DOI:10.11916/j.issn.1005-9113.16068

# On the Girth of Tanner (5,7) Quasi-Cyclic LDPC Codes

*Hengzhou Xu, Baoming Bai*, Dan Feng and Cheng Sun*

(*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*)

**Abstract**: The girth plays an important role in the design of LDPC codes. In order to determine the girth of Tanner (5,7) quasi-cyclic (QC) LDPC codes with length $7p$ for $p$ being a prime with the form $35m + 1$, the cycles of lengths 4, 6, 8, and 10 are analyzed. Then these cycles are classified into sixteen categories, each of which can be expressed as an ordered block sequence, or a certain type. It is also shown that the existence of these cycles is equal to polynomial equations over $F_p$ who has a 35th unit root. We check if these polynomial equations have a 35th unit root and obtain the girth values of Tanner (5,7) QC LDPC codes.

**Keywords**: LDPC codes; quasi-cyclic; Tanner graph; girth

**CLC number**: TN911 **Document code**: A **Article ID**: 1005-9113(2017)06-0080-10

## 1 Introduction

LDPC codes, proposed by Gallager[1], are a class of linear codes which can approach Shannon capacity[2]. Later, Tanner[3] presented a bipartite graph, known as Tanner graph, to represent an LDPC code. From the graph theory perspective, the iterative process of the decoding algorithms[4] based on belief propagation for LDPC codes, which results in good decoding performance and has low decoding complexity, can be intuitively understood. But short cycles, especially cycles with length 4, seriously degrade the iterative decoding performance of an LDPC code. For the shortest cycles, their length is called the girth. In the iterative decoding, the exact LLRs can be obtained in the first $g/2$ iterations, where $g$ is the girth value[5]. That is, girth plays an important role in the design of LDPC codes. Research results show that LDPC codes with large girth, small number of short cycles, and no harmful trapping set perform very well[6]. Structured LDPC codes whose girth is at least six are generally constructed based on algebraic structures, such as finite field[7], partial geometry[8]. Furthermore, LDPC codes with larger girth (more than 8) are also proposed in Refs. [9-17]. Moreover, with regard to circulant permutation matrices (CPMs) based $(\gamma, \rho)$-regular QC LDPC codes[18], Fossorier showed that the girth of such codes is at most 12. So to design such $(\gamma,\rho)$-regular QC LDPC codes with girth 12 (or to prove the girth of such codes is 12) is an interesting problem.

A QC LDPC code is defined by the null space of sparse matrix $\boldsymbol{H}$ that consists of CPMs and zero matrices of the same size. If each column or row of $\boldsymbol{H}$ has constant number of nonzero elements, denoted by $\gamma,\rho$, respectively, the QC LDPC code is $(\gamma,\rho)$-regular. Tanner[19] proposed a kind of $(\gamma,\rho)$-regular QC LDPC codes and we call them Tanner $(\gamma,\rho)$ QC LDPC codes for short here. According to Ref. [18], it can be seen that the girth of Tanner $(\gamma,\rho)$ QC LDPC codes is not more than 12. It is also shown in Ref. [18] that as the size of CPMs increases, the girth of Tanner $(\gamma,\rho)$ QC LDPC codes can be up to 12. For Tanner (3,5) QC LDPC codes with length $5p$ for $p$ being a prime with the form $15m + 1$, Kim et al.[20] had determined their girth. For Tanner (3,7) QC LDPC codes with length $7p$ for $p$ being a prime with the form $21m + 1$, the girth was obtained by Gholami[21]. As a matter of fact, they classified short cycles in Tanner (3,5) and (3,7) QC LDPC codes into several equivalent classes, respectively, and presented the existence conditions for the cycles whose lengths are less than 10, namely, a series of polynomial equations over $\boldsymbol{F}_p$ which have a 15th or 21th unit roots. Finally, by checking the existence of solutions for these polynomial equations, the girth values were obtained.

In this paper, the cycles of Tanner (5,7) QC LDPC codes with length $7p$ for $p$ being a prime with the form $35m + 1$, are first classified and then the equivalent relation is defined. Based on the equivalent relation, the cycles of lengths 4, 6, 8, and 10 are

Received 2016-03-15.

Sponsored by the National Natural Science Foundation of China (Grant Nos. 61372074 and 91438101) and the National High Technology Research and Development Program of China (Grant No. 2015AA01A709).

* Corresponding author. E-mail: bmbai@mail.xidian.edu.cn.

classified into sixteen equivalent classes. Thereinto, the cycles of lengths 4 and 6 have only one equivalent class, the cycles of lengths 8 and 10 have five and nine classes, respectively. On the basis of these sixteen equivalent classes, the sufficient and necessary existence conditions of short cycles in Tanner (5,7) QC LDPC codes are proposed. According to these conditions, polynomial equations over $\boldsymbol{F}_p$ which have a 35th unit root can be derived. Applying the Euclidean division algorithm to these equations over $\boldsymbol{F}_p$ and $(x^{35}-1)$ (or its simplified form), all remainder polynomials can be also obtained. Unlike Refs.[20] and [21], we check if all the remainder polynomials over $\boldsymbol{F}_p$ are equal to zero, not just the last remainder polynomial, since all the remainder polynomials possibly equal zero over $\boldsymbol{F}_p$ and result in candidate girth values. But there are 1 826 polynomial equations, which are about 7.2 times larger than those of Tanner (3,7) QC LDPC codes[21]. Moreover, in order to check if the remainder polynomials over $\boldsymbol{F}_p$ equal zero, we need to factor the coefficients of the remainder polynomials. Considering all needed calculation, this is a huge amount of work. Therefore, we do it with the aid of computer. For convenience, all cases and the candidate girth values are recorded in tables, just like those given in Refs.[20] and [21]. By following the candidate girth values obtained in each equivalent class, we obtain the girths of Tanner (5,7) QC LDPC codes.

## 2 Cycles in Tanner (5,7) Quasi-Cyclic LDPC Codes

A $(\gamma,\rho)$-regular QC LDPC code with length $p\rho$ is defined by the null space of the following matrix:

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{I}(p_{0,0}) & \boldsymbol{I}(p_{0,1}) & \cdots & \boldsymbol{I}(p_{0,\rho-1}) \\ \boldsymbol{I}(p_{1,0}) & \boldsymbol{I}(p_{1,0}) & \cdots & \boldsymbol{I}(p_{1,\rho-1}) \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{I}(p_{\gamma-1,0}) & \boldsymbol{I}(p_{\gamma-1,1}) & \cdots & \boldsymbol{I}(p_{\gamma-1,\rho-1}) \end{bmatrix} \tag{1}$$

where, for $0\leqslant i\leqslant\gamma-1, 0\leqslant j\leqslant\rho-1$, $\boldsymbol{I}(p_{i,j})$ represents a CPM of size $p\times p$ and $p_{i,j}$ is the shift value. In the CPM $\boldsymbol{I}(p_{i,j})$, the single element "1" is at the $((r+p_{i,j}) \bmod p)$th column and $r$th row and the elements at the remaining positions are "0". Obviously, $\boldsymbol{I}(0)$ is the $p\times p$ identity matrix. As another example, if $p=3$, then

$$\boldsymbol{I}(2)=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Fossorier[18] represented a cycle of length $2i$, denoted by $2i$-cycle for short, in $\boldsymbol{H}$ as an ordered block sequence:

$(j_0,l_0)$; $(j_1,l_1)$; $(j_2,l_2)$; …; $(j_k,l_k)$; …; $(j_{i-1},l_{i-1})$; $(j_0,l_0)$

This cycle can be also denoted by type $(j_0,j_1,\cdots,j_k,\cdots,j_{i-1})$ for brevity. Clearly, $j_k$ does not equal $j_{k+1}$, $l_k$ does not equal $l_{k+1}$. The block $(j_k,l_k)$ represents the $j_k$th column and $l_k$th row CPM $\boldsymbol{I}(j_k,l_k)$ and semicolon between $(j_k,l_k)$ and $(j_{k+1},l_{k+1})$ represents the column $-j_{k+1}$ and row-$l_k$ CPM $\boldsymbol{I}(j_{k+1},l_k)$. Furthermore, the sufficient and necessary existence condition of a $2i$-cycle in $\boldsymbol{H}$ was also presented by Fossorier:

$$\sum_{k=0}^{i-1}(p_{j_k,l_k}-p_{j_{k+1},l_k})=0 \pmod p \tag{2}$$

We specify the shift value $p_{i,j}=\alpha^{\rho i+\gamma j}$ in $\boldsymbol{H}$, where $\alpha$ is a primitive 35th unit root of $\boldsymbol{F}_p$. Here we focus on $\gamma=5$ and $\rho=7$, then a Tanner (5,7) QC LDPC code with length $7p$ can be given by the null space of the following matrix:

$$\boldsymbol{H}=\begin{bmatrix} \alpha^{0} & \alpha^{5} & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} & \alpha^{30} \\ \alpha^{7} & \alpha^{12} & \alpha^{17} & \alpha^{22} & \alpha^{27} & \alpha^{32} & \alpha^{2} \\ \alpha^{14} & \alpha^{19} & \alpha^{24} & \alpha^{29} & \alpha^{34} & \alpha^{4} & \alpha^{9} \\ \alpha^{21} & \alpha^{26} & \alpha^{31} & \alpha & \alpha^{6} & \alpha^{11} & \alpha^{16} \\ \alpha^{28} & \alpha^{33} & \alpha^{3} & \alpha^{8} & \alpha^{13} & \alpha^{18} & \alpha^{23} \end{bmatrix}$$

where $p\equiv 1 \pmod{35}$ is a prime. That is, $p$ belongs to $\{71,211,281,421,491,631,\cdots\}$. This set is denoted by $\boldsymbol{P}_{35}$.

According to Eq.(1), the sufficient and necessary existence condition of a $2i$-cycle in $\boldsymbol{H}$, whose type is $(j_0,j_1,\cdots,j_k,\cdots,j_{i-1})$ in Tanner (5,7) QC LDPC codes, is given by

$$\sum_{k=0}^{i-1}(\alpha^{7j_k}-\alpha^{7j_{k+1}})\alpha^{5l_k}=0 \pmod p$$

with $j_0=j_i, j_k\neq j_{k+1}$, and $l_k\neq l_{k+1}$. According to Ref.[22], the above equation is called basic equation in the remaining paper. Notice that we assume that $l_0=0$. In order to classify cycles in $\boldsymbol{H}$ into block sequences, same as defined in Ref.[22], we give the equivalent relation of cycles in Tanner (5,7) QC LDPC codes as the following.

