$n$ possible values. If the parity check is satisfied, the error probability is closely approximated by the probability of two bit errors, and there are $n(n-1/2)$equally likely error values. The improvement when the KV algorithm is used comes almost entirely from the possibility of correcting $n/(n-1)$ times as many erasures.

If the inner code is a $(n, k, 3)$ Hamming code, an error-free symbol has a very low probability of error. Symbols with a corrected bit, on the other hand, are much more likely to be in error. Even though the number of possible error values could be counted, the improvement in the number of errors corrected is negligible. Thus the performance is calculated from (7).

For an inner code of lower rate, codewords with few bit errors have high reliability. When the number of errors approaches $d/2$, it is necessary to distinguish between cases where a second codeword is fairly close and the more common case that there is only a single likely transmitted symbol. When the number of errors exceeds $d/2$, some vectors are close to a codeword different from the one transmitted, while other vectors are far from all codewords.

*Example 5:* Consider the projective geometry code $(21, 12, 6)$ for which the necessary details can readily be worked out. Let the average number of bit errors in an inner codeword be $2$. It follows from the binomial distribution that the probability of $0$ or $1$ error in a block is $0.39$, and in this case the decision has a high reliability. Two errors are corrected, but the probability of decoding error (if four errors actually occur) is $0.12$. The $280$ weight $3$ error patterns are uniquely decoded, and for simplicity, we merge this set with the double errors. The remaining $1120$ weight $3$ error patterns are in $380$ cosets which gives a list of four possibilities. The remaining errors of weight $4$ are treated as erasures, and in our estimate we neglect the contributions from weight $5$ errors. In this way, we can apply (4) to get

$$K/N < 0.39 + 0.32(1-0.12)^2 + 0.16/4 = 0.68.$$

This can be compared to standard errors-and-erasures decoding of the RS code where the bound on the rate is $0.63$. There is a gain from the small list size of weight $3$ errors, and a small gain associated with distinguishing the different reliabilities.

## VII. Conclusion

The aim of this correspondence has been to give a more accessible version of the bound on list decoding. Using the simpler expressions it is possible to characterize the errors patterns that are typically decoded by the Koetter–Vardy algorithm.

The cases discussed cover most of the situations that are important for applications. As demonstrated in specific cases, the improvements are significant only for fairly low rates, sets of symbols with large error probability, or a small set of alternatives with high probabilities.

In all cases the performance is still far from maximum likelihood decoding.

## References

[1] R. Koetter and A. Vardy, "Algebraic soft-decision decoding of Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. IT-49, pp. 2809–2825, Nov. 2003.

[2] V. Guruswami and M. Sudan, "Improved decoding of Reed–Solomon and algebraic-geometric codes," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1757–1767, Sep. 1999.

[3] J. Jiang and K. R. Narayanan, "Performance analysis of algebraic soft decoding of Reed-Solomon codes over binary symmetric and erasure channels," in *Proc. IEEE Int. Symp. Information Theory*, Adelaide, Australia, Sep. 2005, pp. 1186–1190.

# Quasi-Cyclic Low-Density Parity-Check Codes With Girth Larger Than 12

Sunghwan Kim, Jong-Seon No, *Member, IEEE*, Habong Chung, *Member, IEEE*, and Dong-Joon Shin, *Member, IEEE*

***Abstract*—A quasi--cyclic (QC) low-density parity-check (LDPC) code can be viewed as the protograph code with circulant permutation matrices (or circulants). In this correspondence, 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 that always exist 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 $14$ or $18$. We also propose a couple of shift value assigning rules for circulants of a QC LDPC code guaranteeing the girth $14$.**

***Index Terms*—Girth, low-density parity-check (LDPC) codes, protograph, protograph codes, quasi--cyclic (QC) codes.**

## 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 the 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 $12$.

Manuscript received May 12, 2005; revised December 2, 2006. This work was supported by the Information Technology Research Center (ITRC) Program and the Information and Telecommunication National Scholarship Program of the Korean Ministry of Information and Communications. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Nice, France, June 2007.

