Protograph Codes with Circulant Permutation Matrices [1]

*Sunghwan Kim, *Min-Ho Jang$^{\text{O}}$, *Jong-Seon No, **Habong Chung, and
***Dong-Joon Shin
*Seoul National University, **Hongik University, ***Hanyang University
{nodoubt, mhjang}@ccl.snu.ac.kr, jsno@snu.ac.kr,
habchung@hongik.ac.kr, 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 $6g$.

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.

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.

Thorpe [4] introduced the concept of *protograph codes*, a class of LDPC codes constructed from a protograph in such a way that the 1's in the incidence matrix of the protograph are replaced by $p \times p$ permutation matrices and the 0's by $p \times p$ zero matrices. If these $p \times p$ permutation matrices are circulant, the protograph codes become QC LDPC codes. Thorpe, Andrews, and Dolinar [5] discussed the construction of protograph codes using circulants. Up to now, however, few works have been reported for designing the protographs which guarantee the large girth.

In this paper, we derived the relationship between the girth of the protograph and the length of the inevitable cycles in its protograph codes with circulants. In Section II, we briefly summarize the known properties of QC LDPC codes. In Section III, we identify all the subgraph patterns of protographs, which bring the inevitable $2i$-cycles, $i = 6, 7, 8, 9, 10$, 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 $6g$.

II. QC LDPC Codes

In this section, we introduce some definitions and notations.

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 $(r + p_{j,l}) \bmod p$ for row r, $0 \leq r \leq p-1$, and $p_{j,l}$ is an integer $\bmod p$, $0 \leq j \leq J-1$, $0 \leq l \leq L-1$. 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 $p \times p$ permutation matrices. Thus a cycle of length $2i$

[1] This work was supported in part by BK21 and ITRC program.

in a conventional QC LDPC code can be expressed as the following sequence

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

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

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

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.

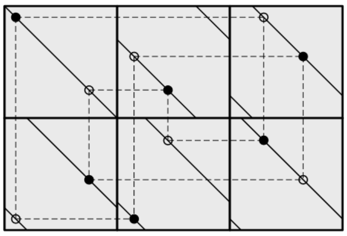


Figure 1: An inevitable cycle of length 12 in QC LDPC codes.

Let $\begin{bmatrix} I(p_{q,u}) & I(p_{q,v}) & I(p_{q,w}) \\ I(p_{r,u}) & I(p_{r,v}) & I(p_{r,w}) \end{bmatrix}$ denote the submatrix of the parity-check matrix consisting of those six blocks in Fig. 1. The closed path in Fig. 1 satisfies the condition in (3), that is,

$$(p_{q,u} - p_{r,u}) + (p_{r,v} - p_{q,v}) + (p_{q,w} - p_{r,w}) + (p_{r,u} - p_{q,u}) + (p_{q,v} - p_{r,v}) + (p_{r,w} - p_{q,w}) = 0$$

for any shift values.

Tanner [2] proposed an algebraic method of assigning shift values in (J, L) QC LDPC codes which have the girth 12. Especially, for a prime p which reduces to 1 mod 30, the shift values $p_{j,l}$ are determined as

$$p_{j,l} = b^j a^l, \quad 0 \leq j \leq 2, \; 0 \leq l \leq 4$$

where a and b are non-zero integers of orders 5 and 3 in the finite field F_p, respectively. For such primes $p \geq 181$, Tanner's $(3, 5)$ QC LDPC code achieves the girth 12 [6].

Thorpe [4] 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.

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.*

$$\begin{bmatrix} 1100\cdots 0000 \\ 1010\cdots 0000 \\ 0101\cdots 0000 \\ 0010\cdots 0000 \\ \vdots\,\vdots\,\vdots\,\vdots\;\ddots\;\vdots\,\vdots\,\vdots\,\vdots \\ 0000\cdots 0100 \\ 0000\cdots 1010 \\ 0000\cdots 0101 \\ 0000\cdots 0011 \end{bmatrix}$$

□

It is clear that an inevitable cycle is constructed by combining two or more simple cycles. Myung, Yang, and Kim [3] 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 [3] *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, $i = 6, 7, 8, 9, 10$.

