www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 01 No.2 (2012), pp. 1-16.

www.ui.ac.ir

ON THE GIRTH OF TANNER (3,7) QUASI-CYCLIC LDPC CODES

M. GHOLAMI* AND F. SADAT MOSTAFAIEE

Communicated by Alireza Abdollahi

Abstract. S. Kim et al. have been analyzed the girth of some algebraically structured quasi-cyclic (QC) low-density parity-check (LDPC) codes, i.e. Tanner $(3,5)$ of length $5p$, where p is a prime of the form $15m+1$. In this paper, by extension this method to Tanner $(3,7)$ codes of length $7p$, where p is a prime of the form $21m+1$, the girth values of Tanner $(3,7)$ codes will be derived. As an advantage, the rate of Tanner $(3,7)$ codes is about 0.17 more than the rate of Tanner $(3,5)$ codes.

1. Introduction

Low-density parity-check (LDPC) codes proposed by Gallager [2] are excellent error-correcting codes that achieve performance close to the the Shannon capacity [6]. The construction methods are divided into random-like codes, such as [5], and structured codes, such as [1],[7]. Unlike the long length codes, it has been seen that for medium length LDPC codes the structured codes can outperform the pseudo-random ones [4].

The code rate of a forward error correction code is the proportion of the data-stream that is useful (non-redundant). That is, if the code rate is k/n, for every k bits of useful information, the coder generates totally n bits of data, of which $n-k$ are redundant. On the other hand, for a given noisy channel with capacity C, the maximum achievable mutual information between the sender and the receiver, the Shannon theorem [6] states that if $R<C$, then there exist codes with rate R that allow the probability of error at the receiver to be made arbitrarily small. This means that, theoretically, it

MSC(2010): Primary: 11T71; Secondary: 97K30; 94C15;

Keywords: LDPC codes, Tanner graph, girth.

Received: 24 January 2012, Accepted: 27 March 2012.

∗Corresponding author.

is possible to transmit information nearly without error at any rate below a limiting rate, C. So, the construction of codes with high rates, not greater than the channel capacity, is of interest.

On the other hand, the design-rate of a code with the parity-check matrix $H = (h_{i,j})_{h\times n}$ is $R = 1 - h/n$, while the (actual) rate of this code is $R' = 1 - h'/n$, where h' is the rank of H. It is clear that $R \leq R'$. In many constructions, such as the codes proposed in this paper, the difference between the actual rate and the design rate is negligible; So we use the word "rate" instead of "actual-rate" or "design-rate".

A (c, r) regular LDPC code is defined as a LDPC code represented by a parity-check matrix H in which each column has weight c and each row has weight r. Fossorier has studied a class of (c, r) regular QC LDPC codes composed by c rows of r circulant permutation matrices [1]. He showed that such codes cannot have a Tanner graph representation [8] with girth larger than 12. Moreover, he has derived some necessary and sufficient conditions for the codes to have a girth of $g = 2g'$, $g' \leq 6$. By considering these conditions, Tanner [9], et al, have introduced a class of algebraically structured (c, r) regular QC LDPC codes, called Tanner (c, r) codes in this paper, which their girths are upper bounded by 12. Because of some linearly dependence between of the equations of parity check matrix of Tanner codes, the actual rate will always be a bit more than the design rate [7]. Tanner also observed that as the prime increases, the girths of Tanner $(3, 5)$ codes do attain the maximum of twelve [7]. In fact, after using a computer search, it was seen that Tanner $(3, 5)$ codes with length $5p$, where p is a prime of the form $15m + 1$, mostly have girth $g = 12$ [7]. Finally, by a theoretical method for these codes, S. Kim, et al, [3] proved that:

$$g = \begin{cases} 8 & p = 31 \\ 10 & p = 61, 151 \\ 12 & \text{else} \end{cases}$$

In fact, he has analyzed the cycles of these Tanner $(3, 5)$ codes and expressed the conditions for the existence of cycles of lengths 4, 6, 8 and 10 in terms of polynomial equations in a 15th root of unity of the prime field F_p. Then, by checking the existence of solutions for these equations over F_p, he has derived the girths of Tanner $(3, 5)$ codes.

In this paper, by following this method for Tanner $(3, 7)$ codes with length $7p$, we will classify the cycles of lengths 4, 6, 8 and 10 in classes of the equivalence-relation similar to the equivalence-relation introduced by Kim [3]. Here, the size of each classes, containing the whole possible cycles which must be checked, enlarges exponentially by the girth of Tanner $(3, 5)$ codes. For example, for a Tanner $(3, 7)$ code with girth 10, we have 185 possible cycles which is about 3.7 times larger than the possible cycles of a Tanner $(3, 5)$ code with girth 10.

2. Cycles in Tanner (3,7) Codes

To the LDPC code with the parity-check matrix H, we can associate a graph referred to as its *Tanner graph* of H, or TG(H). In fact, it is a bipartite graph where the two disjoint sets collect the check nodes and the bit nodes associated to the rows and columns of H, respectively. An edge connects a check node to a bit node if a nonzero entry exists in the intersection of the corresponding row and column of H. So, the girth of a Tanner code with a parity-check matrix H represented by (2.1), is the length of the shortest cycle in its Tanner graph $\mathrm{TG}(H)$.

Let p, s be two integers such that $0 \leq s \leq p-1$. By a $p \times p$ circulant permutation matrix $I_p(s)$, or simply $I(s)$ when p is known, we mean the identity matrix of size p for which each column is shifted s position to the below. For example if $p = 3$ then $I(1) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. For this convention, it is clear that $I(0) = I$ is the identity matrix.

One (c, r) QC LDPC code of length $n = rp$ can be represented by a parity-check matrix H consists of $p \times p$ circulant permutation matrices as following:

$$H = \begin{pmatrix} I(p_{0,0}) & I(p_{0,1}) & I(p_{0,2}) & \cdots & I(p_{0,r-1}) \\ I(p_{1,0}) & I(p_{1,1}) & I(p_{1,2}) & \cdots & I(p_{1,r-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I(p_{c-1,0}) & I(p_{c-1,1}) & I(p_{c-1,2}) & \cdots & I(p_{c-1,r-1}) \end{pmatrix}, \tag{2.1}$$

Fossorier [1] has cited the existence of a cycle of length $2l$, briefly $2l$ cycle, in $TG(H)$ by the following sub-matrices of H:

$$I(p_{i_0,j_0}), I(p_{i_1,j_0}), I(p_{i_1,j_1}), \ldots, I(p_{i_{k-1},j_k}), I(p_{i_k,j_k}), \ldots, I(p_{i_0,j_{l-1}}), I(p_{i_0,j_0}),$$

where $i_k \neq i_{k+1}$ and $j_k \neq j_{k+1}$ for each k such that $\sum_{k=0}^{l-1} p_{i_k,j_k} - p_{i_{k+1},j_k} \equiv 0 \bmod p$. Briefly, this sequence of sub-matrices can be shown by the chain $(i_0, j_0), (i_1, j_0), \ldots, (i_{l-1}, j_{l-1}), (i_0, j_{l-1}), (i_0, j_0)$, and it is famous to be of type $(i_0, i_1, \ldots, i_{l-1})$. Fossorier also proved that the girth of (c, r) QC LDPC codes represented by the parity-check matrix in (2.1) is upper bounded by 12.

Tanner [9] has introduced some (c, r) QC LDPC codes with an algebraic structure, called Tanner codes in this paper, which can be defined as following:

From algebra, $\mathrm{ord}_m a$, for some integers a, m where $1 \leq a \leq m-1$ and $(a, m) = 1$, is the smallest positive integer k such that $a^k \equiv 1 \bmod m$. The existence of such k follows from the Euler's theorem which says $a^{\varphi(m)} \equiv 1 \bmod m$ where $(a, m) = 1$ and $\varphi(m)$ is the number of elements i, $1 \leq i \leq m-1$ such that $(i, m) = 1$. Let $m \geq 1$, $1 \leq a, b \leq m-1$ and $1 \leq c < r \leq \varphi(m)$ be some integers such that $\mathrm{ord}_m a = r$ and $\mathrm{ord}_m b = c$. From [9], the general form of a parity-check matrix of a Tanner (c, r) code has been shown by H in (2.1), where $p_{i,j} \equiv b^i a^j \bmod m$ for each $0 \leq i \leq c-1$, $0 \leq j \leq r-1$.

A conjecture for $(3, 5)$ Tanner codes [7] with the block size p, where p is a prime of the form $15m+1$, was that these codes mostly have girth $g = 12$. Later, by a theoretical method, S. Kim, et al, proved that for $(3, 5)$ Tanner codes, $g = 8$ if $p = 31$, $g = 10$ if $p = 61, 151$ and elsewhere $g = 12$ [3]. By following this method for $(3, 7)$ Tanner codes, instead of $(3, 5)$ Tanner codes, we can gain similar conclusion. At first, we have the following definitions and notations from [3].

Let p be a prime such that $p-1$ is divisible by two values 3 and 7. Thus, p can takes values in $\{43, 127, 211, 337, \ldots\}$. Also, let α be a primitive 21th root of unity in F_p and $a = \alpha^3$, $b = \alpha^7$ be two elements of F_p with orders 7 and 3, respectively. Now, let $H = (p_{i,j} = \alpha^{7i+3j})_{0\leq i\leq 2, 0\leq j\leq 6}$ be the parity-check matrix of a $(3,7)$ Tanner code, represented by (2.1), as following:

$$H = \begin{pmatrix} I(\alpha^0) & I(\alpha^3) & I(\alpha^6) & I(\alpha^9) & I(\alpha^{12}) & I(\alpha^{15}) & I(\alpha^{18}) \\ I(\alpha^7) & I(\alpha^{10}) & I(\alpha^{13}) & I(\alpha^{16}) & I(\alpha^{19}) & I(\alpha^1) & I(\alpha^4) \\ I(\alpha^{14}) & I(\alpha^{17}) & I(\alpha^{20}) & I(\alpha^2) & I(\alpha^5) & I(\alpha^8) & I(\alpha^{11}) \end{pmatrix}. \tag{2.2}$$

The necessary and sufficient condition to have a $2l$ cycle of type $(i_0, i_1, \ldots, i_{l-1})$ in TG(H) is:

$$\sum_{k=0}^{l-1}(\alpha^{7i_k} - \alpha^{7i_{k+1}})\alpha^{3j_k} = 0 \qquad (\text{mod } p).$$

for some j_k, $1 \leq j_k \leq 7$, $j_k \neq j_{k+1}$. This equation will be called the basic equation. Without loss of generality, we can assume that $j_0 = 0$.

