Girth Analysis of Tanner's $(3,5)$ QC LDPC Codes[1]

Sunghwan Kim, Jong-Seon No
School of Electrical Eng. & Com. Sci.
Seoul National University, Seoul, Korea
Email: {nodoubt, jsno}@snu.ac.kr

Habong Chung
School of Electron. & Electrical Eng.
Hong-Ik University, Seoul, Korea
Email: habchung@wow.hongik.ac.kr

Dong-Joon Shin
Division of Electrical & Com. Eng.
Hanyang University, Seoul, Korea
Email: djshin@hanyang.ac.kr

***Abstract*— In this paper, the cycles of Tanner's $(3,5)$ quasi-cyclic (QC) low-density parity-check (LDPC) codes are analyzed and their girth values are derived. The conditions for the existence of cycles of lengths 4, 6, 8, and 10 in Tanner's $(3,5)$ QC LDPC codes of length $5p$ are expressed in terms of polynomial equations in a 15-th root of unity of the prime field F_p. By checking the existence of solutions for these equations over F_p, the girths of Tanner's $(3,5)$ QC LDPC codes are derived.**

I. Introduction

It is well known that the performance of randomly constructed irregular low-density parity-check (LDPC) codes closely approach the Shannon limit for the additive white Gaussian noise (AWGN) channel as the code length becomes larger [4]. However, for short to medium lengths (say, less than 5,000 information bits), regular LDPC codes can perform better than irregular ones and algebraically constructed regular LDPC codes outperform randomly constructed ones. A quasi-cyclic (QC) LDPC code [1], [2], [5] can be considered as one of such algebraic constructions, which is based on circulant permutation matrices. QC LDPC codes can be encoded in linear time with shift registers [3] and require small memory space to store the code graph for decoding, especially compared with randomly constructed codes.

QC LDPC codes are (J,L) regular LDPC codes of length Lp whose parity check matrix H is a $J\times L$ array of $p\times p$ circulant permutation matrices [1]. Since the cycle structures in QC LDPC codes are determined by the shift values of circulant permutation matrices, it is important to find the proper shift values which make no short cycles. Shift values can be selected either randomly or algebraically. In the random selection of shift values, it takes too much computations to find the proper shift values which yield a large girth. Therefore, it is desirable to have algebraic methods to find good shift values. Few such methods have been known to guarantee a large girth and Tanner's QC LDPC code [5] is one of such constructions. Using computer search, it is shown that Tanner's $(3,5)$ QC LDPC codes with prime p of the form $15m+1$ mostly have girth 12 [5], which is the maximum girth that QC LDPC codes can have. However, the theoretical analysis for girths of Tanner's $(3,5)$ QC LDPC codes cannot be found in any literature.

In this paper, the cycles of Tanner's $(3,5)$ QC LDPC codes of length $5p$, where p is a prime of the form $15m+1$, are analyzed and their girth values are derived. The conditions for the existence of cycles of lengths 4, 6, 8, and 10 in Tanner's $(3,5)$ QC LDPC codes are expressed in terms of polynomial equations in a 15-th root of unity of the prime field F_p. By checking the existence of solutions for these equations over F_p, the girths of Tanner's $(3,5)$ QC LDPC codes are derived.

[1]This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications.

II. Cycles in Tanner's (3, 5) QC LDPC Codes

The parity check matrix of (J,L) QC LDPC codes of length $n=Lp$ can be represented by using $p\times p$ circulant permutation matrices [1] as

$$H=\begin{bmatrix} I(p_{0,0}) & I(p_{0,1}) & \cdots & I(p_{0,L-1}) \\ I(p_{1,0}) & I(p_{1,1}) & \cdots & I(p_{1,L-1}) \\ \vdots & & \cdots & \vdots \\ I(p_{J-1,1}) & I(p_{J-1,1}) & \cdots & I(p_{J-1,L-1}) \end{bmatrix}$$

where $p_{j,l}$, $0\le j\le J-1$ and $0\le l\le L-1$, is an integer $\bmod p$ and $I(p_{j,l})$ is the $p\times p$ circulant permutation matrix with 1 at column $(r+p_{j,l}) \bmod p$ for row r, $0\le r\le p-1$. It follows that $I(0)$ represents the $p\times p$ identity matrix.