**Definition 1** Type $(j_0,j_1,j_2,\cdots,j_{i-1})$ is equivalent to type $(k_0,k_1,k_2,\cdots,k_{i-1})$ in Tanner (5,7) QC LDPC codes if one of the following conditions holds:

1) There exists some $c\in\{0,1,2,3,4\}$ such that $k_s=j_s+c \pmod 5$, for all $s$.

2) There exists some $c\in\{0,1,2,3,4\}$ such that $k_s=j_s\times c \pmod 5$, for all $s$.

3) There is some $c\in\{0,1,2,\cdots,i-1\}$ s.t. $k_s=j_{s+c}$ for all $s$.

4) There is some $c\in\{0,1,2,\cdots,i-1\}$ s.t. $k_s=j_{i-1-s+c}$ for all $s$.

We can easily find all such types $(j_0,j_1,j_2,\cdots,j_{i-1})$ of $2i$-cycles in Tanner (5,7) QC LDPC codes, where $0\leqslant j_k\leqslant 4, j_k\neq j_{k+1}$, and $j_i\neq j_0$ for $0\leqslant k\leqslant i-1$. On the basis of the above equivalent relation, we partition all types of cycles with lengths not more than 10 in Tanner (5,7) QC LDPC codes into the following sixteen equivalent classes:

1)4-cycles: There is only one class $(0,1)$ for all 4-cycles.

2)6-cycles: There is only one class $(0,1,2)$ for all 6-cycles.

3)8-cycles: There are five equivalent classes, i.e., $(0,1,0,1)$, $(0,1,0,2)$, $(0,1,0,4)$, $(0,1,2,3)$, and $(0,1,3,2)$ for all 8-cycles.

4) 10-cycles: There are nine equivalent classes, i.e., $(0,1,2,3,4)$, $(0,1,2,4,3)$, $(0,1,3,2,4)$, $(0,1,4,2,3)$, $(0,1,0,2,3)$, $(0,1,0,2,4)$, $(0,1,0,3,4)$, $(0,1,2,0,1)$, and $(0,1,3,0,1)$ for all 10-cycles.

Based on these sixteen equivalent classes and (2), we can obtain the specific basic equations. We assume, for convenience, that $t = l_1 - l_0 \pmod 7$, $u = l_2 - l_1 \pmod 7$, $v = l_3 - l_2 \pmod 7$, and $w = l_4 - l_3 \pmod 7$. It is clear that $t, u, v$, and $w$ belong to $\{\pm 1, \pm 2, \pm 3\}$. Now, what we are going to do is to check if these basic equations over $\boldsymbol{F}_p$ have solutions, and then candidate girth values $g$ can be obtained.

## 2.1 4-cycles

Under the equivalent relation in Definition 1, all 4-cycles belong to the unique class $(0, 1)$ which corresponds to the block sequence: $(0,0)$; $(1,0)$; $(1,t)$; $(0,t)$, and $t$ is not equal to 0. According to the values of these blocks, the basic equation can be given as:

$$\sum_{k=0}^{1} (\alpha^{7j_k} - \alpha^{7j_{k+1}})\alpha^{5l_k} = (1-\alpha^7)(1-\alpha^{5t}) = 0 \pmod p$$

Because $\alpha$ is a primitive 35th unit root, then $\alpha^7 \neq 1$, $\alpha^{5t} \neq 1$, where $-3 \leqslant t \leqslant 3$ and $t \neq 0$. Therefore, the above equation is not satisfied and there is no 4-cycle in Tanner (5,7) QC LDPC codes.

## 2.2 6-cycles

All 6-cycles belong to the unique class $(0,1,2)$ which corresponds to the block sequence: $(0,0)$; $(1,0)$; $(1,t)$; $(2,t)$; $(2;t+u)$; $(0,t+u)$, $(t+u) \pmod 7$ is not equal to 0. The basic equation can be written as:

$$\sum_{k=0}^{2} (\alpha^{7j_k} - \alpha^{7j_{k+1}})\alpha^{5l_k} = (1-\alpha^7)(1+\alpha^{5t+7} - \alpha^{5(t+u)} - \alpha^{5(t+u)+7}) = 0 \pmod p$$

Since $\alpha^7 \neq 1$, the basic equation can be modified as:

$$1 + \alpha^{5t+7} - \alpha^{5(t+u)} - \alpha^{5(t+u)+7} = 0 \pmod p \quad (3)$$

As mentioned in Ref.[21], this modified form of the basic equation is called modified basic equation. In this case, Eq.(3) is the modified basic equation. So, there is a 6-cycle in Tanner (5,7) QC LDPC codes if and only if Eq.(3) is satisfied. For different values of $t$ and $u$, we can obtain various modified basic equations. Consider $t$ to be a variable, we can use $t$ to express the values of $u$. If $t + u = 0 \pmod 7$, these cases are called invalid cases, and the other cases are valid cases, such as defined in Ref.[21]. We list all cases of $(t,u)$ and the corresponding modified basic equations in Table 1. Thereinto, the cases, labeled by "×", are invalid. We check the existence of the solution for Eq.(3) in each valid case as follows.

**Table 1 All cases of $(t,u)$ and modified basic equations**

| No. | $(t,u)$ | Modified basic equations |
|---|---|---|
| 1 | $(t,t)$ | $1 + \alpha^{5t+7} - \alpha^{10t} - \alpha^{10t+7}$ |
| 2 | $(t,2t)$ | $1 + \alpha^{5t+7} - \alpha^{15t} - \alpha^{15t+7}$ |
| 3 | $(t,3t)$ | $1 + \alpha^{5t+7} - \alpha^{20t} - \alpha^{20t+7}$ |
| × | $(t,-t)$ | |
| 5 | $(t,-2t)$ | $1 + \alpha^{5t+7} - \alpha^{-5t} - \alpha^{-5t+7}$ |
| 6 | $(t,-3t)$ | $1 + \alpha^{5t+7} - \alpha^{-10t} - \alpha^{-10t+7}$ |

### 2.2.1 Case $(t,t)$

According to Table 1, the modified basic equation is $1 + \alpha^{5t+7} - \alpha^{10t} - \alpha^{10t+7}$. Set $x = \alpha^{5t+7}$. For $0 \leqslant i \leqslant 35$, we can obtain the values of $x^i$, listed in Table 2. Then the modified basic equation becomes $1 + x - x^{16} - x^{30}$. Since $x^{35} - 1$ can be factorized as:

$$x^{35} - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(1 - x + x^5 - x^6 + x^7 - x^8 + x^{10} - x^{11} + x^{12} - x^{13} + x^{14} - x^{16} + x^{17} - x^{18} + x^{19} - x^{23} + x^{24})$$

and $x$ is a primitive 35th root of unity of $\boldsymbol{F}_p$, we have

$$1 - x + x^5 - x^6 + x^7 - x^8 + x^{10} - x^{11} + x^{12} - x^{13} + x^{14} - x^{16} + x^{17} - x^{18} + x^{19} - x^{23} + x^{24} = 0 \pmod p \quad (4)$$

The modified basic equation $1 + x - x^{16} - x^{30}$ can be factorized as

$$1 + x - x^{16} - x^{30} = (1-x)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^{15} + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)$$

It is easy to check that $1 - x \neq 0 \pmod p$, $x^2 + x + 1 \neq 0 \pmod p$, $x^4 + x^3 + x^2 + x + 1 \neq 0 \pmod p$, and $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \neq 0 \pmod p$. There are many polynomials like these, such as $x^2 + 1$, $x^3 + x^2 + x + 1, \cdots$. We can directly eliminate these factors from modified basic equations, since they are not equal to zero in $\boldsymbol{F}_p$. The eliminated form of modified basic equation is called reduced form. Here the reduced form is $x^{15} + x + 1$. By applying the Euclidean division algorithm to $x^{15} + x + 1$ and Eq.(4), the remainder polynomials are $x^{14} - x^{13} + x^{12} - x^{11} + x^7 - x^6 + 1$, $x^{11} - x^8 + x^6$, $-x^{10} + x^8 - x^6 + 1$, $x^9 - x^8 - x^7 + x^6 + x$, $-x^8 + x^2 + x + 1$, $x^7 + x^6 + x^3 + x - 1$, $-x^6 - x^4 - x^3 + x + 2$, $x^5 - x^2 + 1$, $-x^4 - 2x^3 + 2x + 2$, $4x^3 + x^2 - 2x - 3$, $-(1/16)x^2 + (3/8)x + 11/16$, $192x + 272$, $71/2\,304$.

It is clear that the remainder $71/2\,304$ equals zero in $\boldsymbol{F}_{71}$. When $p \in \boldsymbol{P}_{35} \backslash \{71\}$, the remainder polynomials cannot be equal to zero in $\boldsymbol{F}_p$. So the basic equation has no solution in $\boldsymbol{F}_p$, $p \in \boldsymbol{P}_{35} \backslash \{71\}$.

