24 \\ 135 & 77 & 144 & 189 & 62 & 110 & 173 & 41 & 154 \end{matrix}\right.$$

$$\left.\begin{matrix} 109 & 186 & 101 & 61 & 123 & 4 & 177 & 218 & 143 & 202 \\ 146 & 163 & 171 & 67 & 45 & 102 & 48 & 63 & 97 & 113 \\ 59 & 149 & 124 & 220 & 117 & 82 & 79 & 118 & 69 & 19 \end{matrix}\right]$$

$$\mathbf{P}_{457} = \left[\begin{matrix} 1 & 369 & 432 & 372 & 168 & 297 & 370 & 344 & 347 \\ 240 & 359 & 398 & 165 & 104 & 445 & 142 & 300 & 106 \\ 18 & 244 & 7 & 298 & 282 & 319 & 262 & 251 & 305 \end{matrix}\right.$$

$$\left.\begin{matrix} 83 & 8 & 210 & 257 & 234 & 430 & 91 & 218 & 10 & 34 \\ 269 & 92 & 130 & 442 & 406 & 375 & 361 & 222 & 115 & 391 \\ 123 & 144 & 124 & 56 & 99 & 428 & 267 & 268 & 180 & 155 \end{matrix}\right]$$

$$\mathbf{P}_{571} = \left[\begin{matrix} 1 & 27 & 158 & 269 & 411 & 248 & 415 & 356 & 476 \\ 103 & 497 & 286 & 299 & 79 & 420 & 491 & 124 & 493 \\ 331 & 372 & 337 & 534 & 143 & 435 & 325 & 210 & 531 \end{matrix}\right.$$

$$\left.\begin{matrix} 290 & 407 & 140 & 354 & 422 & 545 & 440 & 460 & 429 & 163 \\ 178 & 238 & 145 & 489 & 70 & 177 & 211 & 558 & 220 & 230 \\ 62 & 532 & 89 & 119 & 358 & 530 & 35 & 374 & 391 & 279 \end{matrix}\right]$$

$$\mathbf{P}_{1483} = \left[\begin{matrix} 1 & 8 & 64 & 512 & 1130 & 142 & 1136 & 190 & 37 \\ 789 & 380 & 74 & 592 & 287 & 813 & 572 & 127 & 1016 \\ 1144 & 254 & 549 & 1426 & 1027 & 801 & 476 & 842 & 804 \end{matrix}\right.$$

$$\left.\begin{matrix} 296 & 885 & 1148 & 286 & 805 & 508 & 1098 & 1369 & 571 & 119 \\ 713 & 1255 & 1142 & 238 & 421 & 402 & 250 & 517 & 1170 & 462 \\ 500 & 1034 & 857 & 924 & 1460 & 1299 & 11 & 88 & 704 & 1183 \end{matrix}\right]$$

$$\mathbf{P}_{2053} = \left[\begin{matrix} 1 & 8 & 64 & 512 & 2043 & 1973 & 1413 & 1039 & 100 \\ 773 & 25 & 200 & 1600 & 482 & 1803 & 53 & 424 & 1339 \\ 106 & 848 & 625 & 894 & 993 & 1785 & 1962 & 1325 & 335 \end{matrix}\right.$$

$$\left.\begin{matrix} 800 & 241 & 1928 & 1053 & 212 & 1696 & 1250 & 1788 & 1986 & 1517 \\ 447 & 1523 & 1919 & 981 & 1689 & 1194 & 1340 & 455 & 1587 & 378 \\ 627 & 910 & 1121 & 756 & 1942 & 1165 & 1108 & 652 & 1110 & 668 \end{matrix}\right]$$

$$\mathbf{P}_{2281} = \left[\begin{matrix} 1 & 343 & 1318 & 436 & 1283 & 2117 & 773 & 543 & 1488 \\ 849 & 1520 & 1292 & 642 & 1230 & 2186 & 1630 & 245 & 1919 \\ 5 & 1715 & 2028 & 2180 & 1853 & 1461 & 1584 & 434 & 597 \end{matrix}\right.$$

$$\left.\begin{matrix} 1721 & 1805 & 964 & 2188 & 35 & 600 & 510 & 1574 & 1566 & 1103 \\ 1289 & 1894 & 1838 & 878 & 62 & 737 & 1881 & 1941 & 1992 & 1237 \\ 1762 & 2182 & 258 & 1816 & 175 & 719 & 269 & 1027 & 987 & 953 \end{matrix}\right]$$

REFERENCES

[1] 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.