Since each $p\times p$ block, $I(p_{j,l})$, of H is a permutation matrix, a cycle in the graph of a QC LDPC code can be considered as a sequence of corresponding blocks. As in [1], a cycle of length $2i$ in a QC LDPC code is expressed as a block sequence

$$(j_0,l_0);(j_1,l_1);\cdots;(j_k,l_k);\cdots;(j_{i-1},l_{i-1});(j_0,l_0) \quad (1)$$

where (j_k,l_k) stands for the j_k-th row and l_k-th column block, $I(p_{j_k,l_k})$, of H and semicolon between (j_k,l_k) and (j_{k+1},l_{k+1}) can be considered as the block (j_{k+1},l_k). Certainly, $j_k\neq j_{k+1}$ and $l_k\neq l_{k+1}$ for (1) to become a valid block sequence for a cycle. Note that in the representation of a cycle by the block sequence as in (1), some blocks can appear more than once. It is stated in [1] that the necessary and sufficient condition for the existence of the cycle of length $2i$ represented as in (1) is

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

where $j_i=j_0$, $j_k\neq j_{k+1}$, and $l_k\neq l_{k+1}$.

A Tanner's (J,L) QC LDPC code [5] is the one with $p_{j,l}=b^j a^l$, for $0\le j\le J-1$ and $0\le l\le L-1$, where a and b are nonzero integers with orders L and J in the prime field F_p, respectively. We will focus on the case of $J=3$ and $L=5$

in Tanner's QC LDPC codes, where p is a prime and $p-1$ must be some multiple of 15.

Let α be a primitive 15-th root of unity in F_p. Then the shift values become

$$p_{j,l} = \alpha^{5j+3l}, \quad 0 \le j \le 2,\ 0 \le l \le 4,$$

which, in turn, yields the parity-check matrix H given as

$$H = \begin{bmatrix} I(\alpha^0) & I(\alpha^3) & I(\alpha^6) & I(\alpha^9) & I(\alpha^{12}) \\ I(\alpha^5) & I(\alpha^8) & I(\alpha^{11}) & I(\alpha^{14}) & I(\alpha^2) \\ I(\alpha^{10}) & I(\alpha^{13}) & I(\alpha^1) & I(\alpha^4) & I(\alpha^7) \end{bmatrix}.$$

Here, we are going to classify the cycles of length $2i$ in Tanner's (3, 5) QC LDPC code into distinct groups based on sequences of their row block indices. More specifically, we say that the cycles of length $2i$ represented in (1) belong to the group $(j_0, j_1, \cdots, j_{i-1})$. Then we can define the equivalence relation between groups as follows:

Definition 1: Two groups $(j_0, j_1, \cdots, j_{i-1})$ and $(j'_0, j'_1, \cdots, j'_{i-1})$ in Tanner's $(3,5)$ QC LDPC codes are said to be equivalent if either of the following conditions is satisfied:

i) There exists some $r \in \{0,1,2\}$ such that $j'_k = j_k + r$ (mod 3), for all k.

ii) $j'_k = 2j_k$ (mod 3), for all k.

iii) There exists some $d \in \{0, 1, \cdots, i-1\}$ such that $j'_k = j_{k+d}$, for all k.

iv) There exists some $d \in \{0, 1, \cdots, i-1\}$ such that $j'_k = j_{i-1-k+d}$, for all k. □

The next lemma which we state without proof justifies why we introduced the equivalence relation between groups.

Lemma 1: In Tanner's $(3,5)$ QC LDPC codes, if there exists a cycle of length $2i$ belonging to a group $(j_0, j_1, \cdots, j_{i-1})$, then there must be a cycle belonging to each of the groups $(j'_0, j'_1, \cdots, j'_{i-1})$ equivalent to $(j_0, j_1, \cdots, j_{i-1})$. □

Under the equivalence relation in Definition 1, the set of groups is partitioned into equivalent classes. Then it is not difficult to see that all the cycles of length 4 belong to the unique class $(0,1)$, and all the cycles of length 6 belong to the unique class $(0,1,2)$. Similarly, we can see that there are two inequivalent classes, namely $(0,1,0,1)$ and $(0,1,0,2)$, for the cycles of length 8, and the unique class $(0,1,2,0,1)$ for the cycles of length 10.