S. Kim and J.-S. No are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: nodoubt@ccl.snu.ac.kr; jsno@snu.ac.kr)).

H. Chung is with the School of Electronics and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@wow.hongik.ac.kr).

D.-J. Shin is with the Division of Electrical and Computer Engineering, Hanyang University, Seoul 133-791, Korea (e-mail: djshin@hanyang.ac.kr).

Communicated by T. J. Richardson, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2007.901193

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 a fast encoding algorithm for a special class of QC LDPC codes and derived the upper bound of their girths.

Thorpe [7] 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 [8] 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 correspondence, we derived the relationship between the girth of the protograph and the length of the inevitable cycles in its protograph codes with circulants. We also investigate into the design of a protograph which guarantees the girth larger than or equal to $14$ or $18$ when its protograph code becomes a QC LDPC code. 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 $6g$. Using the combinatorial design, we propose the construction methods of the protographs, whose protograph codes have girth larger than or equal to $14$ or $18$ in Section IV. In Section V, we propose shift value assigning rules for the 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 $p \times p$ 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 $p \times p$ circulant 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 $2i$ in a conventional QC LDPC code can be expressed as the following sequence:

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

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

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

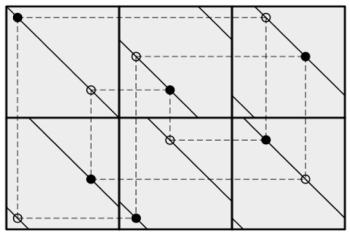

Fig. 1. An inevitable cycle of length 12 in QC LDPC codes.

where $j_i = j_0, j_k \neq j_{k+1}$, and $l_k \neq l_{k+1}$. This condition (3) is generalized to show that the length of a cycle in a protograph code can be calculated by using the length of the cycle in the corresponding protograph and the shift values of their circulants in [9].

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.

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

$$\begin{aligned} &(p_{q,u} - p_{r,u}) + (p_{r,v} - p_{q,v}) \\ &+ (p_{q,w} - p_{r,w}) + (p_{r,u} - p_{q,u}) \\ &+ (p_{q,v} - p_{r,v}) + (p_{r,w} - p_{q,w}) = 0 \end{aligned}$$

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 $1 \bmod 30$, 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 nonzero 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 $12$ [10].

Let us define the incidence matrix of the bipartite graph with two sets, $G_1$ 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 [7] 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 the incidence matrix of a fully connected protograph with $p \times p$ circulants and $0$'s with zero matrices.

In this correspondence, 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 I:* Let $C_{2i}$ be an $i \times i$ 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:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 1 \end{bmatrix}. \qquad \square$$

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 $r$ edges are shared by 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. $\square$

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 length smaller than $2i$ are included in it. Therefore, $P_{2i}$ does not contain $P_{2k}, k < i$. 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 $p \times p$ circulants 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 exhaustively searched for the candidate submatrices for $P_{2i}$ having up to ten 1's, and finally obtained all the incidence matrices for $P_{2i}$'s, $i = 6, 7, 8, 9, 10$, as given in the following list:

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

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

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

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

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

Note that in the above list, all $P_{2i}$ but the fourth one in $P_{20}$ have $i$ 1's. In Fig. 2, the inevitable $2i$-cycle from the fourth one in $P_{20}$ and the inevitable 24-cycle obtained from a submatrix pattern having ten 1's are depicted. Also, note that many submatrices in the above list can be generated by using Theorem 1. They correspond to "two simple cycles sharing edges." However, the first one for $P_{16}$ and the first and fourth ones for $P_{20}$ cannot be obtained by Theorem 1.

The discussion in this section up to this point is summarized as follows.

