IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 December 2023, accepted 27 December 2023, date of publication 19 January 2024, date of current version 23 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3355926

RESEARCH ARTICLE

Tanner (3, 23)-Regular QC-LDPC Codes: Cycle Structure and Girth Distribution

QI WANG[1], JINGPING CHE[1], HUAAN LI[2], ZHEN LUO[1], BO ZHANG[3], AND HUI LIU[3]
[1]School of Network Engineering, Zhoukou Normal University, Zhoukou, Henan 466001, China
[2]School of Physics and Telecommunication Engineering, Zhoukou Normal University, Zhoukou 466001, China
[3]Henan Provincial Research Center of Wisdom Education and Intelligent Technology Application Engineering Technology, Zhengzhou Railway Vocational Technical College, Zhengzhou 450018, China

Corresponding authors: Huaan Li (liha@zknu.edu.cn), Bo Zhang (boboo313313@hotmail.com), and Hui Liu (xdliuhui@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 62172457, in part by the Development Project of Henan Provincial Department of Science and Technology under Grant 232102320066 and Grant 232102211069, and in part by the Key Scientific Research Project in Colleges and Universities of Henan Province under Grant 22A510018 and Grant 23B510008.

ABSTRACT This paper studies a class of quasi-cyclic LDPC (QC-LDPC) codes, i.e., Tanner (3, 23)-regular QC-LDPC codes of code length $23p$ with p being a prime and $p \equiv 1 \pmod{69}$. We first analyze the cycle structure of Tanner (3, 23)-regular QC-LDPC codes, and divide their cycles of lengths 4, 6, 8, and 10 into five equivalent types. We propose the sufficient and necessary condition for the existence of these five types of cycles, i.e., the polynomial equations in a 69th unit root of the prime field $\mathbb{F}_p$. We check the existence of solutions for such polynomial equations by using the Euclidean division algorithm and obtain the candidate girth values of Tanner (3, 23)-regular QC-LDPC codes. We summarize the results and determine the girth distribution of Tanner (3, 23)-regular QC-LDPC codes.

INDEX TERMS LDPC codes, quasi-cyclic (QC), girth, Euclidean division algorithm, prime field.

I. INTRODUCTION

It is well-known that low-density parity-check (LDPC) codes with iterative decoding have the performance extremely close to Shannon capacity [1]. Under the framework of iterative decoding, some structural properties of an LDPC code affect the performance, such as cycle distribution and girth of its Tanner graph [2], variable node (VN) connectivity, row redundancy of its parity-check matrix and other structures [3]. Girth plays an important role in the design and construction of LDPC codes [4]. Hence, constructing LDPC codes with large girth and determining the girth of good LDPC codes are interesting problems in coding theory [5], [6], [7], [8].

In 2001, Tanner proposed a class of famous quasi-cyclic LDPC (QC-LDPC) codes constructed from the multiplicative group over the prime fields [9]. For simplicity's sake, this class of QC-LDPC codes is called Tanner QC-LDPC codes in this paper. It is shown in [10] that the maximum girth value of the fully-connected QC-LDPC codes is 12. Tanner QC-LDPC codes are fully-connected and their largest girth is 12. Hence, determining the girths of Tanner QC-LDPC codes is a very challenging problem.

In 2006, Kim presented the girth distribution of Tanner (3, 5)-regular QC-LDPC codes of code length $5p$ with p being a prime and $p \equiv 1 \pmod{15}$ [11]. The girth distribution of Tanner (3, 5)-regular QC-LDPC codes is given as follows: 1) The minimum girth of Tanner (3, 5)-regular QC-LDPC codes is 8, and there is only one code with girth 8; 2) There are two Tanner (3, 5)-regular QC-LDPC codes with girth 10; 3) The remaining Tanner (3, 5)-regular QC-LDPC codes have girth 12. This result shows that most Tanner (3, 5)-regular QC-LDPC codes have the largest girth value 12. This work is significant and encouraging. It is of interest to determine the girth of other classes of Tanner QC-LDPC codes. For the next few years, the girth problems of several classes of Tanner (γ, ρ)-regular QC-LDPC codes of code length ρp have been solved when p is a prime and $p \equiv 1 \pmod{\gamma\rho}$, e.g., $(\gamma, \rho) = (3, 7)$ [12], (3, 11) [13], (3, 13) [14], (3, 17) [15], and (3, 19) [16]. The results of these works are similar to the conclusion of Tanner (3, 5)-regular QC-LDPC codes in [11]. That is, there are several Tanner (γ, ρ)-regular QC-LDPC codes with girth less than 12, and most Tanner

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

(γ, ρ)-regular QC-LDPC codes have the largest girth value 12. Furthermore, the girths of Tanner (γ, ρ)-regular QC-LDPC codes of finite code lengths are determined based on the cycle-counting algorithm in [17]. Moreover, a conjecture is also given in [17] as follows: Let γ and ρ be two different prime numbers, there exists a minimum prime p_0 such that for $p \geq p_0$, Tanner (γ, ρ)-regular QC-LDPC codes with code length ρp have girth 12 for p being a prime and $p \equiv 1 \pmod{\gamma\rho}$.

In this paper, we study the girth distribution of Tanner (3, 23)-regular QC-LDPC codes with code length $23p$ for p being a prime and $p \equiv 1 \pmod{69}$. The cycle structure of Tanner (3, 23)-regular QC-LDPC codes is first analyzed, and then their cycles of lengths 4, 6, 8, and 10 are divided into five equivalent types. The sufficient and necessary condition for the existence of these five types of cycles, i.e., the polynomial equations in a 69th unit root of the prime field $\mathbb{F}_p$, is proposed. The existence of solutions for such polynomial equations is checked by using the Euclidean division algorithm, and the candidate girth values of Tanner (3, 23)-regular QC-LDPC codes are obtained. Finally, we summarize these obtained candidate girth values and determine the girths of Tanner (3, 23)-regular QC-LDPC codes.

The main contributions of this paper are given as follows.

- We analyze the cycle structure of Tanner (3, 23)-regular QC-LDPC codes of length $23p$ for p being a prime and $p \equiv 1 \pmod{69}$, and present five equivalent types of cycles with length not more than 10.
- Furthermore, we propose the sufficient and necessary condition for the existence of cycles in Tanner (3, 23)-regular QC-LDPC codes, and employ the Euclidean division algorithm to obtain their candidate girth values.
- We determine the girth distribution of Tanner (3, 23)-regular QC-LDPC codes, and numerical results are also provided.

II. TANNER (3, 23)-REGULAR QC-LDPC CODES AND THEIR CYCLE STRUCTURE

Let $\mathbb{F}_p$ a prime field with p being a prime. The parity-check matrix of a Tanner (γ, ρ)-regular QC-LDPC code of length ρp is

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

where $0 \leq i \leq \gamma - 1$ and $0 \leq j \leq \rho - 1$. It is noticed that $\mathbf{I}(a^ib^j)$ is a circulant permutation matrix (CPM) of size $p \times p$ which is created by shifting every row (or column) of an identity matrix of size $p \times p$ to the right (or left) $(a^ib^j \pmod p)$ positions. Moreover, the orders of nonzero elements a and b in $\mathbb{F}_p$ are γ and ρ, respectively. Let $p = \gamma\rho i + 1$. It is easy to see that there is a primitive $(\gamma\rho)$-th unit root in $\mathbb{F}_p$, and for simplicity, we denote it by α. Then b and a can be represented as α^γ and α^ρ, respectively. Hence, the parity-check matrix $\mathbf{H}$ can be rewritten as

$$\mathbf{H} = \left[\mathbf{I}(\alpha^{\rho i+\gamma j})\right], \quad (2)$$

where $0 \leq s \leq \gamma - 1$ and $0 \leq t \leq \rho - 1$.

This paper studies Tanner (3, 23)-regular QC-LDPC codes. That is, $\gamma = 3, \rho = 23$, and $p \equiv 1 \pmod{69}$. The primes of p form a set $\{139, 277, 691, 829, 967, 1381, 1657, 1933, 2347, 3037, 3313, \ldots\}$, and we denote it by P_{69}. Assume that α is a primitive 69th unit root of $\mathbb{F}_p$. Then a Tanner (3, 23)-regular QC-LDPC code of length $23p$ has the following parity-check matrix

$$\mathbf{H} = \left[\mathbf{I}\left(\alpha^{23i+3j}\right)\right].$$

It is shown in [10] that a cycle of length $2s$, called $2s$-cycle, in the Tanner graph of $\mathbf{H}$ in (1) can be marked with the following ordered CPMs:

$$\mathbf{I}(a^{i_0}b^{j_0}), \mathbf{I}(a^{i_1}b^{j_0}), \mathbf{I}(a^{i_1}b^{j_1}), \mathbf{I}(a^{i_2}b^{j_1}), \mathbf{I}(a^{i_2}b^{j_2}), \ldots, \mathbf{I}(a^{i_{k-2}}b^{j_{k-1}}), \mathbf{I}(a^{i_{k-1}}b^{j_{k-1}}), \mathbf{I}(a^{i_0}b^{j_{k-1}}),$$

where $i_k \neq i_{k+1}, j_k \neq j_{k+1}, i_s = i_0$, and $j_s = j_0$ for $0 \leq k \leq s-1$. For simplicity, these ordered CPMs can be written as the following pairs

$$(i_0, j_0); (i_1, j_1); (i_2, j_2); \ldots; (i_{s-2}, j_{s-2}); (i_{s-1}, j_{s-1}); . \quad (3)$$

It is noticed that the semicolon between the pairs (i_k, j_k) and (i_{k+1}, j_{k+1}) represents the CPM $\mathbf{I}(a^{i_{k+1}}b^{j_k})$, and the pair (i_k, j_k) represents the CPM $\mathbf{I}(a^{i_k}b^{j_k})$. For simplicity, the $2s$-cycle marked with (3) is called type $(j_0, j_1, j_2, \ldots, j_{s-1})$. The sufficient and necessary condition for the existence of such a $2s$-cycle had been improved [7]. Assume that the girth is g. For $g \leq 2s \leq (2g-2)$, the sufficient and necessary condition for the existence of a $2s$-cycle marked with (3) is

$$\sum_{k=0}^{s-1} (a^{i_k}b^{j_k} - a^{i_{k+1}}b^{j_k}) = 0 \pmod p \quad (4)$$

with for $0 \leq k \leq s-1$, $i_k \neq i_{k+1}, j_k \neq j_{k+1}, i_s = i_0$, and $j_s = j_0$. Since $a = \alpha^3$ and $b = \alpha^{23}$, the above equation (4) can be rewritten as

$$\sum_{k=0}^{s-1} (\alpha^{23i_k} - \alpha^{23i_{k+1}})\,\alpha^{3j_k} = 0 \pmod p.$$

For the sake of conformity and consistency, the above equation is called basic equation. Without loss of generality, let $j_0 = 0$. According to the type equivalence given in [11], [12], [13], [14], [15], and [16], cycles of lengths 4, 6, 8, and 10 can be also classified into the following five equivalent types.

1) 4-cycles: type (0, 1);
2) 6-cycles: type (0, 1, 2);
3) 8-cycles: types (0, 1, 0, 1) and (0, 1, 0, 2);
4) 10-cycles: type (0, 1, 2, 0, 1).

III. DETERMINING GIRTH DISTRIBUTION OF TANNER (3, 23)-REGULAR QC-LDPC CODES

Assume that $u = j_1 - j_0 \pmod{23}$, $v = j_2 - j_1 \pmod{23}$, $w = j_3 - j_2 \pmod{23}$, and $x = j_4 - j_3 \pmod{23} = j_0 - j_3 \pmod{23}$.

Since $j_k \neq j_{k+1}$ for $0 \leq k \leq 3$, then u, v, w, and x take values in $\{-1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. Next, we consider all types of cycles of length not more than 10.

A. TYPE (0, 1)

All 4-cycles have the unique type (0, 1). Then the corresponding pairs in (3) are (0, 0); (1, u); for $u \neq 0 \pmod{23}$, and the basic equation becomes

$$\begin{aligned}\sum_{k=0}^{1} &(\alpha^{23i_k} - \alpha^{23i_{k+1}})\,\alpha^{3j_k} \\ &= (1-\alpha^{23})(1-\alpha^{3u}) \\ &= 0 \pmod{p}.\end{aligned}$$

Since α is a primitive 69th unit root of $\mathbb{F}_p$, then $\alpha^{23} \neq 1$ and $\alpha^{3u} \neq 1$ with $u \in \{-1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. That is, the above equation is impossible. Hence, Tanner (3, 23)-regular QC-LDPC codes have no 4-cycles.

B. TYPE (0, 1, 2)

All 6-cycles have the unique type (0, 1, 2), and the corresponding ordered pairs in (3) are (0, 0); (1, u); (2, $u+v$); for $u+v \neq 0 \pmod{23}$. The basic equation becomes

$$\begin{aligned}\sum_{k=0}^{2} &(\alpha^{23i_k} - \alpha^{23i_{k+1}})\,\alpha^{3j_k} \\ &= (1-\alpha^{23})(1+\alpha^{3u+23}+\alpha^{3(u+v)-23}) \\ &= 0 \pmod{p}.\end{aligned}$$

Since $\alpha^{23} \neq 1$, the above basic equation can be simplified as

$$1+\alpha^{3u+23}+\alpha^{3(u+v)-23} = 0 \pmod{p}. \tag{5}$$

The above equation is call modified basic equation in this paper. Hence, a 6-cycle exists if only if the modified basic equation in (5) holds for some pairs (u, v). We next consider all pairs of (u, v), and there are two classes of cases. The first case is the pair (u, v) for $u+v = 0 \pmod{23}$. It can be seen from the ordered pairs in (3) that $u+v \neq 0 \pmod{23}$. Hence, there is no 6-cycles in this case. For simplicity, this case is denoted by invalid case, and the corresponding pair is (u, v) for $u+v = 0 \pmod{23}$. The second case is the pair (u, v) for $u+v \neq 0 \pmod{23}$. In the following, we only consider these cases.

Assume that u is a variable and v can be expressed by employing u. Then all pairs (u, v) can be found and we list them in Table 1. It is noticed that the pair with index number 12 is invalid case, and the other pairs are valid cases. According to each valid case, we check whether equation (5) has solution over $\mathbb{F}_p$, and obtain the candidate primes p.

1) PAIR (U, U)

According to this pair (u, u), the modified basic equation (5) becomes

$$\begin{aligned}1+\alpha^{3u+23}+\alpha^{6u-23} &= 1+\alpha^{3u+23}+\alpha^{6u+46} \\ &= 1+\alpha^{3u+23}+\left(\alpha^{3u+23}\right)^2.\end{aligned}$$

Assume that $z = \alpha^{3u+23}$. Then z^k can be expressed as the powers of α for $1 \leq k \leq 69$, and we record them in Table 2. Hence, the modified basic equation (5) becomes

$$z^2+z+1 \neq 0.$$

Since $u \in \{-1, -2, -3, -4, -5, -6, -7, -8, -9, -10, -11, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and

$$z^3 = \left(\alpha^{3u+23}\right)^3 = \alpha^{9u+69} = \alpha^{9u} \neq 1,$$

then

$$z^3-1 = (z-1)\left(z^2+z+1\right) \neq 0.$$

Therefore, $z^2+z+1 \neq 0$. For the pair (u, u), the modified basic equation has no solution over $\mathbb{F}_p$ and there is no 6-cycle in Tanner (3, 23)-regular QC-LDPC codes.