Now, what we are going to do next is to check whether the following equation obtained by substituting $p_{j,l}$ by α^{5j+3l} in (2),

$$\sum_{k=0}^{i-1} \left(\alpha^{5j_k} - \alpha^{5j_{k+1}}\right) \alpha^{3l_k} = 0 \mod p \quad (3)$$

is satisfied for the cycles from each of the equivalent classes $(j_0, j_1, \cdots, j_{i-1})$ upto $i = 5$. Since (3) can be rewritten as

$$\alpha^{3l_0} \sum_{k=0}^{i-1} \left(\alpha^{5j_k} - \alpha^{5j_{k+1}}\right) \alpha^{3(l_k - l_0)} = 0 \mod p,$$

we can assume, without loss of generality, that $l_0 = 0$. Let $t = l_1 - l_0 \mod 5$, $u = l_2 - l_1 \mod 5$, $v = l_3 - l_2 \mod 5$, and $w = l_4 - l_3 \mod 5$. Then t, u, v, and w take the values in $\{\pm 1, \pm 2\}$. Then the representations in (1) of cycles of length upto 10 and their existence conditions are given as:

(i) For 4-cycles in the class $(0,1)$:
$(0,0); (1,t)$, where $t \neq 0$.

$$\begin{aligned} &1 - \alpha^5 + \alpha^{3t+5} - \alpha^{3t} \\ &= (1-\alpha^5)(1-\alpha^{3t}) = 0 \mod p. \end{aligned} \quad (4)$$

(ii) For 6-cycles in the class $(0,1,2)$:
$(0,0); (1,t); (2, t+u)$, where $t + u \neq 0 \mod 5$.

$$\begin{aligned} &1 - \alpha^5 + \alpha^{3t+5} - \alpha^{3t-5} + \alpha^{3(t+u)-5} - \alpha^{3(t+u)} \\ &= (1-\alpha^5)(1 + \alpha^{3t+5} + \alpha^{3(t+u)-5}) = 0 \mod p. \end{aligned} \quad (5)$$

(iii) For 8-cycles in the class $(0,1,0,1)$:
$(0,0); (1,t); (0,t+u); (1,t+u+v)$, where $t+u+v \neq 0 \mod 5$.

$$\begin{aligned} &1 - \alpha^5 + \alpha^{3t+5} - \alpha^{3t} + \alpha^{3(t+u)} - \alpha^{3(t+u)+5} \\ &+ \alpha^{3(t+u+v)+5} - \alpha^{3(t+u+v)} \\ &= (1-\alpha^5)(1 - \alpha^{3t} + \alpha^{3(t+u)} - \alpha^{3(t+u+v)}) \\ &= 0 \mod p. \end{aligned} \quad (6)$$

(iv) For 8-cycles in the class $(0,1,0,2)$:
$(0,0); (1,t); (0,t+u); (2,t+u+v)$, where $t+u+v \neq 0 \mod 5$.

$$\begin{aligned} &1 - \alpha^5 + \alpha^{3t+5} - \alpha^{3t} + \alpha^{3(t+u)} - \alpha^{3(t+u)-5} \\ &+ \alpha^{3(t+u+v)-5} - \alpha^{3(t+u+v)} \\ &= (1-\alpha^5)(1 - \alpha^{3t} - \alpha^{3(t+u)-5} + \alpha^{3(t+u+v)-5}) \\ &= 0 \mod p. \end{aligned} \quad (7)$$

(v) For 10-cycles in the class $(0,1,2,0,1)$:
$(0,0); (1,t); (2,t+u); (0,t+u+v); (1,t+u+v+w)$, where $t+u+v+w \neq 0 \mod 5$.

