Construction of Protographs for QC LDPC Codes With Girth Larger Than 12[1]

Sunghwan Kim, Jong-Seon No[O]
School of Electrical Engineering and Computer Science
Seoul National University
Email: {nodoubt, jsno}@snu.ac.kr

Habong Chung
School of Electronic and Electrical Engineering
Hongik University
Email: habchung@hongik.ac.kr

Dong-Joon Shin
Division of Electronic and Computer Engineering
Hanyang University
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, using 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 that always exist regardless of the shift values of circulants, we propose new combinatorial construction methods of the protographs, whose protograph codes can have girth larger than or equal to 14 or 18. We also propose a couple of shift value assigning rules for circulants of a QC LDPC code guaranteeing the girth 14.

1. Introduction

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.

2. 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 $p \times p$ circulants 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 $(r + p_{j,l}) \bmod p$ for row r, $0 \le r \le p-1$, and $p_{j,l}$ is an integer $\bmod p$, $0 \le j \le J-1$, $0 \le l \le L-1$. 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 $p \times p$ permutation 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 $l_k \neq l_{k+1}$.

Thorpe [6] 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*.

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

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

[1]This work was supported by University IT Research Center Project and Laboratory of Excellency Program.

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, $i = 6, 7, 8, 9, 10$.

$$P_{12}=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},\ P_{14}=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

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

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

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

3. 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}.

Some t-designs also have names of their own. A 2-(v, k, λ) design is called a (v, b, r, k, λ) balanced incomplete block design (BIBD), where b is the number of k-subsets and r is the number of k-subsets containing any given element of V. In a BIBD, we have the relationship $vr = bk$ and $\lambda(v-1) = r(k-1)$. The incidence matrix of a BIBD with parameters (v, b, r, k, λ) is a $v \times b$ matrix $A = [a_{i,j}]$, in which $a_{i,j} = 1$ when the i-th element of V occurs in the j-th block of B and $a_{i,j} = 0$, otherwise. The t-design with $\lambda = 1$ is called a Steiner system denoted by $S(t, k, v)$ and especially, $S(2, 3, v)$ is called a Steiner triple system. In a 2-design, if we loosen some of the restrictions, then we have a λ-configuration which is defined as follows.

Definition 1 ([8]) *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). In [8], conditions for the existence of a configuration are given:

i) The necessary conditions for the existence of a configuration (v_r, b_k) are $vr = bk$ and $v \geq r(k-1)+1$.

ii) The necessary conditions are also sufficient for $k = 3$.

iii) For $k = 4$, no nonexistence results concerning configurations (v_r, b_k) are known.

iv) For $k = 5$, the necessary conditions are not sufficient.

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

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. A Steiner system is a t-design with $\lambda = 1$ and t-(v, k, λ) is denoted by $S(t, k, v)$. 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 1 *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.

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 2 *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 3 *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 1 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 row cyclic shift $T^i(F)$ are given. 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 $1 \leq d_H \leq 6$. 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 4 *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 $(J, L) = (3, 4)$ and $(3, 5)$, the minimum sizes of incidence matrices of protographs without P_{12}^T can be obtained from 2-configuration $(6_4, 8_3)_2$ and 2-$(6, 3, 2)$ design, respectively and they are shown as

$$\begin{bmatrix}
1&1&1&1&0&0&0&0\\
1&0&0&0&1&1&1&0\\
0&1&0&0&1&1&0&1\\
0&1&1&0&0&0&1&1\\
0&0&1&1&1&0&1&0\\
1&0&0&1&0&1&0&1
\end{bmatrix},\quad
\begin{bmatrix}
1&1&1&1&1&0&0&0&0&0\\
1&1&0&0&0&1&1&1&0&0\\
1&0&1&0&0&1&0&0&1&1\\
0&1&0&1&0&0&1&0&1&1\\
0&0&1&0&1&0&1&1&1&0\\
0&0&0&1&1&1&0&1&0&1
\end{bmatrix}. \tag{7}$$

Table 1: Minimum Sizes of the Incidence Matrices of Protographs with Girth≥ 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

4. 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. 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 5 *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 $0 \leq m \leq 4$ and $0 \leq k \leq 5$. 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 $p = 37^5$.

□

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 6 *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 $p \geq 4^{15}$.*

□

However, the codes in Theorems 5 and 6 are not practical since the code lengths are too large. From a random search, we find that for $p = 13477$, the girth of the protograph code using the shift values in Theorem 6 is 14.

5. Conclusions And Further Works

Using combinatorial design theory, the protograph codes with girth larger than or equal to 14 or 18 constructed from the protographs are proposed. Two methods for assigning shift values that we have shown in Section 5 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] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protograph," *IPN Progress Report 42-154, JPL*, Aug. 2003.

[7] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, "On the girth of Tanner's (3, 5) quasi-cyclic LDPC codes," *to be published in IEEE Trans. Inform. Theory*, Apr. 2006.

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