2) PAIR (U, 2U)

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes

$$z^{26}+z+1 = 0 \pmod{p}.$$

Since z is a primitive 69th unit root of $\mathbb{F}_p$, then $z-1 \neq 0$, $z^3-1 \neq 0$, and $z^{23}-1 \neq 0$. That is,

$$z^3-1 = (z-1)(z^2+z+1) \neq 0$$

and

$$\begin{aligned}z^{23}-1 = (z-1)(&z^{22}+z^{21}+z^{20}+z^{19}+z^{18}+z^{17}+z^{16} \\ &+z^{15}+z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^9+z^8 \\ &+z^7+z^6+z^5+z^4+z^3+z^2+z+1) \neq 0.\end{aligned}$$

Hence, $z^2+z+1 \neq 0$ and $z^{22}+z^{21}+z^{20}+z^{19}+z^{18}+z^{17}+z^{16}+z^{15}+z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^9+z^8+z^7+z^6+z^5+z^4+z^3+z^2+z+1 \neq 0$. Moreover, the equation $z^{69}-1=0$ can be factorized into

$$\begin{aligned}&z^{69}-1) \\ &= (z-1)(z^{22}+z^{21}+z^{20}+z^{19}+z^{18}+z^{17}+z^{16} \\ &\quad +z^{15}+z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^9+z^8 \\ &\quad +z^7+z^6+z^5+z^4+z^3+z^2+z+1)(z^2+z+1) \\ &\quad (z^{44}-z^{43}+z^{41}-z^{40}+z^{38}-z^{37} \\ &\quad +z^{35}-z^{34}+z^{32}-z^{31}+z^{29}-z^{28}+z^{26} \\ &\quad -z^{25}+z^{23}-z^{22}+z^{21}-z^{19}+z^{18}-z^{16} \\ &\quad +z^{15}-z^{13}+z^{12}-z^{10}+z^9-z^7+z^6-z^4 \\ &\quad +z^3-z+1) = 0.\end{aligned}$$

TABLE 1. All pairs (u, v), modified basic equations, and p in type (0, 1, 2).

No	(u, v)	Modified basic equation	Modified basic equation	p
1	(u, u)	$1+\alpha^{3u+23}+\alpha^{6u-23}$	$1+z+z^2$	None
2	$(u, 2u)$	$1+\alpha^{3u+23}+\alpha^{9u-23}$	$1+z+z^{26}$	139,277
3	$(u, 3u)$	$1+\alpha^{3u+23}+\alpha^{12u-23}$	$1+z+z^{50}$	89839
4	$(u, 4u)$	$1+\alpha^{3u+23}+\alpha^{15u-23}$	$1+z+z^5$	55201
5	$(u, 5u)$	$1+\alpha^{3u+23}+\alpha^{18u-23}$	$1+z+z^{29}$	89839
6	$(u, 6u)$	$1+\alpha^{3u+23}+\alpha^{21u-23}$	$1+z+z^{53}$	55201
7	$(u, 7u)$	$1+\alpha^{3u+23}+\alpha^{24u-23}$	$1+z+z^8$	139,277
8	$(u, 8u)$	$1+\alpha^{3u+23}+\alpha^{27u-23}$	$1+z+z^{32}$	89839
9	$(u, 9u)$	$1+\alpha^{3u+23}+\alpha^{30u-23}$	$1+z+z^{56}$	55201
10	$(u, 10u)$	$1+\alpha^{3u+23}+\alpha^{33u-23}$	$1+z+z^{11}$	139,277
11	$(u, 11u)$	$1+\alpha^{3u+23}+\alpha^{36u-23}$	$1+z+z^{35}$	None
12	$(u, -u)$	None	None	None
13	$(u, -2u)$	$1+\alpha^{3u+23}+\alpha^{66u-23}$	$1+z+z^{68}$	None
14	$(u, -3u)$	$1+\alpha^{3u+23}+\alpha^{63u-23}$	$1+z+z^{44}$	139,277
15	$(u, -4u)$	$1+\alpha^{3u+23}+\alpha^{60u-23}$	$1+z+z^{20}$	89839
16	$(u, -5u)$	$1+\alpha^{3u+23}+\alpha^{57u-23}$	$1+z+z^{65}$	55201
23	$(u, -6u)$	$1+\alpha^{3u+23}+\alpha^{54u-23}$	$1+z+z^{41}$	89839
18	$(u, -7u)$	$1+\alpha^{3u+23}+\alpha^{51u-23}$	$1+z+z^{17}$	55201
19	$(u, -8u)$	$1+\alpha^{3u+23}+\alpha^{48u-23}$	$1+z+z^{62}$	139,277
20	$(u, -9u)$	$1+\alpha^{3u+23}+\alpha^{45u-23}$	$1+z+z^{38}$	89839
21	$(u, -10u)$	$1+\alpha^{3u+23}+\alpha^{42u-23}$	$1+z+z^{14}$	55201
22	$(u, -11u)$	$1+\alpha^{3u+23}+\alpha^{39u-23}$	$1+z+z^{59}$	139,277

TABLE 2. z^k represented by the powers of α.

z^k	α^j	z^k	α^j	z^k	α^j	z^k	α^j	z^k	α^j	z^k	α^j
z	α^{3u+23}	z^2	α^{6u+46}	z^3	α^{9u}	z^4	α^{12u+23}	z^5	α^{15u+46}	z^6	α^{18u}
z^7	α^{21u+23}	z^8	α^{24u+46}	z^9	α^{27u}	z^{10}	α^{30u+23}	z^{11}	α^{33u+46}	z^{12}	α^{36u}
z^{13}	α^{39u+23}	z^{14}	α^{42u+46}	z^{15}	α^{45u}	z^{16}	α^{48u+23}	z^{17}	α^{51u+46}	z^{18}	α^{54u}
z^{19}	α^{57u+23}	z^{20}	α^{60u+46}	z^{21}	α^{63u}	z^{22}	α^{66u+23}	z^{23}	α^{46}	z^{24}	α^{3u}
z^{25}	α^{6u+23}	z^{26}	α^{9u+46}	z^{27}	α^{12u}	z^{28}	α^{15u+23}	z^{29}	α^{18u+46}	z^{30}	α^{21u}
z^{31}	α^{24u+23}	z^{32}	α^{27u+46}	z^{33}	α^{30u}	z^{34}	α^{33u+23}	z^{35}	α^{36u+46}	z^{36}	α^{39u}
z^{37}	α^{42u+23}	z^{38}	α^{45u+46}	z^{39}	α^{48u}	z^{40}	α^{51u+23}	z^{41}	α^{54u+46}	z^{42}	α^{57u}
z^{43}	α^{60u+23}	z^{44}	α^{63u+46}	z^{45}	α^{66u}	z^{46}	α^{23}	z^{47}	α^{3u+46}	z^{48}	α^{6u}
z^{49}	α^{9u+23}	z^{50}	α^{12u+46}	z^{51}	α^{15u}	z^{52}	α^{18u+23}	z^{53}	α^{21u+46}	z^{54}	α^{24u}
z^{55}	α^{27u+23}	z^{56}	α^{30u+46}	z^{57}	α^{33u}	z^{58}	α^{36u+23}	z^{59}	α^{39u+46}	z^{60}	α^{42u}
z^{61}	α^{45u+23}	z^{62}	α^{48u+46}	z^{63}	α^{51u}	z^{64}	α^{54u+23}	z^{65}	α^{57u+46}	z^{66}	α^{60u}
z^{67}	α^{63u+23}	z^{68}	α^{66u+46}	z^{69}	$\alpha^0(=1)$						

Since $z-1\neq 0$, $z^{22}+z^{21}+z^{20}+z^{19}+z^{18}+z^{17}+z^{16}+z^{15}+z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^9+z^8+z^7+z^6+z^5+z^4+z^3+z^2+z+1\neq 0$, $z^2+z+1\neq 0$, then

$$\begin{aligned}
&z^{44}-z^{43}+z^{41}-z^{40}+z^{38}-z^{37}+z^{35}-z^{34}+z^{32}\\
&\quad -z^{31}+z^{29}-z^{28}+z^{26}-z^{25}+z^{23}-z^{22}+z^{21}-z^{19}\\
&\quad +z^{18}-z^{16}+z^{15}-z^{13}+z^{12}-z^{10}+z^9-z^7+z^6-z^4\\
&\quad +z^3-z+1=0 \pmod p
\end{aligned}\tag{6}$$

Furthermore, the modified basic equation $z^{26}+z+1$ can be factorized into

$$\begin{aligned}
z^{26}+z+1=(z^2+z+1)(&z^{24}-z^{23}+z^{21}-z^{20}+z^{18}\\
&-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^9-z^8+z^6\\
&-z^5+z^3-z^2+1).
\end{aligned}$$

Since $z^2+z+1\neq 0$, then $z^{26}+z+1$ becomes $z^{24}-z^{23}+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^9-z^8+z^6-z^5+z^3-z^2+1$. This equation is called reduced form of $z^{26}+z+1$. By applying the Euclidean division algorithm to the reduced form and equation (6), we can obtain the remainder polynomials as follows:

$$\begin{aligned}
&z^{21}-z^{20}-z^{19}+z^{18}-z^{16}+z^{15}-z^{13}+z^{12}-z^{10}\\
&\quad +z^9-z^7+z^6-z^4+z^3-z+1,\ z^{20}+z^{19}-z^{18}+z^{16}\\
&\quad -z^{15}+z^{13}-z^{12}+z^{10}-z^9+z^7-z^6+z^4-z^3,\ 2z^{19}
\end{aligned}$$

$$- z^{18} - z^{17} + 2z^{16} - z^{15} - z^{14} + 2z^{13} - z^{12} - z^{11} + 2z^{10} - z^9 - z^8 + 2z^7 - z^6 - z^5 + 2z^4 - z^3 - z + 1, (1/4)z^{18} - (1/4)z^{17} + (1/4)z^{15} - (1/4)z^{14} + (1/4)z^{12} - (1/4)z^{11} + (1/4)z^9 - (1/4)z^8 + (1/4)z^6 - (1/4)z^5 - (1/4)z^3 + (1/2)z^2 + (1/4)z - 3/4, 4z^4 - 4z^3 - 4z^2 + 4z + 4, (25/4)z^3 + 3z^2 - (21/4)z - 19/4, (1376/625)z^2 + (1292/625)z - 312/625, -(539375/473344)z - 1278125/236672, 18225164032/465480625.$$

The remainder 18225164032/465480625 equals zero over $\mathbb{F}_{139}$ and $\mathbb{F}_{277}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{139, 277\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 139$ and $p = 277$.

3) PAIR $(U, 3U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{50} + z + 1 = 0 \pmod p$, and it can be factorized into

$$z^{50} + z + 1 = (z^2 + z + 1)(z^{48} - z^{47} + z^{45} - z^{44} + z^{42} - z^{41} + z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1).$$

By applying the Euclidean division algorithm to the reduced form $z^{48} - z^{47} + z^{45} - z^{44} + z^{42} - z^{41} + z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), the remainder polynomials are given as follows:

$$z^{44} - z^{43} + z^{41} - z^{40} + z^{38} - z^{37} + z^{35} - z^{34} + z^{32} - z^{31} + z^{29} - z^{28} + z^{26} - z^{25} + z^{23} - z^{22} + z^{21} - z^{19} + z^{18} - z^{16} + z^{15} - z^{13} + z^{12} - z^{10} + z^9 - z^7 + z^6 - z^4 + z^3 - z + 1, -z^{25} + z^{24} - z^{22} + z^{21} - z^{19} + z^{18} - z^{16} + z^{15} - z^{13} + z^{12} - z^{10} + z^9 - z^7 + z^6 - z^4 + z^3 - z^2 + 1, z^{18} - z^{16} + z^{15} - z^{13} + z^{12} - z^{10} + z^9 - z^7 + z^6 - z^4 + z^3 - z + 1, -z^{17} + z^{16} - z^{14} + z^{13} - z^{11} + z^{10} - z^8 + z^7 - z^4 + 2z^3 - 3z^2 + 2z, z^6 - z^5 - z^2 + z + 1, 3z^5 + 4z^3 - 4z^2 - 4z - 3, -(4/3)z^4 + (8/3)z^3 - z^2 + (2/3)z, (55/4)z^3 - 7z^2 - z - 3, - (257/3025)z^2 + (1574/3025)z + 1312/3025, (35803900/66049)z + 25836525/66049, 5933776111/423774960400.$$

The remainder 5933776111/423774960400 equals zero over $\mathbb{F}_{89839}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{89839\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 89839$.

4) PAIR $(U, 4U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^5 + z + 1 = 0 \pmod p$, and it can be factorized into

$$z^5 + z + 1 = (z^2 + z + 1)(z^3 - z^2 + 1).$$

By applying the Euclidean division algorithm to the reduced form $z^3 - z^2 + 1$ and equation (6), the remainder polynomials are given as follows:

$$- 35z^2 + 119z + 111, (1983/175)z + 1507/175, 1380025/3932289.$$

The remainder 1380025/3932289 equals zero over $\mathbb{F}_{55201}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{55201\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 55201$.

5) PAIR $(U, 5U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{29} + z + 1 = 0 \pmod p$, and it can be factorized into

$$z^{29} + z + 1 = (z^2 + z + 1)(z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1).$$

By applying the Euclidean division algorithm to the reduced form $z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), the remainder polynomials are given as follows:

$$z^{21} - z^{20} + z^{18} - z^{17} - z^{16} + z^{15} - z^{13} + z^{12} - z^{10} + z^9 - z^7 + z^6 - z^4 + z^3 - z + 1, z^{17} + z^{16} - z^{15} + z^{13} - z^{12} + z^{10} - z^9 + z^7 - z^6, -7z^{16} + z^{15} + 6z^{14} - 7z^{13} + z^{12} + 6z^{11} - 7z^{10} + z^9 + 7z^8 - 10z^7 + 6z^6 - z^4 + z^3 - z + 1, (1/49)z^{15} - (1/49)z^{14} + (1/49)z^{12} - (1/49)z^{11} + (8/49)z^9 - (2/7)z^8 + (11/49)z^7 - (1/49)z^6 - (1/7)z^5 - (1/49)z^4 + (8/49)z^3 - (1/7)z^2 - (1/49)z + 8/49, 49z^{10} - 49z^9 + 49z^7 - 49z^6 - 49z^5 + 49z^4 - 49z^2 + 49z + 49, (8/49)z^9 - (2/7)z^8 + (11/49)z^7 - (1/49)z^6 - (1/7)z^5 - (2/49)z^4 + (8/49)z^3 - (6/49)z^2 - (2/49)z + 1/7, -(49/16)z^8 + (147/32)z^7 - (49/32)z^6 - (147/32)z^5 + (147/16)z^4 - (147/16)z^2 + (245/16)z + 539/32, (4/49)z^7 - (12/49)z^6 + (20/49)z^5 - (8/49)z^4 - (16/49)z^3 + (40/49)z^2 + (32/49)z - 4/49, (49/4)z^5 - (49/4)z^4 + (49/4)z^3 + (245/4)z^2 + 49z + 49/4, -(12/49)z^4 + (4/7)z^2 + (8/49)z$$

$$-12/49, (245/6)z^3+(245/6)z^2+(343/12)z + 49/2, (122/245)z^2+(34/245)z-96/245, (781501/14884)z + 354809/7442, -1337163676/12464159449.$$

The remainder $-1337163676/12464159449$ equals zero over $\mathbb{F}_{89839}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{89839\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 89839$.

