Design of Multiple-Edge Protographs for QC LDPC Codes Avoiding Short Inevitable Cycles

Hosung Park, Seokbeom Hong, Jong-Seon No, *Fellow, IEEE*, and Dong-Joon Shin, *Senior Member, IEEE*

***Abstract*—There have been lots of efforts on the construction of quasi-cyclic (QC) low-density parity-check (LDPC) codes with large girth. However, most of them focus on protographs with single edges and little research has been done for the construction of QC LDPC codes lifted from protographs with multiple (i.e., parallel) edges. Compared to single-edge protographs, multiple-edge protographs have benefits such that QC LDPC codes lifted from them can potentially have larger minimum Hamming distance. In this paper, all subgraph patterns of multiple-edge protographs, which prevent QC LDPC codes from having large girth by inducing inevitable cycles, are fully investigated based on a graph-theoretic approach. By using combinatorial designs, a systematic construction method of multiple-edge protographs is proposed for regular QC LDPC codes with girth at least 12 and another method is proposed for regular QC LDPC codes with girth at least 14. Moreover, a construction algorithm of QC LDPC codes based on certain liftings of multiple-edge protographs is proposed and it is shown that the resulting QC LDPC codes have larger upper bounds on the minimum Hamming distance than those lifted from single-edge protographs. Simulation results are provided to compare the performance of the proposed QC LDPC codes with progressive edge-growth (PEG) LDPC codes and with PEG QC LDPC codes.**

***Index Terms*—Design theory, girth, inevitable cycle, minimum Hamming distance, multiple-edge protograph, quasi-cyclic (QC) low-density parity-check (LDPC) codes.**

I. Introduction

LOW-DENSITY parity-check (LDPC) codes [1] have been one of the major research topics in coding theory over the past decade due to their near capacity-approaching performance. Since low decoding complexity can be achieved by various iterative decoding algorithms, LDPC codes have been adopted in many practical applications. Especially, quasi-cyclic (QC) LDPC codes are well suited for hardware implementation using simple shift registers due to the regularity in their parity-check matrices.

Thorpe [2] introduced the concept of *protograph-based LDPC codes*, a class of LDPC codes lifted from protographs. QC LDPC codes belong to the protograph-based LDPC codes because they can be regarded as being lifted from protographs using cyclic permutations. Therefore, the performance of QC LDPC codes mainly depends on how to design their protographs as well as how to assign shift values that specify the cyclic permutations.

The performance of LDPC codes under message-passing iterative decoding algorithms depends on the girth of the codes because a message sent by a node along a cycle propagates back to the node itself after some iterations, which causes dependences among messages and performance degradation. Therefore, there have been lots of efforts to construct QC LDPC codes with large girth [3]–[12]. In [4], necessary and sufficient conditions on determining the girth of QC LDPC codes from circulant permutation matrices have been derived and some families of QC LDPC codes have been constructed. Most of QC LDPC codes with large girth are constructed based on algebraic structures [3]–[7], [9], [11] while some optimization algorithms and greedy search algorithms are used to find QC LDPC codes with large girth [8], [10], [12]. Various combinatorial designs have also been widely used to construct QC LDPC codes in order to guarantee girth at least 6 [7], [9], [13]–[15].

The girth of QC LDPC codes constructed from protographs is determined by the structure of the protograph, the lift size, and all the shift values. The papers [3], [5], [7], and [16] discuss an upper bound on the girth of QC LDPC codes, which depends only on the structure of the protograph. Especially, in [5], all substructures of multiple-edge protographs, which inevitably give rise to cycles of length up to 12, are searched but no construction method of multiple-edge protographs for QC LDPC codes with large girth is provided. The paper [7] identifies all substructures of single-edge protographs which inevitably give rise to cycles of length up to 20 in QC LDPC codes, and by using combinatorial designs, some single-edge protographs for girth larger than or equal to 18 and other single-edge protographs for girth larger than or equal to 14 are constructed.

Although the behavior of iterative message-passing decoders is mostly dominated by the pseudoweight of pseudocodewords [17], [18], the minimum Hamming distance still plays an important role because it characterizes the undetectable errors and provides an upper bound on the minimum pseudoweight of a code. Smarandache and Vontobel [19] derived two upper bounds on the minimum Hamming distance of QC LDPC

Manuscript received June 18, 2011; revised June 10, 2012; accepted February 18, 2013. Date of publication March 07, 2013; date of current version June 12, 2013. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2009-0081441). This paper was presented in part at the 2011 IEEE International Symposium on Information Theory.

H. Park, S. Hong, and J.-S. No are with the Department of Electrical Engineering and Computer Science, Institute of New Media and Communications, Seoul National University, Seoul 151-744, Korea (e-mail: hpark1@snu.ac.kr; fousbyus@ccl.snu.ac.kr; jsno@snu.ac.kr).