*Fact 1:* 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 2:* 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:* It is certain that an inevitable cycle must be formed from two simple cycles connected to each other. Thus, the inevitable cycle of the smallest length obtained from two given cycles occurs when two simple cycles share edges. Now, let us assume that the inevitable cycle of the smallest length is formed by two simple cycles $C_1$ of length $2l$

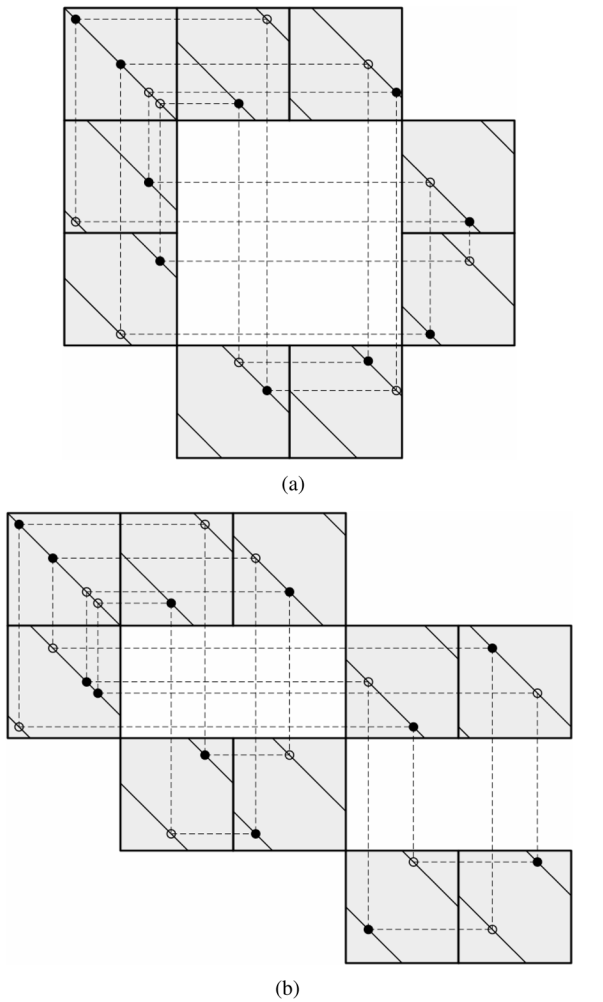

Fig. 2. Some inevitable cycles of $P_{20}$ and $P_{24}$. (a) $P_{20}$. (b) $P_{24}$.

and $C_2$ of length $2k$ sharing $r$ edges. Assume that the $r$ shared edges form $m$ disjoint paths, $R_1, R_2, \ldots, R_m$. We name the remaining $m$ disjoint paths in the cycle $C_1$ connecting $R_i$'s as $U_1, U_2, \ldots, U_m$, and those in the cycle $C_2$ as $Q_1, Q_2, \ldots, Q_m$. Also, let $A_i$ and $B_i, i = 1, 2, \ldots, m$, 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 $R_1$.

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 $\sigma$ and $\mu$ 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 2-cycle $U_1 - Q_1$ and the 2-cycle $U_2 - Q_2$ in Case i), and the 4-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

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

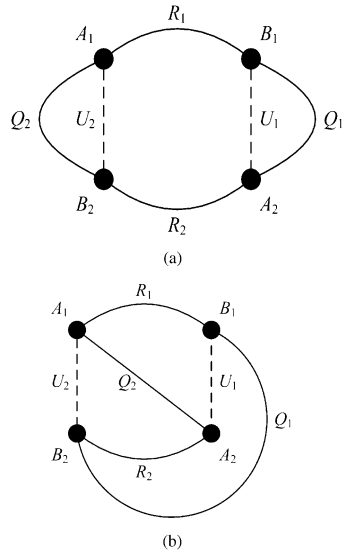

Fig. 3. Overlapping patterns of two simple cycles when $m = 2$. (a) Case (i). (b) Case (ii).

Theorem 2 tells us that in order to design a protograph code with girth larger than or equal to $6g$, it is necessary to have a protograph of girth at least $2g$, 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. Note that the results in this section can be directly applied to design irregular protographs.

## 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 $t$-$(v, k, \lambda)$ design and $\lambda$-configuration $(v_r, b_k)_\lambda$ for the systematic construction of protographs without $P_{2i}$.