**Table 2 Representation of $x^i$**

| $x^i$ | Values | $x^i$ | Values | $x^i$ | Values | $x^i$ | Values | $x^i$ | Values | $x^i$ | Values |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $x$ | $\alpha^{5t+7}$ | $x^2$ | $\alpha^{10t+14}$ | $x^3$ | $\alpha^{15t+21}$ | $x^4$ | $\alpha^{20t+28}$ | $x^5$ | $\alpha^{25t}$ | $x^6$ | $\alpha^{30t+7}$ |
| $x^7$ | $\alpha^{14}$ | $x^8$ | $\alpha^{5t+21}$ | $x^9$ | $\alpha^{10t+28}$ | $x^{10}$ | $\alpha^{15t}$ | $x^{11}$ | $\alpha^{20t+7}$ | $x^{12}$ | $\alpha^{25t+14}$ |
| $x^{13}$ | $\alpha^{30t+21}$ | $x^{14}$ | $\alpha^{28}$ | $x^{15}$ | $\alpha^{5t}$ | $x^{16}$ | $\alpha^{10t+7}$ | $x^{17}$ | $\alpha^{15t+14}$ | $x^{18}$ | $\alpha^{20t+21}$ |
| $x^{19}$ | $\alpha^{25t+28}$ | $x^{20}$ | $\alpha^{30t}$ | $x^{21}$ | $\alpha^{7}$ | $x^{22}$ | $\alpha^{5t+14}$ | $x^{23}$ | $\alpha^{10t+21}$ | $x^{24}$ | $\alpha^{15t+28}$ |
| $x^{25}$ | $\alpha^{20t}$ | $x^{26}$ | $\alpha^{25t+7}$ | $x^{27}$ | $\alpha^{30t+14}$ | $x^{28}$ | $\alpha^{21}$ | $x^{29}$ | $\alpha^{5t+28}$ | $x^{30}$ | $\alpha^{10t}$ |
| $x^{31}$ | $\alpha^{15t+7}$ | $x^{32}$ | $\alpha^{20t+14}$ | $x^{33}$ | $\alpha^{25t+21}$ | $x^{34}$ | $\alpha^{30t+28}$ | $x^{35}$ | $\alpha^0 = 1$ | | |

*2.2.2 Case (t,2t)*

According to Tables 1 and 2, the modified basic equation $1+\alpha^{5t+7}-\alpha^{15t}-\alpha^{15t+7}$ can be written as $1+x-x^{10}-x^{31}$. This equation can be factorized as:

$$1+x-x^{10}-x^{31}=(1+x)(1-x)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)(x^{21}+x^{11}+x+1)$$

We can see that the reduced form is $x^{21}+x^{11}+x+1$. By applying the Euclidean division algorithm to $x^{21}+x^{11}+x+1$ and Eq. (4), the remainder polynomials are

$$x^{19}-x^{18}+x^{17}-x^{16}+x^{12}-x^{11}+x^{10}-x^8+x^7-x^6+x^5-x^4+x^2-x+1$$
$$x^{17}-x^{14}+x^{10}+x^5-x^4+1$$
$$-x^{15}+x^{14}-x^8+x^6-x^5-x^9-x^4+1$$
$$-x^8-x^5+x^4+x-1$$
$$x^6-x^5-x^4-x^2+x+1$$
$$-4x^5-2x^4+4x+1$$
$$-(1/4)x^4-(1/4)x+5/8$$
$$4x^2-4x-4$$
$$-x+1/8,\ -71/16$$

Obviously, if $p=71$, then the remainder $-71/16$ is equal to zero in $\boldsymbol{F}_{71}$. When $p\in\boldsymbol{P}_{35}\backslash\{71\}$, $-71/16$ cannot equal zero in $\boldsymbol{F}_p$. Then the basic equation has no solution in $\boldsymbol{F}_p$, $p\in\boldsymbol{P}_{35}$ apart from $p=71$.

*2.2.3 Case (t,3t)*

Under Tables 1 and 2, the modified basic equation $1+\alpha^{5t+7}-\alpha^{20t}-\alpha^{20t+7}$ can be modified as $1+x-x^{11}-x^{25}$. This equation can be factorized as:

$$1+x-x^{11}-x^{25}=(1-x)(x^4+x^3+x^2+x+1)(x^{20}+x^{15}+x^{10}+x^6+x^5+x+1)$$

It is clear that the reduced form is $x^{20}+x^{15}+x^{10}+x^6+x^5+x+1$. By applying the Euclidean division algorithm to $x^{20}+x^{15}+x^{10}+x^6+x^5+x+1$ and Eq. (4), the remainder polynomials are $x^{17}-x^{16}+x^{12}-x^{11}+x^7-x^6+x^3-x+1$, $x^{16}+x^{11}+x^6-x^3+x$, $x^4-x^2+1$, $-2x^3+x^2+2x-2$, $(1/4)x^2-(1/2)x+1/2$, 4.

Since all remainder polynomials are not equal to zero in $\boldsymbol{F}_p$, $p\in\boldsymbol{P}_{35}$, the basic equation has no solution in $\boldsymbol{F}_p$.

*2.2.4 Case (t,-2t)*

With Tables 1 and 2, the modified basic equation $1+\alpha^{5t+7}-\alpha^{-5t}-\alpha^{-5t+7}$ can be modified as $1+x-x^6-x^{20}$. This equation can be factorized as:

$$1+x-x^6-x^{20}=(1-x)(x^4+x^3+x^2+x+1)(x^{15}+x^{10}+x^5+x+1)$$

Obviously, the reduced form is $x^{15}+x^{10}+x^5+x+1$. By applying the Euclidean division algorithm to $x^{15}+x^{10}+x^5+x+1$ and Eq. (4), the remainder polynomials are $x^5-x^3+1$, $-3x^4+3x^3-x^2+3x-1$, $-(1/3)x^3+(2/3)x^2+(2/3)x+2/3$, $-13x^2-9x-7$, $(38/169)x+31/169$, $-11\,999/1\,444$ $(=(71\times13^2)/1\,444)$.

We can see that the remainder $-11\,999/1\,444$ equals zero in $\boldsymbol{F}_{71}$. When $p\in\boldsymbol{P}_{35}\backslash\{71\}$, the remainders cannot equal zero in $\boldsymbol{F}_p$, $p\in\boldsymbol{P}_{35}\backslash\{71\}$. So the basic equation has no solution in $\boldsymbol{F}_p$, $p\in\boldsymbol{P}_{35}\backslash\{71\}$.

*2.2.5 Case (t,-3t)*

Based on Tables 1 and 2, the modified basic equation $1+\alpha^{5t+7}-\alpha^{-10t}-\alpha^{-10t+7}$ becomes polynomial equation in $x$, i.e., $1+x-x^5-x^{26}$. This equation can be factorized as:

$$1+x-x^5-x^{26}=(1-x)(1+x)(x^4+x^3+x^2+x+1)(x^{20}-x^{19}+x^{18}-x^{17}+x^{16}+x^{10}-x^9+x^8-x^7+x^6+1)$$

It is obvious that the reduced form is $x^{20}-x^{19}+x^{18}-x^{17}+x^{16}+x^{10}-x^9+x^8-x^7+x^6+1$. By applying the Euclidean division algorithm to $x^{20}-x^{19}+x^{18}-x^{17}+x^{16}+x^{10}-x^9+x^8-x^7+x^6+1$ and Eq. (4), the remainder polynomials are

$$x^{17}-x^{16}+x^{12}-x^{11}+x^{10}-x^9+x^7-x^6+x^5-x^4+x^2-x+1$$
$$x^{16}-x^{15}+x^{14}-2x^{13}+2x^{12}-x^{11}+x^{10}-x^8+x^7+x^4-2x^3+x^2-x+1$$
$$-x^{15}+2x^{14}-2x^{13}+2x^{12}-2x^{11}+x^{10}-x^8+x^7-x^6+x^4-x^3+2x^2-2x+1$$
$$x^{14}-2x^{13}+2x^{12}-2x^{11}+2x^{10}-x^9-x^8+x^7-x^6+x^5+x^4-x^3+x^2-2x+2$$
$$-x^9+x^5+1$$
$$x^8-x^7+2x^6-x^5-x^4+x^3-x^2+x-1$$
$$x^7+x^6-x^5$$
$$5x^6-3x^5-x^4+x^3-x^2+x-1$$
$$(4/25)x^5+(3/25)x^4-(3/25)x^3+(3/25)x^2-$$

$$(3/25)x + 8/25$$
$$(125/16)x^4 - (125/16)x^3 + (125/16)x^2 - (225/16)x + 25/2$$
$$(16/125)x^2 + (16/125)x - 16/125$$
$$(-975/16)x + 175/4$$
$$1\ 136/38\ 025\ (=71\times 2^4/38\ 025)$$

It is easy to know that the remainder 1 136/38 025 equals zero in $\boldsymbol{F}_{71}$. When $p \in \boldsymbol{P}_{35}\backslash\{71\}$, then 1 136/38 025 cannot equal zero in $\boldsymbol{F}_p$. So the basic equation has no solution in $\boldsymbol{F}_p$, $p \in \boldsymbol{P}_{35}$ apart from $p = 71$.

By following the conclusion drawn in Section 2.1, it can be also concluded that Tanner (5,7) QC LDPC code with length 497 ($=71\times7$) has girth 6, and that Tanner (5,7) QC LDPC codes with length $7p$ have girth at least 8, $p \in \boldsymbol{P}_{35}\backslash\{71\}$.

### 2.3 8-cycles

All 8-cycles can be partitioned into five equivalent classes. As mentioned in Sections 2.1 and 2.2, by applying the Euclidean algorithm to the reduced form of basic equation and Eq.(4), we check the existence of the solutions for the basic equation, and obtain the candidate girth values $g$. To save space, all equivalent classes of 8-cycles and their corresponding modified basic equations are tabulated in Table 3 and the candidate girth values g are recorded in Table 4.

**Table 3 All equivalent classes of 8-cycles and their modified basic equations**

| Equivalent class | Modified basic equation |
|---|---|
| (0,1,0,1) | $1-\alpha^{5t}+\alpha^{5(t+u)}-\alpha^{5(t+u+v)}$ |
| (0,1,0,2) | $1-\alpha^{5t}+(1+\alpha^7)(\alpha^{5(t+u)}-\alpha^{5(t+u+v)})$ |
| (0,1,0,4) | $1-\alpha^{5t}+(1+\alpha^7+\alpha^{14}+\alpha^{21})\cdot(\alpha^{5(t+u)}-\alpha^{5(t+u+v)})$ |
| (0,1,2,3) | $1+\alpha^{5t+7}+\alpha^{5(t+u)+14}-(1+\alpha^7+\alpha^{14})\alpha^{5(t+u+v)}$ |
| (0,1,3,2) | $1+(1+\alpha^7)(\alpha^{5t+7}-\alpha^{5(t+u+v)})-\alpha^{5(t+u)+14}$ |

Note that all cases of $(t,u,v)$ are listed in Table 4, and the cases, labeled by "×", are invalid ($t+u+v=0 \pmod 7$). By eliminating those polynomials which do not equal zero in $\boldsymbol{F}_p$, $p \in \boldsymbol{P}_{35}$, the reduced forms of the modified basic equations are obtained (Here we omit to record them). After applying the Euclidean algorithm to the reduced forms of basic equations and Eq.(4), we check if there exist the remainder polynomials which are equal to zero in $\boldsymbol{F}_p$, and obtain the candidate girth values $g$, as listed in Table 4. Since the equivalent class (0,1,0,1) has no candidate girth value, then we do not record it in Table 4. And its valid cases $(t,u,v)$, as listed in Table 4, are the same as the other four equivalent classes. Based on the conclusions in Sections 2.1 and 2.2, we can see from Table 4 that Tanner (5,7) QC LDPC codes with length $7p$ have girth 8, $p \in G_8$, where $G_8 = \{211,281,421,491,631,701,911,1\,051,2\,311,4\,271,5\,531,7\,211,237\,301,354\,551\}$.