6) PAIR $(U, 6U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{53}+z+1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} z^{53}&+z+1 \\ &= (z^2+z+1)(z^{51}-z^{50}+z^{48}-z^{47}+z^{45} \\ &\quad -z^{44}+z^{42}-z^{41}+z^{39}-z^{38}+z^{36}-z^{35}+z^{33} \\ &\quad -z^{32}+z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21} \\ &\quad -z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^9 \\ &\quad -z^8+z^6-z^5+z^3-z^2+1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{51}-z^{50}+z^{48}-z^{47}+z^{45}-z^{44}+z^{42}-z^{41}+z^{39}-z^{38}+z^{36}-z^{35}+z^{33}-z^{32}+z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^9-z^8+z^6-z^5+z^3-z^2+1$ and equation (6), the remainder polynomials are given as follows:

$$\begin{aligned} &-z^{28}+z^{27}-z^{25}+z^{24}-z^{22}+z^{21}-z^{19}+z^{18}-z^{16} \\ &\quad +z^{15}-z^{13}+z^{12}-z^{10}+z^9-z^7+z^6-z^5+z^3 \\ &\quad -z^2+1, z^{15}-z^{13}+z^{12}-z^{10}+z^9-z^7+z^6-z^4 \\ &\quad +z^3-z+1, -z^{14}+z^{13}-z^{10}+2z^9-2z^8+z^7-z^5 \\ &\quad +2z^3-3z^2+2z, z^{12}-z^{11}+z^9-z^8-z^5+z^4 \\ &\quad -z^2+z+1, z^{11}-2z^{10}+2z^9-2z^8+z^6-z^5-z^4 \\ &\quad +3z^3-2z^2+2z, z^9+z^8-z^7+z^5-z^4-z^3 \\ &\quad -z^2-z+1, -11z^8+5z^7+5z^6-9z^5+3z^4+7z^3 \\ &\quad +11z-6, (14/121)z^7-(19/121)z^6+(10/121)z^5 \\ &\quad +(4/121)z^4-(9/121)z^3-(1/11)z+25/121, \\ &\quad -(121/196)z^6 \\ &\quad +(121/98)z^5-(121/98)z^4+(121/196)z^3-(121/14)z^2 \\ &\quad +(4477/196)z+2299/196, -(196/121)z^3+(392/121)z^2 \\ &\quad +(588/121)z+196/121, -(121/4)z^2+(121/98)z \\ &\quad +1089/196, (27816/5929)z+13060/5929, \\ &\quad -327286729/193432464. \end{aligned}$$

The remainder $-327286729/193432464$ equals zero over $\mathbb{F}_{55201}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{55201\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 55201$.

7) PAIR $(U, 7U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^8+z+1 = 0 \pmod p$, and it can be factorized into

$$z^8+z+1 = (z^2+z+1)(z^6-z^5+z^3-z^2+1).$$

By applying the Euclidean division algorithm to the reduced form $z^6-z^5+z^3-z^2+1$ and equation (6), the remainder polynomials are given as follows:

$$\begin{aligned} &-4z^5+3z^4+z^3-3z^2+8z+9, (1/16)z^4+(3/16)z^3 \\ &\quad +(19/16)z^2+(7/4)z+7/16, 32z^3-176z^2-384z-96, \\ &\quad (311/64)z^2+(133/16)z+65/32, -(258304/96721)z \\ &\quad +43584/96721, 3724048663/1042514944. \end{aligned}$$

The remainder $3724048663/1042514944$ equals zero over $\mathbb{F}_{139}$ and $\mathbb{F}_{277}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{139, 277\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 139$ and $p = 277$.

8) PAIR $(U, 8U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{32}+z+1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} z^{32}+z+1 = (z^2+z+1)(&z^{30}-z^{29}+z^{27}-z^{26}+z^{24} \\ &-z^{23}+z^{21}-z^{20}+z^{18}-z^{17} \\ &+z^{15}-z^{14}+z^{12}-z^{11}+z^9-z^8 \\ &+z^6-z^5+z^3-z^2+1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^9-z^8+z^6-z^5+z^3-z^2+1$ and equation (6), we can obtain 13 remainder polynomials. For convenience, we only give the last remainder, i.e., $135400640782876/64818037431225$. The remainder $135400640782876/64818037431225$ equals zero over $\mathbb{F}_{89839}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{89839\}$. For $p \in P_{69}$, the remaining 12 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 89839$.

9) PAIR $(U, 9U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{56}+z+1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} z^{56}+z+1 = (z^2+z+1)(&z^{54}-z^{53}+z^{51}-z^{50}+z^{48} \\ &-z^{47}+z^{45}-z^{44}+z^{42}-z^{41}+z^{39} \\ &-z^{38}+z^{36}-z^{35}+z^{33}-z^{32}+z^{30} \\ &-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21} \\ &-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12} \\ &-z^{11}+z^9-z^8+z^6-z^5+z^3-z^2+1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{54}-z^{53}+z^{51}-z^{50}+z^{48}-z^{47}+z^{45}-z^{44}+z^{42}-z^{41}+z^{39}-z^{38}+z^{36}-z^{35}+z^{33}-z^{32}+z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}-z^{8}+z^{6}-z^{5}+z^{3}-z^{2}+1$ and equation (6), we can obtain 13 remainder polynomials. For convenience, we only give the last remainder, i.e., 240777271457728201/668765977460100. The remainder 240777271457728201/668765977460100 equals zero over $\mathbb{F}_{55201}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{55201\}$. For $p \in P_{69}$, the remaining 12 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 55201$.

10) PAIR $(U, 10U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{11}+z+1 = 0 \pmod p$, and it can be factorized into

$$z^{11}+z+1 = (z^2+z+1)(z^9-z^8+z^6-z^5+z^3-z^2+1).$$

By applying the Euclidean division algorithm to the reduced form $z^9-z^8+z^6-z^5+z^3-z^2+1$ and equation (6), we can obtain 5 remainder polynomials. For convenience, we only give the last remainder, i.e., 1219929052/3339106225. The remainder 1219929052/3339106225 equals zero over $\mathbb{F}_{139}$ and $\mathbb{F}_{277}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{139, 277\}$. For $p \in P_{69}$, the remaining 4 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 139$ and $p = 277$.

11) PAIR $(U, 11U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{35}+z+1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned}z^{35}+z+1 = (z^2+z+1)(&z^{33}-z^{32}+z^{30}-z^{29}+z^{27}\\&-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}\\&-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}\\&-z^{8}+z^{6}-z^{5}+z^{3}-z^{2}+1).\end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{33}-z^{32}+z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}-z^{8}+z^{6}-z^{5}+z^{3}-z^{2}+1$ and equation (6), the remainder polynomials are given as follows:

$$\begin{aligned}&z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}-z^{10}\\&+z^{9}-z^{7}+z^{6}-z^{4}+z^{3}-z+1,\ z^{11},\ -z^{10}\\&+z^{9}-z^{7}+z^{6}-z^{4}+z^{3}-z+1,\ z^{9}-z^{8}+z^{6}\\&-z^{5}+z^{3}-z^{2}+1,\ 1.\end{aligned}$$

All remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$.

12) PAIR $(U, -2U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{68}+z+1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned}z^{68}+z+1 = (z^2+z+1)(&z^{66}-z^{65}+z^{63}-z^{62}+z^{60}\\&-z^{59}+z^{57}-z^{56}+z^{54}-z^{53}+z^{51}-z^{50}\\&+z^{48}-z^{47}+z^{45}-z^{44}+z^{42}-z^{41}+z^{39}\\&-z^{38}+z^{36}-z^{35}+z^{33}-z^{32}+z^{30}-z^{29}\\&+z^{27}-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}\\&-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}-z^{8}\\&+z^{6}-z^{5}+z^{3}-z^{2}+1).\end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{66}-z^{65}+z^{63}-z^{62}+z^{60}-z^{59}+z^{57}-z^{56}+z^{54}-z^{53}+z^{51}-z^{50}+z^{48}-z^{47}+z^{45}-z^{44}+z^{42}-z^{41}+z^{39}-z^{38}+z^{36}-z^{35}+z^{33}-z^{32}+z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}-z^{8}+z^{6}-z^{5}+z^{3}-z^{2}+1$ and equation (6), the remainder polynomials are given as follows:

$$\begin{aligned}&-z^{43}+z^{42}-z^{40}+z^{39}-z^{37}+z^{36}-z^{34}+z^{33}-z^{31}\\&+z^{30}-z^{28}+z^{27}-z^{25}+z^{24}-z^{22}+z^{21}-z^{20}\\&+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}-z^{8}\\&+z^{6}-z^{5}+z^{3}-z^{2}+1,\ 1.\end{aligned}$$

All remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$.

13) PAIR $(U, -3U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{44}+z+1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned}z^{44}+z+1 = (z^2+z+1)(&z^{42}-z^{41}+z^{39}-z^{38}+z^{36}\\&-z^{35}+z^{33}-z^{32}+z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}\\&+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}-z^{8}\\&+z^{6}-z^{5}+z^{3}-z^{2}+1).\end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{42}-z^{41}+z^{39}-z^{38}+z^{36}-z^{35}+z^{33}-z^{32}+z^{30}-z^{29}+z^{27}-z^{26}+z^{24}-z^{23}+z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}-z^{8}+z^{6}-z^{5}+z^{3}-z^{2}+1$ and equation (6), the remainder polynomials are given as follows:

$$\begin{aligned}&z^{21}-z^{20}+z^{18}-z^{17}+z^{15}-z^{14}+z^{12}-z^{11}+z^{9}\\&-z^{8}+z^{6}-z^{5}+z^{3}-z^{2}-z+1,\ -z^{19}+z^{18}-z^{16}+z^{15}\\&-z^{13}+z^{12}-z^{10}+z^{9}-z^{7}+z^{6}-z^{4}+z^{3}+z^{2},\ z^{4}\\&+z^{3}-z^{2}-z+1,\ -116z^{3}+26z^{2}\\&+121z-79,\ (267/841)z^{2}\\&-(2719/6728)z+1119/6728,\ (30685567/1140624)z\\&-5803741/380208,\ 43917445872/1119624283129.\end{aligned}$$

The remainder 43917445872/1119624283129 equals zero over $\mathbb{F}_{139}$ and $\mathbb{F}_{277}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{139, 277\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero.

Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 139$ and $p = 277$.

14) PAIR $(U, -4U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{20} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} &z^{20} + z + 1 \\ &= (z^2 + z + 1)(z^{18} - z^{17} + z^{15} - z^{14} + z^{12} \\ &\quad - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), we can obtain 6 remainder polynomials. For convenience, we only give the last remainder, i.e., $319218180775/7425145407744$. The remainder $319218180775/7425145407744$ equals zero over $\mathbb{F}_{89839}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{89839\}$. For $p \in P_{69}$, the remaining 5 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 89839$.

15) PAIR $(U, -5U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{65} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} &z^{65} + z + 1 \\ &= (z^2 + z + 1)(z^{63} - z^{62} + z^{60} - z^{59} + z^{57} \\ &\quad - z^{56} + z^{54} - z^{53} + z^{51} - z^{50} + z^{48} - z^{47} + z^{45} \\ &\quad - z^{44} + z^{42} - z^{41} + z^{39} - z^{38} + z^{36} - z^{35} + z^{33} \\ &\quad - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} \\ &\quad - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 \\ &\quad - z^8 + z^6 - z^5 + z^3 - z^2 + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{63} - z^{62} + z^{60} - z^{59} + z^{57} - z^{56} + z^{54} - z^{53} + z^{51} - z^{50} + z^{48} - z^{47} + z^{45} - z^{44} + z^{42} - z^{41} + z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), the remainder polynomials are given as follows:

$$\begin{aligned} &- z^{40} + z^{39} - z^{37} + z^{36} - z^{34} + z^{33} - z^{31} + z^{30} - z^{28} \\ &\quad + z^{27} - z^{25} + z^{24} - z^{22} + z^{21} - z^{19} + z^{18} - z^{17} + z^{15} \\ &\quad - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1, \\ &\quad + z^3 - z + 1, -22042z^2 + 29199z - 16638, \\ &\quad - (2959/485849764)z + 18401/242924882, \\ &\quad - 26819392822564/8755681. \end{aligned}$$

The remainder $-26819392822564/8755681$ equals zero over $\mathbb{F}_{55201}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{55201\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 55201$.

16) PAIR $(U, -6U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{41} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} &z^{41} + z + 1 \\ &= (z^2 + z + 1)(z^{39} - z^{38} + z^{36} - z^{35} + z^{33} \\ &\quad - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} \\ &\quad - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} \\ &\quad + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), we can obtain 13 remainder polynomials. For convenience, we only give the last remainder, i.e., $531618295894375/1837859751450813321$. The remainder $531618295894375/1837859751450813321$ equals zero over $\mathbb{F}_{89839}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{89839\}$. For $p \in P_{69}$, the remaining 12 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 89839$.

17) PAIR $(U, -7U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{17} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} z^{17} + z + 1 = (z^2 + z + 1)(z^{15} - z^{14} + z^{12} - z^{11} + z^9 \\ - z^8 + z^6 - z^5 + z^3 - z^2 + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), the remainder polynomials are given as follows:

$$\begin{aligned} &z^{12} + z^{11} - z^{10} + z^8 - z^7 - z^4 + z^3 - z + 1, 5z^{11} - z^{10} \\ &\quad - 4z^9 + 6z^8 - 3z^7 - 2z^6 + 4z^5 - 6z^4 + 2z^3 \\ &\quad + 4z^2 - 7z + 5, \\ &\quad (1/25)z^{10} - (6/25)z^9 + (4/25)z^8 + (3/25)z^7 - (8/25)z^6 \\ &\quad + (6/25)z^5 + (1/25)z^4 - (7/25)z^3 + (11/25)z^2 - (8/25)z \\ &\quad - 1/5, 150z^9 - 125z^8 - 50z^7 + 200z^6 - 175z^5 + 150z^3 \\ &\quad - 275z^2 + 250z + 150, (1/900)z^8 - (1/450)z^7 \\ &\quad + (1/450)z^6 \\ &\quad - (1/900)z^5 - (1/180)z^2 - (7/450)z + 1/150, 900z^3 \\ &\quad + 2700z^2 + 1800z - 900, (13/60)z^2 + (17/50)z \\ &\quad - 119/900, (55524/169)z - 19296/169, \\ &\quad 9328969/770728644. \end{aligned}$$

The remainder $9328969/770728644$ equals zero over $\mathbb{F}_{55201}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69}\backslash\{55201\}$. For $p \in P_{69}$, the other remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 55201$.