To classify cycles in H of a certain type, such as defined in [3], the equivalence relation between $2l$ cycles in Tanner $(3,7)$ codes can be defined as following:

Definition 2.1. Two cycles of types $(i_0, i_1, \ldots, i_{l-1})$ and $(i'_0, i'_1, \ldots, i'_{l-1})$ are equivalent if (at least) one of the following conditions be hold:

(1) There exists some $r \in \{0, 1, 2\}$ such that $i'_k = i_k + r \bmod 3$, for all k.
(2) $i'_k = 2i_k \bmod 3$, for all k.
(3) There exists some $d \in \{0, 1, \ldots, l-1\}$ such that $i'_k = i_{k+d}$, for all k.
(4) There exists some $d \in \{0, 1, \ldots, l-1\}$ such that $i'_k = i_{l-1-k+d}$, for all k.

Let $t = j_1 - j_0 \bmod 7, u = j_2 - j_1 \bmod 7, v = j_3 - j_2 \bmod 7$, and $w = j_4 - j_3 \bmod 7$. Then t, u, v, and w take the values in $\{\pm 1, \pm 2, \pm 3\}$.

To verify all candidate values p to have cycles of length up to 10 in Tanner $(3,7)$ codes, i.e. TG(H) for H in (2.2), the representation of the existence cycles are given as:

2.1. **All cycles of length 4.**

According to the equivalence relation defined, all cycles of length 4 belong to the unique class $(0,1)$ i.e. chain $(0,0), (1,0), (1,t), (0,t)$ where$t \neq 0$. The basic equation corresponding to this chain is:

$$\begin{aligned} \sum_{k=0}^{1}(\alpha^{7i_k} - \alpha^{7i_{k+1}})\alpha^{3j_k} &= (1-\alpha^7) + (\alpha^{3t+7} - \alpha^{3t}) \\ &= (1-\alpha^7)(1-\alpha^{3t}) \\ &= 0 \quad \bmod p. \end{aligned}$$

Since α is a primitive 21th root of unity, then $\alpha^7 \neq 1$ and $\alpha^{3t} \neq 1$. So, the above equation can't be satisfied and TG(H) is free of cycles of length 4.

TABLE 1. valid (t,u) and modified their basic equation

(t,u)	$1+\alpha^{3t+7}+\alpha^{3(t+u)-7}$
(t,t)	$1+\alpha^{3t+7}+\alpha^{6t-7}=0$ (b.1)
$(t,2t)$	$1+\alpha^{3t+7}+\alpha^{9t-7}=0$ (b.2)
$(t,3t)$	$1+\alpha^{3t+7}+\alpha^{12t-7}=0$ (b.3)
$(t,-2t)$	$1+\alpha^{3t+7}+\alpha^{-3t-7}=0$ (b.4)
$(t,-3t)$	$1+\alpha^{3t+7}+\alpha^{-6t-7}=0$ (b.5)

2.2. **All cycles of length 6.** All cycles of length 6 belong to the unique class $(0,1,2)$, i.e. chain $(0,0),(1,0),(1,t),(2,t),(2,t+u),(0,t+u)$ where $t+u\neq 0 \bmod 7$. The basic equation corresponding to this chain is:

$$\sum_{k=0}^{2}(\alpha^{7i_k}-\alpha^{7i_{k+1}})\alpha^{3j_k} = 1-\alpha^7+\alpha^{7+3t}-\alpha^{14+3t}+\alpha^{14+3(t+u)}-\alpha^{3(t+u)}$$
$$= (1-\alpha^7)(1+\alpha^{3t+7}+\alpha^{3(t+u)-7}) = 0 \pmod{p},$$

But $\alpha^7\neq 1$, so

$$1+\alpha^{3t+7}+\alpha^{3(t+u)-7}=0 \bmod p. \tag{2.3}$$

For the existence of a cycle of length 6 in this class, equation (2.3), must be solved for some possible values of t and u. The condition $t+u\neq 0 \bmod 7$ depending on the choice of t and u is either true or false. If this is true, then the pair (t,u) is called valid case. Value of u can be expressed in terms of t. All valid cases of (t,u), substituted in the equation (2.3) are listed in Table 1. For each case the solutions can be analyzed as the following:

- **Equation (b.1)**

This equation do not have solution, otherwise we will end up with an obvious contradiction such as $(\alpha^{3t+7})^3=1$.

- **Equation (b.2)**

By setting $y=\alpha^{3t+7}$, (b.2) become polynomial equation in y:

$$1+y+y^{17}=0 \bmod p. \tag{2.4}$$

The values of y^i, $1\le i\le 20$, are listed in Table 2.

Since $y^{21}-1$ is factorized as:

$$y^{21}-1=(y-1)(y^2+y+1)(y^6+y^5+y^4+y^3+y^2+y+1)(y^{12}-y^{11}+y^9-y^8+y^6-y^4+y^3-y+1)$$

and y is a primitive 21th root of unity, we have:

$$y^{12} - y^{11} + y^9 - y^8 + y^6 - y^4 + y^3 - y + 1 = 0 \bmod p. \tag{2.5}$$

The equation (2.4) is factorized as:

$$1 + y + y^{17} = (y^2 + y + 1)(y^{15} - y^{14} + y^{12} - y^{11} + y^9 - y^8 + y^6 - y^5 + y^3 - y^2 + 1).$$

By applying Euclidean division algorithm to:

$$y^{15} - y^{14} + y^{12} - y^{11} + y^9 - y^8 + y^6 - y^5 + y^3 - y^2 + 1,$$

and (2.5), in order to find their common roots we have:

$$y^{15} - y^{14} + y^{12} - y^{11} + y^9 - y^8 + y^6 - y^5 + y^3 - y^2 + 1 =$$
$$(y^{12} - y^{11} + y^9 - y^8 + y^6 - y^4 + y^3 - y + 1)y^3 - y^8 + y^7 - y^5 + y^4 - y^2 + 1$$

$$y^{12} - y^{11} + y^9 - y^8 + y^6 - y^4 + y^3 - y + 1 = (-y^8 + y^7 - y^5 + y^4 - y^2 + 1)(-y^4) + y^3 - y + 1$$

$$-y^8 + y^7 - y^5 + y^4 - y^2 + 1 = (y^3 - y + 1)(-y^5 + y^4 - y^3 + y^2 - y + 2) - 3y^2 + 3y - 1$$

$$y^3 - y + 1 = (-3y^2 + 3y - 1)(-\tfrac{1}{3}y - \tfrac{1}{3}) - \tfrac{1}{3}y + \tfrac{2}{3}$$

$$-3y^2 + 3y - 1 = (-\tfrac{1}{3}y + \tfrac{2}{3})(9y + 9) - 7.$$

Since the remainder -7 of the last division can not be zero in F_p, $p \in P_{21}$, the equation (b.2) do not have solution.

- **Equation (b.3)**

The left side of this equation can be re-written as:

$$1 + \alpha^{3t+7} + \alpha^{12t-7} = \alpha^{3t+7}(1 + \alpha^{9t-14} + (\alpha^{9t-14})^2).$$

Since α^{9t-14} is not a third root of unity, this equation do not have solution.

- **Equation (b.4)**

The left side of this equation can be re-written as:

TABLE 2. y^i

y	α^{3t+7}	y^{11}	α^{-9t-7}
y^2	α^{6t-7}	y^{12}	α^{-6t}
y^3	α^{9t}	y^{13}	α^{-3t+7}
y^4	α^{-9t+7}	y^{14}	α^{-7}
y^5	α^{-6t-7}	y^{15}	α^{3t}
y^6	α^{-3t}	y^{16}	α^{6t+7}
y^7	α^{7}	y^{17}	α^{9t-7}
y^8	α^{3t-7}	y^{18}	α^{-9t}
y^9	α^{6t}	y^{19}	α^{-6t+7}
y^{10}	α^{9t+7}	y^{20}	α^{-3t-7}

$$1 + \alpha^{3t+7} + \alpha^{-3t-7} = \alpha^{-3t-7}(1 + \alpha^{3t+7} + (\alpha^{3t+7})^2).$$

Since α^{3t+7} is not a third root of unity, this equation do not have solution.

- **Equation (b.5)**

Let $y = \alpha^{3t+7}$. Then (b.5) can be modified as follow:

$$1 + y + y^5 = (1 + y + y^2)(y^3 - y^2 + 1) = 0 \bmod p.$$

Since $1+y+y^2 \neq 0$, then $y^3 - y^2 + 1 = 0 \bmod p$. By applying Euclidean division algorithm to (2.5) and $y^3 - y^2 + 1$, we have

$$y^{12} - y^{11} + y^9 - y^8 + y^6 - y^4 + y^3 - y + 1 = (y^3 - y^2 + 1)(y^9 - y^5 - y^4 + y^2 + y + 2) + y^2 - 2y - 1$$

$$y^3 - y^2 + 1 = (y^2 - 2y - 1)(y + 1) + 3y + 2$$

$$y^2 - 2y - 1 = (3y + 2)(\tfrac{1}{3}y - \tfrac{8}{9}) + \tfrac{7}{9}.$$

Since the remainder $\frac{7}{9}$ of the last division can not be zero in F_p, $p \in P_{21}$, the equation (b.5) do not have solution.

As a result of this subsection, the TG(H) is free of cycles of length 6 and hence has a girth of at least 8.

2.3. **All cycles of length 8.** There are two inequivalent classes, (0, 1, 0, 1) and (0, 1, 0, 2), for the cycles of length 8. Each of these classes will be investigated in two separate parts.

