Construction of Protographs for QC LDPC Codes With Girth Larger Than 12[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 Electron. & Com. Eng.
Hanyang University, Seoul, Korea
Email: djshin@hanyang.ac.kr

***Abstract*— A quasi-cyclic (QC) low-density parity-check (LDPC) code can be viewed as the protograph code with circulant permutation matrices. In this paper, we find all the subgraph patterns of protographs of QC LDPC codes having inevitable cycles of length $2i$, $i = 6,7,8,9,10$, i.e., the cycles existing regardless of the shift values of circulants. It is also derived that if the girth of the protograph is $2g$, $g \geq 2$, its protograph code cannot have the inevitable cycles of length smaller than $6g$. Based on these subgraph patterns, we propose new combinatorial construction methods of the protographs, whose protograph codes can have girth larger than or equal to 14. We also propose a couple of shift value assigning rules for circulants of a QC LDPC code guaranteeing the girth 14.**

I. Introduction

Since the low-density parity-check (LDPC) code exhibits the capacity-approaching performance for many channels such as binary erasure channel (BEC), binary symmetric channel (BSC), and additive white Gaussian noise (AWGN) channel, it has been one of the major research topics for many coding theorists at least for the last decade. It is known that the message-passing decoder of LDPC codes is relatively easy to implement due to the sparseness of the parity-check matrix, but the encoding complexity of LDPC codes is quite high. Thus many researchers have been working on designing efficiently encodable LDPC codes.

Although the random construction shows good asymptotic performance, its randomness hinders the ease of analysis and implementation. In an effort toward the algebraic constructions of LDPC codes, a quasi-cyclic (QC) LDPC code is getting more attention due to its linear-time encodability and small size of required memory.

A (J, L) regular LDPC code is defined in terms of a parity-check matrix H in which each column contains J 1's and each row contains L 1's. Originally, a QC LDPC code is defined as a (J, L) regular LDPC code of length Lp whose parity-check matrix H is a $J \times L$ array of $p \times p$ circulant permutation matrices (shortly, circulants) [1]. Fossorier derived a necessary and sufficient condition for the existence of cycles of given length in QC LDPC codes. Fossorier [1] and Tanner [2] also showed that these QC LDPC codes have a girth at most 12.

Zhong and Zhang [3] proposed the construction method of block-type LDPC codes which are suitable for the encoder/decoder hardware implementation. Vasic and Milenkovic [4], and Ammar, Honary, Kou, Xu, and Lin [5] introduced new combinatorial constructions of LDPC codes which have good structures for low-complexity implementation. Myung, Yang, and Kim [6] proposed the fast encoding algorithm for a special class of QC LDPC codes and derived the upper bound of their girths.

O'Sullivan, Brevik, and Wolski [7] proposed a construction method of LDPC codes by using a seed matrix which is the concatenation of two incidence matrices for Fano planes and circulant permutation matrices. They showed one special case of constructing an LDPC code with girth 14 by using the Magma algorithm. Milenkovic and Laendner [8] proposed structured LDPC codes with girth 6 by using Latin squares and Steiner triple systems.

In this paper, we find all the subgraph patterns of protographs of QC LDPC codes having inevitable cycles of length upto 20 i.e., the cycles existing regardless of the shift values of circulants. Also, we derive the relation between the girth of the protograph and the inevitable cycle length of its protograph code. Based on these subgraph patterns, we propose new combinatorial construction methods of the protographs, whose protograph codes can have girth larger than or equal to 14, and a couple of shift value assigning rules for circulants of a QC LDPC code guaranteeing the girth 14.