$$\begin{aligned} &1 - \alpha^5 + \alpha^{3t+5} - \alpha^{3t-5} + \alpha^{3(t+u)-5} - \alpha^{3(t+u)} + \alpha^{3(t+u+v)} \\ &- \alpha^{3(t+u+v)+5} + \alpha^{3(t+u+v+w)+5} - \alpha^{3(t+u+v+w)} \\ &= (1-\alpha^5)(1 + \alpha^{3t+5} + \alpha^{3(t+u)-5} + \alpha^{3(t+u+v)} \\ &\quad -\alpha^{3(t+u+v+w)}) = 0 \mod p. \end{aligned} \quad (8)$$

III. Girth for Tanner's $(3,5)$ QC LDPC Codes

The girth of a Tanner's $(3,5)$ QC LDPC code can be summarized as in the following theorem.

Theorem 1: The girth g of Tanner's (3,5) QC LDPC codes of length $5p$ is given as

$$g = \begin{cases} 8, & \text{if } p = 31 \\ 10, & \text{if } p = 61 \text{ or } 151 \\ 12, & \text{if } p \in P_{15} \backslash \{31, 61, 151\}, \end{cases}$$

where P_{15} is the set of prime numbers p of the form $15m+1$, m a positive integer. □

To prove the above theorem, we investigate the existence of cycles of length 4, 6, 8, and 10 for all possible values of p.

A. 4-cycles

Since α is a primitive 15-th root of unity, $\alpha^5 \neq 1$ and $\alpha^{3t} \neq 1$. Thus (4) cannot be satisfied, which, in turn, implies the nonexistence of 4-cycles.

B. 6-cycles

Since $t + u \neq 0$ mod 5, the only possible cases are $u = t$, $2t$, and $-2t$. Again $\alpha^5 \neq 1$, so the existence condition in (5) becomes

$$1 + \alpha^{3t+5} + \alpha^{3t+3u-5} = 0 \mod p. \tag{9}$$

For each of the above three cases, (9) can be modified as

$$\begin{aligned} &1 + \alpha^{3t+5} + \alpha^{6t-5} \\ &\quad = 1 + \alpha^{3t+5} + (\alpha^{3t+5})^2 = 0 \mod p, \quad \text{for } u = t \end{aligned}$$

$$\begin{aligned} &1 + \alpha^{3t+5} + \alpha^{9t-5} \\ &\quad = 1 + \alpha^{9t-5} + (\alpha^{9t-5})^2 = 0 \mod p, \quad \text{for } u = 2t \end{aligned}$$

$$\begin{aligned} &1 + \alpha^{3t+5} + \alpha^{-3t-5} = \alpha^{-3t-5}\left(1 + \alpha^{3t+5} + (\alpha^{3t+5})^2\right) \\ &\quad = 0 \mod p, \quad \text{for } u = -2t. \end{aligned}$$

These equations do not have solutions since α^{3t+5} and α^{9t-5} are not a third root of unity. Thus, there are no cycles of length 6 in Tanner's (3, 5) QC LDPC codes.

C. 8-cycles

Again since $\alpha^5 \neq 1$, the existence conditions (6) and (7) become

$$1 - \alpha^{3t} + \alpha^{3t+3u} - \alpha^{3t+3u+3v} = 0 \mod p \tag{10}$$

and

$$1 - \alpha^{3t} - \alpha^{3t+3u-5} + \alpha^{3t+3u+3v-5} = 0 \mod p, \tag{11}$$

respectively.

Table I shows all possible combinations of (t, u, v) in terms of t. In Table I, 'x' means the cases of $t + u + v = 0$ mod 5, which should be excluded. Thus there remain 13 cases to be considered.

TABLE I

(t, u, v) FOR 8-CYCLES.