18) PAIR $(U, -8U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{62} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} &z^{62} + z + 1 \\ &= (z^2 + z + 1)(z^{60} - z^{59} + z^{57} - z^{56} + z^{54} \\ &\quad - z^{53} + z^{51} - z^{50} + z^{48} - z^{47} + z^{45} - z^{44} + z^{42} \\ &\quad - z^{41} + z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} \\ &\quad - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} \\ &\quad - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 \\ &\quad + z^6 - z^5 + z^3 - z^2 + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{60} - z^{59} + z^{57} - z^{56} + z^{54} - z^{53} + z^{51} - z^{50} + z^{48} - z^{47} + z^{45} - z^{44} + z^{42} - z^{41} + z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), we can obtain 8 remainder polynomials. For convenience, we only give the last remainder, i.e., 27415516563568/12699665468281. The remainder 27415516563568/12699665468281 equals zero over $\mathbb{F}_{139}$ and $\mathbb{F}_{277}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69} \backslash \{139, 277\}$. For $p \in P_{69}$, the remaining 7 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 139$ and $p = 277$.

19) PAIR $(U, -9U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{38} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} z^{38} + z + 1 = (z^2 + z + 1)(&z^{36} - z^{35} + z^{33} - z^{32} + z^{30} \\ &- z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} \\ &+ z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 \\ &- z^8 + z^6 - z^5 + z^3 - z^2 + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{36} - z^{35} + z^{33} - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), we can obtain 14 remainder polynomials. For convenience, we only give the last remainder, i.e., 48533273775/1375445569. The remainder 48533273775/1375445569 equals zero over $\mathbb{F}_{89839}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69} \backslash \{89839\}$. For $p \in P_{69}$, the remaining 13 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 89839$.

20) PAIR $(U, -10U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{14} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} z^{14} + z + 1 = (&z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1) \\ &\times (z^2 + z + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), we can obtain 9 remainder polynomials. For convenience, we only give the last remainder, i.e., $-186497441015625/44579150804644$. The remainder $-186497441015625/44579150804644$ equals zero over $\mathbb{F}_{55201}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69} \backslash \{55201\}$. For $p \in P_{69}$, the remaining 8 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 55201$.

21) PAIR $(U, -11U)$

Assume that $z = \alpha^{3u+23}$. According to Tables 1 and 2, the modified basic equation becomes $z^{59} + z + 1 = 0 \pmod p$, and it can be factorized into

$$\begin{aligned} z^{59} + z + 1 = (z^2 + z + 1)(&z^{57} - z^{56} + z^{54} - z^{53} + z^{51} \\ &- z^{50} + z^{48} - z^{47} + z^{45} - z^{44} + z^{42} - z^{41} \\ &+ z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} \\ &- z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} \\ &+ z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 \\ &- z^8 + z^6 - z^5 + z^3 - z^2 + 1). \end{aligned}$$

By applying the Euclidean division algorithm to the reduced form $z^{57} - z^{56} + z^{54} - z^{53} + z^{51} - z^{50} + z^{48} - z^{47} + z^{45} - z^{44} + z^{42} - z^{41} + z^{39} - z^{38} + z^{36} - z^{35} + z^{33} - z^{32} + z^{30} - z^{29} + z^{27} - z^{26} + z^{24} - z^{23} + z^{21} - z^{20} + z^{18} - z^{17} + z^{15} - z^{14} + z^{12} - z^{11} + z^9 - z^8 + z^6 - z^5 + z^3 - z^2 + 1$ and equation (6), we can obtain 9 remainder polynomials. For convenience, we only give the last remainder, i.e., 5856306300/248451405601. The remainder 5856306300/248451405601 equals zero over $\mathbb{F}_{139}$ and $\mathbb{F}_{277}$, but nonzero in $\mathbb{F}_p$ for $p \in P_{69} \backslash \{139, 277\}$. For $p \in P_{69}$, the remaining 8 remainders over $\mathbb{F}_p$ do not equal zero. Hence, the basic equation has no solution over $\mathbb{F}_p$ apart from $p = 139$ and $p = 277$.

Based on the aforementioned twenty-one valid pairs (u, v), we can obtain the following conclusion: The girth of Tanner (3, 23)-regular QC-LDPC code of length $23p$ is 6 for $p = 139, 277, 55201$, or 89839. To facilitate reading, the modified basic equations, the reduced forms, and the primes p are recorded in Table 1 for type (0, 1, 2).

C. *TYPE* (0, 1, 0, 1)

There are two types for all 8-cycles. The first type (0, 1, 0, 1) has the ordered following pairs: (0, 0); $(1, u)$; $(0, u + v)$; $(1, u + v + w)$; for $u + v + w \neq 0 \pmod{23}$, and the basic equation becomes

$$\sum_{k=0}^{3} (\alpha^{23 i_k} - \alpha^{23 i_{k+1}})\, \alpha^{3 j_k}$$

TABLE 3. Representation of A^k by the powers of α.

A^k	α^l	A^k	α^l	A^k	α^l	A^k	α^l	A^k	α^l
A	α^{3i}	A^2	α^{6i}	A^3	α^{9i}	A^4	α^{12i}	A^5	α^{15i}
A^6	α^{18i}	A^7	α^{21i}	A^8	α^{24i}	A^9	α^{27i}	A^{10}	α^{30i}
A^{11}	α^{33i}	A^{12}	α^{36i}	A^{13}	α^{39i}	A^{14}	α^{42i}	A^{15}	α^{45i}
A^{16}	α^{48i}	A^{17}	α^{51i}	A^{18}	α^{54i}	A^{19}	α^{57i}	A^{20}	α^{60i}
A^{21}	α^{63i}	A^{22}	α^{66i}	A^{23}	α^{0}				

TABLE 4. All invalid cases (u, v, w) of types (0, 1, 0, 1) and (0, 1, 0, 2) for 8-cycles.

$(u,-11u,10u)$	$(u,-10u,9u)$	$(u,-9u,8u)$	$(u,-8u,7u)$	$(u,-7u,6u)$	$(u,-6u,5u)$
$(u,-5u,4u)$	$(u,-4u,3u)$	$(u,-3u,2u)$	$(u,-2u,1u)$	$(u,10u,-11u)$	$(u,11u,11u)$
$(u,1u,-2u)$	$(u,2u,-3u)$	$(u,3u,-4u)$	$(u,4u,-5u)$	$(u,5u,-6u)$	$(u,6u,-7u)$
$(u,7u,-8u)$	$(u,8u,-9u)$	$(u,9u,-10u)$			

$$= (1-\alpha^{23})(1-\alpha^{3u}+\alpha^{3(u+v)}-\alpha^{3(u+v+w)})$$
$$= 0 \pmod p.$$

Since $\alpha^{23} \neq 1$, the modified basic equation can be represented as

$$1-\alpha^{3u}+\alpha^{3(u+v)}-\alpha^{3(u+v+w)} = 0 \pmod p. \quad (7)$$

Let $A = \alpha^{3u}$. It is easy to obtain A^k for $1 \leq k \leq 23$, and we record them in Table 3. It is obvious that A is a primitive 23th unit root of $\mathbb{F}_p$ for $p \in P_{69}$. Since

$$\begin{aligned} A^{23}-1 = (A-1)(&A^{22}+A^{21}+A^{20}+A^{19}+A^{18} \\ &+A^{17}+A^{16}+A^{15}+A^{14}+A^{13}+A^{12} \\ &+A^{11}+A^{10}+A^{9}+A^{8}+A^{7}+A^{6} \\ &+A^{5}+A^{4}+A^{3}+A^{2}+A+1) = 0 \pmod p \end{aligned}$$

and $A \neq 1$, then

$$\begin{aligned} &A^{22}+A^{21}+A^{20}+A^{19}+A^{18}+A^{17}+A^{16}+A^{15}+A^{14} \\ &+A^{13}+A^{12}+A^{11}+A^{10}+A^{9}+A^{8}+A^{7}+A^{6}+A^{5} \\ &+A^{4}+A^{3}+A^{2}+A+1 = 0 \pmod p. \end{aligned} \quad (8)$$

As shown in type (0, 1, 2), invalid cases (u, v, w) have the form of $u+v+w = 0 \pmod{23}$ (See Table 4) and the other cases are valid (See Tables 5 and 6). For each valid case (u, v, w), we can easily derive the modified basic equation and its reduced form based on equation (7). We apply the Euclidean division algorithm to the reduced form of the modified basic equation and equation (8), then check whether the remainders equal zero over $\mathbb{F}_p$ for $p \in P_{69}$, and the candidate prime p can be obtained. For simplicity, we only give all the prime values of p in the following subsection.

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

The other type of 8-cycles is (0, 1, 0, 2), and its ordered pairs are $(0, 0); (1, u); (0, u+v); (2, u+v+w)$; for $u+v+w \neq 0 \pmod{23}$. The basic equation becomes

$$\sum_{k=0}^{3}(\alpha^{23i_k}-\alpha^{23i_{k+1}})\alpha^{3j_k}$$
$$= (1-\alpha^{23})(1-\alpha^{3u}-\alpha^{3(u+v)-23}+\alpha^{3(u+v+w)-23})$$
$$= 0 \pmod p.$$

Since $\alpha^{23} \neq 1$, the modified basic equation becomes

$$1-\alpha^{3u}-\alpha^{3(u+v)-23}+\alpha^{3(u+v+w)-23} = 0 \pmod p. \quad (9)$$

Let $a = \alpha^{3u+23}$. For $1 \leq k \leq 69$, a^k has been recorded in Table 2. Similar to type (0, 1, 0, 1), invalid cases (u, v, w) are recorded in Table 4 and valid cases are recorded in Tables 5 and 6. By applying the Euclidean division algorithm to the reduced form of the modified basic equation and equation (6) and checking whether the remainders equal zero over $\mathbb{F}_p$ for $p \in P_{69}$, the prime values p are obtained. For types (0, 1, 0, 1) and (0, 1, 0, 2), we record the obtained primes p in the set S_8, i.e., $S_8 = \{691, 829, 967, 1381, 1657, 1933, 2347, 3037, 3313, 3727, 4003, 4831, 4969, 5107, 5521, 6073, 6211, 6763, 7177, 7867, 9109, 10627, 10903, 11317, 11593, 11731, 12007, 12421, 12973, 14629, 14767, 16561, 18217, 18493, 21391, 21943, 24151, 24979, 25117, 27739, 33811, 37813, 38917, 41263, 45541, 74521, 83077, 102259, 105019, 124477, 145177, 220663, 223423, 351763, 383917, 424351, 434977, 578497, 790327, 794191, 897553, 990289, 1075021, 1145539, 1259113, 1270429, 1379173, 1476463, 1603009, 2173777, 2270239, 2322127, 2522503, 2596057, 2916493, 3998413, 4274689, 4278829, 4609063, 4846147, 5086681, 5220403, 5858239, 9231373, 9970087, 10305703, 11316139, 14323159, 16411237, 16896031, 11828119, 16896031, 23893321, 74773921, 171715057, 211679719, 213726811, 7140766807, 16316789491\}$.

Based on the conclusion in Subsection III-B and the prime values p in the above set S_8, we can obtain the girth-8 distribution of Tanner (3, 23)-regular QC-LDPC codes. There are 100 codes with girth 8, and they are Tanner (3, 23)-regular QC-LDPC codes of length $23p$ for $p \in S_8$.

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

All 10-cycles correspond to the unique type (0, 1, 2, 0, 1), and its corresponding ordered pairs are $(0, 0); (1, u); (2, u+v); (0, u+v+w); (1, u+v+w+x)$; with

TABLE 5. All valid cases (u, v, w) of types (0, 1, 0, 1) and (0, 1, 0, 2) for 8-cycles.