II. QC LDPC Codes

A conventional (J, L) QC LDPC code of length $n = Lp$ can be defined as the one with the parity-check matrix given by a $J \times L$ array of $p \times p$ circulant permutation matrices shown as

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

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

A cycle in the bipartite graph of a QC LDPC code can be considered as a sequence of the corresponding $p \times p$ permuta-

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

tion matrices. Thus a cycle of length $2i$ in a conventional QC LDPC code can be expressed as the following sequence

$$(j_0, l_0); (j_1, l_1); \cdots ; (j_k, l_k); \cdots ; (j_{i-1}, l_{i-1}); (j_0, l_0) \quad (2)$$

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, we have $j_k \neq j_{k+1}$ and $l_k \neq l_{k+1}$ for (2) to be a valid expression for a cycle. Fossorier [1] showed that the necessary and sufficient condition for the existence of the cycle of length $2i$ is

$$\sum_{k=0}^{i-1} (p_{j_k,l_k} - p_{j_{k+1},l_k}) = 0 \mod p \quad (3)$$

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

It is known that the girth of any conventional QC LDPC code in (1) is upper-bounded by 12 [1]. That is, there always exist the cycles of length 12 in the QC LDPC codes regardless of p and the shift values of circulants. Such a cycle is depicted in Fig. 1.

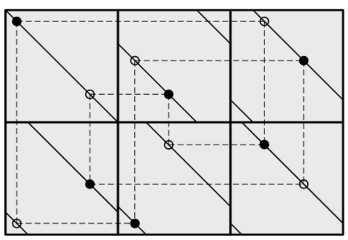


Fig. 1. An inevitable cycle of length 12 in QC LDPC codes.

Let us define the incidence matrix of the bipartite graph with two groups, G_1 of check nodes and G_2 of variable nodes, as the $|G_1| \times |G_2|$ matrix $M = [m_{ij}]$ such that $m_{ij} = 1$ if the i-th node in G_1 is connected to the j-th node in G_2 and $m_{ij} = 0$, otherwise.

Thorpe [9] proposed a new method of constructing LDPC codes from a bipartite graph with relatively small number of variable nodes and check nodes, called a *protograph*. A protograph is copied p times and the endpoints of copied edges of the same type are permuted to result in the larger graph. Then, the incidence matrix of this larger graph can serve as a parity-check matrix of an LDPC code, called a protograph code. It is manifest that the parity-check matrix of a protograph code can be obtained from the incidence matrix of protograph with the replacement of each 1 and 0 by some $p \times p$ permutation and zero matrices, respectively. Then, a conventional (J, L) QC LDPC code of length Lp in (1) can be regarded as a protograph code obtained by the replacement of 1's in a fully-connected protograph with $p \times p$ circulants.

In this paper, we are only considering the quasi-cyclic type protograph codes obtained from the replacement of 1's with circulants. Thus, hereafter the term protograph code implies the one so obtained. We will also use the terms 'the incidence matrix of the protograph' and 'the protograph', interchangeably.

Certainly, the girth of the protograph code depends on the protograph and the shift values of circulants. In the next section, we obtain all the inevitable cycle patterns of length $2i$, $6 \leq i \leq 10$, that always exist regardless of the shift values for the corresponding circulants and analyze the relationship between the girth of the protograph code and that of the protograph.

III. Cycle Analysis of Protographs and Protograph Codes

As one can see in Fig. 1, there always exist cycles of length 12 in the conventional QC LDPC code in (1) regardless of p and the shift values. Other than these cycles of length 12, we can also find many such cycles of length larger than 12 that always occur for any p and the shift values, which we will call *inevitable cycles*. Certainly, the inevitable cycles are caused by the structure of the protograph. For example, if a protograph contains a fully-connected bipartite subgraph consisting of three variable nodes and two check nodes or vice versa, then in its protograph code, the inevitable cycle of length 12 shown in Fig. 1 must occur.

A cycle is said to be *simple* if it does not contain any subcycles of smaller length. The following lemma can be easily deduced.

Lemma 1: Let C_{2i} be an incidence matrix of a simple cycle of length $2i$, $i \geq 2$. Then, under the row and column permutations, C_{2i} can be uniquely expressed as follows.

$$\begin{bmatrix} 1\,1\,0\,0 \cdots 0\,0\,0\,0 \\ 1\,0\,1\,0 \cdots 0\,0\,0\,0 \\ 0\,1\,0\,1 \cdots 0\,0\,0\,0 \\ 0\,0\,1\,0 \cdots 0\,0\,0\,0 \\ \vdots\;\vdots\;\vdots\;\vdots\;\ddots\;\vdots\;\vdots\;\vdots\;\vdots \\ 0\,0\,0\,0 \cdots 0\,1\,0\,0 \\ 0\,0\,0\,0 \cdots 1\,0\,1\,0 \\ 0\,0\,0\,0 \cdots 0\,1\,0\,1 \\ 0\,0\,0\,0 \cdots 0\,0\,1\,1 \end{bmatrix}$$

□

It is clear that an inevitable cycle is constructed by combining two or more simple cycles. Myung, Yang, and Kim [6] expressed the length of the inevitable cycle in terms of the lengths of its two constituent simple cycles when they share some edges as in the following theorem.