	(t,u,v)			(t,u,v)	
1	(t,t,t)		9	$(t,-t,t)$	
2	$(t,t,2t)$		10	$(t,-t,2t)$	
3	$(t,t,-t)$		11	$(t,-t,-t)$	
4	$(t,t,-2t)$	x	12	$(t,-t,-2t)$	
5	$(t,2t,t)$		13	$(t,-2t,t)$	x
6	$(t,2t,2t)$	x	14	$(t,-2t,2t)$	
7	$(t,2t,-t)$		15	$(t,-2t,-t)$	
8	$(t,2t,-2t)$		16	$(t,-2t,-2t)$	

As mentioned in the previous section, all 8-cycles belong to either the equivalence class $(0, 1, 0, 1)$ or $(0, 1, 0, 2)$.

1) The class $(0, 1, 0, 1)$*:* Note that all the terms in the left-hand side of (10) are the 5-th roots of unity. Thus, by setting $z = \alpha^{3t}$, (10) for each of the above 13 cases becomes some polynomial equation in z. Also, z is a primitive 5-th root of unity which should satisfy

$$z^4 + z^3 + z^2 + z + 1 = 0. \tag{12}$$

Therefore, for a cycle in the equivalent class $(0, 1, 0, 1)$ to exist, (12) and the polynomial equation in z obtained from (10) should have at least one common solution in F_p.

Next, we will give the detailed explanation about the nonexistence of a common solution in F_p for two cases in Table I. The remaining 11 cases can be done similarly, and the tips are summarized in Table II.

i) The case of (t, t, t):
Equation (10) becomes

$$1 - z + z^2 - z^3 = -(z - 1)(z^2 + 1) = 0 \mod p,$$

which cannot be true since z is a primitive 5-th root of unity.

ii) The case of $(t, -2t, 2t)$:
Equation (10) becomes

$$1 - z + z^4 - z = (z - 1)(z^3 + z^2 + z - 1) = 0 \mod p.$$

Since $z \neq 1$, $z^3 + z^2 + z - 1 = 0 \mod p$. By applying the Euclidean division algorithm to (12) and $z^3 + z^2 + z - 1$, we have

$$z^4 + z^3 + z^2 + z + 1 = z(z^3 + z^2 + z - 1) + 2z + 1$$

$$z^3 + z^2 + z - 1 = \frac{1}{8}(4z^2 + 2z + 3)(2z + 1) - \frac{11}{8}$$

It is clear that the remainder $-11/8$ of the last division cannot be zero in F_p, $p \in P_{15}$. Thus $(0, 0); (1, t); (0, -t); (1, t)$ cannot be a cycle.

We summarize the results of all 13 cases in Table II. In the third column, 'Original form' of Table II, we rewrite (10) by replacing α^{3t} by z. Next column, 'Reduced form' lists the factors of the original form survived after removing those factors such as z, $z - 1$, $z + 1$, $z^2 + 1$, $z^2 - z + 1$, and $z^2 + z + 1$, which are obviously nonzero for any p in P_{15}. In the last column, 'p' of Table II, we put the value of p for the existence of corresponding 8-cycles. We have proved that there are no cycles of length 8 in the class $(0, 1, 0, 1)$.

2) The class $(0, 1, 0, 2)$*:* By setting $y = \alpha^{3t+5}$, (11) for each of 13 cases in Table I becomes some polynomial equation in y. In Table III y^i, $1 \leq i \leq 14$, can be represented as the powers of α.

Since $y^{15} - 1$ is factorized as

$$\begin{aligned} y^{15} - 1 = (y - 1)(y^2 + y + 1)(y^4 + y^3 + y^2 + y + 1) \\ \times (y^8 - y^7 + y^5 - y^4 + y^3 - y + 1) \end{aligned}$$

and y is a primitive 15-th root of unity, we have

$$y^8 - y^7 + y^5 - y^4 + y^3 - y + 1 = 0. \tag{13}$$

TABLE II

EXISTENCE OF 8-CYCLES IN $(0,1,0,1)$.