[2] Q. Huang, L. Tang, S. He, Z. Xiong, and Z. Wang, "Low-complexity encoding of quasi-cyclic codes based on galois Fourier transform," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 1757–1767, Jun. 2014.

[3] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Decoding of quasi-cyclic LDPC codes with section-wise cyclic structure," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Feb. 2014, pp. 1–10.

[4] Z. Xu, J. Zhu, Q. Cheng, and Z. Zhang, "An iterative decoding scheme for CPM-QC-LDPC codes based on matrix transform," *IEICE Trans. Commun.*, vol. E102.B, no. 3, pp. 496–509, 2019.

[5] Y. Chen, H. Cui, J. Lin, and Z. Wang, "Fine-grained bit-flipping decoding for LDPC codes," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 5, pp. 896–900, May 2020.

[6] H. Liu, Q. Huang, G. Deng, and J. Chen, "Quasi-cyclic representation and vector representation of RS-LDPC codes," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1033–1042, Apr. 2015.

[7] Q. Diao, J. Li, S. Lin, and I. F. Blake, "New classes of partial geometries and their associated LDPC codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 2947–2965, Jun. 2016.

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

[9] M. Asif, W. Zhou, M. Ajmal, Z. Akhtar, and N. Khan, "A construction of high performance quasicyclic LDPC codes: A combinatoric design approach," *Wireless Commun. Mobile Comput.*, vol. 2019, Jan. 2019, Art. no. 7468792.

[10] A. Farsiabi and A. H. Banihashemi, "Error floor estimation of LDPC decoders—A code independent approach to measuring the harmfulness of trapping sets," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 2667–2679, May 2020.

[11] 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 Trans. Commun.*, vol. 62, no. 8, pp. 2626–2637, Aug. 2014.

[12] H. Zhu, L. Pu, H. Xu, and B. Zhang, "Construction of quasi-cyclic LDPC codes based on fundamental theorem of arithmetic," *Wireless Commun. Mobile Comput.*, vol. 2018, Apr. 2018, Art. no. 5264724.

[13] M. Gholami and A. Nassaj, "LDPC codes based on mobius transformations," *IET Commun.*, vol. 13, no. 11, pp. 1615–1624, Jul. 2019.

[14] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[15] M. Karimi and A. H. Banihashemi, "On the girth of quasi-cyclic protograph LDPC codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4542–4552, Jul. 2013.

[16] X.-Q. 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.

[17] R. Tanner, D. Sridhara, and T. Fuja, "A class of group-structured LDPC codes," in *Proc. Int. Symp. Commun. Theory Appl.*, 2001, pp. 365–370.

[18] 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.

[19] M. Gholami and F. Mostafaiee, "On the girth of tanner (3,7) quasi-cyclic LDPC codes," *Trans. Combinatorics*, vol. 1, no. 2, pp. 1–16, 2012.

[20] H. Xu, B. Bai, D. Feng, and C. Sun, "On the girth of tanner (3,11) quasi-cyclic LDPC codes," *Finite Fields Their Appl.*, vol. 46, pp. 65–89, Jul. 2017.

[21] H. Xu, H. Li, D. Feng, B. Zhang, and H. Zhu, "On the girth of Tanner (3, 13) quasi-cyclic LDPC codes," *IEEE Access*, vol. 7, pp. 5153–5179, 2019.