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

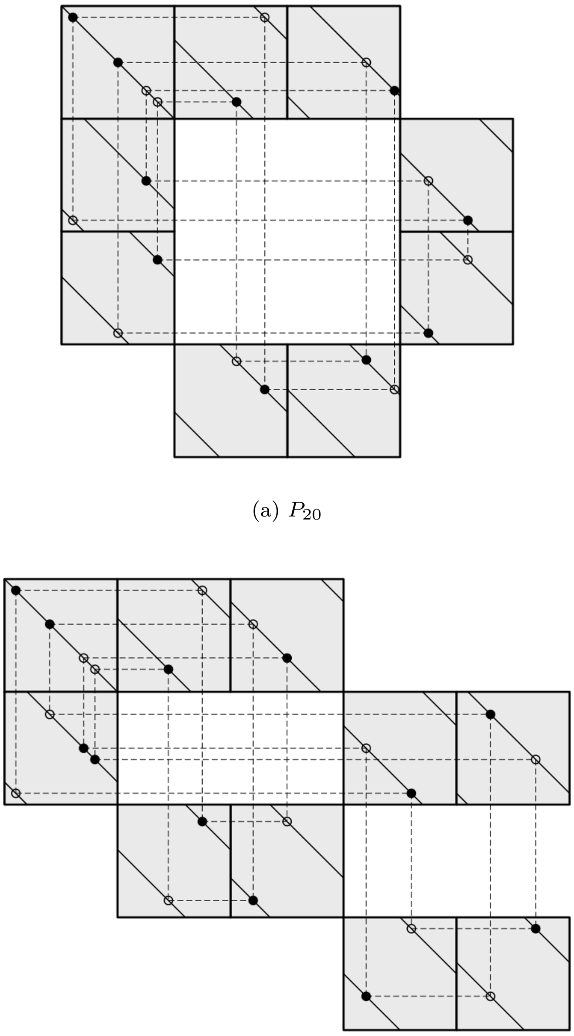
$$P_{14} = \begin{bmatrix} 1\,1\,1 \\ 1\,1\,0 \\ 1\,0\,1 \end{bmatrix}$$

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

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

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

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. Also in Fig. 2, the inevitable 24-cycle obtained from a submatrix pattern having ten 1's is depicted.



(a) P_{20}

(b) P_{24}

Figure 2: Some inevitable cycles of P_{20} and P_{24}.

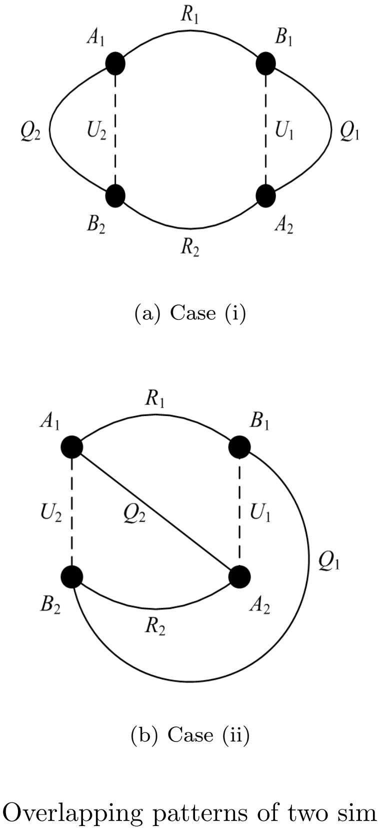
The discussion in this section upto this point is summarized as in the following theorem.

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* $2i$. □

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.*

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)

Figure 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.

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] S. Myung, K. Yang, and J. Kim, “Quasi-cyclic LDPC codes for fast encoding,” *to be published in IEEE Trans. Inform. Theory*, Aug. 2005.

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

[5] J. Thorpe, K. Andrews, and S. Dolinar, “Methodologies for designing LDPC codes using protographs and circulants,” in *Proc. Int. Symp. Information Theory*, 2004, pp. 236.

[6] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, “On the girth of Tanner's (3, 5) quasi-cyclic LDPC codes,” submitted to *IEEE Trans. Inform. Theory*, Jan. 2005.