	(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	$(t,t,-t)$	$(z-1)^2$		
5	$(t,2t,t)$	z^4-z^3+z-1		
7	$(t,2t,-t)$	z^3-z^2-z+1		
8	$(t,2t,-2t)$	z^3-2z+1	z^2+z-1	
9	$(t,-t,t)$	$2(z-1)$		
10	$(t,-t,2t)$	z^2+z-2	$z+2$	
11	$(t,-t,-t)$	z^4+z-2	z^3+z^2+z+2	
12	$(t,-t,-2t)$	z^3+z-2	z^2+z+2	
14	$(t,-2t,2t)$	z^4-2z+1	z^3+z^2+z-1	
15	$(t,-2t,-t)$	z^4-z^3-z+1		
16	$(t,-2t,-2t)$	z^4-z^2-z+1	z^3+z^2-1	

TABLE III

REPRESENTATION OF y^i.

y	α^{3t+5}	y^8	α^{9t-5}
y^2	α^{6t-5}	y^9	α^{12t}
y^3	α^{9t}	y^{10}	α^5
y^4	α^{12t+5}	y^{11}	α^{3t-5}
y^5	α^{-5}	y^{12}	α^{6t}
y^6	α^{3t}	y^{13}	α^{9t+5}
y^7	α^{6t+5}	y^{14}	α^{12t-5}

It is clear that y also has to satisfy the following equation

$$y^{10}+y^5+1=0. \tag{14}$$

Therefore, for a cycle in equivalence class $(0,1,0,2)$ to exist, (13) and the polynomial equation in y obtained from (11) should have at least one common solution in F_p.

Like the previous class, we will give the detailed explanation about the existence of a common solution in F_p for a case $(t,2t,-2t)$ in Table I. The remaining 12 cases can be done similarly, and the tips are summarized in Table IV.

Using y^i in Table III, (11) becomes

$$1-y^6-y^8+y^{11}=0 \mod p.$$

By multiplying y^{10} on both sides and using (14), the above equation can be modified as

$$\begin{aligned} &y^6-y^5-y^3-y-1\\ &\quad=(y^2-y+1)(y^2+y+1)(y^2-y-1)=0 \mod p. \end{aligned}$$

Since y is neither a third root nor a 6-th root of unity, we have $y^2-y-1=0 \mod p$. By applying the Euclidean division algorithm to (13) and y^2-y-1, the remainder polynomials become

$$11y+8, \quad \frac{31}{11^2}.$$

It is clear that the remainder $31/11^2$ of the last division is equal to zero in F_{31} and $y^2-y-1=0 \mod p$ has a solution, namely $y=19$ when p is 31. Thus, cycles of length 8 in the case of $(t,2t,-2t)$ exist when p is 31.

Similarly to Table II, we summarize the results of all 13 cases in Table IV. We have proved that when $p=31$, there are cycles of length 8 in the class $(0,1,0,2)$.

TABLE IV

EXISTENCE OF 8-CYCLES IN $(0,1,0,2)$.

	Original form	Reduced form	p
1	$y^8-y^6-y^2+1$		
2	$y^{14}-y^6-y^2+1$	y^4+y+1	
3	$y^{11}-y^6-y^2+1$	y^4-2y^3+2y-2	
5	$y^{14}-y^8-y^6+1$		
7	$y^8+y^6-y^2-1$	y^3-y+1	
8	$y^{11}-y^8-y^6+1$	y^2-y-1	31
9	$y^{11}-y^6-y^5+1$	$y^4-2y^3+y^2+y-2$	
10	$y^6+y^5-y^2-1$	y^3+y^2+1	31
11	$y^{14}-y^6-y^5+1$	y^3-y+1	
12	$y^8-y^6-y^5+1$	y^3-y^2-y+2	31
14	$y^{14}-y^{11}+y^6-1$	y^3-2y^2+2	31
15	$y^{14}-y^8+y^6-1$		
16	$y^{14}+y^6-y^2-1$	y^4-y+1	

D. 10-cycles

Since $\alpha^5\neq 1$, the existence condition (8) becomes

$$1+\alpha^{3t+5}+\alpha^{3t+3u-5}+\alpha^{3t+3u+3v}-\alpha^{3t+3u+3v+3w}=0 \mod p. \tag{15}$$