### 2.4 10-cycles

All 10-cycles are divided into nine equivalent classes. For each equivalent class, its corresponding modified basic equation is tabulated in Table 5. And all cases of $(t,u,v,w)$ and the corresponding candidate girth values $g$ are recorded in Table 6.

**Table 4 All cases $(t,u,v)$ and candidate girth values**

| No. | $(t,u,v)$ | (0,1,0,2) | (0,1,0,4) | (0,1,2,3) | (0,1,3,2) |
|---|---|---|---|---|---|
| 1 | $(t,t,t)$ | 71 | | 71 | 211 |
| 2 | $(t,t,2t)$ | 421 | 701 | 421 | 421 |
| 3 | $(t,t,3t)$ | 71,211 | 211 | 421 | 71 |
| 4 | $(t,t,-t)$ | 911 | | | |
| × | $(t,t,-2t)$ | | | | |
| 6 | $(t,t,-3t)$ | | | 71 | 71,211 |
| 7 | $(t,2t,t)$ | 71 | | 701 | 281 |
| 8 | $(t,2t,2t)$ | | | 211 | 71,211 |
| 9 | $(t,2t,3t)$ | 71,211 | 211 | 211 | 421 |
| 10 | $(t,2t,-t)$ | 911 | | 211 | |
| 11 | $(t,2t,-2t)$ | 7 211 | 211,5 531 | 71 | 5 531 |
| × | $(t,2t,-3t)$ | | | | |
| 13 | $(t,3t,t)$ | 71 | | 2 311 | 281 |
| 14 | $(t,3t,2t)$ | 421 | 701 | 71 | 71 |
| × | $(t,3t,3t)$ | | | | |
| 16 | $(t,3t,-t)$ | 71,911 | | 491 | |
| 17 | $(t,3t,-2t)$ | 1 051 | 211 | 281 | 71 |
| 18 | $(t,3t,-3t)$ | 237 301 | 421,4 271 | 71 | 4 271 |
| 19 | $(t,-t,t)$ | | | | |
| 20 | $(t,-t,2t)$ | 354 551 | 4 271 | | 4 271 |
| 21 | $(t,-t,3t)$ | 211,421 | 5 531 | | 5 531 |
| 22 | $(t,-t,-t)$ | 911 | | | |
| 23 | $(t,-t,-2t)$ | 71,7 211 | 5 531 | | 5 531 |
| 24 | $(t,-t,-3t)$ | 237 301 | 4 271 | 71 | 4 271 |
| × | $(t,-2t,t)$ | | | | |
| 26 | $(t,-2t,2t)$ | 354 551 | 4 271 | 71 | 4 271 |
| 27 | $(t,-2t,3t)$ | | | 2 311 | 281 |
| 28 | $(t,-2t,-t)$ | 911 | | 491 | |
| 29 | $(t,-2t,-2t)$ | 1 051 | 211 | 71 | 421 |
| 30 | $(t,-2t,-3t)$ | 631 | 701 | 281 | 421 |
| 31 | $(t,-2t,t)$ | 71 | | 211 | 71,211 |
| × | $(t,-2t,2t)$ | | | | |
| 33 | $(t,-3t,3t)$ | 211,421 | 5 531 | 71 | 5 531 |
| 34 | $(t,-3t,-t)$ | 911 | | 211 | |
| 35 | $(t,-3t,-2t)$ | | | 701 | 71,281 |
| 36 | $(t,-3t,-3t)$ | 631 | 701 | 211 | 71 |

**Table 5 All equivalent classes of 10-cycles and their modified basic equations**

| Equivalent class | Modified basic equation |
|---|---|
| (0,1,2,3,4) | $1+\alpha^{5t+7}+\alpha^{5(t+u)+14}+\alpha^{5(t+u+v)+21}+\alpha^{5(t+u+v+w)+28}$ |
| (0,1,2,4,3) | $1+\alpha^{5t+7}+(1+\alpha^7)\alpha^{5(t+u)+14}-\alpha^{5(t+u+v)+21}-(1+\alpha^7+\alpha^{14})\alpha^{5(t+u+v+w)}$ |
| (0,1,2,4,3) | $1+(1+\alpha^7)\alpha^{5t+7}-\alpha^{5(t+u)+14}+(1+\alpha^7)\alpha^{5(t+u+v)+14}+\alpha^{5(t+u+v+w)+28}$ |
| (0,1,4,2,3) | $1+(1+\alpha^7+\alpha^{14})\alpha^{5t+7}-(1+\alpha^7)\alpha^{5(t+u)+14}+\alpha^{5(t+u+v)+14}-(1+\alpha^7+\alpha^{14})\alpha^{5(t+u+v+w)}$ |
| (0,1,0,2,3) | $1-\alpha^{5t}+(1+\alpha^7)\alpha^{5(t+u)}+\alpha^{5(t+u+v)+14}-(1+\alpha^7+\alpha^{14})\cdot\alpha^{5(t+u+v+w)}$ |
| (0,1,0,2,4) | $1-\alpha^{5t}+(1+\alpha^7)\alpha^{5(t+u)}+(1+\alpha^7)\alpha^{5(t+u+v)+14}+\alpha^{5(t+u+v+w)+28}$ |
| (0,1,0,3,4) | $1-\alpha^{5t}+(1+\alpha^7+\alpha^{14})\alpha^{5(t+u)}+\alpha^{5(t+u+v)+21}+\alpha^{5(t+u+v+w)+28}$ |
| (0,1,2,0,1) | $1+\alpha^{5t+7}-(1+\alpha^7)\alpha^{5(t+u)}+\alpha^{5(t+u+v)}-\alpha^{5(t+u+v+w)}$ |
| (0,1,3,0,1) | $1+(1+\alpha^7)\alpha^{5t+7}-(1+\alpha^7+\alpha^{14})\alpha^{5(t+u)}+\alpha^{5(t+u+v)}-\alpha^{5(t+u+v+w)}$ |