2.3.1. *8-Cycles in the class* $(0,1,0,1)$. For 8-Cycles in the class $(0,1,0,1)$ i.e. chain $(0,0)$, $(1,0)$, $(1,t)$, $(0,t)$, $(0,t+u)$, $(1,t+u)$, $(1,t+u+v)$, $(0,t+u+v)$, where $t+u+v \neq 0 \bmod 7$, the basic equation

Table 3. All cases for 8-cycles

	(t,u,v)			(t,u,v)	
1	(t,t,t)		19	$(t,-t,t)$	
2	$(t,t,2t)$		20	$(t,-t,2t)$	
3	$(t,t,3t)$		21	$(t,-t,3t)$	
4	$(t,t,-t)$		22	$(t,-t,-t)$	
5	$(t,t,-2t)$	x	23	$(t,-t,-2t)$	
6	$(t,t,-3t)$		24	$(t,-t,-3t)$	
7	$(t,2t,t)$		25	$(t,-2t,t)$	x
8	$(t,2t,2t)$		26	$(t,-2t,2t)$	
9	$(t,2t,3t)$		27	$(t,-2t,3t)$	
10	$(t,2t,-t)$		28	$(t,-2t,-t)$	
11	$(t,2t,-2t)$		29	$(t,-2t,-2t)$	
12	$(t,2t,-3t)$	x	30	$(t,-2t,-3t)$	
13	$(t,3t,t)$		31	$(t,-3t,t)$	
14	$(t,3t,2t)$		32	$(t,-3t,2t)$	x
15	$(t,3t,3t)$	x	33	$(t,-3t,3t)$	
16	$(t,3t,-t)$		34	$(t,-3t,-t)$	
17	$(t,3t,-2t)$		35	$(t,-3t,-2t)$	
18	$(t,3t,-3t)$		36	$(t,-3t,-3t)$	

are as follow:

$$\sum_{k=0}^{3}(\alpha^{7i_k}-\alpha^{7i_{k+1}})\alpha^{3j_k}=1-\alpha^7+\alpha^{3t}(\alpha^7-1)+\alpha^{3(t+u)}(1-\alpha^7)+\alpha^{3(t+u+v)}(\alpha^7-1)=$$

$$(1-\alpha^7)(1-\alpha^{3t}+\alpha^{3(t+u)}-\alpha^{3(t+u+v)})=0 \bmod p,$$

But $\alpha^7\neq 1$, so

$$1-\alpha^{3t}+\alpha^{3(t+u)}-\alpha^{3(t+u+v)}=0 \bmod p. \tag{2.6}$$

All possible cases of (t,u,v) are given in Table 3. In this Table,"x" stand for invalid cases (i.e that they satisfy the equation $t+u+v=0 \bmod 7$).

By setting $z=\alpha^{3t}$, (2.6) for each of the 31 valid cases becomes some polynomial equation in z. Also, z is a primitive 7th root of unity. z^7-1 is factorized as:

$$z^7-1=(z-1)(z^6+z^5+z^4+z^3+z^2+z+1)=0 \bmod p.$$

Since $z\neq 1$, we have:

$$z^6+z^5+z^4+z^3+z^2+z+1=0 \bmod p. \tag{2.7}$$

For existence a cycle in this class (2.7) and the polynomial equation in z obtained from (2.6) should have at least one common solution in F_p. Our results are recorded in Table 4 for all valid cases.

Table 4 is organized as follow:

⋆ second column: all valid cases,

⋆ third column: equation (2.6) in z,

TABLE 4. valid (t, u, v) and modified their basic equation in class(0, 1, 0, 1)

	(t, u, v)	Original form	Reduced form	p
1	(t, t, t)	$z^3 - z^2 + z - 1$		
2	$(t, t, 2t)$	$z^4 - z^2 + z - 1$	$z^3 + z^2 + 1$	
3	$(t, t, 3t)$	$z^5 - z^2 + z - 1$	$z^4 + z^3 + z^2 + 1$	
4	$(t, t, -t)$	$(z - 1)^2$		
6	$(t, t, -3t)$	$z^6 - z^2 + z - 1$	$z^5 + z^4 + z^3 + z^2 + 1$	
7	$(t, 2t, t)$	$z^4 - z^3 + z - 1$		
8	$(t, 2t, 2t)$	$z^5 - z^3 + z - 1$	$z^4 + z^3 + 1$	
9	$(t, 2t, 3t)$	$z^6 - z^3 + z - 1$	$z^4 + z^2 - z + 1$	
10	$(t, 2t, -t)$	$z^3 - z^2 - z + 1$		
11	$(t, 2t, -2t)$	$z^3 - 2z + 1$	$z^2 + z - 1$	
13	$(t, 3t, t)$	$z^5 - z^4 + z - 1$	$z^4 + 1$	
14	$(t, 3t, 2t)$	$z^6 - z^4 + z - 1$	$z^3 - z + 1$	
16	$(t, 3t, -t)$	$z^4 - z^3 - z + 1$		
17	$(t, 3t, -2t)$	$z^4 - z^2 - z + 1$	$z^3 + z^2 - 1$	
18	$(t, 3t, -3t)$	$z^4 - 2z + 1$	$z^3 + z^2 + z - 1$	43
19	$(t, -t, t)$	$2(z - 1)$		
20	$(t, -t, 2t)$	$z^2 + z - 2$	$z + 2$	43
21	$(t, -t, 3t)$	$z^3 + z - 2$	$z^2 + z + 2$	
22	$(t, -t, -t)$	$z^6 + z - 2$	$z^5 + z^4 + z^3 + z^2 + z + 2$	
23	$(t, -t, -2t)$	$z^5 + z - 2$	$z^4 + z^3 + z^2 + z + 2$	
24	$(t, -t, -3t)$	$z^4 + z - 2$	$z^3 + z^2 + z + 2$	43
26	$(t, -2t, 2t)$	$z^6 - 2z + 1$	$z^5 + z^4 + z^3 + z^2 + z - 1$	43
27	$(t, -2t, 3t)$	$z^6 - z^2 - z + 1$	$z^5 + z^4 + z^3 + z^2 - 1$	
28	$(t, -2t, -t)$	$z^6 - z^5 - z + 1$		
29	$(t, -2t, -2t)$	$z^6 - z^4 - z + 1$	$z^5 + z^4 - 1$	
30	$(t, -2t, -3t)$	$z^6 - z^3 - z + 1$	$z^3 + z^2 - 1$	
31	$(t, -3t, t)$	$z^6 - z^5 + z - 1$	$z^4 - z^3 + z^2 - z + 1$	
33	$(t, -3t, 3t)$	$z^5 - 2z + 1$	$z^4 + z^3 + z^2 + z - 1$	
34	$(t, -3t, -t)$	$z^5 - z^4 - z + 1$		
35	$(t, -3t, -2t)$	$z^5 - z^3 - z + 1$	$z^4 + z^3 - 1$	
36	$(t, -3t, -3t)$	$z^5 - z^2 - z + 1$	$z^3 + z - 1$	

⋆ fourth column: the third column after eliminate those factors that can not be zero in F_p, such as: $z, z - 1, z + 1, z^2 + 1, z^2 - z + 1, z^2 + z + 1$, and $z^4 + z^3 + z^2 + z + 1$,
⋆ last column: the value of p that there is a cycle.

2.3.2. *8-Cycles in the class (0, 1, 0, 2).* The basic equation for 8-Cycles in the class $(0, 1, 0, 2)$ i.e. chain $(0, 0)$, $(1, 0)$, $(1, t)$, $(0, t)$, $(0, t + u)$, $(2, t + u)$, $(2, t + u + v)$, $(0, t + u + v)$, $(0, 0)$, where $t + u + v \neq 0 \bmod 7$, is:

$$\sum_{k=0}^{3}(\alpha^{7i_k} - \alpha^{7i_{k+1}})\alpha^{3j_k} = 1 - \alpha^7 + \alpha^{3t}(\alpha^7 - 1) + \alpha^{3(t+u)}(1 - \alpha^{14}) + \alpha^{3(t+u+v)}(\alpha^{14} - 1) =$$

$$(1 - \alpha^7)(1 - \alpha^{3t} - \alpha^{3(t+u)-7} + \alpha^{3(t+u+v)-7}) = 0 \bmod p.$$

But $\alpha^7 \neq 1$, So

$$1 - \alpha^{3t} - \alpha^{3(t+u)-7} + \alpha^{3(t+u+v)-7} = 0 \bmod p. \tag{2.8}$$

The results are recorded in Table 5, which is similar to Table 4 by using $y = \alpha^{3t+7}$ for (2.8) and all valid cases in Table 3, and eliminate those factors such as:

$$y,\ y-1,\ y+1,\ y^2+1,\ y^2-y+1,\ y^2+y+1,\ y^4+y^3+y^2+y+1,\ y^6+y^5+y^4+y^3+y^2+y+1,\ y^4+1,\ y^6+y^3+1,\ \ldots .$$

The p values in the last column of Table 5, values that for them the equation (2.5) and the equations in the third column after removal of those factors which are nonzero for any p, have a common solution.

Table 5. valid (t, u, v) and modified their basic equation in class(0, 1, 0, 2)