Similarly to the previous subsection, we excluded the 13 cases (t,u,v,w) such that $t+u+v+w=0 \mod 5$. We will give the detailed explanation about the existence of a common solution of (13) and (15) in F_p for 3 cases. The remaining 48 cases can be done similarly, and the tips are summarized in Table V.

i) The case of $(t,t,2t,-t)$:

By using y^i in Table III, (15) becomes

$$1+y+y^2+y^9-y^3=0 \mod p.$$

By multiplying y on both sides and using (14), we have

$$(y-1)(y^2+y+1)(y^2+y-1)=0 \mod p.$$

Since $y\neq 1$ and $y^3\neq 1$, y should satisfy $y^2+y-1=0 \mod p$. By applying Euclidean division algorithm to (13) and y^2+y-1, the remainder polynomials become

$$-25y+16, \quad \frac{31}{5^4}.$$

It is clear that the remainder $31/5^4$ of the last division is equal to zero in F_{31} and $y^2+y-1=0 \mod p$ has a solution, namely $y=18$, when p is 31. Thus, the cycles of length 10 in the case of $(t,t,2t,-t)$ exist when p is 31.

ii) The case of $(t,t,2t,2t)$:

By using y^i in Table III, (15) becomes

$$1+y+y^2+y^9-y^6=0 \mod p.$$

By multiplying y on both sides and using (14), we have

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

Since $y \neq -1$ and $y^3 \neq 1$, y should satisfy $y^3-y^2+2y-1=0 \mod p$. By applying Euclidean division algorithm to (13) and $y^3 - y^2 + 2y - 1$, the remainder polynomials become

$$-4y^2 - 2y + 3, \quad \frac{1}{2^3}(28y - 17), \quad \frac{61}{2^2 7^2}.$$

It is clear that the remainder $61/2^2 7^2$ of the last division is equal to zero in F_{61} and $y^3 - y^2 + 2y - 1 = 0 \mod p$ has a solution, namely $y = 42$, when p is 61. Thus, the cycles of length 10 in the case of $(t, t, 2t, 2t)$ exist when p is 61.

iii) The case of $(t, t, -2t, t)$:

By using y^i in Table III, (15) becomes

$$\begin{aligned} 1 + y + y^2 + 1 - y^6 &= (y^2 + y + 1)(y^4 - y^3 + y - 2) \\ &= 0 \mod p. \end{aligned}$$

Since y is not a third root of unity, we have $y^4-y^3+y-2=0 \mod p$. By applying the Euclidean division algorithm to (13) and $y^4 - y^3 + y - 2$, the remainder polynomials become

$$2y^3 - 2y + 3, \quad \frac{1}{2}(2y^2 - 3y - 1), \quad \frac{1}{2}(7y + 9), \quad \frac{151}{7^2}.$$

It is clear that the remainder $151/7^2$ of the last division is equal to zero in F_{151} and $y^4 - y^3 + y - 2 = 0 \mod p$ has a solution, namely $y = 85$, when p is 151. Thus, the cycles of length 10 in the case of $(t, t, -2t, t)$ exist when p is 151.

Similarly to Tables II and IV, we summarize the results of all 51 cases in Table V. When p is in $P_{15}\backslash\{31, 61, 151\}$, the girth is greater than 10. It is known [5] [1] that QC LDPC codes have girth not greater than 12. Thus when p is in $P_{15}\backslash\{31, 61, 151\}$, the girth of Tanner's $(3, 5)$ QC LDPC codes is 12.

IV. Conclusions

In this paper, conditions for cycles of lengths 4, 6, 8, and 10 in Tanner's (3, 5) QC LDPC codes are expressed as simple polynomial equations in a primitive 15-th root of unity in F_p. By checking the existence of solutions for these equations, their girths are derived. When p is 31, the girth of the code is 8, and when p is 61 or 151, the girth of the code is 10. For the remaining values p in $P_{15}\backslash\{31, 61, 151\}$, the girth becomes 12. Similarly to $(3, 5)$ case, the other Tanner's (J, L) QC LDPC codes can also be analyzed.

References

[1] M. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inform. Theory*, vol. 50, no. 8, pp. 1788-1793, Aug. 2004.