**Table 6 All cases $(t,u,v,w)$ and associated candidate girth values**

| No. | $(t,u,v,w)$ | (0,1,2,3,4) | (0,1,2,4,3) | (0,1,3,2,4) | (0,1,4,2,3) | (0,1,0,2,3) | (0,1,0,2,4) | (0,1,0,3,4) | (0,1,2,0,1) | (0,1,3,0,1) |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | $(t,t,t,t)$ | | 43 261 | | 71,66 851 | 491 | 491 | 631 | 631 | 421 |
| 2 | $(t,t,t,2t)$ | | 28 771 | 911 | | 9 941 | 281 | 1 051 | 71 | |
| 3 | $(t,t,t,3t)$ | | 66 851 | 43 621 | 66 851 | 211 | 4 481 | 12 601 | 701 | 421 |
| 4 | $(t,t,t,-t)$ | 701 | | 5 741,30 661 | 421 | | 211 | | 55 721 | |
| 5 | $(t,t,t,-2t)$ | 701 | 5 741 | 71 | | 71,207 061 | 71,491,911 | 71,211,911 | 3 011 | |
| × | $(t,t,2t,-3t)$ | | | | | | | | | |
| 7 | $(t,t,2t,t)$ | | 38 011 | 421,164 431 | 38 011 | 211 | | 631 | 71 | 71 |
| 8 | $(t,t,2t,2t)$ | | | 701,28 771 | 28 771 | 71,701,911 | 491 | | 211 | 71,211 |
| × | $(t,t,2t,3t)$ | | | | | | | | | |
| 10 | $(t,t,2t,-t)$ | 71,631 | 491 | 557 831 | 1 471 | 281 | 9 521 | 71 | 281,491 | 71,631,701 |
| 11 | $(t,t,2t,-2t)$ | 421 | 19 391 | 30 941 | 281 | 701 | | 421,701 | 211,4 621 | 55 511 |
| 12 | $(t,t,2t,-3t)$ | 71 | 71,3 851 | 7 001 | 9 871 | 343 141 | 704 761 | 5 741 | 437 501 | 159 671 |
| 13 | $(t,t,3t,t)$ | | 66 851 | 66 851 | 43 261 | 10 781 | | 7 001 | 631 | 421 |
| × | $(t,t,3t,2t)$ | | | | | | | | | |
| 15 | $(t,t,3t,3t)$ | 421 | 71,491 | 3 221 | 30 941 | 3 011 | 349 931 | 32 971 | 3 571 | 104 021 |
| 16 | $(t,t,3t,-t)$ | | | | | 1 471 | 491 | 71 | 21 701 | 911 |
| 17 | $(t,t,3t,-2t)$ | 71,631 | 2 731 | 7 211 | 71,281 | 71,6 581 | 44 171 | 281,51 521 | 13 931 | 281,491 |
| 18 | $(t,t,3t,-3t)$ | 211 | 203 911 | 71,211 | 211,281 | 211 | | 211 | 446 881 | 211,1 051 |
| 19 | $(t,t,-t,t)$ | 71 | 71,911 | | | | | | 237 301 | 354 551 |
| 20 | $(t,t,-t,2t)$ | 211 | 71 | 374 291 | 5 881 | 71,211 | 11 411 | 3 361 | | 211 |
| 21 | $(t,t,-t,3t)$ | | 30 941 | 19 391 | 71,491 | 71,43 331 | | 71,281 | 421 | 631 |
| × | $(t,t,-t,-t)$ | | | | | | | | | |
| 23 | $(t,t,-t,-2t)$ | 701 | 71,211,421 | 71,211 | 5 741 | 71,3 361 | 71,281 | 71,211 | 911 | 911 |
| 24 | $(t,t,-t,-3t)$ | 71 | 9 871 | 71 | 71,3 851 | 71,281 | 71,421,491 | 71,43 331 | 71,211 | 1 051 |
| 25 | $(t,t,-2t,t)$ | 71 | 71,211 | 71 | 71,211,911 | 141 961 | 71,911 | 71,911 | 9 521 | 71,47 041,162 821 |
| 26 | $(t,t,-2t,2t)$ | | 211,701 | 211,701 | 211,701 | 71 | 71,7 211 | 71 | 71 | 9 268 631 |
| 27 | $(t,t,-2t,3t)$ | 491 | 491 | 71,631 | 71,4 831,20 441 | 2 731 | 18 481 | 71 | 281,18 061 | 23 632 351 |
| 28 | $(t,t,-2t,-t)$ | 701 | 421 | 5 741 | | 11 411 | 4 831 | 71 | 71,1 471 | 211,3 221 |
| 29 | $(t,t,-2t,-2t)$ | 421 | 281 | 3 221 | 19 391 | 47 741 | 71 | 4 691 | 3 338 441 | 701,3 851 |
| 30 | $(t,t,-2t,-3t)$ | 211 | 211,281 | 71 | 203 911 | 281,974 411 | 911,2 591 | 71,491 | 71,12 041 | 71,1 471 |
| × | $(t,t,-3t,t)$ | | | | | | | | | |
| 32 | $(t,t,-3t,2t)$ | 211 | 5 881 | 701,18 481 | 71 | 4 691 | 299 671 | 211,1 051 | 301 841 | 281,421,845 951 |
| 33 | $(t,t,-3t,3t)$ | 491 | 71,4 831 | 4 271 | 491 | | | | 763 771 | 10 151 |
| 34 | $(t,t,-3t,-t)$ | 71,631 | 1 471 | 71,211 | 491 | 71,281 | 631 | 71,211 | 71,491 | 3 361 |
| 35 | $(t,t,-3t,-2t)$ | 71,631 | 71,281 | 71 | 2 731 | 631,701 | 71,211 | 403 621 | 2 801 | 7 561 |
| 36 | $(t,t,-3t,-3t)$ | | 911 | 28 771 | 911 | 4 481 | 12 601 | | 71,281 | 2 381,8 821 |
| 37 | $(t,2t,t,t)$ | | | 164 431 | 164 431 | 211 | 71,211 | 71,211 | 8 821 | 4 201 |
| 38 | $(t,2t,t,2t)$ | | 38 011 | 71,38 011 | 164 431 | 71 | 47 881 | 2 731 | 71,281 | 71,4 201 |
| × | $(t,2t,t,3t)$ | | | | | | | | | |
| 40 | $(t,2t,t,-t)$ | 71 | | 631,15 204 111 | 8 681 | | 71 | | 211,631 | 242 621 |
| 41 | $(t,2t,t,-2t)$ | | | | | 71 | 8 191 | 211 | | |
| 42 | $(t,2t,t,-3t)$ | 71 | 10 501 | 13 441 | 8 681 | 718 271 | 1 634 011 | 71,281,4 271 | 21 911 | 71,242 621 |
| 43 | $(t,2t,2t,t)$ | | 28 771 | 71 | 71,911 | 281,421,491 | 631 | 71 | 4 201 | 8 821 |
| × | $(t,2t,2t,2t)$ | | | | | | | | | |
| 45 | $(t,2t,2t,3t)$ | 491 | 71,631 | 71 | 71,491 | 631,3 211 | 281 | 50 051 | 71,4 271 | 10 151 |
| 46 | $(t,2t,2t,-t)$ | 71,631 | 7 211 | 211,281 | 2 731 | 4 831 | 11 411 | 71,281 | 211,281 | 7 561 |
| 47 | $(t,2t,2t,-2t)$ | | 374 291 | 2 521 | 71 | | | | 71,16 661 | 845 951 |
| 48 | $(t,2t,2t,-3t)$ | 71,631 | 557 831 | 71 | 281,491 | 71,2 731 | 24 781 | 71,421 | 2 381 | 3 361 |
| × | $(t,2t,3t,t)$ | | | | | | | | | |
| 50 | $(t,2t,3t,2t)$ | 281 | 6 581 | 2 591 | 71,1 051 | 71,5 741,18 691 | 278 741 | 421,631 | 71,437 501 | 159 671 |
| 51 | $(t,2t,3t,3t)$ | 71,631 | 211,281 | 211,7 211 | 71 | 211 | 71,281 | 3 011 | 71 | 71 |
| 52 | $(t,2t,3t,-t)$ | 15 121 | 71 | 71,421 | 4 481 | 2 591 | 71,701 | 9 311 | 281,491 | 631,701 |
| 53 | $(t,2t,3t,-2t)$ | 15 121 | 491,11 621 | 4 481 | 16 451 | 631 | 4 621 | 211,1 471 | 211 | 71,211 |
| 54 | $(t,2t,3t,-3t)$ | 71 | | 71,9 871 | 154 981 | 211 | | 71,211 | 211,4 621 | 55 511 |
| 55 | $(t,2t,-t,t)$ | 2 311 | 67 061 | 2 521 | 54 881 | | | | 71,5 881 | 281,285 251 |

**Table 6(Continued)**

| No. | $(t,u,v,w)$ | (0,1,2,3,4) | (0,1,2,4,3) | (0,1,3,2,4) | (0,1,4,2,3) | (0,1,0,2,3) | (0,1,0,2,4) | (0,1,0,3,4) | (0,1,2,0,1) | (0,1,3,0,1) |
|---|---|---|---|---|---|---|---|---|---|---|
| 56 | $(t,2t,-t,2t)$ | 15 121 | 701 | 9 941 | 421,701 | 911 | 71,9 521 | 281,2 381 | 71 191 | 491,296 731 |
| 57 | $(t,2t,-t,3t)$ | 15 121 | 71 | 4 481 | 71,421 | 28 001 | 421 | | 71,211,701 | 192 431 |
| 58 | $(t,2t,-t,-t)$ | 701 | 71 | 5 741 | 30 661 | 71,17 921 | 33 181 | 491,3 851,8 191 | 33 811 | 13 931 |
| × | $(t,2t,-t,-2t)$ | | | | | | | | | |
| 60 | $(t,2t,-t,-3t)$ | 71,631 | 71,1 471 | 491 | 71,211 | 67 271 | 19 181 | 71,421 | 911 | |
| 61 | $(t,2t,-2t,t)$ | 211 | 71,2 731 | 71,281 | 4 201 | | 491 | 281 | 71 | 71 |
| 62 | $(t,2t,-2t,2t)$ | 71 | 4 271 | 281,491,1 051 | 281,491 | 5 531 | 71 | 5 531 | 211,421 | 7 211 |
| 63 | $(t,2t,-2t,3t)$ | 491 | 4 271 | 71,4 831 | 71 | 71,281 | 71,211 | 631 | | |
| × | $(t,2t,-2t,-t)$ | | | | | | | | | |
| 65 | $(t,2t,-2t,-2t)$ | 421 | 281 | 19 391 | 3 221 | 10 711 | 491,4 621 | | 1 051 | 71,211,491 |
| 66 | $(t,2t,-2t,-3t)$ | 2 311 | 2 521 | 67 061 | 71,491,1 051 | 57 751 | 2 731 | 16 381 | 911 | 911 |
| 67 | $(t,2t,-3t,t)$ | 71 | 4 271 | 71 | 281,491 | 281,2 591 | 4 271 | 4 271 | 71,24 151 | 71,27 136 621 |
| 68 | $(t,2t,-3t,2t)$ | 71 | 152 041 | 13 441 | 71 | 21 211 | 10 501 | 71,491 | 71,7 001 | 491,2 311 |
| 69 | $(t,2t,-3t,3t)$ | 71 | 281,491 | 71,4 271 | 4 271 | 71 | | 71 | 8 553 581 | 71,112 771 |
| 70 | $(t,2t,-3t,-t)$ | 71 | 9 871 | 3 851 | | | 6 581 | 3 851 | 1 773 241 | 1 388 381 |
| 71 | $(t,2t,-3t,-2t)$ | 2 311 | 2 521 | 71,491 | 67 061 | 1 051 | 71 | 18 481 | 393 961 | 491,15 541,24 151 |
| 72 | $(t,2t,-3t,-3t)$ | 211 | 2 521 | 71,18 481 | 701,374 291 | 280 351 | 71,631 | 71,13 441 | 71,75 181 | 71,348 461 |
| 73 | $(t,3t,t,t)$ | | 43 261 | 66 851 | | 631 | 631 | 491 | 71 | |
| × | $(t,3t,t,2t)$ | | | | | | | | | |
| 75 | $(t,3t,t,3t)$ | 211 | 19 531 | 4 201 | 11 971 | 4 271,867 371 | 281,3 571 | 71,6 301 | 3 011 | |
| 76 | $(t,3t,t,-t)$ | 211 | 71,281 | 71,2 731 | 11 971 | | | | 55 721 | 71 |
| 77 | $(t,3t,t,-2t)$ | 15 121 | 421,701 | 211,701 | 491 | 71,281 | 911 | 421 | 631 | 421 |
| 78 | $(t,3t,t,-3t)$ | 15 121 | 7 211 | 9 941 | 491 | 42 491 | 71,631 | 211 | 701 | 421 |
| × | $(t,3t,2t,t)$ | | | | | | | | | |
| 80 | $(t,3t,2t,2t)$ | 211,421 | 4 691 | 71 | 71,211 | 63 841,318 641 | 1 180 901 | 281,453 461 | 71,211 | 71,211,1 051 |
| 81 | $(t,3t,2t,3t)$ | 15 121 | 491,9 941 | 701 | 7 211 | 126 211 | 11 621 | 125 231 | | 911 |
| 82 | $(t,3t,2t,-t)$ | 15 121 | 701 | 701 | 9 941 | 71 | 71,211 | 281 | 33 811 | 281,491 |
| 83 | $(t,3t,2t,-2t)$ | 281 | 12 391 | 71,1 051 | 273 001 | 701 | | 71,701 | 71,631 | 421,104 021 |
| 84 | $(t,3t,2t,-3t)$ | 71,631 | 71,211 | 1 471 | 71 | 71 | 71,281 | 211 | 701 | 71,421 |
| 85 | $(t,3t,3t,t)$ | | 211,701,4 481 | | 71,211,701 | 71,1 471 | | | 211,7 351 | 71,9 268 631 |
| 86 | $(t,3t,3t,2t)$ | 211 | 71,211 | 4 691 | 203 911 | 71,281 | 71,491 | 2 591 | 701,3 361 | 71,1 471 |
| 87 | $(t,3t,3t,3t)$ | 701 | 30 661 | 71 | | 71,631 | 5 741 | 19 531 | | 211,3 221 |
| 88 | $(t,3t,3t,-t)$ | 421 | 30 941 | 71,491 | 19 391 | 71,421 | 3 851 | 6 581 | 421,2 311 | 701,3 851 |
| 89 | $(t,3t,3t,-2t)$ | 491 | 4 271 | 71 | 71,4 831 | 130 621 | 5 881 | 4 201 | 11 621 | 23 632 351 |
| 90 | $(t,3t,3t,-3t)$ | 71 | | 71,911 | 71,911,12 041 | 71 | | 71 | 71,1 229 211 | 71,47 041 |
| 91 | $(t,3t,-t,t)$ | 211 | 71,281 | 11 971 | 71,2 731 | | | | 71,16 661 | 845 951 |
| 92 | $(t,3t,-t,2t)$ | 71,631 | 7 211 | 2 731 | 211,281 | 71,211 | 71 | 3 361 | 71,4 201 | 8 821 |
| 93 | $(t,3t,-t,3t)$ | | | | 211 | 3 011 | 71,701 | 2 801 | 281,911,2 381 | 3 361 |
| 94 | $(t,3t,-t,-t)$ | 71,631 | 71 | 71,211 | 71,557 831 | 71,281 | 65 101 | 71,211 | 211,281 | 7 561 |
| 95 | $(t,3t,-t,-2t)$ | 71 | 13 441 | 10 501 | 152 041 | | 74 761 | 22 751 | 71,4 271 | 4 691,10 151 |
| × | $(t,3t,-t,-3t)$ | | | | | | | | | |
| 97 | $(t,3t,-2t,t)$ | 15 121 | 71,421 | 71 | 16 451 | 631 | 3 851 | 491 | 1 051 | 71,211 |
| 98 | $(t,3t,-2t,2t)$ | 281 | 211,12 391 | 273 001 | 71,1 051 | 211 | | 211 | 71,829 151 | 159 671 |
| 99 | $(t,3t,-2t,3t)$ | 491,15 121 | 11 621 | 16 451 | 4 481 | 46 831 | 701 | 39 551 | 71,281 | 631,701,3 221 |
| 100 | $(t,3t,-2t,-t)$ | 71 | 7 001 | 3 851 | 154 981 | 211,281 | 274 471 | 6 091 | 85 751 | 55 511 |
| × | $(t,3t,-2t,-2t)$ | | | | | | | | | |
| 102 | $(t,3t,-2t,-3t)$ | 71,631 | 71,281 | 2 731 | 71 | | 71 | 71 | 71 | 71 |
| 103 | $(t,3t,-3t,t)$ | 281 | 273 001 | 12 391 | 2 591 | 2 311 | 16 451 | 4 201 | 1 051 | 71,211 |
| 104 | $(t,3t,-3t,2t)$ | 2 311 | 54 881 | 67 061 | 71,211,4 831 | | 21 211 | 1 051 | 71 | 71 |
| 105 | $(t,3t,-3t,3t)$ | 71 | | 71,911 | 71,911 | 4 271 | | 4 271 | 71,911 | 911 |
| × | $(t,3t,-3t,-t)$ | | | | | | | | | |
| 107 | $(t,3t,-3t,-2t)$ | 211 | 211,281 | 203 911 | 71 | 491 | 71,281 | 281 | 631 | 421 |
| 108 | $(t,3t,-3t,-3t)$ | 211 | 2 521 | 421,374 291 | 18 481 | 26 251 | 4 481 | | | |
| 109 | $(t,-t,t,t)$ | 71 | 71,911 | | 71 | 522 061 | 211,2 521 | 522 061 | | 71 |
| 110 | $(t,-t,t,2t)$ | 71 | 281,421,491 | 4 271 | 71 | 211,2 731 | 128 591 | 211,2 731 | 71 | 71 |