$(u,-11u,-11u)$	$(u,-11u,-10u)$	$(u,-11u,-9u)$	$(u,-11u,-8u)$	$(u,-11u,-7u)$	$(u,-11u,-6u)$
$(u,-11u,-5u)$	$(u,-11u,-4u)$	$(u,-11u,-3u)$	$(u,-11u,-2u)$	$(u,-11u,-1u)$	$(u,-11u,1u)$
$(u,-11u,2u)$	$(u,-11u,3u)$	$(u,-11u,4u)$	$(u,-11u,5u)$	$(u,-11u,6u)$	$(u,-11u,7u)$
$(u,-11u,8u)$	$(u,-11u,9u)$	$(u,-11u,11u)$	$(u,-10u,-11u)$	$(u,-10u,-10u)$	$(u,-10u,-9u)$
$(u,-10u,-8u)$	$(u,-10u,-7u)$	$(u,-10u,-6u)$	$(u,-10u,-5u)$	$(u,-10u,-4u)$	$(u,-10u,-3u)$
$(u,-10u,-2u)$	$(u,-10u,-1u)$	$(u,-10u,1u)$	$(u,-10u,2u)$	$(u,-10u,3u)$	$(u,-10u,4u)$
$(u,-10u,5u)$	$(u,-10u,6u)$	$(u,-10u,7u)$	$(u,-10u,8u)$	$(u,-10u,10u)$	$(u,-10u,11u)$
$(u,-9u,-11u)$	$(u,-9u,-10u)$	$(u,-9u,-9u)$	$(u,-9u,-8u)$	$(u,-9u,-7u)$	$(u,-9u,-6u)$
$(u,-9u,-5u)$	$(u,-9u,-4u)$	$(u,-9u,-3u)$	$(u,-9u,-2u)$	$(u,-9u,-1u)$	$(u,-9u,1u)$
$(u,-9u,2u)$	$(u,-9u,3u)$	$(u,-9u,4u)$	$(u,-9u,5u)$	$(u,-9u,6u)$	$(u,-9u,7u)$
$(u,-9u,9u)$	$(u,-9u,10u)$	$(u,-9u,11u)$	$(u,-8u,-11u)$	$(u,-8u,-10u)$	$(u,-8u,-9u)$
$(u,-8u,-8u)$	$(u,-8u,-7u)$	$(u,-8u,-6u)$	$(u,-8u,-5u)$	$(u,-8u,-4u)$	$(u,-8u,-3u)$
$(u,-8u,-2u)$	$(u,-8u,-1u)$	$(u,-8u,1u)$	$(u,-8u,2u)$	$(u,-8u,3u)$	$(u,-8u,4u)$
$(u,-8u,5u)$	$(u,-8u,6u)$	$(u,-8u,8u)$	$(u,-8u,9u)$	$(u,-8u,10u)$	$(u,-8u,11u)$
$(u,-7u,-11u)$	$(u,-7u,-10u)$	$(u,-7u,-9u)$	$(u,-7u,-8u)$	$(u,-7u,-7u)$	$(u,-7u,-6u)$
$(u,-7u,-5u)$	$(u,-7u,-4u)$	$(u,-7u,-3u)$	$(u,-7u,-2u)$	$(u,-7u,-1u)$	$(u,-7u,1u)$
$(u,-7u,2u)$	$(u,-7u,3u)$	$(u,-7u,4u)$	$(u,-7u,5u)$	$(u,-7u,7u)$	$(u,-7u,8u)$
$(u,-7u,9u)$	$(u,-7u,10u)$	$(u,-7u,11u)$	$(u,-6u,-11u)$	$(u,-6u,-10u)$	$(u,-6u,-9u)$
$(u,-6u,-8u)$	$(u,-6u,-7u)$	$(u,-6u,-6u)$	$(u,-6u,-5u)$	$(u,-6u,-4u)$	$(u,-6u,-3u)$
$(u,-6u,-2u)$	$(u,-6u,-1u)$	$(u,-6u,1u)$	$(u,-6u,2u)$	$(u,-6u,3u)$	$(u,-6u,4u)$
$(u,-6u,6u)$	$(u,-6u,7u)$	$(u,-6u,8u)$	$(u,-6u,9u)$	$(u,-6u,10u)$	$(u,-6u,11u)$
$(u,-5u,-11u)$	$(u,-5u,-10u)$	$(u,-5u,-9u)$	$(u,-5u,-8u)$	$(u,-5u,-7u)$	$(u,-5u,-6u)$
$(u,-5u,-5u)$	$(u,-5u,-4u)$	$(u,-5u,-3u)$	$(u,-5u,-2u)$	$(u,-5u,-1u)$	$(u,-5u,1u)$
$(u,-5u,2u)$	$(u,-5u,3u)$	$(u,-5u,5u)$	$(u,-5u,6u)$	$(u,-5u,7u)$	$(u,-5u,8u)$
$(u,-5u,9u)$	$(u,-5u,10u)$	$(u,-5u,11u)$	$(u,-4u,-11u)$	$(u,-4u,-10u)$	$(u,-4u,-9u)$
$(u,-4u,-8u)$	$(u,-4u,-7u)$	$(u,-4u,-6u)$	$(u,-4u,-5u)$	$(u,-4u,-4u)$	$(u,-4u,-3u)$
$(u,-4u,-2u)$	$(u,-4u,-1u)$	$(u,-4u,1u)$	$(u,-4u,2u)$	$(u,-4u,4u)$	$(u,-4u,5u)$
$(u,-4u,6u)$	$(u,-4u,7u)$	$(u,-4u,8u)$	$(u,-4u,9u)$	$(u,-4u,10u)$	$(u,-4u,11u)$
$(u,-3u,-11u)$	$(u,-3u,-10u)$	$(u,-3u,-9u)$	$(u,-3u,-8u)$	$(u,-3u,-7u)$	$(u,-3u,-6u)$
$(u,-3u,-5u)$	$(u,-3u,-4u)$	$(u,-3u,-3u)$	$(u,-3u,-2u)$	$(u,-3u,-1u)$	$(u,-3u,1u)$
$(u,-3u,3u)$	$(u,-3u,4u)$	$(u,-3u,5u)$	$(u,-3u,6u)$	$(u,-3u,7u)$	$(u,-3u,8u)$
$(u,-3u,9u)$	$(u,-3u,10u)$	$(u,-3u,11u)$	$(u,-2u,-11u)$	$(u,-2u,-10u)$	$(u,-2u,-9u)$
$(u,-2u,-8u)$	$(u,-2u,-7u)$	$(u,-2u,-6u)$	$(u,-2u,-5u)$	$(u,-2u,-4u)$	$(u,-2u,-3u)$
$(u,-2u,-2u)$	$(u,-2u,-1u)$	$(u,-2u,2u)$	$(u,-2u,3u)$	$(u,-2u,4u)$	$(u,-2u,5u)$
$(u,-2u,6u)$	$(u,-2u,7u)$	$(u,-2u,8u)$	$(u,-2u,9u)$	$(u,-2u,10u)$	$(u,-2u,11u)$
$(u,-1u,-11u)$	$(u,-1u,-10u)$	$(u,-1u,-9u)$	$(u,-1u,-8u)$	$(u,-1u,-7u)$	$(u,-1u,-6u)$
$(u,-1u,-5u)$	$(u,-1u,-4u)$	$(u,-1u,-3u)$	$(u,-1u,-2u)$	$(u,-1u,-1u)$	$(u,-1u,1u)$
$(u,-1u,2u)$	$(u,-1u,3u)$	$(u,-1u,4u)$	$(u,-1u,5u)$	$(u,-1u,6u)$	$(u,-1u,7u)$
$(u,-1u,8u)$	$(u,-1u,9u)$	$(u,-1u,10u)$	$(u,-1u,11u)$	$(u,1u,-11u)$	$(u,1u,-10u)$
$(u,1u,-9u)$	$(u,1u,-8u)$	$(u,1u,-7u)$	$(u,1u,-6u)$	$(u,1u,-5u)$	$(u,1u,-4u)$
$(u,1u,-3u)$	$(u,1u,-1u)$	$(u,1u,1u)$	$(u,1u,2u)$	$(u,1u,3u)$	$(u,1u,4u)$
$(u,1u,5u)$	$(u,1u,6u)$	$(u,1u,7u)$	$(u,1u,8u)$	$(u,1u,9u)$	$(u,1u,10u)$
$(u,1u,11u)$	$(u,2u,-11u)$	$(u,2u,-10u)$	$(u,2u,-9u)$	$(u,2u,-8u)$	$(u,2u,-7u)$
$(u,2u,-6u)$	$(u,2u,-5u)$	$(u,2u,-4u)$	$(u,2u,-2u)$	$(u,2u,-1u)$	$(u,2u,1u)$
$(u,2u,2u)$	$(u,2u,3u)$	$(u,2u,4u)$	$(u,2u,5u)$	$(u,2u,6u)$	$(u,2u,7u)$
$(u,2u,8u)$	$(u,2u,9u)$	$(u,2u,10u)$	$(u,2u,11u)$	$(u,3u,-11u)$	$(u,3u,-10u)$
$(u,3u,-9u)$	$(u,3u,-8u)$	$(u,3u,-7u)$	$(u,3u,-6u)$	$(u,3u,-5u)$	$(u,3u,-3u)$
$(u,3u,-2u)$	$(u,3u,-1u)$	$(u,3u,1u)$	$(u,3u,2u)$	$(u,3u,3u)$	$(u,3u,4u)$
$(u,3u,5u)$	$(u,3u,6u)$	$(u,3u,7u)$	$(u,3u,8u)$	$(u,3u,9u)$	$(u,3u,10u)$
$(u,3u,11u)$	$(u,4u,-11u)$	$(u,4u,-10u)$	$(u,4u,-9u)$	$(u,4u,-8u)$	$(u,4u,-7u)$
$(u,4u,-6u)$	$(u,4u,-4u)$	$(u,4u,-3u)$	$(u,4u,-2u)$	$(u,4u,-1u)$	$(u,4u,1u)$
$(u,4u,2u)$	$(u,4u,3u)$	$(u,4u,4u)$	$(u,4u,5u)$	$(u,4u,6u)$	$(u,4u,7u)$
$(u,4u,8u)$	$(u,4u,9u)$	$(u,4u,10u)$	$(u,4u,11u)$	$(u,5u,-11u)$	$(u,5u,-10u)$

TABLE 6. All valid cases (u, v, w) of types (0, 1, 0, 1) and (0, 1, 0, 2) for 8-cycles.

$(u, 5u, -9u)$	$(u, 5u, -8u)$	$(u, 5u, -7u)$	$(u, 5u, -5u)$	$(u, 5u, -4u)$	$(u, 5u, -3u)$
$(u, 5u, -2u)$	$(u, 5u, -1u)$	$(u, 5u, 1u)$	$(u, 5u, 2u)$	$(u, 5u, 3u)$	$(u, 5u, 4u)$
$(u, 5u, 5u)$	$(u, 5u, 6u)$	$(u, 5u, 7u)$	$(u, 5u, 8u)$	$(u, 5u, 9u)$	$(u, 5u, 10u)$
$(u, 5u, 11u)$	$(u, 6u, -11u)$	$(u, 6u, -10u)$	$(u, 6u, -9u)$	$(u, 6u, -8u)$	$(u, 6u, -6u)$
$(u, 6u, -5u)$	$(u, 6u, -4u)$	$(u, 6u, -3u)$	$(u, 6u, -2u)$	$(u, 6u, -1u)$	$(u, 6u, 1u)$
$(u, 6u, 2u)$	$(u, 6u, 3u)$	$(u, 6u, 4u)$	$(u, 6u, 5u)$	$(u, 6u, 6u)$	$(u, 6u, 7u)$
$(u, 6u, 8u)$	$(u, 6u, 9u)$	$(u, 6u, 10u)$	$(u, 6u, 11u)$	$(u, 7u, -11u)$	$(u, 7u, -10u)$
$(u, 7u, -9u)$	$(u, 7u, -7u)$	$(u, 7u, -6u)$	$(u, 7u, -5u)$	$(u, 7u, -4u)$	$(u, 7u, -3u)$
$(u, 7u, -2u)$	$(u, 7u, -1u)$	$(u, 7u, 1u)$	$(u, 7u, 2u)$	$(u, 7u, 3u)$	$(u, 7u, 4u)$
$(u, 7u, 5u)$	$(u, 7u, 6u)$	$(u, 7u, 7u)$	$(u, 7u, 8u)$	$(u, 7u, 9u)$	$(u, 7u, 10u)$
$(u, 7u, 11u)$	$(u, 8u, -11u)$	$(u, 8u, -10u)$	$(u, 8u, -8u)$	$(u, 8u, -7u)$	$(u, 8u, -6u)$
$(u, 8u, -5u)$	$(u, 8u, -4u)$	$(u, 8u, -3u)$	$(u, 8u, -2u)$	$(u, 8u, -1u)$	$(u, 8u, 1u)$
$(u, 8u, 2u)$	$(u, 8u, 3u)$	$(u, 8u, 4u)$	$(u, 8u, 5u)$	$(u, 8u, 6u)$	$(u, 8u, 7u)$
$(u, 8u, 8u)$	$(u, 8u, 9u)$	$(u, 8u, 10u)$	$(u, 8u, 11u)$	$(u, 9u, -11u)$	$(u, 9u, -9u)$
$(u, 9u, -8u)$	$(u, 9u, -7u)$	$(u, 9u, -6u)$	$(u, 9u, -5u)$	$(u, 9u, -4u)$	$(u, 9u, -3u)$
$(u, 9u, -2u)$	$(u, 9u, -1u)$	$(u, 9u, 1u)$	$(u, 9u, 2u)$	$(u, 9u, 3u)$	$(u, 9u, 4u)$
$(u, 9u, 5u)$	$(u, 9u, 6u)$	$(u, 9u, 7u)$	$(u, 9u, 8u)$	$(u, 9u, 9u)$	$(u, 9u, 10u)$
$(u, 9u, 11u)$	$(u, 10u, -10u)$	$(u, 10u, -9u)$	$(u, 10u, -8u)$	$(u, 10u, -7u)$	$(u, 10u, -6u)$
$(u, 10u, -5u)$	$(u, 10u, -4u)$	$(u, 10u, -3u)$	$(u, 10u, -2u)$	$(u, 10u, -1u)$	$(u, 10u, 1u)$
$(u, 10u, 2u)$	$(u, 10u, 3u)$	$(u, 10u, 4u)$	$(u, 10u, 5u)$	$(u, 10u, 6u)$	$(u, 10u, 7u)$
$(u, 10u, 8u)$	$(u, 10u, 9u)$	$(u, 10u, 10u)$	$(u, 10u, 11u)$	$(u, 11u, -11u)$	$(u, 11u, -10u)$
$(u, 11u, -9u)$	$(u, 11u, -8u)$	$(u, 11u, -7u)$	$(u, 11u, -6u)$	$(u, 11u, -5u)$	$(u, 11u, -4u)$
$(u, 11u, -3u)$	$(u, 11u, -2u)$	$(u, 11u, -1u)$	$(u, 11u, 1u)$	$(u, 11u, 2u)$	$(u, 11u, 3u)$
$(u, 11u, 4u)$	$(u, 11u, 5u)$	$(u, 11u, 6u)$	$(u, 11u, 7u)$	$(u, 11u, 8u)$	$(u, 11u, 9u)$
$(u, 11u, 10u)$					

$u + v + w + x \neq 0 \pmod{23}$. The basic equation is

$$\sum_{k=0}^{4} (\alpha^{23 i_k} - \alpha^{23 i_{k+1}})\, \alpha^{3 j_k} = (1 - \alpha^{23}) \cdot (1 + \alpha^{3u+23} + \alpha^{3(u+v)-23} + \alpha^{3(u+v+w)} - \alpha^{3(u+v+w+x)}) = 0 \pmod{p}.$$

Since $\alpha^{23} \neq 1$, the modified basic equation becomes

$$1 + \alpha^{3u+23} + \alpha^{3(u+v)-23} + \alpha^{3(u+v+w)} - \alpha^{3(u+v+w+x)} = 0 \pmod{p}. \tag{10}$$

It is similar to the above three types (0, 1, 2), (0, 1, 0, 1), and (0, 1, 0, 2), we can obtain 463 invalid cases (u, v, w, x) with $u + v + w + x = 0 \pmod{23}$ (See Tables 7 and 8) and 10185 valid cases. Based on equation (10), it is easy to find the modified basic equation and the reduced form for each valid case. We apply the Euclidean division algorithm to the reduced form of the modified basic equation and equation (6), and check whether the resulting remainders equal zero in $\mathbb{F}_p$ for $p \in P_{69}$, the candidate primes p can be obtained. Combined with the aforementioned conclusions, we can summarize the obtained primes p and determine the girth-10 distribution of Tanner (3, 23)-regular QC-LDPC codes. In order to reduce space, valid cases, modified basic equations, and reduced forms are omitted, and the primes p are given. Tanner (3, 23)-regular QC-LDPC codes with length $23p$ have girth 10 for $p \in S_{10}$, where $S_{10} = \{$5659, 7039, 7591, 8419, 8971, 9661, 12697, 13249, 15319, 15733, 16699, 17389, 19183, 19597, 20011, 20149, 20287, 20563, 21529, 23599, 24841, 26083, 26497, 28429, 28843, 29671, 29947, 30223, 30637, 31051, 31189, 31327, 31741, 32569, 32707, 32983, 35053, 36433, 36571, 36847, 37123, 37537, 37951, 39607, 39883, 40849, 41539, 41953, 42643, 43609, 44851, 45127, 45403, 45817, 46093, 46507, 47059, 48163, 48991, 49681, 49957, 50647, 50923, 51061, 51199, 51613, 52027, 52579, 53269, 53407, 53959, 56167, 56443, 56857, 57271, 58237, 58789, 59341, 59617, 60169, 60859, 61687, 62929, 64033, 64171, 65413, 65551, 65827, 66103, 66931, 67759, 68311, 68863, 69001, 69691, 69829, 70381, 70657, 71209, 71347, 71761, 71899, 72727, 73141, 73417, 73693, 74383, 75211, 77419, 77557, 79903, 80317, 81283, 81421, 81559, 81973, 82387, 82939, 84181, 84319, 84457, 85009, 85147, 85837, 87631, 89977, 91081, 91771, 91909, 92737, 93151, 93703, 93979, 95083, 95773, 96601, 98533, 98809, 99223, 100189, 100741, 102397, 102673, 103087, 106123, 106537, 107089, 108883, 109297, 111091, 113023, 113161, 113989, 117991, 119233, 119923, 121579, 126271, 126547, 128341, 129169, 130411, 130687, 132619, 132757, 133033, 136069, 136483, 136621, 138139, 138967, 140761, 143797, 144763, 146833, 147661, 147799, 149731, 150559, 150697, 152629, 153319, 153457, 153871, 156217, 157321, 162289, 163117, 163393, 165049, 165601, 167809, 168499, 169327,

TABLE 7. All invalid cases (u, v, w, x) of type $(0, 1, 2, 0, 1)$ for 10-cycles.