	(t,u,v)	Original form	Reduced form	p
1	(t,t,t)	$y^{17}-y^{15}-y^2+1$		
2	$(t,t,2t)$	$y^{15}-y^{11}+y^2-1$	$y^{11}-y^{10}+y^9-y^7+y^6-y^4+y^3-y+1$	
3	$(t,t,3t)$	$y^{15}-y^5+y^2-1$	$y^{11}-y^{10}+y^9+y^5-y^4+y^3-y+1$	43
4	$(t,t,-t)$	$y^{15}-y^8+y^2-1$	$y^{12}+y^9+y^6-y^5+y^3-y^2+1$	
6	$(t,t,-3t)$	$y^{20}-y^{15}-y^2+1$	$y^{17}+y^{14}-y^{12}+y^{11}-y^9+y^8-y^6+y^5-y^3+y^2-1$	
7	$(t,2t,t)$	$y^{17}+y^{15}-y^{11}-1$	$y^{14}+y^{12}+y^{11}+y^9+y^6+y^3+1$	
8	$(t,2t,2t)$	$y^{17}+y^{15}-y^5-1$	$y^{14}+y^{12}+y^{11}+y^9+y^8+y^6+y^5+y^3+1$	
9	$(t,2t,3t)$	$y^{20}-y^{17}-y^{15}+1$	$y^{17}-y^{12}-y^9-y^6-y^3-1$	43
10	$(t,2t,-t)$	$y^{17}+y^{15}-y^2-1$		
11	$(t,2t,-2t)$	$y^{17}+y^{15}-y^8-1$	$y^{14}+y^{12}+y^{11}+y^9+y^8+y^6+y^3+1$	127
13	$(t,3t,t)$	$y^{15}+y^{11}-y^5-1$	$y^{12}+y^9+y^8+y^6+y^5+y^3+1$	
14	$(t,3t,2t)$	$y^{20}-y^{15}-y^{11}+1$	$y^{13}+y^{10}-y^9-y^8+y^7-y^6+y^4-y^3-1$	
16	$(t,3t,-t)$	$y^{17}-y^{15}-y^{11}+1$	$y^{14}-y^{12}+y^{11}-y^9-y^6-y^3-1$	
17	$(t,3t,-2t)$	$y^{15}+y^{11}-y^2-1$	$y^{12}+y^9+y^8+y^6+y^5+y^3+y^2+1$	43
18	$(t,3t,-3t)$	$y^{15}+y^{11}-y^8-1$	$y^{12}+y^9+y^8+y^6+y^3+1$	43
19	$(t,-t,t)$	$y^{15}+y^{14}-y^8-1$	$y^6-y^4+y^3-y+1$	
20	$(t,-t,2t)$	$y^{15}+y^{14}-y^2-1$	$y^{12}+y^{11}+y^9+y^8+y^6+y^5+y^3+y^2+1$	43
21	$(t,-t,3t)$	$y^{17}-y^{15}-y^{14}+1$	$y^{13}-y^{12}-y^8+y^7-y^6-y^2+y-1$	127
22	$(t,-t,-t)$	$y^{20}-y^{15}-y^{14}+1$	$y^{17}+y^{14}-y^{12}-y^9-y^6-y^3-1$	
23	$(t,-t,-2t)$	$y^{15}+y^{14}-y^5-1$	$y^{11}+y^8+y^5+y^2-y+1$	127
24	$(t,-t,-3t)$	$y^{15}+y^{14}-y^{11}-1$	$y^{11}+y^8-y^7+y^6+y^2-y+1$	43
26	$(t,-2t,2t)$	$y^{20}+y^{15}-y^8-1$	$y^{17}+y^{14}+y^{12}+y^{11}+y^9+y^8+y^6+y^3+1$	43
27	$(t,-2t,3t)$	$y^{20}+y^{15}-y^2-1$	$y^{17}+y^{14}+y^{12}+y^{11}+y^9+y^8+y^6+y^5+y^3+y^2+1$	
28	$(t,-2t,-t)$	$y^{20}+y^{15}-y^5-1$		
29	$(t,-2t,-2t)$	$y^{20}+y^{15}-y^{11}-1$	$y^{14}-y^{13}+y^{11}+y^6-y^5+y^3-y+1$	43
30	$(t,-2t,-3t)$	$y^{20}+y^{15}-y^{17}-1$	$y^{16}-y^{15}+y^{14}-y^{13}+y^{12}+y^8-y^7+y^6+y^2-y+1$	
31	$(t,-3t,t)$	$y^{20}-y^{15}-y^5+1$		
33	$(t,-3t,3t)$	$y^{15}-y^8+y^5-1$	$y^{12}+y^9+y^6-y^5+y^3+1$	127
34	$(t,-3t,-t)$	$y^{15}-y^{11}+y^5-1$	$y^{12}+y^9-y^8+y^6-y^5+y^3+1$	
35	$(t,-3t,-2t)$	$y^{17}-y^{15}-y^5+1$	$y^{14}-y^{12}+y^{11}-y^9+y^8-y^6+y^5-y^3-1$	
36	$(t,-3t,-3t)$	$y^{15}+y^5-y^2-1$	$y^{10}-y^8+y^7+y^6-y^5+y^3+1$	

We see from Table 4 and 5 that for $p \in \{43, 127\}$, the girth of the codes are 8.

2.4. **All cycles of length 10.** There is an unique class $(0,1,2,0,1)$ for all cycles of length 10 . The basic equation for chain (0,0), (1,0), $(1,t)$, $(2,t)$, $(2,t+u)$, $(0,t+u)$, $(0,t+u+v)$, $(1,t+u+v)$, $(1,t+u+v+w)$, $(0,t+u+v+w)$, $(0,0)$ where $t+u+v+w \neq 0 \bmod 7$, corresponding to this class is:

$$\sum_{k=0}^{4}(\alpha^{7i_k} - \alpha^{7i_{k+1}})\alpha^{3j_k} = 1 - \alpha^7 + \alpha^{3t}(\alpha^7 - \alpha^{14}) + \alpha^{3(t+u)}(\alpha^{14} - 1) + \alpha^{3(t+u+v)}(1 - \alpha^7) +$$

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

But $\alpha^7 \neq 1$, so:

$$1 + \alpha^{3t+7} + \alpha^{3(t+u)-7} + \alpha^{3(t+u+v)} - \alpha^{3(t+u+v+w)} = 0 \bmod p. \tag{2.9}$$

All possible cases of (t, u, v, w) are given in Table 10. In Table 10 "x" stand for invalid cases (i.e that they satisfy the equation $t + u + v + w = 0 \bmod 7$). Table 6 is similar to Table 5 by using y^i for (2.9) and consideration all valid cases in table 10. In fact, the Euclidian division algorithm has been used to check such cases to find a possible solution. For example, for the case $(t, -2t, t, t)$, No. 145 in Table 10, the original form is $y^{20} - y^{15} + y + 2$ which is reduced to

$$y^{18} - y^{17} + y^{15} - y^{14} - y^{13} + 2y^{12} - y^{11} - y^{10} + 2y^9 - y^8 - y^7 + 2y^6 - y^5 - y^4 + 2y^3 - y^2 - y + 2.$$

Now, the remainders can be arranged respectively as the following:

$$-y^{11}+y^{10}+y^7+y^6-2y^5+2y^3-2y^2+2, \quad y^7-y^6+y^4-y^3+y+1, \quad y^6-y^5+y^4+2y^3-2y^2+2,$$

$$-y^5-y^4+y^3-y+1, \quad 4y^4-3y^2+3y, \quad \frac{1}{4}y^3-\frac{1}{4}y+1, y^2-13y, \quad 42y+1, \quad \frac{547}{1764}=\frac{547}{2^2 3^2 7^2}$$

But the last remainder $\frac{547}{2^2 3^2 7^2}$ is non-zero if $p > 547$. Because of some complexity, all other such cases has been checked by computer. Now, based on Table 6, we find that for $p \in \{211, 337, 379, 421, 463, 547, 631, 757, 1429, 2437, 3109\}$ the girth is 10.

Table 6. Valid (t, u, v, w) and modified their basic equation for 10-cycles

	(t,u,v,w)	Original form	Reduced form	p
1	(t,t,t,t)	$y^{18} - y^3 - y^2 - y - 1$	$y^{16} - y^{15} + y^{13} - y^{12} + y^{10} - y^9 + y^7 - y^6 + y^4 - y^3 - 1$	
2	$(t,t,t,2t)$	$y^{12} - y^3 - y^2 - y - 1$	$y^{10} - y^9 + y^7 - y^6 + y^4 - y^3 - 1$	
3	$(t,t,t,3t)$	$y^6 - y^3 - y^2 - y - 1$	$y^4 - y^3 + 1$	
4	$(t,t,t,-t)$	$y^9 - y^3 - y^2 - y - 1$	$y^7 - y^6 + y^4 - y^3 - 1$	43
5	$(t,t,t,-2t)$	$y^{15} - y^3 - y^2 - y - 1$	$y^{13} - y^{12} + y^{10} - y^9 + y^7 - y^6 + y^4 - y^3 - 1$	43
7	$(t,t,2t,t)$	$y^{18} - y^{12} + y^2 + y + 1$	$y^{16} - y^{15} + y^{13} - y^{12} + 1$	
8	$(t,t,2t,2t)$	$y^{18} - y^6 + y^2 + y + 1$	$y^{16} - y^{15} + y^{13} - y^{12} + y^{10} - y^9 + y^7 - y^6 + 1$	43
10	$(t,t,2t,-t)$	$y^{18} - y^3 + y^2 + y + 1$	$y^{16} - y^{15} + y^{13} - y^{12} + y^{10} - y^9 + y^7 - y^6 + y^4 - y^3 + 1$	379
11	$(t,t,2t,-2t)$	$y^{18} - y^9 + y^2 + y + 1$	$y^{16} - y^{15} + y^{13} - y^{12} + y^{10} - y^9 + 1$	421
12	$(t,t,2t,-3t)$	$y^{18} - y^{15} + y^2 + y + 1$	$y^{16} - y^{15} + 1$	463
13	$(t,t,3t,t)$	$y^{12} - y^6 + y^2 + y + 1$	$y^{10} - y^9 + y^7 - y^6 + 1$	
15	$(t,t,3t,3t)$	$y^{15} - y^{12} - y^2 - y - 1$	$y^{13} - y^{12} - 1$	
16	$(t,t,3t,-t)$	$y^{18} - y^{12} - y^2 - y - 1$	$y^{16} - y^{15} + y^{13} - y^{12} - 1$	43
17	$(t,t,3t,-2t)$	$y^{12} - y^3 + y^2 + y + 1$	$y^{10} - y^9 + y^7 - y^6 + y^4 - y^3 + 1$	211
18	$(t,t,3t,-3t)$	$y^{12} - y^9 + y^2 + y + 1$	$y^{10} - y^9 + 1$	43
19	$(t,t,-t,t)$	$y^{15} - y^9 + y^2 + y + 1$	$y^{13} - y^{12} + y^{10} - y^9 + 1$	43
20	$(t,t,-t,2t)$	$y^{15} - y^3 + y^2 + y + 1$	$y^{13} - y^{12} + y^{10} - y^9 + y^7 - y^6 + y^4 - y^3 + 1$	
21	$(t,t,-t,3t)$	$y^{18} - y^{15} - y^2 - y - 1$	$y^{16} - y^{15} - 1$	

Table 7. (continued)