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

Communicated by P. O. Vontobel, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2013.2250574

codes, where one bound is applied when QC LDPC codes are explicitly given and the other bound can be applied even when only the protographs are given. It is shown by experiments that these upper bounds are very close to the actual minimum Hamming distance when the lift size for a protograph is large enough. Also, through several examples in [19], we can see that when the size and row- and column-weights of incidence matrices of protographs are given, these two upper bounds increase as the number of multiple edges increases in the protographs. Therefore, these upper bounds can be increased if multiple-edge protographs are used to construct QC LDPC codes, compared to the case of single-edge protographs. These two upper bounds are extended to cover puncturing cases and tightened for some specific cases [20].

In this paper, multiple-edge protographs, which can be lifted to QC LDPC codes with large girth, are investigated. A search for all single- and multiple-edge subgraphs, which inevitably generate cycles of certain lengths in QC LDPC codes, is systematically performed based on a graph-theoretic approach as an extension of the results in [5], [7], and [16]. Construction methods of multiple-edge protographs using various combinatorial designs are proposed and a lifting algorithm to construct regular QC LDPC codes with large girth is also proposed.

The remainder of the paper is organized as follows. Section II introduces QC LDPC codes, protographs, and the concept of inevitable cycles. In Section III, all single- and multiple-edge subgraphs that generate inevitable cycles in QC LDPC codes are fully searched. Based on these subgraph patterns, Section IV describes a design method for multiple-edge protographs of regular QC LDPC codes having girth larger than or equal to 12. In Section V, construction methods of multiple-edge protographs are proposed for regular QC LDPC codes having girth 14 when the variable node degree is 3 and they are generalized for regular QC LDPC codes with variable node degree larger than 3. In Section VI, a construction algorithm of QC LDPC codes that are lifted from multiple-edge protographs is proposed. It is also shown that the proposed QC LDPC codes have larger upper bounds on the minimum Hamming distance than those lifted from single-edge protographs and the performance of the proposed QC LDPC codes is verified via numerical analysis. Finally, the conclusions are provided in Section VII.

II. Inevitable Cycles of QC LDPC Codes

A. QC LDPC Codes

Let $\mathcal{C}$ be a binary LDPC code whose parity-check matrix H is a $J \times L$ array of $z \times z$ circulants or zero matrices as follows:

$$H = \begin{bmatrix} H_{0,0} & H_{0,1} & \cdots & H_{0,L-1} \\ H_{1,0} & H_{1,1} & \cdots & H_{1,L-1} \\ \vdots & \vdots & \ddots & \vdots \\ H_{J-1,0} & H_{J-1,1} & \cdots & H_{J-1,L-1} \end{bmatrix}$$

where a *circulant* $H_{j,l}$ is defined to be a matrix where each row is cyclically shifted to the right by one position with respect to the row above it. Such an LDPC code is called *quasi-cyclic* because applying circular shifts to the length-z subblocks of a codeword gives another codeword. Also, a bipartite graph, which has H as its incidence matrix, is called the *Tanner graph* of $\mathcal{C}$.

The *weight* of a circulant $H_{j,l}$ is defined as the number of the nonzero elements in its zeroth column and denoted by $\mathrm{wt}(H_{j,l})$. A circulant is entirely described by the positions of the nonzero elements in its zeroth column. Let i, $0 \leq i \leq z-1$, be the index of the $(i+1)$st element in the zeroth column. Then, the *shift value* (s) of a circulant is/are defined as the index (indices) of the nonzero element(s) in the zeroth column. Note that a shift value takes value in the set $\{0, 1, \ldots, z-1\} \cup \{\infty\}$, where ∞ is used as the shift value of a zero matrix $H_{i,j}$.

QC LDPC codes can be fully represented by binary polynomials as shown, e.g., in [19]. This polynomial representation is based on the isomorphism between $z \times z$ binary circulants and the polynomial ring $\mathbb{F}_2[x]/\langle x^z + 1\rangle$. The *polynomial parity-check matrix* $H(x)$ of $\mathcal{C}$ is defined as

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

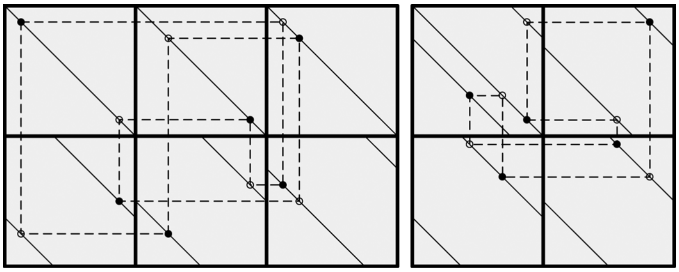
where $h_{j,l}(x) = \sum_{i=0}^{z-1} h_{j,l,i}x^i \in \mathbb{F}_2[x]/\langle x^z + 1\rangle$ and $h_{j,l,i}$ is the element with index i in the zeroth column of $H_{j,l}$. We can see that the number of nonzero terms in $h_{j,l}(x)$, which is denoted by $\mathrm{wt}(h_{j,l}(x))$, is equal to $\mathrm{wt}(H_{j,l})$ and the degrees of all nonzero terms in $h_{j,l}(x)$ are equivalent to the shift values of $H_{j,l}$.