$(u, -11u, -11u, -2u)$	$(u, -11u, -10u, -3u)$	$(u, -11u, -9u, -4u)$	$(u, -11u, -8u, -5u)$
$(u, -11u, -6u, -7u)$	$(u, -11u, -5u, -8u)$	$(u, -11u, -4u, -9u)$	$(u, -11u, -3u, -10u)$
$(u, -11u, -1u, 11u)$	$(u, -11u, 1u, 9u)$	$(u, -11u, 2u, 8u)$	$(u, -11u, 3u, 7u)$
$(u, -11u, 5u, 5u)$	$(u, -11u, 6u, 4u)$	$(u, -11u, 7u, 3u)$	$(u, -11u, 8u, 2u)$
$(u, -11u, -7u, -6u)$	$(u, -11u, -2u, -11u)$	$(u, -11u, 4u, 6u)$	$(u, -11u, 9u, 1u)$
$(u, -11u, 11u, -1u)$	$(u, -10u, -11u, -3u)$	$(u, -10u, -10u, -4u)$	$(u, -10u, -9u, -5u)$
$(u, -10u, -7u, -7u)$	$(u, -10u, -6u, -8u)$	$(u, -10u, -5u, -9u)$	$(u, -10u, -4u, -10u)$
$(u, -10u, -2u, 11u)$	$(u, -10u, -1u, 10u)$	$(u, -10u, 1u, 8u)$	$(u, -10u, 2u, 7u)$
$(u, -10u, 4u, 5u)$	$(u, -10u, 5u, 4u)$	$(u, -10u, 6u, 3u)$	$(u, -10u, 7u, 2u)$
$(u, -10u, -8u, -6u)$	$(u, -10u, -3u, -11u)$	$(u, -10u, 3u, 6u)$	$(u, -10u, 8u, 1u)$
$(u, -10u, 10u, -1u)$	$(u, -10u, 11u, -2u)$	$(u, -9u, -11u, -4u)$	$(u, -9u, -10u, -5u)$
$(u, -9u, -8u, -7u)$	$(u, -9u, -7u, -8u)$	$(u, -9u, -6u, -9u)$	$(u, -9u, -5u, -10u)$
$(u, -9u, -3u, 11u)$	$(u, -9u, -2u, 10u)$	$(u, -9u, -1u, 9u)$	$(u, -9u, 1u, 7u)$
$(u, -9u, 3u, 5u)$	$(u, -9u, 4u, 4u)$	$(u, -9u, 5u, 3u)$	$(u, -9u, 6u, 2u)$
$(u, -9u, -9u, -6u)$	$(u, -9u, -4u, -11u)$	$(u, -9u, 2u, 6u)$	$(u, -9u, 7u, 1u)$
$(u, -9u, 9u, -1u)$	$(u, -9u, 10u, -2u)$	$(u, -9u, 11u, -3u)$	$(u, -8u, -11u, -5u)$
$(u, -8u, -9u, -7u)$	$(u, -8u, -8u, -8u)$	$(u, -8u, -7u, -9u)$	$(u, -8u, -6u, -10u)$
$(u, -8u, -4u, 11u)$	$(u, -8u, -3u, 10u)$	$(u, -8u, -2u, 9u)$	$(u, -8u, -1u, 8u)$
$(u, -8u, 2u, 5u)$	$(u, -8u, 3u, 4u)$	$(u, -8u, 4u, 3u)$	$(u, -8u, 5u, 2u)$
$(u, -8u, -10u, -6u)$	$(u, -8u, -5u, -11u)$	$(u, -8u, 1u, 6u)$	$(u, -8u, 6u, 1u)$
$(u, -8u, 8u, -1u)$	$(u, -8u, 9u, -2u)$	$(u, -8u, 10u, -3u)$	$(u, -8u, 11u, -4u)$
$(u, -7u, -10u, -7u)$	$(u, -7u, -9u, -8u)$	$(u, -7u, -8u, -9u)$	$(u, -7u, -7u, -10u)$
$(u, -7u, -5u, 11u)$	$(u, -7u, -4u, 10u)$	$(u, -7u, -3u, 9u)$	$(u, -7u, -2u, 8u)$
$(u, -7u, 1u, 5u)$	$(u, -7u, 2u, 4u)$	$(u, -7u, 3u, 3u)$	$(u, -7u, 4u, 2u)$
$(u, -7u, -11u, -6u)$	$(u, -7u, -6u, -11u)$	$(u, -7u, -1u, 7u)$	$(u, -7u, 5u, 1u)$
$(u, -7u, 7u, -1u)$	$(u, -7u, 8u, -2u)$	$(u, -7u, 9u, -3u)$	$(u, -7u, 10u, -4u)$
$(u, -6u, -11u, -7u)$	$(u, -6u, -10u, -8u)$	$(u, -6u, -9u, -9u)$	$(u, -6u, -8u, -10u)$
$(u, -6u, -6u, 11u)$	$(u, -6u, -5u, 10u)$	$(u, -6u, -4u, 9u)$	$(u, -6u, -3u, 8u)$
$(u, -6u, -1u, 6u)$	$(u, -6u, 1u, 4u)$	$(u, -6u, 2u, 3u)$	$(u, -6u, 3u, 2u)$
$(u, -7u, 11u, -5u)$	$(u, -6u, -7u, -11u)$	$(u, -6u, -2u, 7u)$	$(u, -6u, 4u, 1u)$
$(u, -6u, 6u, -1u)$	$(u, -6u, 7u, -2u)$	$(u, -6u, 8u, -3u)$	$(u, -6u, 9u, -4u)$
$(u, -6u, 11u, -6u)$	$(u, -5u, -11u, -8u)$	$(u, -5u, -10u, -9u)$	$(u, -5u, -9u, -10u)$
$(u, -5u, -7u, 11u)$	$(u, -5u, -6u, 10u)$	$(u, -5u, -5u, 9u)$	$(u, -5u, -4u, 8u)$
$(u, -5u, -2u, 6u)$	$(u, -5u, -1u, 5u)$	$(u, -5u, 1u, 3u)$	$(u, -5u, 2u, 2u)$
$(u, -6u, 10u, -5u)$	$(u, -5u, -8u, -11u)$	$(u, -5u, -3u, 7u)$	$(u, -5u, 3u, 1u)$
$(u, -5u, 5u, -1u)$	$(u, -5u, 6u, -2u)$	$(u, -5u, 7u, -3u)$	$(u, -5u, 8u, -4u)$
$(u, -5u, 10u, -6u)$	$(u, -5u, 11u, -7u)$	$(u, -4u, -11u, -9u)$	$(u, -4u, -10u, -10u)$
$(u, -4u, -8u, 11u)$	$(u, -4u, -7u, 10u)$	$(u, -4u, -6u, 9u)$	$(u, -4u, -5u, 8u)$
$(u, -4u, -3u, 6u)$	$(u, -4u, -2u, 5u)$	$(u, -4u, -1u, 4u)$	$(u, -4u, 1u, 2u)$
$(u, -5u, 9u, -5u)$	$(u, -4u, -9u, -11u)$	$(u, -4u, -4u, 7u)$	$(u, -4u, 2u, 1u)$
$(u, -4u, 4u, -1u)$	$(u, -4u, 5u, -2u)$	$(u, -4u, 6u, -3u)$	$(u, -4u, 7u, -4u)$
$(u, -4u, 9u, -6u)$	$(u, -4u, 10u, -7u)$	$(u, -4u, 11u, -8u)$	$(u, -3u, -11u, -10u)$
$(u, -3u, -9u, 11u)$	$(u, -3u, -8u, 10u)$	$(u, -3u, -7u, 9u)$	$(u, -3u, -6u, 8u)$
$(u, -3u, -4u, 6u)$	$(u, -3u, -3u, 5u)$	$(u, -3u, -2u, 4u)$	$(u, -3u, -1u, 3u)$
$(u, -4u, 8u, -5u)$	$(u, -3u, -10u, -11u)$	$(u, -3u, -5u, 7u)$	$(u, -3u, 1u, 1u)$
$(u, -3u, 3u, -1u)$	$(u, -3u, 4u, -2u)$	$(u, -3u, 5u, -3u)$	$(u, -3u, 6u, -4u)$
$(u, -3u, 8u, -6u)$	$(u, -3u, 9u, -7u)$	$(u, -3u, 10u, -8u)$	$(u, -3u, 11u, -9u)$
$(u, -2u, -10u, 11u)$	$(u, -2u, -9u, 10u)$	$(u, -2u, -8u, 9u)$	$(u, -2u, -7u, 8u)$
$(u, -2u, -5u, 6u)$	$(u, -2u, -4u, 5u)$	$(u, -2u, -3u, 4u)$	$(u, -2u, -2u, 3u)$
$(u, -3u, 7u, -5u)$	$(u, -2u, -11u, -11u)$	$(u, -2u, -6u, 7u)$	$(u, -2u, -1u, 2u)$
$(u, -2u, 2u, -1u)$	$(u, -2u, 3u, -2u)$	$(u, -2u, 4u, -3u)$	$(u, -2u, 5u, -4u)$
$(u, -2u, 7u, -6u)$	$(u, -2u, 8u, -7u)$	$(u, -2u, 9u, -8u)$	$(u, -2u, 10u, -9u)$
$(u, -1u, -11u, 11u)$	$(u, -1u, -10u, 10u)$	$(u, -1u, -9u, 9u)$	$(u, -1u, -8u, 8u)$

TABLE 8. All invalid cases (u, v, w, x) of type (0, 1, 2, 0, 1) for 10-cycles.