[22] H. Xu, Y. Duan, X. Miao, and H. Zhu, "Girth analysis of Tanner's (3, 17)-regular QC-LDPC codes based on Euclidean division algorithm," *IEEE Access*, vol. 7, pp. 94917–94930, 2019.

[23] H. Xu, H. Zhu, M. Xu, B. Zhang, and S. Zhu, "Girth analysis of tanner (5,11) quasi-cyclic LDPC codes," in *Proc. 14th Int. Conf. Comput. Intell. Secur. (CIS)*, Nov. 2018, pp. 210–214.

[24] 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.

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

[26] 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.

[27] F. Amirzade and M.-R. Sadeghi, "Lower bounds on the lifting degree of QC-LDPC codes by difference matrices," *IEEE Access*, vol. 6, pp. 23688–23700, 2018.

[28] M.-R. Sadeghi, "Optimal search for Girth-8 quasi cyclic and spatially coupled multiple-edge LDPC codes," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1466–1469, Sep. 2019.

[29] H. Xu, H. Li, M. Xu, D. Feng, and H. Zhu, "Two classes of QC-LDPC cycle codes approaching gallager lower bound," *Sci. China Inf. Sci.*, vol. 62, no. 10, Oct. 2019, Art. no. 209305.

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

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

[32] H. Xu, C. Chen, M. Zhu, B. Bai, and B. Zhang, "Nonbinary LDPC cycle codes: Efficient search, design, and code optimization," *Sci. China Inf. Sci.*, vol. 61, no. 8, Aug. 2018, Art. no. 089303.

[33] J. Zhang, B. Bai, S. Li, M. Zhu, and H. Li, "Tail-biting globally-coupled LDPC codes," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8206–8219, Dec. 2019.

[34] L. Song, Q. Huang, and Z. Wang, "Construction of multiple-burst-correction codes in transform domain and its relation to LDPC codes," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 40–54, Jan. 2020.

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

[36] F. Abedi and M. Gholami, "Some explicit constructions of type-II, III, IV, v QCLDPC codes with girth 6," *China Commun.*, vol. 17, no. 5, pp. 89–109, May 2020.

[37] S. Mo, L. Chen, D. J. Costello, D. G. M. Mitchell, R. Smarandache, and J. Qiu, "Designing protograph-based quasi-cyclic spatially coupled LDPC codes with large girth," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5326–5337, Sep. 2020.

MANJIE ZHOU received the B.S. degree from Anyang Normal University, Anyang, China. She is currently a Teaching Assistant with the School of Network Engineering, Zhoukou Normal University. Her research interests include LDPC coding and modern educational technology.

HAI ZHU received the Ph.D. degree from the School of Computer Science and Technology, Xidian University, Xi'an, China. He is currently a Professor with the School of Network Engineering, Zhoukou Normal University. His research interests include information theory, LDPC coding, cloud computing, and the Internet-of-Things technology.

HENGZHOU XU received the B.S. and M.S. degrees from the School of Mathematics and Statistics, Zhengzhou University, China, in 2009 and 2013, respectively, and the Ph.D. degree in communication and information system from Xidian University, China, in 2017. He is currently an Associate Professor with the School of Network Engineering, Zhoukou Normal University, Zhoukou, China. He is also a Visiting Scholar with the School of Mathematical Sciences, Shanghai Jiao Tong University, for the period January 2021–December 2021. His research interests include information theory, channel coding, and combinatorial designs.

BO ZHANG received the B.S. and M.S. degrees from the Second Artillery Engineering College, Xi'an, China, and the Ph.D. degree from the School of Telecommunications Engineering, Xidian University, Xi'an. He is currently an Associate Professor with the Henan Provincial Research Center of Wisdom Education and Intelligent Technology Application Engineering Technology, Zhengzhou, China. His research interests include information theory, LDPC coding, capacity region, and transmission strategies for interference channels.

KAIXUAN XIE received the M.S. degree from Henan University, Kaifeng, China. He is currently a Lecturer with Zhoukou Normal University. His research interests include LDPC coding and administrative law.