**Table 6(Continued)**

| No. | $(t,u,v,w)$ | (0,1,2,3,4) | (0,1,2,4,3) | (0,1,3,2,4) | (0,1,4,2,3) | (0,1,0,2,3) | (0,1,0,2,4) | (0,1,0,3,4) | (0,1,2,0,1) | (0,1,3,0,1) |
|---|---|---|---|---|---|---|---|---|---|---|
| 111 | $(t,-t,t,3t)$ | | 71,211,701 | 211,701 | | 71,1 051 | 71,1 471 | 71,1 051 | 71 | |
| × | $(t,-t,t,-t)$ | | | | | | | | | |
| 113 | $(t,-t,t,-2t)$ | 71 | | 71,911 | 71 | 7 841 | 71,141 961 | 7 841 | 71 | 71 |
| 114 | $(t,-t,t,-3t)$ | 71 | 4 271 | 281,491,16 451 | 71 | 39 761 | 281,2 591 | 39 761 | 71 | 71 |
| 115 | $(t,-t,2t,t)$ | 2 311 | 491 | 2 521 | 4 831 | 687 541 | 71,701 | 1 471,343 561 | | 71 |
| 116 | $(t,-t,2t,2t)$ | 211 | 4 691 | 71,211 | 71 | 6 091 | 1 542 031 | 701 | 701 | 421 |
| 117 | $(t,-t,2t,3t)$ | 281 | 6 581 | 71,1 051 | 2 591 | 491 | 71,17 291 | 71,281 | 211 | 71,211 |
| 118 | $(t,-t,2t,-t)$ | 71 | 71 | | 71,911 | 495 461 | 631,2 591 | 631,1 051 | | 911 |
| × | $(t,-t,2t,-2t)$ | | | | | | | | | |
| 120 | $(t,-t,2t,-3t)$ | 211 | 71,5 881 | 71 | 18 481 | 1 253 071 | 17 011 | 423 431 | | |
| 121 | $(t,-t,3t,t)$ | | 19 531 | 11 971 | 4 201 | 71,631 | 440 651 | 71 | | 71 |
| 122 | $(t,-t,3t,2t)$ | 491 | 71,631 | 491 | 71 | 211,4 621 | 71,2 381 | 71,370 441 | | |
| 123 | $(t,-t,3t,3t)$ | 421 | 71,491 | 30 941 | 3 221 | 491,701 | 3 221 | 281,491 | 211 | 71,211 |
| 124 | $(t,-t,3t,-t)$ | 2 311 | 4 831 | 54 881 | 71,211 | 217 351 | 211,1 197 281 | 281,421 | | 911 |
| 125 | $(t,-t,3t,-2t)$ | 71 | 71 | 4 271 | 71,271,491 | 2 591,2 691 011 | 1 747 271 | 281,421,631 | 5 531 | 7 211 |
| × | $(t,-t,3t,-3t)$ | | | | | | | | | |
| × | $(t,-t,-t,t)$ | | | | | | | | | |
| 128 | $(t,-t,-t,2t)$ | 71 | 71 | 71,911 | | 837 271 | 211,2 381 | 421 | 4 271 | 354 551 |
| 129 | $(t,-t,-t,3t)$ | | 18 481 | 2 521 | 5 881 | 911 | 36 541 | 211,281,3 221 | | |
| 130 | $(t,-t,-t,-t)$ | 701 | 71 | 71,211,30 661 | 5 741 | 211,491 | 147 211 | 2 311,134 401 | | 911 |
| 131 | $(t,-t,-t,-2t)$ | 71 | 71,7 001 | 154 981 | 3 851 | 211,110 951 | 71,19 531 | 71,8 681 | 211 | 1 051 |
| 132 | $(t,-t,-t,-3t)$ | 421 | 71,3 221 | 71,281 | 491 | 211,491 | 385 631 | 71,1 051 | 701 | 631 |
| 133 | $(t,-t,-2t,t)$ | 701 | 5 741 | 421 | 71 | 71,421 | 34 231 | 9 871 | | 71 |
| × | $(t,-t,-2t,2t)$ | | | | | | | | | |
| 135 | $(t,-t,-2t,3t)$ | 71 | 71 | 281,491 | 4 271 | 211,491,701,3 221 | 71,185 221 | 2 102 171 | 5 531 | 211,421 |
| 136 | $(t,-t,-2t,-t)$ | 71 | 13 441 | 152 041 | 10 501 | 71,701 | 211,2 731 | 421,491 | | 911 |
| 137 | $(t,-t,-2t,-2t)$ | 71,491 | 71 | 71,4 271 | 71,631 | 71,37 871 | 71,211 | 2 318 471 | 71 | 71,281 |
| 138 | $(t,-t,-2t,-3t)$ | 281 | 2 591 | 273 001 | 6 581 | 211,421 | 281,4 201 | 325 921 | 701 | 631 |
| 139 | $(t,-t,-3t,t)$ | 71 | 10 501 | 8 681 | 13 441 | 71,421 | 435 401 | 76 231 | | 71 |
| 140 | $(t,-t,-3t,2t)$ | 71 | 491,3 851 | 9 871 | 7 001 | 71,14 771 | 421,631 | 71,631 | 701 | 421 |
| × | $(t,-t,-3t,3t)$ | | | | | | | | | |
| 142 | $(t,-t,-3t,-t)$ | 211 | 4 201 | 71,2 731 | 631,19 531 | 491 | 281,3 571 | 18 131 | | 911 |
| 143 | $(t,-t,-3t,-2t)$ | 211 | 71 | 211,281 | 4 691 | 48 371 | 532 421 | 79 801 | 211 | 1 051 |
| 144 | $(t,-t,-3t,-3t)$ | | | 211,701 | 211,701 | 589 471 | 701,35 141 | 2 153 551 | 4 271 | 237 301 |
| 145 | $(t,-2t,t,t)$ | 71 | 71,911 | 71 | 71 | 211,2 521 | 211,701 | 211,701,25 411 | 71,6 091 | 281,4 691 |
| 146 | $(t,-2t,t,2t)$ | 71,211 | 11 971 | 19 531 | 71,281 | 4 481 | 13 441 | 71,631 | 281,491 | 211,281 |
| 147 | $(t,-2t,t,3t)$ | 281 | 71,1 051 | 6 581 | 71,12 391 | 421,4 621 | 211,4 691 | 71 | 443 591 | 211,1 051,2 381 |
| 148 | $(t,-2t,t,-t)$ | 71 | 71,911 | | | | | | 71,16 381 | 281,4 691 |
| 149 | $(t,-2t,t,-2t)$ | 211 | 2 731 | 4 201 | 71,281 | 281 | 19 531 | 5 741 | 71,11 131 | 211,281 |
| 150 | $(t,-2t,t,-3t)$ | 281 | 273 001 | 2 591 | 12 391 | | 211,7 001 | 3 221 | 1 239 421 | 211,421,1 051 |
| 151 | $(t,-2t,2t,t)$ | 211 | 11 971 | 71,281 | 19 531 | | 280 351 | 491,26 251 | 911 | 911 |
| 152 | $(t,-2t,2t,2t)$ | 71 | 154 981 | 281 | 7 001 | 4 201 | | 421,2 311 | 631 | 421 |
| 153 | $(t,-2t,2t,3t)$ | 211 | 71,211 | 71,211,203 911 | 4 691 | 281 | 491,97 441 | 491 | 71,211 | 1 051 |
| × | $(t,-2t,2t,-t)$ | | | | | | | | | |
| 155 | $(t,-2t,2t,-2t)$ | | 211,701 | 211,701 | 211,701 | 4 271 | | 4 271 | 354 551 | 237 301 |
| 156 | $(t,-2t,2t,-3t)$ | 71 | 152 041 | | 13 441 | 71,1 051 | 211 | | 71 | 71 |
| 157 | $(t,-2t,3t,t)$ | 15 121 | 4 481 | 71 | 11 621 | 98 491 | 2 731 | 211,281 | 911 | |
| 158 | $(t,-2t,3t,2t)$ | 15 121 | 9 941 | 7 211 | 421,701 | 71 | 2 521 | 71,701 | 211,701 | 192 431 |
| 159 | $(t,-2t,3t,3t)$ | 71,631 | 71,211,281 | 71 | 7 211 | 71,4 831 | 71,15 541 | 33 369 | 71,71 191 | 211,296 731 |
| 160 | $(t,-2t,3t,-t)$ | 211 | 18 481 | 5 881 | 2 521 | 491,1 471 | 71,17 431 | 66 571 | 33 811 | 1 051,13 931 |
| × | $(t,-2t,3t,-2t)$ | | | | | | | | | |
| 162 | $(t,-2t,3t,-3t)$ | 491 | 71,4 831 | 491 | 4 271 | | | | 71,211,5 881 | 285 251 |
| 163 | $(t,-2t,-t,t)$ | 701 | | 421 | 30 661 | | | | 281,491 | 71,13 931 |
| × | $(t,-2t,-t,2t)$ | | | | | | | | | |
| 165 | $(t,-2t,-t,3t)$ | 2 311 | 4 831 | 71,491 | 54 881 | 441 421 | 59 221 | 71,491 | 421,491 | 126 211,285 251 |
| 166 | $(t,-2t,-t,-t)$ | 71,631 | 71 | 557 831 | 71,211 | 20 231 | 110 321 | 3 361 | 21 701 | 8 821 |
| 167 | $(t,-2t,-t,-2t)$ | 15 121 | 16 451 | 71,11 621 | 71,421,701 | 211,421,701 | 2 311 | 127 261 | 71,211 | 192 431 |
| 168 | $(t,-2t,-t,-3t)$ | 15 121 | 491 | 7 211 | 421,701 | 71,1 051 | 71,421 | 71,421 | 12 041 | 296 731 |
| 169 | $(t,-2t,-2t,t)$ | | 71,281 | | 71 | 71,211 | 421 | 45 361 | | 911 |
| 170 | $(t,-2t,-2t,2t)$ | 421 | 19 391 | 281 | 30 941 | 211 | | 211 | 71,631 | 104 021 |
| × | $(t,-2t,-2t,3t)$ | | | | | | | | | |
| 172 | $(t,-2t,-2t,-t)$ | 71,631 | 71 | 211,281 | 281 | 71,211 | 71 | 71,421 | 33 811 | 281,491,631 |
| 173 | $(t,-2t,-2t,-2t)$ | | | 43 261 | 43 261 | 491 | 204 331 | | 701 | 421 |
| 174 | $(t,-2t,-2t,-3t)$ | 211 | 71 | 4 691 | 211,281 | 71 | 71,2 521 | 211,281 | 71,211 | 211,1 051 |
| 175 | $(t,-2t,-3t,t)$ | 15 121 | 7 211 | 491 | 9 941 | 118 861 | 71 | 20 161 | 13 931 | 281,491 |
| 176 | $(t,-2t,-3t,2t)$ | 71,631 | 557 831 | 491 | 71 | 1 471,9 241 | 71 | 4 691 | 631 | 421 |
| 177 | $(t,-2t,-3t,3t)$ | 211 | 203 911 | 211,281 | 71,211 | 71,701 | | 71,701 | 446 881 | 211,1 051 |
| 178 | $(t,-2t,-3t,-t)$ | 15 121 | 491 | 701 | 7 211 | 7 351 | 12 671 | | 21 701 | 911 |
| 179 | $(t,-2t,-3t,-2t)$ | 281 | 2 591 | 6 581 | 5 741,273 001 | 71,3 361 | 920 641 | 71,5 881 | 3 571 | 104 021 |
| × | $(t,-2t,-3t,-3t)$ | | | | | | | | | |
| × | $(t,-3t,t,t)$ | | | | | | | | | |