$(u,-1u,-6u,6u)$	$(u,-1u,-5u,5u)$	$(u,-1u,-4u,4u)$	$(u,-1u,-3u,3u)$	$(u,-2u,6u,-5u)$
$(u,-2u,11u,-10u)$	$(u,-1u,-7u,7u)$	$(u,-1u,-2u,2u)$	$(u,-1u,-1u,1u)$	$(u,-1u,1u,-1u)$
$(u,-1u,2u,-2u)$	$(u,-1u,3u,-3u)$	$(u,-1u,5u,-5u)$	$(u,-1u,6u,-6u)$	$(u,-1u,7u,-7u)$
$(u,3u,2u,-6u)$	$(u,3u,3u,-7u)$	$(u,3u,4u,-8u)$	$(u,3u,5u,-9u)$	$(u,3u,6u,-10u)$
$(u,2u,3u,-6u)$	$(u,2u,4u,-7u)$	$(u,2u,5u,-8u)$	$(u,2u,6u,-9u)$	$(u,2u,7u,-10u)$
$(u,2u,8u,-11u)$	$(u,2u,9u,11u)$	$(u,2u,10u,10u)$	$(u,2u,11u,9u)$	$(u,3u,-11u,7u)$
$(u,3u,-10u,6u)$	$(u,3u,-9u,5u)$	$(u,3u,-8u,4u)$	$(u,3u,-7u,3u)$	$(u,3u,-6u,2u)$
$(u,3u,-5u,1u)$	$(u,3u,-3u,-1u)$	$(u,3u,-2u,-2u)$	$(u,3u,-1u,-3u)$	$(u,3u,1u,-5u)$
$(u,1u,4u,-6u)$	$(u,1u,5u,-7u)$	$(u,1u,6u,-8u)$	$(u,1u,7u,-9u)$	$(u,1u,8u,-10u)$
$(u,1u,9u,-11u)$	$(u,1u,10u,11u)$	$(u,1u,11u,10u)$	$(u,2u,-11u,8u)$	$(u,2u,-10u,7u)$
$(u,2u,-9u,6u)$	$(u,2u,-8u,5u)$	$(u,2u,-7u,4u)$	$(u,2u,-6u,3u)$	$(u,2u,-5u,2u)$
$(u,2u,-4u,1u)$	$(u,2u,-2u,-1u)$	$(u,2u,-1u,-2u)$	$(u,2u,1u,-4u)$	$(u,2u,2u,-5u)$
$(u,-1u,10u,-10u)$	$(u,-1u,11u,-11u)$	$(u,1u,-11u,9u)$	$(u,1u,-10u,8u)$	$(u,1u,-9u,7u)$
$(u,1u,-8u,6u)$	$(u,1u,-7u,5u)$	$(u,1u,-6u,4u)$	$(u,1u,-5u,3u)$	$(u,1u,-4u,2u)$
$(u,1u,-3u,1u)$	$(u,1u,-1u,-1u)$	$(u,1u,1u,-3u)$	$(u,1u,2u,-4u)$	$(u,1u,3u,-5u)$
$(u,3u,7u,-11u)$	$(u,3u,8u,11u)$	$(u,3u,9u,10u)$	$(u,3u,10u,9u)$	$(u,3u,11u,8u)$
$(u,4u,-11u,6u)$	$(u,4u,-10u,5u)$	$(u,4u,-9u,4u)$	$(u,4u,-8u,3u)$	$(u,4u,-7u,2u)$
$(u,4u,-6u,1u)$	$(u,4u,-4u,-1u)$	$(u,4u,-3u,-2u)$	$(u,4u,-2u,-3u)$	$(u,4u,-1u,-4u)$
$(u,4u,1u,-6u)$	$(u,4u,2u,-7u)$	$(u,4u,3u,-8u)$	$(u,4u,4u,-9u)$	$(u,4u,5u,-10u)$
$(u,4u,6u,-11u)$	$(u,4u,7u,11u)$	$(u,4u,8u,10u)$	$(u,4u,9u,9u)$	$(u,4u,10u,8u)$
$(u,4u,11u,7u)$	$(u,5u,-11u,5u)$	$(u,5u,-10u,4u)$	$(u,5u,-9u,3u)$	$(u,5u,-8u,2u)$
$(u,5u,-7u,1u)$	$(u,5u,-5u,-1u)$	$(u,5u,-4u,-2u)$	$(u,5u,-3u,-3u)$	$(u,5u,-2u,-4u)$
$(u,5u,-1u,-5u)$	$(u,5u,1u,-7u)$	$(u,5u,2u,-8u)$	$(u,5u,3u,-9u)$	$(u,5u,4u,-10u)$
$(u,5u,5u,-11u)$	$(u,5u,6u,11u)$	$(u,5u,7u,10u)$	$(u,5u,8u,9u)$	$(u,5u,9u,8u)$
$(u,5u,10u,7u)$	$(u,5u,11u,6u)$	$(u,6u,-11u,4u)$	$(u,6u,-10u,3u)$	$(u,6u,-9u,2u)$
$(u,6u,-8u,1u)$	$(u,6u,-6u,-1u)$	$(u,6u,-5u,-2u)$	$(u,6u,-4u,-3u)$	$(u,6u,-3u,-4u)$
$(u,6u,-2u,-5u)$	$(u,6u,-1u,-6u)$	$(u,6u,1u,-8u)$	$(u,6u,2u,-9u)$	$(u,6u,3u,-10u)$
$(u,6u,4u,-11u)$	$(u,6u,5u,11u)$	$(u,6u,6u,10u)$	$(u,6u,7u,9u)$	$(u,6u,8u,8u)$
$(u,6u,9u,7u)$	$(u,6u,10u,6u)$	$(u,6u,11u,5u)$	$(u,7u,-11u,3u)$	$(u,7u,-10u,2u)$
$(u,7u,-9u,1u)$	$(u,7u,-7u,-1u)$	$(u,7u,-6u,-2u)$	$(u,7u,-5u,-3u)$	$(u,7u,-4u,-4u)$
$(u,7u,-3u,-5u)$	$(u,7u,-2u,-6u)$	$(u,7u,-1u,-7u)$	$(u,7u,1u,-9u)$	$(u,7u,2u,-10u)$
$(u,7u,3u,-11u)$	$(u,7u,4u,11u)$	$(u,7u,5u,10u)$	$(u,7u,6u,9u)$	$(u,7u,7u,8u)$
$(u,7u,8u,7u)$	$(u,7u,9u,6u)$	$(u,7u,10u,5u)$	$(u,7u,11u,4u)$	$(u,8u,-11u,2u)$
$(u,8u,-10u,1u)$	$(u,8u,-8u,-1u)$	$(u,8u,-7u,-2u)$	$(u,8u,-6u,-3u)$	$(u,8u,-5u,-4u)$
$(u,8u,-4u,-5u)$	$(u,8u,-3u,-6u)$	$(u,8u,-2u,-7u)$	$(u,8u,-1u,-8u)$	$(u,8u,1u,-10u)$
$(u,8u,2u,-11u)$	$(u,8u,3u,11u)$	$(u,8u,4u,10u)$	$(u,8u,5u,9u)$	$(u,8u,6u,8u)$
$(u,8u,7u,7u)$	$(u,8u,8u,6u)$	$(u,8u,9u,5u)$	$(u,8u,10u,4u)$	$(u,8u,11u,3u)$
$(u,9u,-11u,1u)$	$(u,9u,-9u,-1u)$	$(u,9u,-8u,-2u)$	$(u,9u,-7u,-3u)$	$(u,9u,-6u,-4u)$
$(u,9u,-5u,-5u)$	$(u,9u,-4u,-6u)$	$(u,9u,-3u,-7u)$	$(u,9u,-2u,-8u)$	$(u,9u,-1u,-9u)$
$(u,9u,1u,-11u)$	$(u,9u,2u,11u)$	$(u,9u,3u,10u)$	$(u,9u,4u,9u)$	$(u,9u,5u,8u)$
$(u,9u,6u,7u)$	$(u,9u,7u,6u)$	$(u,9u,8u,5u)$	$(u,9u,9u,4u)$	$(u,9u,10u,3u)$
$(u,9u,11u,2u)$	$(u,10u,-10u,-1u)$	$(u,10u,-9u,-2u)$	$(u,10u,-8u,-3u)$	$(u,10u,-7u,-4u)$
$(u,10u,-6u,-5u)$	$(u,10u,-5u,-6u)$	$(u,10u,-4u,-7u)$	$(u,10u,-3u,-8u)$	$(u,10u,-2u,-9u)$
$(u,10u,-1u,-10u)$	$(u,10u,1u,11u)$	$(u,10u,2u,10u)$	$(u,10u,3u,9u)$	$(u,10u,4u,8u)$
$(u,10u,5u,7u)$	$(u,10u,6u,6u)$	$(u,10u,7u,5u)$	$(u,10u,8u,4u)$	$(u,10u,9u,3u)$
$(u,10u,10u,2u)$	$(u,10u,11u,1u)$	$(u,11u,-11u,-1u)$	$(u,11u,-10u,-2u)$	$(u,11u,-9u,-3u)$
$(u,11u,-8u,-4u)$	$(u,11u,-7u,-5u)$	$(u,11u,-6u,-6u)$	$(u,11u,-5u,-7u)$	$(u,11u,-4u,-8u)$
$(u,11u,-3u,-9u)$	$(u,11u,-2u,-10u)$	$(u,11u,-1u,-11u)$	$(u,11u,1u,10u)$	$(u,11u,2u,9u)$
$(u,11u,3u,8u)$	$(u,11u,4u,7u)$	$(u,11u,5u,6u)$	$(u,11u,6u,5u)$	$(u,11u,7u,4u)$
$(u,11u,8u,3u)$	$(u,11u,9u,2u)$	$(u,11u,10u,1u)$	$(u,-1u,4u,-4u)$	$(u,-1u,9u,-9u)$
$(u,-1u,8u,-8u)$				

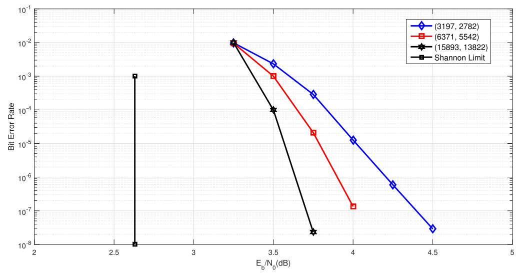


FIGURE 1. The bit error performance of Tanner (3, 23)-regular (3197, 2782), (6371, 5542), and (15893, 13822) QC-LDPC codes.

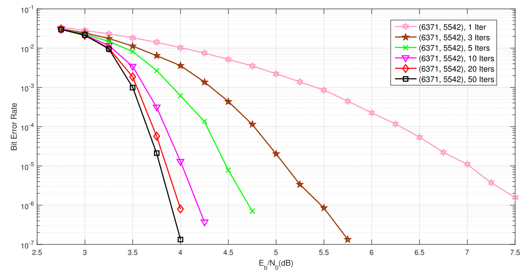


FIGURE 2. The rate of decoding convergence of the Tanner (3, 23)-regular (6371, 5542) QC-LDPC code.

170707, 173191, 173743, 174157, 174571, 176779, 178987, 189613, 190027, 192373, 194167, 195271, 197203, 198031, 198859$\} \cup S_{A10}$. Note that the set S_{10} has 1620 prime values p and the set S_{A10} is given in Appendix A for easy reading.

In conclusion, we determine the girth distribution of Tanner (3, 23)-regular QC-LDPC codes. That is, there are 4 codes of girth 6, 100 codes of girth 8, 1620 codes of girth 10, and the remaining codes have girth 12.

IV. SIMULATION RESULTS

In this section, we provide the performance of Tanner (3, 23)-regular QC-LDPC codes. In these simulations, the BPSK modulated additive white Gaussian noise (AWGN) channel and sum-product algorithm (SPA) with 50 iterations are assumed.

Consider the prime fields $\mathbb{F}_{139}$, $\mathbb{F}_{277}$, and $\mathbb{F}_{691}$, and their primitive 69th unit roots are chosen as 4, 3, and 30, respectively. According to the definition of $\mathbf{H}$ in (2) and the primitive 69th unit roots, we can easily construct three Tanner (3, 23)-regular QC-LDPC codes of lengths 3197 ($= 23 \times 139$), 6371 ($= 23 \times 277$), and 15893 ($= 23 \times 691$). They are Tanner (3, 23)-regular (3197, 2782), (6371, 5542), and (15893, 13822) QC-LDPC codes, and their parity-check matrices have two redundant rows. The girth of Tanner (3, 23)-regular (3197, 2782) and (6371, 5542) QC-LDPC codes is 6, and the girth of the Tanner (3, 23)-regular (15893, 13822) QC-LDPC code is 8. The bit error performance of these three codes decoded with the SPA (50 iterations) are shown in Figure 1. It can be seen from Figure 1 that, at the bit error rates (BERs) of 10^{-7}, Tanner (3, 23)-regular (3197, 2782), (6371, 5542), and (15893, 13822) QC-LDPC codes perform about 1.6 dB, 1.3 dB, and 1 dB from the Shannon limit, respectively.

Furthermore, the decoding convergence performance of the Tanner (3, 23)-regular (6371, 5542) QC-LDPC code is shown in Figure 2. The SPA with 1, 3, 5, 10, 20, and 50 iterations is employed to decode this code. We can see from Figure 2 that this code has fast decoding convergence rate. 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. Besides, no error floor is observed down to BER $\approx 1.3 \times 10^{-7}$.

V. CONCLUSION

In this paper, we studied the girth distribution of Tanner (3, 23)-regular QC-LDPC codes of length $23p$ with p being a prime and $p \equiv 1 \pmod{69}$. We first analyzed the cycle structure of Tanner (3, 23)-regular QC-LDPC codes, and presented the sufficient and necessary condition for the existence of cycles of lengths 4, 6, 8, and 10. We divided these cycles into five equivalent types and applied the Euclidean division algorithm to check the existence of cycles corresponding to these five equivalent types. Then the candidate prime values p are obtained. By summarizing the obtained primes p, the girth distribution of Tanner (3,23)-regular QC-LDPC codes is determined. That is, there are 4 codes of girth 6 for $p = 139, 277, 55201$, or 89839, 100 codes of girth 8 for $p \in S_8$ (S_8 is given in Subsection III-D, 1620 codes of girth 10 for $p \in S_{10}$ (S_{10} is given in Subsection III-E), and the remaining codes have girth 12, such as for $p = 34501$, 36709, 54787, 55339, 58099, 62653, 62791, 63067, 68449, 72313, 74797, 76039, 79627, 84871, 86113, 86389, ….

APPENDIX A

In the following, we provide the remaining elements in the prime set S_{10} for (3, 23)-regular Tanner's QC-LDPC codes of code length $23p$ and girth 10 with $p \in S_{10}$. Note that the elements in S_{10} which are less than 200000 are given in Subsection III-E, and the remaining elements in S_{10} form a new set, denoted by S_{A10}. That is, S_{A10} is a subset of S_{10}, and the elements in S_{A10} are greater than 200000. The prime subset S_{A10} is given as follows.