Theorem 1 ([6]): If there are r edge overlaps between two simple cycles of lengths $2k$ and $2l$ in the protograph, then there is an inevitable cycle of length $2(2l + 2k - r)$ in its protograph code. □

Let P_{2i} denote the incidence matrix of the subgraph of a protograph, which gives rise to an inevitable $2i$-cycle such that no inevitable cycles of smaller length are included in it. It is manifest that if the protograph contains a subgraph whose incidence matrix is P_{2i} or its transpose P_{2i}^T, then the girth of its protograph code is upper bounded by $2i$. Or conversely, if a protograph does not contain P_{2k} and P_{2k}^T for all $k \leq i$, then the resulting protograph code could have the girth larger than $2i$ by choosing appropriate shift values.

It can be easily shown that the smallest length of an inevitable cycle is 12 and P_{12} is as follows

$$P_{12} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}. \tag{4}$$

The existence of P_{12} makes the girth of the conventional QC LDPC code upper-bounded by 12. To exclude the subgraph pattern P_{12}, the protograph must not be fully-connected and the protograph should be expanded by properly adding 0's while preserving the row and column weights. In constructing protograph code, 1's and 0's in the protograph are replaced by $p \times p$ permutation matrices and $p \times p$ zero matrices, respectively.

In search of P_{2i}, we set the following restrictions on P_{2i}.

1) The number of rows is not larger than that of columns.

2) The weight of the j-th row is not smaller than that of the $(j+1)$-st row.

3) Columns are arranged by their weights in decreasing order as far as they can be.

4) The weight of any column or row is not smaller than 2.

5) P_{2i} does not contain P_{2k} or P_{2k}^T for all $k < i$.

Restrictions 1), 2), and 3) are needed to avoid the multiple count of the equivalent patterns. We searched for the candidate submatrices for P_{2i} having upto ten 1's, and finally obtained the following list of all P_{2i}'s, $i = 6, 7, 8, 9, 10$.

$$P_{12} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$P_{14} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$P_{16} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$P_{18} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$P_{20} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Note that in the above list, all P_{2i} but the fourth one in P_{20} have i 1's. The inevitable $2i$-cycle from the fourth one in P_{20} is depicted in Fig. 2.

The discussion in this section upto this point is summarized as in the following theorem.

Theorem 2: If a protograph contains the submatrix P_{2i} or P_{2i}^T for $i \geq 6$, then its protograph code cannot have the girth larger than $2i$. $\square$

Using Theorem 1, we can derive the relationship between the girth of the protograph and the minimum length of the inevitable cycles in its protograph code as in the following theorem.

Theorem 3: Let the girth of a protograph be $2g$, $g \geq 2$. Then the length of an inevitable cycle in its protograph code with circulants is larger than or equal to $6g$, which means that its protograph code could have the girth larger than or equal to $6g$ by choosing the appropriate shift values of circulants.

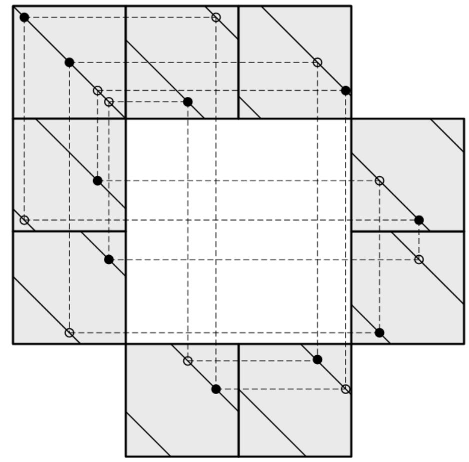
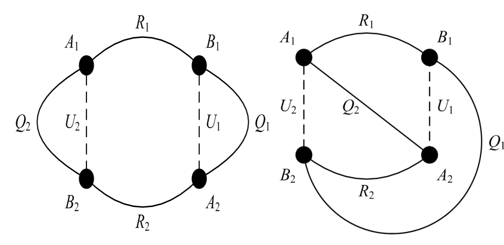


Fig. 2. An inevitable cycle of of P_{20}.