**Table 6(Continued)**

| No. | $(t,u,v,w)$ | (0,1,2,3,4) | (0,1,2,4,3) | (0,1,3,2,4) | (0,1,4,2,3) | (0,1,0,2,3) | (0,1,0,2,4) | (0,1,0,3,4) | (0,1,2,0,1) | (0,1,3,0,1) |
|---|---|---|---|---|---|---|---|---|---|---|
| 182 | $(t,-3t,t,2t)$ | 2 311 | 71,491 | 4 831 | 2 521 | 766 501 | 71,7 841 | 262 781 | 21 911 | 71,421,242 621 |
| 183 | $(t,-3t,t,3t)$ | 15 121 | 4 481 | 11 621 | 71 | 281,21 491 | 71 | 26 111 | 8 821 | 4 201 |
| 184 | $(t,-3t,t,-t)$ | 2 311 | 71,67 061 | 54 881 | 2 521 | | | | 211,631 | 71,281,242 621 |
| 185 | $(t,-3t,t,-2t)$ | 15 121 | 71,421 | 16 451 | 71 | 71,34 511 | 3 361 | 7 351 | 71,281 | 4 201 |
| 186 | $(t,-3t,t,-3t)$ | | 211,164 431 | 38 011 | | 71,211 | 421 | 1 471 | | |
| 187 | $(t,-3t,2t,t)$ | 71 | 71,281,491 | 71 | 4 271 | 128 591 | 281,491 | 281,491 | 3 439 801 | 71,112 771 |
| 188 | $(t,-3t,2t,2t)$ | 71 | 154 981 | 1 051,7 001 | 71,211 | 16 451 | 3 221 | 7 001 | 4 831 | 1 388 381 |
| 189 | $(t,-3t,2t,3t)$ | 71 | 8 681 | 10 501 | | 71,211 | 4 201 | 5 881 | 1 022 141 | 491,2 311 |
| 190 | $(t,-3t,2t,-t)$ | 211 | 71 | 5 881 | 374 291 | 71,281 | 71 | 4 831,6 791 | 4 649 261 | 71,348 461 |
| 191 | $(t,-3t,2t,-2t)$ | 71 | 4 271 | 281,491,701 | 491 | 71 | 71 | 71 | 898 661 | 27 136 621 |
| 192 | $(t,-3t,2t,-3t)$ | 2 311 | 54 881 | 4 831 | 67 061 | 211 | 71,491 | 10 501 | 4 567 151 | 491,15 541 |
| 193 | $(t,-3t,3t,t)$ | 281 | 71,1 051 | 12 391 | 6 581 | 71 | 47 741 | 10 711 | 421 | 631 |
| 194 | $(t,-3t,3t,2t)$ | 71 | 8 681 | 1 051 | 10 501 | 631 | 130 621 | 71,281 | 911 | 911 |
| 195 | $(t,-3t,3t,3t)$ | 701 | 30 661 | | 71 | 281 | 281 | | 71 | 71 |
| × | $(t,-3t,3t,-t)$ | | | | | | | | | |
| 197 | $(t,-3t,3t,-2t)$ | 491 | 491 | 71,4 831 | 71,631 | 421,16 381 | 1 051 | 57 751 | | 71 |
| 198 | $(t,-3t,3t,-3t)$ | 71 | 281,491,2 591 | 4 271 | 4 271 | 5 531 | 71,421 | 5 531 | 7 211 | 211,421 |
| 199 | $(t,-3t,-t,t)$ | 71 | 71 | 8 681 | 152 041 | | | | 763 771 | 10 151 |
| 200 | $(t,-3t,-t,2t)$ | 71,631 | 491 | 1 471 | 557 831 | 911 | 71,211 | 2 381 | 2 801 | 7 561 |
| × | $(t,-3t,-t,3t)$ | | | | | | | | | |
| 202 | $(t,-3t,-t,-t)$ | | | | | 2 801 | 16 871 | 13 931 | 71,491 | 3 361 |
| 203 | $(t,-3t,-t,-2t)$ | 71,211,631 | 71 | 71,281 | 71,211 | 21 001 | 911,25 411 | 71,7 561 | 71,281 | 8 821 |
| 204 | $(t,-3t,-t,-3t)$ | 211 | 4 201 | 19 531 | 71,2 731 | 71,30 941 | 71,211,52 361 | 71,12 251 | 301 841 | 281,845 951 |
| 205 | $(t,-3t,-2t,t)$ | 15 121 | 421,701 | 491 | 701 | 71,281 | 1 471 | 17 291 | 71,211 | 192 431 |
| 206 | $(t,-3t,-2t,2t)$ | 211 | 374 291 | 71 | 2 521 | | | | 71,281,491 | 13 931 |
| 207 | $(t,-3t,-2t,3t)$ | 71,631 | 2 731 | 71,281 | 7 211 | 22 051 | 11 831 | 71,491 | 12 041 | 296 731 |
| 208 | $(t,-3t,-2t,-t)$ | 15 121 | 16 451 | 71,421 | 11 621 | 281 | 71,631 | 14 071 | 21 701 | |
| 209 | $(t,-3t,-2t,-2t)$ | 491 | 71 | 71,631 | 211,4 271 | 281,421,701 | 71,4 271 | 109 831 | 421,491 | 211,285 251 |
| × | $(t,-3t,-2t,-3t)$ | | | | | | | | | |
| 211 | $(t,-3t,-3t,t)$ | | 491,164 431 | | 71,38 011 | 281 | 71,701 | 9 521 | 71 | 71,281 |
| 212 | $(t,-3t,-3t,2t)$ | 71,631 | 71,211 | 71 | 1 471 | 71,281 | 30 871 | 71,33 461 | 71,281 | 281,631,701 |
| 213 | $(t,-3t,-3t,3t)$ | 71 | | 154 981 | 2 731,9 871 | 701 | | 701 | 829 151 | 159 671 |
| 214 | $(t,-3t,-3t,-t)$ | 421 | 3 221 | 71,491 | 281 | 71 | 361 901 | 137 131 | 85 751 | 55 511 |
| × | $(t,-3t,-3t,-2t)$ | | | | | | | | | |
| 216 | $(t,-3t,-3t,-3t)$ | | 911 | 911 | 71,28 771 | 10 781 | 211 | 7 001 | 1 051 | 71,211 |