	(t,u,v,w)	Original form	Reduced form	p
23	$(t,t,-t,-2t)$	$y^{15}-y^{6}+y^{2}+y+1$	$y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+1$	
24	$(t,t,-t,-3t)$	$y^{15}-y^{12}+y^{2}+y+1$	$y^{13}-y^{12}+1$	43
25	$(t,t,-2t,t)$	$y^{15}-y^{2}-y-2$	$y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-y^{3}+y-2$	337
26	$(t,t,-2t,2t)$	$y^{9}-y^{2}-y-2$	$y^{7}-y^{6}+y^{4}-y^{3}+y-2$	631
27	$(t,t,-2t,3t)$	$y^{3}-y^{2}-y-2$	$y-2$	337
28	$(t,t,-2t,-t)$	$y^{6}-y^{2}-y-2$	$y^{4}-y^{3}+y-2$	463
29	$(t,t,-2t,-2t)$	$y^{12}-y^{2}-y-2$	$y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-y^{3}+y-2$	1429
30	$(t,t,-2t,-3t)$	$y^{18}-y^{2}-y-2$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-y^{3}+y-2$	379
32	$(t,t,-3t,2t)$	$y^{15}-y^{6}-y^{2}-y-1$	$y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}-1$	757
33	$(t,t,-3t,3t)$	$y^{9}-y^{6}-y^{2}-y-1$	$y^{7}-y^{6}-1$	43
34	$(t,t,-3t,-t)$	$y^{12}-y^{6}-y^{2}-y-1$	$y^{10}-y^{9}+y^{7}-y^{6}-1$	43
35	$(t,t,-3t,-2t)$	$y^{18}-y^{6}-y^{2}-y-1$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}-1$	127
36	$(t,t,-3t,-3t)$	$y^{6}-y^{3}+y^{2}+y+1$	$y^{4}-y^{3}+1$	43
37	$(t,2t,t,t)$	$y^{18}+y^{17}-y^{12}+y+1$	$y^{16}-y^{14}+y^{13}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
38	$(t,2t,t,2t)$	$y^{18}+y^{17}-y^{6}+y+1$	$y^{16}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{3}-y^{2}+1$	43
40	$(t,2t,t,-t)$	$y^{18}+y^{17}-y^{3}+y+1$	$y^{12}+y^{9}-y^{8}-y^{5}+1$	127
41	$(t,2t,t,-2t)$	$y^{18}+y^{17}-y^{9}+y+1$	$y^{16}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	
42	$(t,2t,t,-3t)$	$y^{18}+y^{17}-y^{15}+y+1$	$y^{12}-y^{7}-y^{4}+y^{3}+1$	127
43	$(t,2t,2t,t)$	$y^{17}+y^{12}-y^{6}+y+1$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{3}-y^{2}+1$	43
45	$(t,2t,2t,3t)$	$y^{17}-y^{15}+y^{12}+y+1$	$y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
46	$(t,2t,2t,-t)$	$y^{18}-y^{17}-y^{12}-y-1$	$y^{16}-2y^{15}+y^{14}+y^{13}-2y^{12}+y^{11}-y^{9}+y^{8}-y^{6}+y^{5}-y^{3}+y^{2}-1$	127
47	$(t,2t,2t,-2t)$	$y^{17}+y^{12}-y^{3}+y+1$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{4}-y^{2}+1$	757
48	$(t,2t,2t,-3t)$	$y^{17}+y^{12}-y^{9}+y+1$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{10}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
50	$(t,2t,3t,2t)$	$y^{17}-y^{15}+y^{6}+y+1$	$y^{11}-y^{10}+y^{8}-2y^{7}+y^{6}-y^{4}+y^{3}+1$	463
51	$(t,2t,3t,3t)$	$y^{17}-y^{9}+y^{6}+y+1$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}+y^{3}-y^{2}+1$	
52	$(t,2t,3t,-t)$	$y^{17}-y^{12}+y^{6}+y+1$	$y^{15}-y^{14}+y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}+y^{3}-y^{2}+1$	379
53	$(t,2t,3t,-2t)$	$y^{18}-y^{17}-y^{6}-y-1$	$y^{16}-2y^{15}+y^{14}+y^{13}-2y^{12}+y^{11}+y^{10}-2y^{9}+y^{8}+y^{7}-2y^{6}+y^{5}-y^{3}+y^{2}-1$	43
54	$(t,2t,3t,-3t)$	$y^{17}+y^{6}-y^{3}+y+1$	$y^{11}-y^{10}+y^{9}-y^{7}+y^{6}-y^{5}+1$	421
55	$(t,2t,-t,t)$	$y^{17}+y^{9}-y^{3}+y+1$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{7}-y^{5}+y^{4}-y^{2}+1$	547
56	$(t,2t,-t,2t)$	$y^{18}-y^{17}-y^{9}-y-1$	$y^{14}-y^{13}-y^{12}+y^{11}+y^{8}-y^{7}-y^{6}+y^{3}+y^{2}-y-1$	211
57	$(t,2t,-t,3t)$	$y^{17}-y^{12}+y^{9}+y+1$	$y^{9}-y^{5}-y^{4}+y+1$	43
58	$(t,2t,-t,-t)$	$y^{17}-y^{15}+y^{9}+y+1$	$y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	211
60	$(t,2t,-t,-3t)$	$y^{17}+y^{9}-y^{6}+y+1$	$y^{13}-y^{11}+y^{7}-y^{3}-y^{2}+y+1$	43
61	$(t,2t,-2t,t)$	$y^{17}+y^{15}-y^{9}+y+1$	$y^{15}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	
62	$(t,2t,-2t,2t)$	$y^{17}+y^{15}-y^{3}+y+1$	$y^{15}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{4}-y^{2}+1$	127
63	$(t,2t,-2t,3t)$	$y^{18}-y^{17}-y^{15}-y-1$	$y^{14}-y^{13}-y^{12}+y^{9}+y^{8}-y^{7}-y^{6}+y^{3}+y^{2}-y-1$	
65	$(t,2t,-2t,-2t)$	$y^{17}+y^{15}-y^{6}+y+1$	$y^{13}-y^{9}+y^{7}-y^{3}-y^{2}+y+1$	43
66	$(t,2t,-2t,-3t)$	$y^{17}+y^{15}-y^{12}+y+1$	$y^{13}-y^{9}-y^{8}+y^{7}+y^{6}-y^{3}-y^{2}+y+1$	
67	$(t,2t,-3t,t)$	$y^{17}-y^{15}+y+2$	$y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}-y+2$	2437
68	$(t,2t,-3t,2t)$	$y^{17}-y^{9}+y+2$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}-y+2$	631
69	$(t,2t,-3t,3t)$	$y^{17}-y^{3}+y+2$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}-y+2$	43
70	$(t,2t,-3t,-t)$	$y^{17}-y^{6}+y+2$	$y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}-y+2$	211
71	$(t,2t,-3t,-2t)$	$y^{17}-y^{12}+y+2$	$y^{15}-y^{14}+y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}-y+2$	43
72	$(t,2t,-3t,-3t)$	$y^{18}-y^{17}-y-2$	$y^{16}-2y^{15}+y^{14}+y^{13}-2y^{12}+y^{11}+y^{10}-2y^{9}+y^{8}+y^{7}-2y^{6}+y^{5}+y^{4}-2y^{3}+y^{2}+y-2$	3109
73	$(t,3t,t,t)$	$y^{12}+y^{11}-y^{6}+y+1$	$y^{10}-y^{8}+y^{7}-y^{5}+y^{3}-y^{2}+1$	
75	$(t,3t,t,3t)$	$y^{15}-y^{12}-y^{11}-y-1$	$y^{13}-y^{12}-y^{9}+y^{8}-y^{6}+y^{5}-y^{3}+y^{2}-1$	43
76	$(t,3t,t,-t)$	$y^{18}-y^{12}-y^{11}-y-1$	$y^{16}-y^{15}+y^{13}-y^{12}-y^{9}+y^{8}-y^{6}+y^{5}-y^{3}+y^{2}-1$	43
77	$(t,3t,t,-2t)$	$y^{12}+y^{11}-y^{3}+y+1$	$y^{10}-y^{8}+y^{7}-y^{5}+y^{4}-y^{2}+1$	
78	$(t,3t,t,-3t)$	$y^{12}+y^{11}-y^{9}+y+1$	$y^{10}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	
80	$(t,3t,2t,2t)$	$y^{15}-y^{11}-y^{6}-y-1$	$y^{8}-y^{7}+y^{5}-y^{4}+y^{3}-y+1$	
81	$(t,3t,2t,3t)$	$y^{11}-y^{9}+y^{6}+y+1$	$y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}+y^{3}-y^{2}+1$	43
82	$(t,3t,2t,-t)$	$y^{12}-y^{11}-y^{6}-y-1$	$y^{10}-2y^{9}+y^{8}+y^{7}-2y^{6}+y^{5}-y^{3}+y^{2}-1$	211
83	$(t,3t,2t,-2t)$	$y^{18}-y^{11}-y^{6}-y-1$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-2y^{9}+y^{8}+y^{7}-2y^{6}+y^{5}-y^{3}+y^{2}-1$	
84	$(t,3t,2t,-3t)$	$y^{11}+y^{6}-y^{3}+y+1$	$y^{9}-y^{8}+y^{6}-y^{5}+y^{4}-y^{2}+1$	
85	$(t,3t,3t,t)$	$y^{15}-y^{11}-y-2$	$y^{13}-y^{12}+y^{10}-2y^{9}+y^{8}+y^{7}-2y^{6}+y^{5}+y^{4}-2y^{3}+y^{2}+y-2$	631
86	$(t,3t,3t,2t)$	$y^{11}-y^{9}+y+2$	$y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}-y+2$	379
87	$(t,3t,3t,3t)$	$y^{11}-y^{3}+y+2$	$y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}-y+2$	463
88	$(t,3t,3t,-t)$	$y^{11}-y^{6}+y+2$	$y^{9}-y^{8}+y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}-y+2$	1429

TABLE 8. (continued)