Proof: Without loss of generality, we can assume that the inevitable cycle of the smallest length is formed by two simple cycles C_1 of length $2l$ and C_2 of length $2k$ sharing r edges. Assume that the r shared edges form m disjoint paths, $R_1, R_2, \cdots, R_m$. We name the other m disjoint paths in the cycle C_1 connecting R_i's as $U_1, U_2, \cdots, U_m$, and those in the cycle C_2 as $Q_1, Q_2, \cdots, Q_m$. Also, let A_i and B_i, $i = 1, 2, \cdots, m$, be the two end nodes of the path R_i. Fig. 3 shows two possible patterns of the overlapping cycles for the case when $m = 2$. For the sake of simplicity, the subscripts for U and Q are numbered in increasing order as the cycle goes clockwise starting from the (outgoing) end node of R_1.



(a) Case (i) (b) Case (ii)

Fig. 3. Overlapping patterns of two simple cycles.

It is clear that each of the nodes A_i and B_i is incident to exactly three paths, namely R_i, $U_{\sigma(i)}$, and $Q_{\mu(i)}$, where σ and μ are some permutations of 1 through m. Therefore, there always exists a cycle consisting of only U's and Q's. Fig. 3 shows such cycles, the cycle $U_1 - Q_1$ or the cycle $U_2 - Q_2$ in Case (i), and the cycle $U_1 - Q_1 - U_2 - Q_2$ in Case (ii).

Since $\sum_{i=1}^{m} L(U_i) = 2l - r$ and $\sum_{i=1}^{m} L(Q_i) = 2k - r$, the length of this cycle is less than or equal to $(2l-r)+(2k-r)$, where $L(\cdot)$ denotes the length of the path. Since the girth is $2g$, we have

$$(2l - r) + (2k - r) \geq 2g.$$

Therefore, using Theorem 1, we can conclude that the length of the inevitable cycle is lower bounded as

$$2(2l+2k-r) \geq 2(2l+2k-(l+k-g)) = 2(l+k+g) \geq 6g.$$

□

Theorem 3 tells us that in order to design a protograph code with girth larger than or equal to $6g$, we need a protograph of girth $2g$, i.e., the protograph which does not contain the submatrices P_{2i}, for all $i < 3g$. Once the protograph of girth $2g$ is obtained, its protograph code could have the girth larger than or equal to $6g$ by choosing the appropriate shift values of circulants.

IV. Combinatorial Design of Protographs

In this section, using the well-known combinatorial design theory, we will design the protographs so that the derived protograph codes have the girth larger than 12, especially larger than or equal to 14 or 18. More specifically, we use t-(v,k,λ) design and λ-configuration $(v_r,b_k)_\lambda$ for the systematic construction of protographs without P_{2i}.

Definition 1 ([11]): A λ-configuration $(v_r,b_k)_\lambda$ is an incidence structure of v points and b blocks such that each block contains k points, each point belongs to r blocks, and any two different points are contained in at most λ blocks. □

A 1-configuration $(v_r,b_k)_1$ is simply called a configuration (v_r,b_k).

A. Protograph Codes with Girth Larger Than or Equal to 18

From Theorem 3, it is manifest that in order to construct a protograph code with girth larger than or equal to 18, we need a protograph with girth at least 6. From the definition of Steiner system, it is clear that the incidence matrix of the $S(2,k,v)$ does not contain the submatrix $\begin{bmatrix}1&1\\1&1\end{bmatrix}$. Thus it can serve as a protograph with girth 6.