*Definition 1 ([11]):* A $t$-$(v, k, \lambda)$ design is a pair $(V, B)$, where $V$ is a $v$-set of points and $B$ is a collection of $k$-subsets (blocks) of $V$ with the property that every $t$-subset of $V$ is contained in exactly $\lambda$ blocks in $B$. $\square$

Some $t$-designs also have names of their own. A 2-$(v, k, \lambda)$ design is called a $(v, b, r, k, \lambda)$ 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 $(v, b, r, k, \lambda)$ 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 $\lambda$-configuration which is defined as follows.

*Definition 2([11]):* A $\lambda$-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 $\lambda$ blocks. $\square$

A 1-configuration $(v_r, b_k)_1$ is simply called a configuration $(v_r, b_k)$. In [11], conditions for the existence of a configuration are given as follows:

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

TABLE I
PARAMETERS OF $S(2,k,v)$ AND $(v_r,b_k)$, (S:STEINER SYSTEM, C: CONFIGURATION)
(a) $k=3$ (b) $k=4$

(a)

| $v$ | 6 | 7 | 8 | 9 | 12 | 13 | 14 | 15 | 18 | 19 | 20 | 21 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b$ | 4 | 7 | 8 | 12 | 20 | 26 | 28 | 35 | 48 | 57 | 60 | 70 | 88 | 100 | 104 | 117 |
| $r$ | 2 | 3 | 3 | 4 | 5 | 6 | 6 | 7 | 8 | 9 | 9 | 10 | 11 | 12 | 12 | 13 |
| $(J,L)$ | (3,2) | (3,3) | (3,3) | (3,4) | (3,5) | (3,6) | (3,6) | (3,7) | (3,8) | (3,9) | (3,9) | (3,10) | (3,11) | (3,12) | (3,12) | (3,13) |
| | C | S | C | S | C | S | C | S | C | S | C | S | C | S | C | S |

(b)

| $v$ | 12 | 13 | 15 | 16 | 24 | 25 | 27 | 28 | 36 | 37 | 39 | 40 | 48 | 49 | 51 | 52 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $b$ | 9 | 13 | 15 | 20 | 42 | 50 | 54 | 63 | 99 | 111 | 117 | 130 | 180 | 196 | 204 | 221 |
| $r$ | 3 | 4 | 4 | 5 | 7 | 8 | 8 | 9 | 11 | 12 | 12 | 13 | 15 | 16 | 16 | 17 |
| $(J,L)$ | (4,3) | (4,4) | (4,4) | (4,5) | (4,7) | (4,8) | (4,8) | (4,9) | (4,11) | (4,12) | (4,12) | (4,13) | (4,15) | (4,16) | (4,16) | (4,17) |
| | C | S | C | S | C | S | C | S | C | S | C | S | C | S | C | S |

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.

Note that the construction of LDPC codes with girth larger than 4 using combinatorial designs such as Steiner systems and BIBD has been widely studied [5], [12], [13].

### A. Protograph Codes With Girth Larger Than or Equal to 18

From Theorem 2, it is enough to start with a protograph of girth at least 6, in order to construct a protograph code with girth larger than or equal to 18. 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.

*Fact 2:* The protograph codes constructed from Steiner systems $S(2,k,v)$ have $(J,L)=(k,\frac{v-1}{k-1})$ 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 $((v-1)_{r-1},(b-r)_k)$.

Table I lists the parameters of Steiner system $S(2,k,v)$ and configuration $(v_r,b_k)$ derived from Steiner system. In Table I, $J$ and $L$ denote the column and row weights of parity-check matrix of the protograph code, respectively. All Steiner systems and configurations in Table I can serve as the protographs with girth larger than 4 for $(J,L)=(k,r)$ quasi--cyclic protograph codes.