$S_{A10} = \{$200929, 202999, 204793, 204931, 205483, 207967, 209623, 210037, 212383, 214729, 215833, 217351, 223837, 224113, 224251, 226183, 229081, 231841, 232117, 233221, 239431, 240259, 241639, 242329, 244261, 244399, 246193, 253369, 257371, 260269, 260959, 263443, 267307, 267721, 269377, 270343, 275449, 278071, 278209, 278347, 279451, 281797, 282487, 287731, 288973, 291457, 292837, 296011, 297391, 300427, 301531, 303049, 303187, 303463, 304153, 304429, 306913, 308569, 309259, 310087, 310363, 310501, 313399, 314779, 314917, 318919, 319057, 320851, 321403, 322093, 324301, 324439, 324991, 331339, 334099, 334513, 335893, 339067, 345139, 346933, 352867, 353833, 356869, 362941, 364321, 365839, 372739, 372877, 373291, 373567, 373981, 379501, 385159, 388057, 391231, 392473, 393853, 398683, 409033, 409861, 410413, 414691, 417727, 420349, 426973, 430009, 431803, 432907, 436081, 442843, 445741, 454711, 464647, 466717, 469753, 478861, 483829, 484243, 490591, 501493, 501769, 502597, 505357, 507979, 509221, 512671, 515293, 521641, 523573, 525781, 528679, 537787, 544549, 544963, 552001, 554209, 556693, 560281, 561109, 568699, 576703, 577531, 580981, 587467, 588433, 595333, 597403, 597679, 598093, 598369, 599611, 600577, 601819, 607339, 612307, 612583, 615343, 616999, 619897, 622243, 623071, 624037, 625831, 627349, 631903, 636043, 638527, 639631, 639907, 640873, 641701, 660607, 661849, 662953, 673579, 680203, 681997, 682411, 687517, 687931, 698557, 702007, 702283, 703249, 705181, 706837, 710839, 717463, 719119, 726157, 729331, 729607, 730297, 730573, 738301, 744511, 755551, 765763, 766453, 768799, 771697, 781357, 787153, 799021, 811441, 815029, 816961, 817237, 823723, 826069, 826759, 827311, 828967, 832693, 846493, 852013, 855739, 873541, 883339, 884029, 885133, 889687, 891067, 905833, 912871, 914941, 929983, 934951, 950269, 962413, 964897, 970969, 972901, 977593, 985597, 991531, 998983, 1008781, 1016371, 1017613, 1030033, 1031413, 1033759, 1042039, 1046179, 1069639, 1096549, 1101931, 1114213, 1120423, 1126357, 1130497, 1140571, 1149403, 1149817, 1150921, 1152163, 1164859, 1169827, 1171069, 1173001, 1186111, 1186249, 1193839, 1197289, 1205707, 1206259, 1215367, 1232617, 1233721, 1234687, 1237309, 1241173, 1247383, 1251109, 1265461, 1268359, 1270981, 1281193, 1297063, 1300237, 1306033, 1324387, 1350883, 1354471, 1367581, 1378759, 1406773, 1408567, 1411603, 1415191, 1433821, 1451347, 1460731, 1472599, 1478947, 1485571, 1494403, 1496749, 1505167, 1506823, 1528627, 1533871, 1536631, 1549741, 1565059, 1566577, 1571683, 1572511, 1612393, 1622743, 1632817, 1635163, 1636543, 1638061, 1651861, 1673941, 1685119, 1705819, 1709959, 1727623, 1741699, 1745839, 1749703, 1760881, 1762261, 1767229, 1768747, 1792621, 1811527, 1838299, 1840921, 1844923, 1848787, 1852789, 1868107, 1898467, 1908679, 1912543, 1917511, 1919719, 1924963, 1946767, 1953529, 1972987, 1998793, 1999069, 2001553, 2021563, 2026807, 2064343, 2085319, 2088217, 2155009, 2162737, 2169499, 2173363, 2203447, 2227321, 2229943, 2233531, 2242777, 2252161, 2258233, 2264443, 2270929, 2273827, 2277139, 2278519, 2287627, 2329027, 2340757, 2359801, 2458333, 2459161, 2463163, 2479171, 2494213, 2497939, 2509807, 2511601, 2532991, 2537959, 2557417, 2597299, 2599783, 2601439, 2615791, 2632627, 2639941, 2641459, 2648911, 2678167, 2692519, 2693071, 2705629, 2712943, 2715289, 2755033, 2775457, 2786083, 2806369, 2824447, 2846527, 2869987, 2873851, 2911663, 2943541, 2951269, 3009091, 3025651, 3088717, 3118663, 3131221, 3131497, 3144469, 3146263, 3157579, 3185317, 3233617, 3235411, 3245761, 3279709, 3317521, 3350779, 3365959, 3378931, 3400597, 3432613, 3437857, 3448897, 3480913, 3587449, 3603871, 3606769, 3619327, 3661831, 3662107, 3705853, 3709441, 3723931, 3736351, 3743527, 3749461, 3783961, 3789067, 3839299, 3846613, 3846751, 3898087, 3903883, 3936727, 3984199, 3991237, 3994687, 3995653, 4022563, 4035397, 4071553, 4140001, 4212589, 4244743, 4247917, 4280071, 4298149, 4344931, 4351693, 4375429, 4392679, 4398061, 4446499, 4463059, 4469821, 4500319, 4515913, 4533439, 4545169, 4546963, 4592089, 4621207, 4623691, 4650463, 4707733, 4727329, 4803919, 4813579, 4827241, 4831933, 4853599, 5024857, 5049007, 5117317, 5169481, 5199427, 5246623, 5270497, 5305273, 5335633, 5344051, 5355643, 5466733, 5495989, 5603077, 5608321, 5622949, 5713753, 5759431, 5833537, 5881699, 5929723, 5954287, 5977057, 6028807, 6041089, 6064273, 6101119, 6137137, 6183091, 6190819, 6237739, 6300667, 6374911, 6473029, 6574873, 6697279, 6738541, 6785047, 6831553, 6839281, 6944299, 7145503, 7240033, 7350433, 7371409, 7420261, 7426333, 7427023, 7613461, 7648237, 7903813, 7959151, 7993099, 8116609, 8133031, 8186989, 8282623, 8290903, 8349829, 8358247, 8461471, 8464369, 8548273, 8694691, 8726569, 8734021, 8756101, 8836417, 8949991, 9000499, 9154231, 9323557, 9358471, 9361369, 9475771, 9487501, 9499783, 9526969, 9549739, 9557881, 9737971, 9743077, 9807247, 9866449, 9941383, 9941521, 9998377, 10154869, 10305703, 10480549, 10565557, 10718599, 10753513, 10916767, 10948783, 11012539, 11156749, 11241481, 11316139, 11334079, 11347879, 11396041, 11458417, 11630779, 11681563, 11713717, 11828119, 11860687, 12000757, 12034153, 12065341, 12094183, 12108949, 12137239, 12182503, 12514807, 12541027, 12545581, 12657913, 12696139, 12842971, 12906727, 12925771, 12956269, 13044037, 13282363, 13356331, 13479979, 13517239, 13603903, 13691947, 13752943, 13760671, 13858237, 13978849, 14062891, 14323159, 14479789, 14569213, 14766001, 14851561, 15004051, 15065599, 15116107, 15168271, 15319657, 15354019, 15388381, 15415843, 15523069, 15565159, 15689911, 16133167, 16166287, 16232803, 16406959, 16411237, 16566073, 16676749, 16694551, 16856149, 16896031, 16929013, 17052109, 17068531, 17087713, 17168719, 17243101, 17382481, 17560639, 17587411, 17794411, 18049987, 18087523, 18246499, 18330541, 18590119, 18715423, 18939121, 19042759, 19379617, 19381963, 19499401, 19736347, 20081899, 20183467, 20202097, 20252053, 20292763, 20466643, 20791081, 20808883, 20834551, 20924251, 21056869, 21150709, 21401869, 21487981, 21904327, 23215879, 23261971, 23555773, 23585857, 23893321, 23906293, 23980399, 24049813, 24359347, 24645007, 24707659, 24711109, 25305337, 25317619, 25574299, 25935031, 26104909, 26296729, 26336059, 26463571, 26508421, 27145291, 27282877, 27482839, 27490429, 27688459, 27924301, 28417927, 28584079, 28725943, 28855663, 28974343, 29219431, 29497087, 29712643, 29761219, 30116293, 30426793, 30457291, 30485857, 30584803, 30662083, 30932977, 31631671, 31662583, 31956247, 31973911, 32301937, 32313529, 32818333, 32901133, 33630739, 33741553, 33900667, 34061299, 34483717, 34589839, 34702861, 35037097, 35283289, 35577781, 35617111, 35620699, 36140821, 36279787, 36312079, 36428137, 36821989, 37199557, 37269523, 37274767, 38358757, 38557339, 39844603, 40047187, 40471261, 41053897, 41527099, 41691319, 42114841, 42329431, 42780967, 43047721, 43366777, 43520509, 43618903, 44020069, 44024209, 44073613, 44133919, 44492029, 45208663, 45359497, 45517231, 45680209, 45713743, 46096693, 47314543, 47902147, 47990053, 48091207, 48754159, 49342453, 49729681, 49765423, 49801579, 50005957, 51846463, 51929953, 52484437, 52538257, 53360599, 54379453, 54394771, 54611983, 54730387, 55199173, 55312471, 55435291, 56146681, 56762851, 56983237, 57167191, 57176437, 57329341, 57700837, 58055497, 58080751, 58820569, 59271829, 59518297, 60414331, 60739183, 60944251, 61154563, 61839457, 61876303, 63348487, 63595093, 63625039, 64961431, 65094187, 65467477, 67107331, 67942507, 68198773, 68450623, 69297391, 69358801, 71246503, 71935951, 72983371, 73900657, 74246899, 74616049, 74773921, 75315157, 76202773, 76473253, 77204791, 77431111, 77639767, 77831311, 78384001, 79012177, 79108501, 80157163, 83893237, 84264181, 84714061, 84976123, 85054093, 85884577, 86526553, 86555809, 87266233, 87345859, 88972879, 90028027, 90561949, 90768673, 95306251, 96002047, 96310477, 96940309, 97954609, 98063629, 98919367, 99231247, 100487047, 101617267, 102419323, 103051087, 103123399, 104119621, 104585647, 105699859, 106293949, 106809517, 110060659, 110260621, 110407729, 112523821, 112799683, 112924711, 114275041, 114511297, 116820313, 118674481, 119559751, 119903923, 120442537, 120527131, 120694663, 120872683, 123091447, 123251389, 123315007, 125676601, 128928571, 129102313, 131526559, 137688673, 137754361, 138135103, 138532129, 140287627, 142171879, 143451829, 147921511, 148445359, 148720393, 149961289, 149970949, 151235719, 154332301, 154891201, 156190609, 157246723, 158765413, 159313411, 164831617, 164854939, 165735103, 167889973, 171567259, 171715057, 173381269, 173409697, 173765047, 174489961, 175275733, 176442109, 176649937, 179291257, 180116773, 180406573, 182640517, 185058691, 185726473, 186531013, 190516867, 192075853, 194369689, 194836267, 196003333, 196719967, 196941319, 198587797, 199893139, 202018477, 205541617, 206127841, 206533147, 207943093, 208878181, 209339791, 211679719, 212146159, 213726811, 217780009, 218811973, 232086331, 232366471, 232465279, 232597483, 238095127, 244859887, 247589389, 248603827, 249384493, 250721851, 253960849, 257140783, 257295757, 257427133, 257512417, 259720141, 262862953, 263307727, 266296117, 267191599, 268246333, 271295719, 276384883, 280849873, 284130823, 285732313, 288054853, 288136687, 290567971, 290781319, 294936913, 298347307, 300711109, 301737277, 304131577, 304418341, 306651871, 308586079, 314864527, 315866959, 319860403, 323046961, 326807737, 333488593, 335955757, 338596249, 339527887, 339832177, 343768351, 344996413, 348717169, 352452967, 354127321, 355600057, 357560347, 360430471, 361420483, 366212947, 368424949, 368856751, 376885867, 380728477, 381335401, 389659009, 391072681, 404194963, 405717517, 410200171, 412059169, 416269963, 428160319, 431375443, 442677091, 449256931, 451311337, 451478179, 453450889, 456918967, 460836373, 470870077, 473050339, 473976043, 475310779, 483991393, 488556847, 489138103, 491676751, 492680563, 496717063, 505532917, 508762393, 510244513, 512133319, 521996731, 530038543, 532977253, 550697971, 557367511, 559684393, 563466559, 566701417, 572567797, 584965993, 592693027, 609312367, 628875109, 638374063, 646282981, 646814143, 649986763, 650569123, 652969909, 690059893, 699773989, 709489741, 710397781, 713788717, 714246739, 717070909, 736961263, 760234273, 784820353, 789844243, 797764063, 809530081, 818774287, 826706389, 829355437, 843453931, 858641659, 884405707, 884535151, 902096893, 913365007, 916186003, 932418943, 944097607, 951455353, 957047941, 961317661, 971769781, 1009839289, 1012425823, 1018067263, 1024053841, 1029453781, 1032852721, 1045539613, 1072488943, 1074373747, 1075112461, 1098100501, 1103944801, 1104377569, 1121341219, 1126460743, 1131761599, 1142743363, 1169531647, 1173410551, 1214376817, 1234669027, 1236504427, 1251024097, 1256057233, 1265506783, 1284663943, 1338436609, 1344074323, 1357375729, 1359645691, 1365904681, 1378087873, 1379329597, 1389690361, 1397195491, 1403044897, 1403917747, 1413095023, 1430397049, 1492477453, 1527820219, 1553784091, 1580923723, 1604659723, 1704781621, 1853370913, 1855702561, 1866880699, 1868148367, 1926463717, 1930513327, 1969936477, 1987885309, 2014651237, 2018327281, 2048696941, 2050376539, 2064954169, 2134365547, 2148446929, 2166459241, 2167256467, 2175901891, 2301590497, 2309791009, 2330995951, 2355078469, 2376855973, 2408180869, 2413966519, 2439260539, 2443389913, 2444486599, 2448029197, 2569015591, 2642726083, 2656090141, 2702780923, 2706891391, 2731066231, 2750484487, 2793795373, 2807213113, 2849549581, 2896011007, 2912788357, 2956650691, 2956995829, 2969940781, 3148392031, 3212425963, 3315286333, 3344803153, 3355883449, 3367448401, 3436437913, 3438150217, 3447993067, 3467439061, 3549437833, 3599852821, 3618818851, 3648179179, 3694854091, 3754203889, 3787601269, 3887586823, 4032440593, 4386959971, 4514739277, 4641024457, 4664321341, 4803751987, 4839197563, 5123773849, 5129542801, 5275285291, 5286316183, 5380036813, 5453907799, 5597185747, 5598094891, 5599061719, 5664858187, 5750395141, 5890320379, 5952831067, 6090034807, 6190867819, 6233124661, 6340080871, 6355649893, 6420744493, 6483183559, 6491665867, 6632353003, 6874169161, 6876486319, 6894237949, 7125284587, 7140766807, 7262183347, 7326774109, 7410904429, 7755746143, 8037859957, 8047139767, 8167534003, 8329379713, 8469050893, 8640113899, 8654911087, 8790675211, 9215798149, 9234440707, 9254343067, 9520378501, 9561006943, 9728033311, 9819154159, 9950930497, 10185206197, 10200889759, 10532536051, 10681854259, 10700455417, 10950239143, 11119906969, 11394244483, 11507646673, 11579007301, 12416790121, 12728466847, 12851327143, 13492430569, 13716926071, 13852108111, 14080465681, 14204095879, 14482652329, 14528038321, 14730367297, 14861721907, 15171346297, 15206676367, 15444729541, 15993467359, 16316789491, 16384855093, 16507996909, 17137253311, 17865064759, 19081451959, 19636779277, 19668641821, 19744641457, 19997444209, 20637098359, 21641683159, 23319498889, 23351439127, 23535794707, 23748991183, 24286384159, 25087978687, 25864174591, 26578284433, 26628094291, 26919805039, 26980594867, 28392688837, 28834787017, 29469888271, 31567437763, 31851812569, 32413807357, 34944894889, 35384890501, 35793655747, 36173716303, 37394767903, 40870590049, 43197706543, 43600001659, 44617807411, 45314147269, 47339219713, 50001944479, 50560734079, 54267396829, 55545840697, 56026503943, 56868977521, 63244387357, 66976440451, 74308377001, 74427028297, 80988973423, 88585960777, 114802485799, 128686670353, 131976944461, 160790274823, 169883582101, 177101111269, 191872957501, 194625538897, 196842376693, 203261585797, 214025282059, 231795544819, 243255046327, 247201847293, 252117007507, 290046282943, 338420108251, 396859826749, 504724247593, 587714997127, 601160444077, 634602994237, 688813144249, 924566585233, 963231933211, 990197171437, 1012086362701, 1095440283109, 1240299944053, 1278283326667, 1313043978583, 1359247968343, 1582881185761, 1632706564207, 1862498582797, 2108035008553, 2179767637771, 2731829784967, 4041886638871, 4300501367131, 4384873614241, 4892588415259, 5361373268617, 5415624023749, 6209570658679, 6976413097111, 8026634893171, 10052678938039, 10470435972169, 11602332672583, 15769887150799, 17542606699201, 27378093143953, 31199434481833, 43368407304073, 43748177503243, 53259432776047, 63713248669501, 77440198677379, 350409027072301, 40483096874817}.

REFERENCES

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

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

[3] 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.

[4] H. Xu and B. Bai, "Superposition construction of Q-Ary LDPC codes by jointly optimizing girth and number of shortest cycles," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1285–1288, Jul. 2016.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] S. Kim, J. No, H. Chung, and D. 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

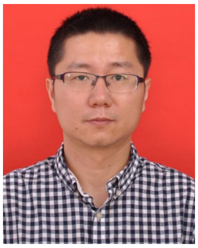
[16] M. Zhou, H. Zhu, H. Xu, B. Zhang, and K. Xie, "A note on the girth of (3,19)-regular Tanner's quasi-cyclic LDPC codes," *IEEE Access*, vol. 9, pp. 28582–28590, 2021.

[17] 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.

QI WANG received the Ph.D. degree from Xidian University, China. He is currently an Associate Professor with the School of Network Engineering, Zhoukou Normal University, Zhoukou, China. His research interests include the Internet of Things technology and channel coding.

JINGPING CHE received the M.S. degree from Xidian University, China. She is currently a Teaching Assistant with the School of Network Engineering, Zhoukou Normal University, Zhoukou, China. Her research interests include 5G techniques and channel coding.

HUAAN LI received the B.S. degree in electrical and information engineering from Harbin Institute of Technology, Harbin, China, in 2013, the M.S. degree in signal and information processing from Lanzhou University, Lanzhou, China, in 2016, and the Ph.D. degree in communication and information system from Xidian University, Xi'an, China, in 2021. He is currently a Lecturer with the School of Physics and Telecommunication Engineering, Zhoukou Normal University, Zhoukou, China. His research interests include information and coding theory and wireless communications.



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 Henan Provincial Research Center of Wisdom Education and Intelligent Technology Application Engineering Technology, Zhengzhou Railway Vocational Technical College, Zhengzhou, China. His research interests include information theory, LDPC coding, capacity region, and transmission strategies for interference channels.

ZHEN LUO received the Ph.D. degree from Xidian University, China. He is currently a Lecturer with the School of Network Engineering, Zhoukou Normal University, Zhoukou, China. His research interests include 5G techniques and channel coding for wireless communications.

HUI LIU received the Ph.D. degree from the School of Computer Science and Technology, Xidian University, Xi'an, China. He is currently an Associate Professor with Henan Provincial Research Center of Wisdom Education and Intelligent Technology Application Engineering Technology, Zhengzhou Railway Vocational Technical College, Zhengzhou, China. His research interests include information theory and the Internet of Things technology.