Theorem 4: The protograph codes constructed from Steiner systems $S(2,k,v)$ have $(J,L) = \left(k, \frac{v-1}{k-1}\right)$ and the girth can be larger than or equal to 18 by choosing the appropriate shift values. □

For example, the incidence matrix of the Steiner triple system $S(2,3,9)$ is given as

$$\begin{bmatrix}
1&0&0&1&0&0&1&0&0&1&0&0\\
1&0&0&0&1&0&0&1&0&0&1&0\\
1&0&0&0&0&1&0&0&1&0&0&1\\
0&1&0&1&0&0&0&0&1&0&1&0\\
0&1&0&0&1&0&1&0&0&0&0&1\\
0&1&0&0&0&1&0&1&0&1&0&0\\
0&0&1&1&0&0&0&1&0&0&0&1\\
0&0&1&0&1&0&0&0&1&1&0&0\\
0&0&1&0&0&1&1&0&0&0&1&0
\end{bmatrix}$$

and this can serve as a protograph for the (3, 4) QC LDPC code with girth larger than or equal to 18.

The configuration (v_r,b_k) can also serve as the protograph without the submatrix pattern $\begin{bmatrix}1&1\\1&1\end{bmatrix}$, which may make a regular (k,r) QC LDPC code with girth larger than or equal to 18. Such a configuration (v_r,b_k) can be constructed from Steiner system as follows.

TABLE I

Minimum Sizes of the Incidence Matrices of Protographs with Girth$\geq$ 6 for $J=3$ (S: Steiner System, C: Configuration).

(J,L)	(3,4)	(3,5)	(3,6)	(3,7)	(3,8)	(3,9)
$v\times b$	9×12	12×20	13×26	15×35	18×48	19×57
	$S(2,3,9)$	$(12_5,20_3)$	$S(2,3,13)$	$S(2,3,15)$	$(18_8,48_3)$	$S(2,3,19)$
	S	C	S	S	C	S

Let F be a $v\times b$ incidence matrix of Steiner system $S(2,k,v)$ with $r = \frac{v-1}{k-1}$. Let F' be a $(v-1)\times(b-r)$ matrix obtained from F by deleting one row of F and the r columns incident to it. Then F' is an incidence matrix of a configuration $((v-1)_{r-1},(b-r)_k)$.

Theorem 5: The protograph codes constructed from configuration (v_r,b_k) have $(J,L)=(k,r)$ and the girth can be larger than or equal to 18 by choosing the appropriate shift values. □

Theorem 6: For $J=3$ and $L=r$, the minimum sizes of the $v\times b$ incidence matrices of protographs with girth$\geq$ 6 obtained from the configuration (v_r,b_3) are given as

(i) $r \neq 2 \mod 3$,

$$v = 2r+1 \text{ and } b = \frac{2r^2+r}{3}. \tag{5}$$

(ii) $r = 2 \mod 3$,

$$v = 2r+2 \text{ and } b = \frac{2r^2+2r}{3}. \tag{6}$$

□

Table I lists minimum sizes of the incidence matrices of protographs with girth$\geq$6 for $J=3$.

B. Protograph Codes with Girth Larger Than or Equal to 14

A 2-$(v,k,2)$ design and a 2-configuration $(v_r,b_k)_2$ can be used to construct the protographs which do not include P_{12} or P_{12}^T.

Note that the incidence matrices of some 2-configurations $(v_r,b_k)_2$ can contain P_{12}^T as their submatrix. For example, consider the following two different 2-configurations $(7_6,14_3)_2$ as

$$\begin{bmatrix}
1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0\\
0&0&1&1&0&0&0&0&1&1&0&0&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1\\
0&0&0&0&1&1&0&0&1&1&1&1&0&0
\end{bmatrix},
\begin{bmatrix}
1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
1&0&1&0&0&0&1&0&0&0&1&1&1&0\\
0&1&0&1&0&0&0&1&0&0&1&1&0&1\\
0&0&1&0&1&0&0&1&1&0&0&0&1&1\\
0&0&0&1&0&1&0&0&1&1&1&0&1&0\\
0&0&0&0&1&1&1&0&0&1&0&1&0&1
\end{bmatrix}.$$

Obviously, the first 2-configuration $(7_6,14_3)_2$ includes P_{12}^T in its incidence matrix whereas the second one does not. It can be shown that in order for a 2-configuration $(v_r,b_k)_2$ to serve as the protograph for the protograph code with girth$\geq$ 14, Hamming distance between any two columns of its incidence matrix should be larger than $2k-6$.