[2] N. Miladinovic and M. Fossorier, "Systematic recursive construction of LDPC codes," *IEEE Commun. Lett.*, vol. 8, no. 5, pp. 302-304, May 2004.

[3] W. W. Peterson and E. J. Weldon Jr., *Error-correcting codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

[4] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 619-637, Feb. 2001.

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

TABLE V

Existence of 10-cycles.

	(t,u,v,w)	Reduced form	p
1	(t,t,t,t)		
3	$(t,t,t,-t)$	y^4+y-1	
4	$(t,t,t,-2t)$	y^4-y^3-1	
6	$(t,t,2t,2t)$	y^3-y^2+2y-1	61
7	$(t,t,2t,-t)$	y^2+y-1	31
8	$(t,t,2t,-2t)$	y^4-y^2-1	31
9	$(t,t,-t,t)$	y^3+y+1	31
10	$(t,t,-t,2t)$	y^4-y^3+1	
12	$(t,t,-t,-2t)$	y^3-y^2+1	
13	$(t,t,-2t,t)$	y^4-y^3+y-2	151
14	$(t,t,-2t,2t)$	y^3-y^2-y+2	31
15	$(t,t,-2t,-t)$	y^3-y^2+y+1	61
16	$(t,t,-2t,-2t)$	$y-2$	151
18	$(t,2t,t,2t)$	y^4-2y^2+y+1	
19	$(t,2t,t,-t)$	$y^4+y^3-2y^2+1$	
20	$(t,2t,t,-2t)$	y^5-y^3+1	
21	$(t,2t,2t,t)$	y^3-2y+2	31
22	$(t,2t,2t,2t)$	y^3-y-1	61
23	$(t,2t,2t,-t)$	$y^4-2y^3+y^2+2y-1$	151
24	$(t,2t,2t,-2t)$	$2y^2-1$	151
25	$(t,2t,-t,t)$	$2y^2-2y-1$	61
26	$(t,2t,-t,2t)$	$y^5-2y^4+y^3+2y^2-2y+1$	31
27	$(t,2t,-t,-t)$	y^2-y-1	31
29	$(t,2t,-2t,t)$	y^5-y^4+1	
30	$(t,2t,-2t,2t)$	$2y^5-2y^4+y^2-y+1$	
32	$(t,2t,-2t,-2t)$	y^4-y+1	
33	$(t,-t,t,t)$		
34	$(t,-t,t,2t)$	y^4-y^2+1	
36	$(t,-t,t,-2t)$		
37	$(t,-t,2t,t)$	y^3-y^2+1	
38	$(t,-t,2t,2t)$	y^4-2y^3+y-1	
39	$(t,-t,2t,-t)$	y^4-2y^3+2y-2	
42	$(t,-t,-t,2t)$	y^3-2y+2	31
43	$(t,-t,-t,-t)$		
44	$(t,-t,-t,-2t)$	y^4-y+1	
45	$(t,-t,-2t,t)$		
47	$(t,-t,-2t,-t)$	y^3-y^2+1	
48	$(t,-t,-2t,-2t)$	y^2-y-1	31
49	$(t,-2t,t,t)$	$2y^2-2y+1$	61
50	$(t,-2t,t,2t)$	y^2+y-1	31
51	$(t,-2t,t,-t)$	y^2-2y+2	61
52	$(t,-2t,t,-2t)$	y^2-y-1	31
53	$(t,-2t,2t,t)$		
54	$(t,-2t,2t,2t)$	y^5-y^4+1	
56	$(t,-2t,2t,-2t)$	y^3+y^2+1	31
57	$(t,-2t,-t,t)$	y^3-y+2	31
59	$(t,-2t,-t,-t)$	$y^4-y^3+y^2+y-1$	31
60	$(t,-2t,-t,-2t)$	y^3-y-1	61
61	$(t,-2t,-2t,t)$	$y^4-y^3-y^2+y-1$	31
62	$(t,-2t,-2t,2t)$	$y^5-y^4+2y^2-y+1$	61
63	$(t,-2t,-2t,-t)$	$2y^3-y^2+1$	31