TABLE II
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) |
|---|---|---|---|---|---|---|
| $v\times b$ | $9\times 12$ | $12\times 20$ | $13\times 26$ | $15\times 35$ | $18\times 48$ | $19\times 57$ |
| | $S(2,3,9)$ | $(12_5,20_3)$ | $S(2,3,13)$ | $S(2,3,15)$ | $(18_8,48_3)$ | $S(2,3,19)$ |
| | S | C | S | S | C | S |

*Fact 3:* 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) $r\neq 2 \bmod 3$

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

ii) $r=2 \bmod 3$

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

*Proof:* From the existence conditions i) and ii) of a configuration, we know that the configuration $(v_r,b_3)$ satisfying $vr=3b$ and $v\geq 2r+1$ always exists. It is not difficult that $v$ and $b$ in (5) and (6) are the minimum integers satisfying the above conditions. □

Table II lists the 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

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

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

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

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 a 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 $[F : T^i(F)]$ 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

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

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

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

In order for $[F : T^i(F)]$ 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, $[F : T^1(F)]$ includes $P_{12}^T$. We can construct the protograph code with girth larger than or equal to 14 by using $[F : T^2(F)]$ as a protograph shown at the top of the page. □

Then, we have the following fact.

*Fact 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 $(J, L) = (3, 4), (3, 5)$, 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

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

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

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

So far, it is explained how to design regular protograph codes by using Steiner systems and configurations. However, irregular protograph codes can also be constructed by using the combinatorial designs such as pairwise balanced designs (PBDs) [11] and the procedure is almost identical to the regular case.

## 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

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

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 $6 \times 10$ 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 4:* 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 $p = 37^5$.

*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 up to $12$, any row cannot be visited more than six times.

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 have 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 at the top of the page by a proper row and column permutations of the parity-check matrix of the protograph code.

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

*Theorem 5:* Set $p_i \in \{4^k | 0 \leq k \leq 14\}$ 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 up to $12$ is $3$. Therefore, (3) cannot be satisfied for the given shift values when $p \geq 4^{15}$. □

Certainly, the bound for $p$ in Theorem 5 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 5 is $14$. When $J > 3$, similar method for the case of $J = 3$ can be applied by using the proper Steiner systems and configurations. Definitely, the code length can be larger than the case of $J = 3$.

## VI. Conclusion and Further Works

All the subgraph patterns in the protographs which make inevitable cycles of length up to $20$ 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 cycles of length smaller than $6g$ by choosing the proper shift values. 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 V are never meant to be practical. They simply show the existence of a protograph code with given girth. It could be interesting to find out the shift value assigning method with the smallest $p$ which ensures the girths $14$ or $18$, though it does not seem easy. Also, it would be desirable to have more efficient and flexible construction method of irregular protograph codes.

## References


[1] M. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. 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. Inf. Syst. Technol. Its Appl.*, Jul. 2001.

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

[4] B. Vasic and O. Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1156–1176, Jun. 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. Inf. Theory*, vol. 50, no. 6, pp. 1257–1268, Jun. 2004.

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

[7] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protograph," IPN Progr. Rep. 42-154, JPL, Aug. 2003.

[8] J. Thorpe, K. Andrews, and S. Dolinar, "Methodologies for designing LDPC codes using protographs and circulants," in *Proc. Int. Symp. Inf. Theory*, 2004, p. 236.

[9] J. Kang, P. Fan, and Z. Cao, "Flexible construction of irregular partitioned permutation LDPC codes with low error floors," *IEEE Commun. Lett.*, vol. 9, no. 6, pp. 534–536, Jun. 2005.

[10] 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*, vol. 52, no. 4, pp. 1739–1744, Apr. 2006.

[11] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*. Boca Raton, FL: CRC, 1996.

[12] D. J. C. MacKay and M. Davey, "Evaluation of Gallager code for short block length and high rate applications," in *Proc. IMA Workshop on Codes, systems and Graphical Models*, 1999.

[13] S. J. Johnson and S. R. Weller, "Regular low-density parity-check codes from combinatorial designs," in *Proc. Information Theory Workshop*, 2001, pp. 90–92.