Now, we would like to design a 2-configuration $(v_r,b_k)_2$ whose incidence matrix does not include P_{12}^T. The following procedure describes the simple way of constructing a 2-configuration $(v_r, b_k)_2$ without P_{12}^T, using a configuration (v_r, b_k)(including 2-$(v, k, 1)$ design).

Let F be an incidence matrix of a configuration (v_r, b_k) and $T^i(F)$ a cyclic row shift of F i times downward. If the Hamming distance between any two columns in F and $T^i(F)$ is larger than $2k-6$, then the matrix $\left[F : T^i(F)\right]$ becomes an incidence matrix of 2-configuration $(v_r, b_k)_2$ without the submatrix pattern P_{12}^T.

Example 1: Suppose that the incidence matrix F of a configuration $(8_3, 8_3)$ and its cyclic shift $T^i(F)$ are given as

$$F = \begin{bmatrix} 1&1&1&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0 \\ 0&0&1&0&1&0&1&0 \\ 1&0&0&0&0&1&1&0 \\ 0&1&0&1&0&0&1&0 \\ 0&1&0&0&0&1&0&1 \\ 1&0&0&0&1&0&0&1 \\ 0&0&1&1&0&0&0&1 \end{bmatrix}, \quad T^1(F) = \begin{bmatrix} 0&0&1&1&0&0&0&1 \\ 1&1&1&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0 \\ 0&0&1&0&1&0&1&0 \\ 1&0&0&0&0&1&1&0 \\ 0&1&0&1&0&0&1&0 \\ 0&1&0&0&0&1&0&1 \\ 1&0&0&0&1&0&0&1 \end{bmatrix},$$

$$T^2(F) = \begin{bmatrix} 1&0&0&0&1&0&0&1 \\ 0&0&1&1&0&0&0&1 \\ 1&1&1&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0 \\ 0&0&1&0&1&0&1&0 \\ 1&0&0&0&0&1&1&0 \\ 0&1&0&1&0&0&1&0 \\ 0&1&0&0&0&1&0&1 \end{bmatrix}.$$

In order for $\left[F : T^i(F)\right]$ to be a 2-configuration $(v_r, b_k)_2$ without P_{12}^T, the Hamming distance d_H between any two columns in F and $T^i(F)$ should satisfy $1 \le d_H \le 6$. Since the Hamming distance between the fourth column of F and the first column of $T^1(F)$ is zero, $\left[F : T^1(F)\right]$ includes P_{12}^T. We can construct the protograph code with girth larger than or equal to 14 by using $\left[F : T^2(F)\right]$ as a protograph shown below.

$$\left[F : T^2(F)\right] = \begin{bmatrix} 1&1&1&0&0&0&0&0&1&0&0&0&1&0&0&1 \\ 0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&1 \\ 0&0&1&0&1&0&1&0&1&1&1&0&0&0&0&0 \\ 1&0&0&0&0&1&1&0&0&0&0&1&1&1&0&0 \\ 0&1&0&1&0&0&1&0&0&0&1&0&1&0&1&0 \\ 0&1&0&0&0&1&0&1&1&0&0&0&0&1&1&0 \\ 1&0&0&0&1&0&0&1&0&1&0&1&0&0&1&0 \\ 0&0&1&1&0&0&0&1&0&1&0&0&0&1&0&1 \end{bmatrix}$$

□

Then, we have the following theorem.