	(t,u,v,w)	Original form	Reduced form	p
89	$(t,3t,3t,-2t)$	$y^{12}-y^{11}-y-2$	$y^{10}-2y^9+y^8+y^7-2y^6+y^5+y^4-2y^3+y^2+y-2$	337
90	$(t,3t,3t,-3t)$	$y^{18}-y^{11}-y-2$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-2y^9+y^8+y^7-2y^6+y^5+y^4-2y^3+y^2+y-2$	337
91	$(t,3t,-t,t)$	$y^{18}-y^{11}-y^3-y-1$	$y^{14}-y^{12}+y^8-y^7-y^6+y^5+y^2-y-1$	757
92	$(t,3t,-t,2t)$	$y^{12}-y^{11}-y^3-y-1$	$y^8-y^7-y^6+y^5+y^2-y-1$	43
93	$(t,3t,-t,3t)$	$y^{11}-y^6+y^3+y+1$	$y^7-y^5-y^2+y+1$	43
94	$(t,3t,-t,-t)$	$y^{11}-y^9+y^3+y+1$	$y^9-y^8-y^7+2y^6-y^5-y^4+2y^3-y^2+1$	127
95	$(t,3t,-t,-2t)$	$y^{15}-y^{11}-y^3-y-1$	$y^{13}-y^{12}+y^{10}-2y^9+y^8+y^7-2y^6+y^5+y^4-2y^3+y^2-1$	43
97	$(t,3t,-2t,t)$	$y^{11}+y^9-y^3+y+1$	$y^9-y^8+y^7-y^5+y^4-y^2+1$	43
98	$(t,3t,-2t,2t)$	$y^{18}-y^{11}-y^9-y-1$	$y^{14}-y^{12}+y^8-y^7-y^6+y^3+y^2-y-1$	463
99	$(t,3t,-2t,3t)$	$y^{12}-y^{11}-y^9-y-1$	$y^8-y^7-y^6+y^3+y^2-y-1$	379
100	$(t,3t,-2t,-t)$	$y^{15}-y^{11}-y^9-y-1$	$y^{13}-y^{12}+y^{10}-2y^9+y^8-y^6+y^5-y^3+y^2-1$	421
102	$(t,3t,-2t,-3t)$	$y^{11}+y^9-y^6+y+1$	$y^7-y^3-y^2+y+1$	
103	$(t,3t,-3t,t)$	$y^{15}+y^{11}-y^9+y+1$	$y^{13}-y^{12}+y^{10}-y^8+y^6-y^5+y^3-y^2+1$	43
104	$(t,3t,-3t,2t)$	$y^{15}+y^{11}-y^3+y+1$	$y^{13}-y^{12}+y^{10}-y^8+y^7-y^5+y^4-y^2+1$	
105	$(t,3t,-3t,3t)$	$y^{18}-y^{15}-y^{11}-y-1$	$y^{14}-y^{12}-y^{11}+y^9+y^8-y^7-y^6+y^3+y^2-y-1$	
107	$(t,3t,-3t,-2t)$	$y^{15}+y^{11}-y^6+y+1$	$(y^8+y^7-y^5-y^4-y^3+y+1)(y^3-y^2+1)$	
108	$(t,3t,-3t,-3t)$	$y^{15}-y^{12}+y^{11}+y+1$	$y^{11}-y^9-y^8+y^7+y^6-y^3-y^2+y+1$	
109	$(t,-t,t,t)$	$y^{15}+y^{14}-y^9+y+1$	$y^{13}-y^{11}+y^{10}-y^8+y^6-y^5+y^3-y^2+1$	
110	$(t,-t,t,2t)$	$y^{15}+y^{14}-y^3+y+1$	$y^{13}-y^{11}+y^{10}-y^8+y^7-y^5+y^4-y^2+1$	
111	$(t,-t,t,3t)$	$y^{18}-y^{15}-y^{14}-y-1$	$y^{16}-y^{15}-y^{12}+y^{11}-y^9+y^8-y^6+y^5-y^3+y^2-1$	
113	$(t,-t,t,-2t)$	$y^{15}+y^{14}-y^6+y+1$	$y^{13}-y^{11}+y^{10}-y^8+y^7-y^5+y^3-y^2+1$	
114	$(t,-t,t,-3t)$	$y^{15}+y^{14}-y^{12}+y+1$	$y^{13}-y^{11}+y^9-y^8+y^6-y^5+y^3-y^2+1$	
115	$(t,-t,2t,t)$	$y^{14}+y^9-y^3+y+1$	$y^{12}-y^{11}+y^9-y^8+y^7-y^5+y^4-y^2+1$	
116	$(t,-t,2t,2t)$	$y^{18}-y^{14}-y^9-y-1$	$y^{16}-y^{15}+y^{13}-2y^{12}+y^{11}+y^{10}-2y^9+y^8-y^6+y^5-y^3+y^2-1$	
117	$(t,-t,2t,3t)$	$y^{14}-y^{12}+y^9+y+1$	$y^{12}-y^{11}-y^{10}+2y^9-y^8+y^6-y^5+y^3-y^2+1$	43
118	$(t,-t,2t,-t)$	$y^{15}-y^{14}-y^9-y-1$	$y^{13}-2y^{12}+y^{11}+y^{10}-2y^9+y^8-y^6+y^5-y^3+y^2-1$	
120	$(t,-t,2t,-3t)$	$y^{14}+y^9-y^6+y+1$	$(y^3-y^2+1)(y^9-y^5+1)$	
121	$(t,-t,3t,t)$	$y^{18}-y^{14}-y^3-y-1$	$y^{16}-y^{15}+y^{13}-2y^{12}+y^{11}+y^{10}-2y^9+y^8+y^7-2y^6+y^5+y^4-2y^3+y^2-1$	
122	$(t,-t,3t,2t)$	$y^{14}-y^{12}+y^3+y+1$	$y^{12}-y^{11}-y^{10}+2y^9-y^8-y^7+2y^6-y^5-y^4+2y^3-y^2+1$	
123	$(t,-t,3t,3t)$	$y^{14}-y^6+y^3+y+1$	$y^{12}-y^{11}+y^9-y^8+y^6-y^5-y^4+2y^3-y^2+1$	43
124	$(t,-t,3t,-t)$	$y^{14}-y^9+y^3+y+1$	$y^{12}-y^{11}+y^9-y^8-y^7+2y^6-y^5-y^4+2y^3-y^2+1$	
125	$(t,-t,3t,-2t)$	$y^{15}-y^{14}-y^3-y-1$	$y^{13}-2y^{12}+y^{11}+y^{10}-2y^9+y^8+y^7-2y^6+y^5+y^4-2y^3+y^2-1$	127
128	$(t,-t,-t,2t)$	$y^{15}-y^{14}-y^6-y-1$	$(y^6-y^5+y^3-y^2+1)(y^7-y^6-1)$	43
129	$(t,-t,-t,3t)$	$y^{14}-y^9+y^6+y+1$	$y^{12}-y^{11}+y^9-y^8-y^7+2y^6-y^5+y^3-y^2+1$	
130	$(t,-t,-t,-t)$	$y^{14}-y^{12}+y^6+y+1$	$y^{12}-y^{11}-y^{10}+2y^9-y^8-y^7+2y^6-y^5+y^3-y^2+1$	
131	$(t,-t,-t,-2t)$	$y^{18}-y^{14}-y^6-y-1$	$y^{16}-y^{15}+y^{13}-2y^{12}+y^{11}+y^{10}-2y^9+y^8+y^7-2y^6+y^5-y^3+y^2-1$	43
132	$(t,-t,-t,-3t)$	$y^{14}+y^6-y^3+y+1$	$y^{12}-y^{11}+y^9-y^8+y^6-y^5+y^4-y^2+1$	
133	$(t,-t,-2t,t)$	$y^{14}+y^{12}-y^6+y+1$	$y^{12}-y^{11}+y^{10}-y^8+y^7-y^5+y^3-y^2+1$	
135	$(t,-t,-2t,3t)$	$y^{15}-y^{14}-y^{12}-y-1$	$y^{13}-2y^{12}+y^{11}-y^9+y^8-y^6+y^5-y^3+y^2-1$	127
136	$(t,-t,-2t,-t)$	$y^{18}-y^{14}-y^{12}-y-1$	$y^{16}-y^{15}+y^{13}-2y^{12}+y^{11}-y^9+y^8-y^6+y^5-y^3+y^2-1$	
137	$(t,-t,-2t,-2t)$	$y^{14}+y^{12}-y^3+y+1$	$y^{12}-y^{11}+y^{10}-y^8+y^7-y^5+y^4-y^2+1$	
138	$(t,-t,-2t,-3t)$	$y^{14}+y^{12}-y^9+y+1$	$y^{12}-y^{11}+y^{10}-y^8+y^6-y^5+y^3-y^2+1$	
139	$(t,-t,-3t,t)$	$y^{18}+y^{14}-y^{12}+y+1$	$y^{16}-y^{15}+y^{13}-y^{11}+y^9-y^8+y^6-y^5+y^3-y^2+1$	
140	$(t,-t,-3t,2t)$	$y^{18}+y^{14}-y^6+y+1$	$y^{16}-y^{15}+y^{13}-y^{11}+y^{10}-y^8+y^7-y^5+y^3-y^2+1$	
142	$(t,-t,-3t,-t)$	$y^{18}+y^{14}-y^3+y+1$	$y^{16}-y^{15}+y^{13}-y^{11}+y^{10}-y^8+y^7-y^5+y^4-y^2+1$	
143	$(t,-t,-3t,-2t)$	$y^{18}+y^{14}-y^9+y+1$	$y^{16}-y^{15}+y^{13}-y^{11}+y^{10}-y^8+y^6-y^5+y^3-y^2+1$	43
144	$(t,-t,-3t,-3t)$	$y^{18}-y^{15}+y^{14}+y+1$	$y^{16}-y^{15}+y^{12}-y^{11}+y^9-y^8+y^6-y^5+y^3-y^2+1$	43
145	$(t,-2t,t,t)$	$y^{20}-y^{15}+y+2$	$y^{18}-y^{17}+y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^9-y^8-y^7+2y^6-y^5-y^4+2y^3-y^2-y+2$	547
146	$(t,-2t,t,2t)$	$y^{20}-y^9+y+2$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^9-y^8-y^7+2y^6-y^5-y^4+2y^3-y^2-y+2$	43
147	$(t,-2t,t,3t)$	$y^{20}-y^3+y+2$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^9-y^8+y^6-y^5+y^3-y^2-y+2$	211
148	$(t,-2t,t,-t)$	$y^{20}-y^6+y+2$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^9-y^8+y^6-y^5-y^4+2y^3-y^2-y+2$	547
149	$(t,-2t,t,-2t)$	$y^{20}-y^{12}+y+2$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}-y^{10}+2y^9-y^8-y^7+2y^6-y^5-y^4+2y^3-y^2-y+2$	43
150	$(t,-2t,t,-3t)$	$y^{20}-y^{18}+y+2$	$y^{18}-y^{17}-y^{16}+2y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^9-y^8-y^7+2y^6-y^5-y^4+2y^3-y^2-y+2$	211
151	$(t,-2t,2t,t)$	$y^{20}+y^{15}-y^9+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{13}-y^{11}+y^{10}-y^8+y^6-y^5+y^3-y^2+1$	
152	$(t,-2t,2t,2t)$	$y^{20}+y^{15}-y^3+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{13}-y^{11}+y^{10}-y^8+y^7-y^5+y^4-y^2+1$	

Table 9. (continued)