Notice that just like the aforementioned, we list all cases of $(t,u,v,w)$ in Table 6, where "×" stands for invalid cases $(t+u+v+w=0 \pmod 7)$. By eliminating those polynomials over $\boldsymbol{F}_p$, which is not equal to zero, we can get the reduced forms of the modified basic equations. By applying the Euclidean algorithm to the reduced forms and Eq. (4), we check if there exists the remainder polynomial over $\boldsymbol{F}_p$ which is equal to zero, and obtain the candidate girth values $g$, tabulated in Table 6. Based on the conclusions drawn in Sections 2.1, 2.2, and 2.3, we can see from Table 6 that Tanner (5, 7) QC LDPC codes with length $7p$ have girth 10, $p \in G_{10}$, where $G_{10} = \{1\,471, 2\,381, 2\,521, 2\,591, 2\,731, 2\,801, 3\,011, 3\,221, 3\,361, 3\,571, 3\,851, 4\,201, 4\,481, 4\,621, 4\,691, 4\,831, 5\,741, 5\,881, 6\,091, 6\,301, 6\,581, 7\,001, 7\,351, 7\,561, 7\,841, 8\,191, 8\,681, 8\,821, 9\,241, 9\,311, 9\,521, 9\,871, 9\,941, 10\,151, 10\,501, 10\,711, 10\,781, 11\,131, 11\,411, 11\,621, 11\,831, 11\,971, 12\,041, 12\,251, 12\,391, 12\,601, 12\,671, 13\,441, 13\,931, 14\,071, 14\,771, 15\,121, 15\,541, 16\,381, 16\,451, 16\,661, 16\,871, 17\,011, 17\,291, 17\,431, 17\,921, 18\,061, 18\,131, 18\,481, 18\,691, 19\,181, 19\,391, 19\,531, 20\,161, 20\,231, 20\,441, 21\,001, 21\,211, 21\,491, 21\,701, 21\,911, 22\,051, 22\,751, 24\,151, 24\,781, 25\,411, 26\,111, 26\,251, 28\,001, 28\,771, 30\,661, 30\,871, 30\,941, 32\,971, 33\,181, 33\,461, 33\,811, 34\,231, 34\,511, 35\,141, 36\,541, 37\,871, 38\,011, 39\,551, 39\,761, 42\,491, 43\,261, 43\,331, 44\,171, 45\,361, 46\,831, 47\,041, 47\,741, 47\,881, 48\,371, 50\,051, 51\,521, 52\,361, 54\,881, 55\,511, 55\,721, 57\,751, 59\,221, 63\,841, 65\,101, 66\,571, 66\,851, 67\,061, 67\,271, 71\,191, 74\,761, 75\,181, 76\,231, 79\,801, 85\,751, 97\,441, 98\,491, 104\,021, 109\,831, 110\,321, 110\,951, 112\,771, 118\,861, 122\,921, 125\,231, 126\,211, 127\,261, 128\,591, 130\,621, 134\,401, 137\,131, 141\,961, 147\,211, 152\,041, 154\,981, 159\,671, 162\,821, 164\,431, 185\,221, 192\,431, 203\,911, 204\,331, 207\,061, 217\,351, 242\,621, 262\,781, 273\,001, 274\,471, 278\,741, 280\,351, 285\,251, 296\,731, 299\,671, 301\,841, 318\,641, 325\,921, 333\,691, 343\,141, 343\,561, 348\,461, 349\,931, 361\,901, 370\,441, 374\,291, 385\,631, 393\,961, 403\,621,

423 431, 435 401, 437 501, 440 651, 441 421, 443 591, 446 881, 453 461, 495 461, 522 061, 532 421, 557 831, 589 471, 687 541, 704 761, 718 271, 763 771, 766 501, 829 151, 837 271, 845 951, 867 371, 898 661, 920 641, 1 022 141, 1 180 901, 1 197 281, 1 239 421, 1 253 071, 1 388 381, 1 542 031, 1 634 011, 1 747 271, 1 773 241, 2 102 171, 2 153 551, 2 318 471, 2 691 011, 3 338 441, 3 439 801, 4 567 151, 4 649 261, 8 553 581, 9 268 631, 23 632 351, 27 136 621}.

## 3 Conclusions

In this paper, we analyzed the cycles of Tanner (5, 7) QC LDPC codes and divided the cycles of lengths 4, 6, 8, and 10 into sixteen equivalent classes. Based on these equivalent classes, we presented the basic equations over $\boldsymbol{F}_p$, $p \in \boldsymbol{P}_{35}$, which have a primitive 35th unit root, and checked these equations have solutions. Then candidate girth values are derived. By summarizing the candidate girth values of all equivalent classes, the girth $g$ of Tanner (5, 7) QC LDPC codes with length $7p$ for $p$ being a prime with the form $35m + 1$ is obtained. That is, Tanner (5, 7) QC LDPC codes has girth 6 if $p = 71$, the girth is 8 if $p \in G_8$ (See Section 2.3), the girth is 10 if $p \in G_{10}$ (See Section 2.4), and 12 otherwise. In other words, when $p$ takes values in {6 791, 9 661, 11 551, 13 721, 14 281, 14 561, …}, Tanner (5, 7) QC LDPC codes with length $7p$ have girth 12.

## References


[1] Gallager R G. Low Density Parity Check Codes. Cambridge: MIT Press, 1963. 4-62.

[2] MacKay D J C, Neal R M. Near Shannon limit performance of low density parity-check codes. Electronics Letters, 1996, 32(18): 1645-1646.

[3] Tanner R. A recursive approach to low complexity codes. IEEE Transactions on Information Theory, 1981, 27(5): 533-547. DOI: 10.1109/TIT.1981.1056404.

[4] Lucas R, Fossorier M, Kou Y, et al. Iterative decoding of one-step majority logic decodable codes based on belief propagation. IEEE Transactions on Communications, 2000, 48(6): 931-937. DOI: 10.1109/26.848552.

[5] Xu H, Bai B. Superposition construction of $q$-ary LDPC codes by jointly optimizing girth and number of shortest cycles. IEEE Communications Letters, 2016, 20(7): 1285-1288. DOI: 10.1109/LCOMM.2016.2564401.

[6] Ryan W E, Lin S. Channel Codes: Classical and Modern. Cambridge: Cambridge University Press, 2009. 429-629.

[7] Song S, Zhou B, Lin S, et al. A unified approach to the construction of binary and nonbinary quasi-cyclic LDPC codes based on finite fields. IEEE Transactions on Communications, 2009, 57(1): 84-93. DOI: 10.1109/TCOMM.2009.0901.060129.

[8] Diao Q, Tai Y, Lin S, et al. LDPC codes on partial geometries: construction, trapping set structure, and puncturing. IEEE Transactions on Information Theory, 2013, 59(12): 7898-7914. DOI: 10.1109/TIT.2013.2280640.

[9] Kim S, No J, Chung H, et al. Quasi-cyclic low-density parity-check codes with girth larger than 12. IEEE Transactions on Information Theory, 2007, 53(8): 2885-2891. DOI: 10.1109/TIT.2007.901193.

[10] Gholami M, Samadieh M, Raeisi G. Column-weight three QC LDPC codes with girth 20. IEEE Communications Letters, 2013, 17(7): 1439-1442. DOI: 10.1109/LCOMM.2013.052013.130474.

[11] Gholami M, Nassaj A. Row and column extensions of 4-cycle free LDPC codes. IEEE Communications Letters, 2016, 20(1): 25-28. DOI: 10.1109/LCOMM.2015.2497299.

[12] Wang R, Li Y, Zhao H, et al. Construction of girth-eight quasi-cyclic low-density parity-check codes with low encoding complexity. IET Communications, 2016, 10(2): 148-153. DOI: 10.1049/iet-com.2015.0056.

[13] Tasdighi A, Banihashemi A, Sadeghi M. Efficient search of girth-optimal QC-LDPC codes. IEEE Transactions on Information Theory, 2016, 62(4): 1552-1564. DOI: 10.1109/TIT.2016.2523979.

[14] Zhang Y, Da X. Construction of girth-eight QC-LDPC codes from arithmetic progression sequence with large column weight. Electronics Letters, 2015, 51(16): 1257-1259. DOI: 10.1049/el.2015.0389.

[15] Xu H, Feng D, Luo R, et al. Construction of quasi-cyclic LDPC codes via masking with successive cycle elimination. IEEE Communications Letters, 2016, 20(12): 2370-2373. DOI: 10.1109/LCOMM.2016.2608938.

[16] Xu H, Feng D, Sun C, et al. Construction of LDPC codes based on resolvable group divisible designs. Proceedings of the 2015 International Workshop on High Mobility Wireless Communications (HMWC). Piscataway: IEEE, 2015. 111-115. DOI: 10.1109/HMWC.2015.7354346.

[17] Zhang G, Sun R, Wang X. Construction of girth-eight QC-LDPC codes from greatest common divisor. IEEE Communications Letters, 2013, 17(2): 369-372. DOI: 10.1109/LCOMM.2012.122012.122292.

[18] Fossorier M P C. Quasi-cyclic low-density parity-check codes from circulant permutation matrices. IEEE Transactions on Information Theory, 2004, 50(8): 1788-1793. DOI: 10.1109/TIT.2004.831841.

[19] Michael Tanner R, Michael R, Sridhara D, et al. A class of group-structured LDPC codes. Proceedings of International Symposium Communication Theory and Applications. CiteSeer$^X$, 2001. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.20.8232&rep=rep1&type=pdf.

[20] Kim S, No J S, Chung H, et al. On the girth of Tanner (3, 5) quasi-cyclic LDPC codes. IEEE Transactions on Information Theory, 2006, 52(4): 1739-1744. DOI: 10.1109/TIT.2006.871060.

[21] Gholami M, Mostafaiee F S. On the girth of Tanner (3, 7) quasi-cyclic LDPC codes. Transactions on Combinatorics, 2012, 1(2): 1-16.

[22] Xu H, Bai B, Feng D, et al. On the girth of Tanner (3, 11) quasi-cyclic LDPC codes. Finite Fields and Their Applications, 2017, 46: 65-89.