Theorem 7: The protograph codes constructed from 2-configuration $(v_r, b_k)_2$(including 2-$(v, k, 2)$ design), without P_{12}^T may have girth larger than or equal to 14 by choosing the appropriate shift values. □

For $(J, L) = (3, 4), (3, 5)$, and $(3, 6)$, the minimum sizes of incidence matrices of protographs without P_{12}^T can be obtained from 2-configuration $(6_4, 8_3)_2$, 2-$(6, 3, 2)$ design, and 2-$(7, 3, 2)$ design, respectively and they are shown as

$$\begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&0&0&0&1&1&1&0 \\ 0&1&0&0&1&1&0&1 \\ 0&1&1&0&0&0&1&1 \\ 0&0&1&1&1&0&1&0 \\ 1&0&0&1&0&1&0&1 \end{bmatrix}, \quad \begin{bmatrix} 1&1&1&1&1&0&0&0&0&0 \\ 1&1&0&0&0&1&1&1&0&0 \\ 1&0&1&0&0&1&0&0&1&1 \\ 0&1&0&1&0&0&1&0&1&1 \\ 0&0&1&0&1&0&1&1&1&0 \\ 0&0&0&1&1&1&0&1&0&1 \end{bmatrix},$$

$$\begin{bmatrix} 1&1&1&1&1&1&0&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&1&1&1&1&0&0&0&0 \\ 1&0&1&0&0&0&1&0&0&0&1&1&1&0 \\ 0&1&0&1&0&0&0&1&0&0&1&1&0&1 \\ 0&0&1&0&1&0&0&1&1&0&0&0&1&1 \\ 0&0&0&1&0&1&0&0&1&1&1&0&1&0 \\ 0&0&0&0&1&1&1&0&0&1&0&1&0&1 \end{bmatrix}. \qquad (7)$$

V. Shift Values for Protograph Codes

In general, for a given p, it is not easy to check the existence of shift values which guarantee the protograph code to have the maximum achievable girth provided by the protograph. Moreover, finding such shift values seems even more difficult. But, certainly such shift values exist if we allow a sufficiently large p. This is because of the fact that it is always possible to prevent $2i$-cycles at least by assigning the shift values so that all the sums of i shift values (allowing repetition) are distinct from one another modulo p, since any $2i$-cycle should satisfy the relationship given in (3).

In this section, we introduce a couple of shift value assigning methods for the exemplary 6×10 protograph in (7) which is obtained from 2-$(6, 3, 2)$ design. This protograph contains P_{14} and the girth of its protograph code is upper bounded by 14. The shift value assigning method in the following theorem guarantees the girth 14 for the protograph codes.

Theorem 8: Let $p_{k,m}$ denote the shift value of the m-th nonzero circulant in the k-th row of the parity-check matrix of the protograph code for $0 \le m \le 4$ and $0 \le k \le 5$. Let $\{a_0, a_1, a_2, a_3, a_4\}$=$\{0, 1, 3, 7, 12\}$ and

$$p_{k,m} = \begin{cases} 0, & \text{if } k = 0 \\ a_m \times 37^{k-1}, & \text{if } k \neq 0. \end{cases}$$

Then the protograph code constructed from the above protograph has the girth 14 for $p = 37^5$.

Proof: It is manifest that in the left-hand side of (3), the number of shift values from a given row is even and exactly half of them have $+$ signs and the other half have $-$ signs. Also it is not difficult to see that in a cycle of length upto 12, any row cannot be visited more than 6 times, and any two rows cannot be visited 6 times simultaneously.

The set $\{0, 1, 3, 7, 12\}$ is chosen so that the sums of two elements (including the sum of an element with itself) are all distinct. Thus, in the left-hand side of (3), the partial sum of the shift values from a given row cannot be cancelled out by those from other rows since it is upper bounded by $36(= 3 \times 12 - 3 \times 0) \times 37^i$, whereas those from other rows are having values of different order with respect to the base 37. □

In the next shift value assigning method, we set to zero as many shift values as possible. For any given shift values, we can always obtain equivalent shift values shown below by a proper row and column permutations of the parity-check matrix of the protograph code.