	(t,u,v,w)	Original form	Reduced form	p
153	$(t,-2t,2t,3t)$	$y^{20}-y^{18}+y^{15}+y+1$	$y^{18}-y^{17}-y^{16}+2y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
155	$(t,-2t,2t,-2t)$	$y^{20}+y^{15}-y^{6}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{3}-y^{2}+1$	43
156	$(t,-2t,2t,-3t)$	$y^{20}+y^{15}-y^{12}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{13}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	
157	$(t,-2t,3t,t)$	$y^{20}+y^{9}-y^{3}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{7}-y^{5}+y^{4}-y^{2}+1$	43
158	$(t,-2t,3t,2t)$	$y^{20}-y^{18}+y^{9}+y+1$	$y^{18}-y^{17}-y^{16}+2y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
159	$(t,-2t,3t,3t)$	$y^{20}-y^{12}+y^{9}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	211
160	$(t,-2t,3t,-t)$	$y^{20}-y^{15}+y^{9}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	211
162	$(t,-2t,3t,-3t)$	$y^{20}+y^{9}-y^{6}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{7}-y^{5}+y^{3}-y^{2}+1$	547
163	$(t,-2t,-t,t)$	$y^{20}+y^{12}-y^{6}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{3}-y^{2}+1$	211
165	$(t,-2t,-t,3t)$	$y^{20}-y^{15}+y^{12}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	547
166	$(t,-2t,-t,-t)$	$y^{20}-y^{18}+y^{12}+y+1$	$y^{18}-y^{17}-y^{16}+2y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
167	$(t,-2t,-t,-2t)$	$y^{20}+y^{12}-y^{3}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{4}-y^{2}+1$	43
168	$(t,-2t,-t,-3t)$	$y^{20}+y^{12}-y^{9}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^{10}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	211
169	$(t,-2t,-2t,t)$	$y^{20}+y^{18}-y^{12}+y+1$	$y^{18}-y^{17}+y^{16}-y^{14}+y^{13}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
170	$(t,-2t,-2t,2t)$	$y^{20}+y^{18}-y^{6}+y+1$	$y^{18}-y^{17}+y^{16}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{3}-y^{2}+1$	
172	$(t,-2t,-2t,-t)$	$y^{20}+y^{18}-y^{3}+y+1$	$y^{18}-y^{17}+y^{16}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{7}-y^{5}+y^{4}-y^{2}+1$	211
173	$(t,-2t,-2t,-2t)$	$y^{20}+y^{18}-y^{9}+y+1$	$y^{18}-y^{17}+y^{16}-y^{14}+y^{13}-y^{11}+y^{10}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	
174	$(t,-2t,-2t,-3t)$	$y^{20}+y^{18}-y^{15}+y+1$	$y^{18}-y^{17}+y^{16}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}+y^{3}-y^{2}+1$	43
175	$(t,-2t,-3t,t)$	$y^{20}-y^{18}+y^{3}+y+1$	$y^{18}-y^{17}-y^{16}+2y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}+1$	211
176	$(t,-2t,-3t,2t)$	$y^{20}-y^{12}+y^{3}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}+1$	
177	$(t,-2t,-3t,3t)$	$y^{20}-y^{6}+y^{3}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}+y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}+1$	43
178	$(t,-2t,-3t,-t)$	$y^{20}-y^{9}+y^{3}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}+y^{12}-y^{11}+y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}+1$	43
179	$(t,-2t,-3t,-2t)$	$y^{20}-y^{15}+y^{3}+y+1$	$y^{18}-y^{17}+y^{15}-y^{14}-y^{13}+2y^{12}-y^{11}-y^{10}+2y^{9}-y^{8}-y^{7}+2y^{6}-y^{5}-y^{4}+2y^{3}-y^{2}+1$	
182	$(t,-3t,t,2t)$	$y^{15}-y^{6}-y^{5}-y-1$	$y^{9}-y^{8}+y^{7}-y^{5}+y^{4}-y^{3}-1$	127
183	$(t,-3t,t,3t)$	$y^{9}-y^{6}-y^{5}-y-1$	$y^{7}-y^{6}-y^{3}+y^{2}-1$	43
184	$(t,-3t,t,-t)$	$y^{12}-y^{6}-y^{5}-y-1$	$y^{10}-y^{9}+y^{7}-y^{6}-y^{3}+y^{2}-1$	127
185	$(t,-3t,t,-2t)$	$y^{18}-y^{6}-y^{5}-y-1$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}-y^{3}+y^{2}-1$	43
186	$(t,-3t,t,-3t)$	$y^{6}+y^{5}-y^{3}+y+1$		
187	$(t,-3t,2t,t)$	$y^{15}-y^{5}-y-2$	$y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-2y^{3}+y^{2}+y-2$	43
188	$(t,-3t,2t,2t)$	$y^{9}-y^{5}-y-2$	$y^{7}-y^{6}+y^{4}-2y^{3}+y^{2}+y-2$	211
189	$(t,-3t,2t,3t)$	$y^{5}-y^{3}+y+2$	$y^{3}-y^{2}-y+2$	631
190	$(t,-3t,2t,-t)$	$y^{6}-y^{5}-y-2$	$y^{4}-2y^{3}+y^{2}+y-2$	3109
191	$(t,-3t,2t,-2t)$	$y^{12}-y^{5}-y-2$	$y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-2y^{3}+y^{2}+y-2$	2437
192	$(t,-3t,2t,-3t)$	$y^{18}-y^{5}-y-2$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-2y^{3}+y^{2}+y-2$	
193	$(t,-3t,3t,t)$	$y^{15}-y^{9}+y^{5}+y+1$	$y^{13}-y^{12}+y^{10}-y^{9}+y^{3}-y^{2}+1$	
194	$(t,-3t,3t,2t)$	$y^{15}+y^{5}-y^{3}+y+1$	$y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-y^{2}+1$	
195	$(t,-3t,3t,3t)$	$y^{18}-y^{15}-y^{5}-y-1$	$y^{14}-y^{12}-y^{11}+y^{9}+y^{8}-y^{6}-y^{5}+y^{3}+y^{2}-y-1$	
197	$(t,-3t,3t,-2t)$	$y^{15}-y^{6}+y^{5}+y+1$	$y^{11}-y^{9}+y^{5}-y^{3}-y^{2}+y+1$	
198	$(t,-3t,3t,-3t)$	$y^{15}-y^{12}+y^{5}+y+1$	$y^{11}-y^{9}-y^{8}+y^{6}+y^{5}-y^{3}-y^{2}+y+1$	127
199	$(t,-3t,-t,t)$	$y^{18}-y^{12}+y^{5}+y+1$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{3}-y^{2}+1$	43
200	$(t,-3t,-t,2t)$	$y^{18}-y^{6}+y^{5}+y+1$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+y^{3}-y^{2}+1$	127
202	$(t,-3t,-t,-t)$	$y^{18}+y^{5}-y^{3}+y+1$	$y^{12}-y^{11}+y^{10}-y^{8}+y^{7}-y^{6}+1$	43
203	$(t,-3t,-t,-2t)$	$y^{18}-y^{9}+y^{5}+y+1$	$y^{16}-y^{15}+y^{13}-y^{12}+y^{10}-y^{9}+y^{3}-y^{2}+1$	43
204	$(t,-3t,-t,-3t)$	$y^{18}-y^{15}+y^{5}+y+1$	$y^{12}-y^{11}+y^{10}-y^{9}-y^{6}+y^{5}-y^{4}+y^{3}+1$	757
205	$(t,-3t,-2t,t)$	$y^{18}-y^{5}-y^{3}-y-1$	$y^{14}-y^{12}+y^{8}-y^{6}+y^{2}-y-1$	43
206	$(t,-3t,-2t,2t)$	$y^{12}-y^{5}-y^{3}-y-1$	$y^{8}-y^{6}+y^{2}-y-1$	211
207	$(t,-3t,-2t,3t)$	$y^{6}-y^{5}-y^{3}-y-1$	$y^{2}-y-1$	211
208	$(t,-3t,-2t,-t)$	$y^{9}-y^{5}-y^{3}-y-1$	$y^{7}-y^{6}+y^{4}-2y^{3}+y^{2}-1$	43
209	$(t,-3t,-2t,-2t)$	$y^{15}-y^{5}-y^{3}-y-1$	$y^{13}-y^{12}+y^{10}-y^{9}+y^{7}-y^{6}+y^{4}-2y^{3}+y^{2}-1$	547
211	$(t,-3t,-3t,t)$	$y^{9}+y^{5}-y^{3}+y+1$	$y^{7}-y^{6}+y^{4}-y^{2}+1$	
212	$(t,-3t,-3t,2t)$	$y^{18}-y^{9}-y^{5}-y-1$	$y^{14}-y^{12}+y^{8}-y^{6}-y^{5}+y^{3}+y^{2}-y-1$	379
213	$(t,-3t,-3t,3t)$	$y^{12}-y^{9}-y^{5}-y-1$	$y^{4}-y-1$	463
214	$(t,-3t,-3t,-t)$	$y^{15}-y^{9}-y^{5}-y-1$	$y^{13}-y^{12}+y^{10}-y^{9}-y^{3}+y^{2}-1$	421
216	$(t,-3t,-3t,-3t)$	$y^{9}-y^{6}+y^{5}+y+1$	$y^{5}-y^{3}-y^{2}+y+1$	43