$$\begin{bmatrix} I(0) & I(0) & I(0) & I(0) & I(0) & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ I(0) & I(p_0) & \mathbf{0} & \mathbf{0} & \mathbf{0} & I(0) & I(0) & I(0) & \mathbf{0} & \mathbf{0} \\ I(0) & \mathbf{0} & I(p_1) & \mathbf{0} & \mathbf{0} & I(p_5) & \mathbf{0} & \mathbf{0} & I(0) & I(0) \\ \mathbf{0} & I(0) & \mathbf{0} & I(p_2) & \mathbf{0} & \mathbf{0} & I(p_7) & \mathbf{0} & I(p_{11}) & I(p_{13}) \\ \mathbf{0} & \mathbf{0} & I(0) & \mathbf{0} & I(p_3) & \mathbf{0} & I(p_8) & I(p_9) & I(p_{12}) & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I(0) & I(p_4) & I(p_6) & \mathbf{0} & I(p_{10}) & \mathbf{0} & I(p_{14}) \end{bmatrix}$$

Then the following theorem tells us an assigning method of nonzero shift values.

Theorem 9: Set $p_i \in \{4^k \mid 0 \leq k \leq 14\}$ and $p_i \neq p_j$ for $i \neq j$. Then the protograph code has the girth 14 for $p \geq 4^{15}$.

Proof: Since the minimum recurrence time for a block in a cycle is 4, the maximum number of visits to a given block in a cycle of length upto 12 is 3. Therefore, (3) cannot be satisfied for the given shift values when $p \geq 4^{15}$. □

However, the codes in Theorems 8 and 9 are not practical since the code lengths are too large. Certainly, the bound for p in Theorem 9 is sufficient but not necessary. From a random search, we find that for $p = 13477$, the girth of the protograph code using the shift values in Theorem 9 is 14.

VI. Conclusions And Further Works

All the subgraph patterns in the protographs which make inevitable cycles of length upto 20 are found and it is also derived that if the girth of the protograph is $2g$, $g \geq 2$, its protograph code may not have the inevitable cycles of length smaller than $6g$ by choosing proper shift values. Using combinatorial design theory, the protograph codes constructed from the protographs with girth larger than or equal to 14 are proposed. For a sufficiently large p, we obtain the protograph code which has the girth 14.

Two methods for assigning shift values that we have shown in Section V are just a tip of the iceberg. It could be interesting to find out the shift value assigning method with the smallest p which ensures the girths 14, though it does not seem easy.

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] R. M. Tanner, D. Sridhara, and T. E. Fuja, "A class of group-structured LDPC codes," in *Proc. Int. Conf. Information Systems Technology and its Applications*, July 2001.

[3] H. Zhong and T. Zhang, "Block-LDPC: A practical LDPC coding system design approach," *IEEE Trans. Circuits and Systems*, vol. 52, no. 4, pp. 766-775, April 2005.

[4] B. Vasic and O. Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," *IEEE Trans. Inform. Theory*, vol. 50, no. 6, pp. 1156-1176, June 2004.

[5] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, "Construction of low-density parity-check codes based on balanced incomplete block designs," *IEEE Trans. Inform. Theory*, vol. 50, no. 6, pp. 1257-1268, June 2004.

[6] S. Myung, K. Yang, and J. Kim, "Quasi-cyclic LDPC codes for fast encoding," *IEEE Trans. Inform. Theory*, vol. 51, no.8, pp. 2894-2901, Aug. 2005.

[7] M. E. O'Sullivan, J. Brevik, and R. Wolski, "The performace of LDPC codes with large girth," in *Proc. 43rd Allerton Conf. on Commun., Control, and Computing*, 2005.

[8] O. Milenkovic and S. Laendner, "Analysis of the cycle-structure of LDPC codes based on Latin squares," in *Proc. Inter. Conf. on Commun.*, pp. 777-781, 2004.

[9] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protograph," *IPN Progress Report 42-154, JPL*, Aug. 2003.

[10] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, "On the girth of Tanner's (3, 5) quasi-cyclic LDPC codes," *accepted for publication in IEEE Trans. Inform. Theory*, Nov. 2005.

[11] C. J. Colbourn and J. H. Dinitz, *The CRC handbook of combinatorial designs*. Boca Raton, FL: CRC Press, 1996.

[12] R. G. Gallager, *Low-density parity-check codes*. Cambridge, MA: MIT Press, 1963.

[13] 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. Inform. Theory*, vol. 50, no. 12, pp. 2966-2984, Dec. 2004.