Table 10. All cases for 10-cycles

	(t,u,v,w)			(t,u,v,w)			(t,u,v,w)			(t,u,v,w)	
1	(t,t,t,t)		19	$(t,t,-t,t)$		37	$(t,2t,t,t)$		55	$(t,2t,-t,t)$	
2	$(t,t,t,2t)$		20	$(t,t,-t,2t)$		38	$(t,2t,t,2t)$		56	$(t,2t,-t,2t)$	
3	$(t,t,t,3t)$		21	$(t,t,-t,3t)$		39	$(t,2t,t,3t)$	x	57	$(t,2t,-t,3t)$	
4	$(t,t,t,-t)$		22	$(t,t,-t,-t)$	x	40	$(t,2t,t,-t)$		58	$(t,2t,-t,-t)$	
5	$(t,t,t,-2t)$		23	$(t,t,-t,-2t)$		41	$(t,2t,t,-2t)$		59	$(t,2t,-t,-2t)$	x
6	$(t,t,t,-3t)$	x	24	$(t,t,-t,-3t)$		42	$(t,2t,t,-3t)$		60	$(t,2t,-t,-3t)$	
7	$(t,t,2t,t)$		25	$(t,t,-2t,t)$		43	$(t,2t,2t,t)$		61	$(t,2t,-2t,t)$	
8	$(t,t,2t,2t)$		26	$(t,t,-2t,2t)$		44	$(t,2t,2t,2t)$	x	62	$(t,2t,-2t,2t)$	
9	$(t,t,2t,3t)$	x	27	$(t,t,-2t,3t)$		45	$(t,2t,2t,3t)$		63	$(t,2t,-2t,3t)$	
10	$(t,t,2t,-t)$		28	$(t,t,-2t,-t)$		46	$(t,2t,2t,-t)$		64	$(t,2t,-2t,-t)$	x
11	$(t,t,2t,-2t)$		29	$(t,t,-2t,-2t)$		47	$(t,2t,2t,-2t)$		65	$(t,2t,-2t,-2t)$	
12	$(t,t,2t,-3t)$		30	$(t,t,-2t,-3t)$		48	$(t,2t,2t,-3t)$		66	$(t,2t,-2t,-3t)$	
13	$(t,t,3t,t)$		31	$(t,t,-3t,t)$	x	49	$(t,2t,3t,t)$	x	67	$(t,2t,-3t,t)$	
14	$(t,t,3t,2t)$	x	32	$(t,t,-3t,2t)$		50	$(t,2t,3t,2t)$		68	$(t,2t,-3t,2t)$	
15	$(t,t,3t,3t)$		33	$(t,t,-3t,3t)$		51	$(t,2t,3t,3t)$		69	$(t,2t,-3t,3t)$	
16	$(t,t,3t,-t)$		34	$(t,t,-3t,-t)$		52	$(t,2t,3t,-t)$		70	$(t,2t,-3t,-t)$	
17	$(t,t,3t,-2t)$		35	$(t,t,-3t,-2t)$		53	$(t,2t,3t,-2t)$		71	$(t,2t,-3t,-2t)$	
18	$(t,t,3t,-3t)$		36	$(t,t,-3t,-3t)$		54	$(t,2t,3t,-3t)$		72	$(t,2t,-3t,-3t)$	
73	$(t,3t,t,t)$		91	$(t,3t,-t,t)$		109	$(t,-t,t,t)$		127	$(t,-t,-t,t)$	x
74	$(t,3t,t,2t)$	x	92	$(t,3t,-t,2t)$		110	$(t,-t,t,2t)$		128	$(t,-t,-t,2t)$	
75	$(t,3t,t,3t)$		93	$(t,3t,-t,3t)$		111	$(t,-t,t,3t)$		129	$(t,-t,-t,3t)$	
76	$(t,3t,t,-t)$		94	$(t,3t,-t,-t)$		112	$(t,-t,t,-t)$	x	130	$(t,-t,-t,-t)$	
77	$(t,3t,t,-2t)$		95	$(t,3t,-t,-2t)$		113	$(t,-t,t,-2t)$		131	$(t,-t,-t,-2t)$	
78	$(t,3t,t,-3t)$		96	$(t,3t,-t,-3t)$	x	114	$(t,-t,t,-3t)$		132	$(t,-t,-t,-3t)$	
79	$(t,3t,2t,t)$	x	97	$(t,3t,-2t,t)$		115	$(t,-t,2t,t)$		133	$(t,-t,-2t,t)$	
80	$(t,3t,2t,2t)$		98	$(t,3t,-2t,2t)$		116	$(t,-t,2t,2t)$		134	$(t,-t,-2t,2t)$	x
81	$(t,3t,2t,3t)$		99	$(t,3t,-2t,3t)$		117	$(t,-t,2t,3t)$		135	$(t,-t,-2t,3t)$	
82	$(t,3t,2t,-t)$		100	$(t,3t,-2t,-t)$		118	$(t,-t,2t,-t)$		136	$(t,-t,-2t,-t)$	
83	$(t,3t,2t,-2t)$		101	$(t,3t,-2t,-2t)$	x	119	$(t,-t,2t,-2t)$	x	137	$(t,-t,-2t,-2t)$	
84	$(t,3t,2t,-3t)$		102	$(t,3t,-2t,-3t)$		120	$(t,-t,2t,-3t)$		138	$(t,-t,-2t,-3t)$	
85	$(t,3t,3t,t)$		103	$(t,3t,-3t,t)$		121	$(t,-t,3t,t)$		139	$(t,-t,-3t,t)$	
86	$(t,3t,3t,2t)$		104	$(t,3t,-3t,2t)$		122	$(t,-t,3t,2t)$		140	$(t,-t,-3t,2t)$	
87	$(t,3t,3t,3t)$		105	$(t,3t,-3t,3t)$		123	$(t,-t,3t,3t)$		141	$(t,-t,-3t,3t)$	x
88	$(t,3t,3t,-t)$		106	$(t,3t,-3t,-t)$	x	124	$(t,-t,3t,-t)$		142	$(t,-t,-3t,-t)$	
89	$(t,3t,3t,-2t)$		107	$(t,3t,-3t,-2t)$		125	$(t,-t,3t,-2t)$		143	$(t,-t,-3t,-2t)$	
90	$(t,3t,3t,-3t)$		108	$(t,3t,-3t,-3t)$		126	$(t,-t,3t,-3t)$	x	144	$(t,-t,-3t,-3t)$	
145	$(t,-2t,t,t)$		163	$(t,-2t,-t,t)$		181	$(t,-3t,t,t)$	x	199	$(t,-3t,-t,t)$	
146	$(t,-2t,t,2t)$		164	$(t,-2t,-t,2t)$	x	182	$(t,-3t,t,2t)$		200	$(t,-3t,-t,2t)$	
147	$(t,-2t,t,3t)$		165	$(t,-2t,-t,3t)$		183	$(t,-3t,t,3t)$		201	$(t,-3t,-t,3t)$	x
148	$(t,-2t,t,-t)$		166	$(t,-2t,-t,-t)$		184	$(t,-3t,t,-t)$		202	$(t,-3t,-t,-t)$	
149	$(t,-2t,t,-2t)$		167	$(t,-2t,-t,-2t)$		185	$(t,-3t,t,-2t)$		203	$(t,-3t,-t,-2t)$	
150	$(t,-2t,t,-3t)$		168	$(t,-2t,-t,-3t)$		186	$(t,-3t,t,-3t)$		204	$(t,-3t,-t,-3t)$	
151	$(t,-2t,2t,t)$		169	$(t,-2t,-2t,t)$		187	$(t,-3t,2t,t)$		205	$(t,-3t,-2t,t)$	
152	$(t,-2t,2t,2t)$		170	$(t,-2t,-2t,2t)$		188	$(t,-3t,2t,2t)$		206	$(t,-3t,-2t,2t)$	
153	$(t,-2t,2t,3t)$		171	$(t,-2t,-2t,3t)$	x	189	$(t,-3t,2t,3t)$		207	$(t,-3t,-2t,3t)$	
154	$(t,-2t,2t,-t)$	x	172	$(t,-2t,-2t,-t)$		190	$(t,-3t,2t,-t)$		208	$(t,-3t,-2t,-t)$	
155	$(t,-2t,2t,-2t)$		173	$(t,-2t,-2t,-2t)$		191	$(t,-3t,2t,-2t)$		209	$(t,-3t,-2t,-2t)$	
156	$(t,-2t,2t,-3t)$		174	$(t,-2t,-2t,-3t)$		192	$(t,-3t,2t,-3t)$		210	$(t,-3t,-2t,-3t)$	x
157	$(t,-2t,3t,t)$		175	$(t,-2t,-3t,t)$		193	$(t,-3t,3t,t)$		211	$(t,-3t,-3t,t)$	
158	$(t,-2t,3t,2t)$		176	$(t,-2t,-3t,2t)$		194	$(t,-3t,3t,2t)$		212	$(t,-3t,-3t,2t)$	
159	$(t,-2t,3t,3t)$		177	$(t,-2t,-3t,3t)$		195	$(t,-3t,3t,3t)$		213	$(t,-3t,-3t,3t)$	
160	$(t,-2t,3t,-t)$		178	$(t,-2t,-3t,-t)$		196	$(t,-3t,3t,-t)$	x	214	$(t,-3t,-3t,-t)$	
161	$(t,-2t,3t,-2t)$	x	179	$(t,-2t,-3t,-2t)$		197	$(t,-3t,3t,-2t)$		215	$(t,-3t,-3t,-2t)$	x
162	$(t,-2t,3t,-3t)$		180	$(t,-2t,-3t,-3t)$	x	198	$(t,-3t,3t,-3t)$		216	$(t,-3t,-3t,-3t)$	

3. **Large conclusion**

Similar to the exactly determined girth of Tanner $(3,5)$ codes in the previous works, we showed that the girth of Tanner $(3,7)$ codes is 8 if $p=43$, 127, the girth is 10 if $p=$211, 337, 379, 421, 463, 547, 631, 757, 1429, 2437, 3109, and in the other cases the girth reachs the upper-bound 12. As an advantage, the rate of Tanner $(3,7)$ codes is about 0.17 more than the rate of Tanner $(3,5)$ codes.

Acknowledgment

This work was supported in part by the research council of Shahrekord University.

References

[1] M. P. C. Fossorier, Quasi-cyclic low-density parity-check codes from circulant permutation matrices, *IEEE Trans. Inf. Theory* **50** (2004), no. 8, 1788–1793.

[2] R. G. Gallager, Low-Density Parity-Check Codes, *Cambridge, MA: MIT. Press*, 1963.

[3] S. Kim, J.-S. No, H. Chung, and D.-J.Shin, On the girth of Tanner's $(3,5)$ quasi-cyclic LDPC codes, *IEEE Trans. Inf. Theory*, **52** (2006), no. 4, 1739–1744.

[4] R. Lucas, M. P. C Fossorier, and Y. Kou, S. Lin, Iterative decoding of onestep majority logic decodable codes based on belief propagation, *IEEE Trans. Commun.* **48** (2000), no. 6, 931-937.

[5] D. J. C. Mackay, Good error-correcting codes based on very sparse matrices, *IEEE Trans. Info. Theory* **45** (1999), no. 2, 399-431.

[6] C. E. Shannon, *The Mathematical Theory of Information*, Urbana, IL:University of IllinoisPress, 1949 (reprinted 1998).

[7] R. M. Tanner, D. Sridhara, and T. E. Fuja, A class of group-structured LDPC codes, *in Proc. Int. Symp. Communication Theory and Applications*, Ambleside, U.K., Jul. 2001.

[8] R. M. Tanner, A recursive approach to low complexity codes, *IEEE Trans. Inform. Theory*, **27** (1981), 533–547.

[9] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, LDPC Block and Convolutional Codes Based on Circulant Matrices, *IEEE Trans. Inf. Theory*, **50** (2004), no. 12, 2966–2984.

Mohammad Gholami
Department of Mathematics, Shahrekord University, P.O. Box 115, Shahrekord, Iran,
Email: gholami-m@sci.sku.ac.ir
Email: gholamimoh@gmail.com

Fahime Sadat Mostafaiee
Department of Mathematics, Malek Ashtar University of Technology, P.O.Box 115/83145, Shahin-Shahr, Iran
Email: fmostafaiee@yahoo.com