The *protograph* [2] of a QC LDPC code $\mathcal{C}$ is a bipartite graph whose incidence matrix is $P = [p_{j,l}]$, where $p_{j,l} = \mathrm{wt}(H_{j,l})$. There are two kinds of nodes in the protograph: namely, check nodes correspond to rows in P and variable nodes correspond to columns in P. The Tanner graph of $\mathcal{C}$ is constructed by copying the protograph z times and cyclically permuting the same z edges. (If $p_{j,l} \geq 2$, there are multiple edges between the check node with index j and the variable node with index l in the protograph.) Such a copy-and-permute operation is called *lifting* and the length of a subblock z is also called the *lift size* of $\mathcal{C}$. A shift value is assigned to each edge in the protograph so that an edge is lifted by using the cyclic permutation with the assigned shift value to generate $\mathcal{C}$. Note that, because of the equivalence of a bipartite graph and its incidence matrix, in this paper, the term "protograph" refers to both of them.

B. Inevitable Cycles

Necessary and sufficient conditions on the existence of cycles in the Tanner graph of QC LDPC codes are derived in terms of shift values in [4]. These conditions are only applied to single-edge protographs but they can be naturally extended to cover the case of multiple-edge protographs as in the upcoming Lemma 1.

Let $G = (V, E)$ denote a graph with a vertex set V and an edge set E. Let v_k (e_k) represent a vertex (an edge) in V (E). A *walk* is an alternating sequence of vertices and edges, denoted by $v_{i_0}e_{i_0}v_{i_1} \cdots v_{i_{n-1}}e_{i_{n-1}}v_{i_n}$, where the vertices v_{i_j} and $v_{i_{j+1}}$ are the endpoints of the edge e_{i_j}. The *length of a walk* W, denoted



(a) (b)

Fig. 1. Examples of inevitable cycles in QC LDPC codes. (a) Inevitable cycle of length 12. (b) Inevitable cycle of length 10.

by $l(W)$, is defined as the number of edges in W. A walk is *closed* if $v_{i_n} = v_{i_0}$ and a walk is *nonreversing* if $e_{i_j} \neq e_{i_{j+1}}$ for $j = 0, 1, \ldots, n-2$. A closed walk is said to be *tailless* if $e_{i_{n-1}} \neq e_{i_0}$. In this paper, only connected graphs are considered and a *cycle* is defined as a closed walk whose traversed vertices and edges are all distinct. Also, the length of the shortest cycle in a graph is called the *girth* of the graph.

Cycles in the Tanner graph of a QC LDPC code are closely related to tailless nonreversing closed (TNC) walks in its protograph. The *shift sum* of a walk W in a protograph, denoted by $s(W)$, is defined as the alternating sum of shift values assigned to the edges in W, that is, $s(W) = \sum_{j=0}^{l(W)-1} (-1)^j (\text{shift value of } e_{i_j})$. Lemma 1 shows necessary and sufficient conditions for a cycle of a certain length in the Tanner graph of a QC LDPC code to be generated from the underlying (single-edge or multiple-edge) protograph. Its proof is directly derived from the results in [4] and [16].

Lemma 1: Let $\mathcal{W}_l$ denote the set of all TNC walks of length l in a protograph. Suppose that a QC LDPC code is lifted from the protograph with lift size z. Then, the Tanner graph of this QC LDPC code has a cycle of length l if and only if there exists a TNC walk $W \in \mathcal{W}_l$ such that $s(W) = 0 \bmod z$ and W does not contain any shorter TNC walks whose shift sum equals zero.

The girth of QC LDPC codes is determined by the structure of the protograph, the lift size, and all the shift values assigned to the edges. However, we can derive an upper bound on the girth of QC LDPC codes lifted from protographs without considering the lift size and the shift values based on the concept of inevitable cycles [3], [5], [7].

Definition 1: An *inevitable cycle* induced by a protograph is defined as a cycle that always appears in the QC LDPC code lifted from the protograph regardless of the lift size and the shift values.

It is well known that a QC LDPC code whose protograph has the 2×3 (or 3×2) all-one matrix as a submatrix must have inevitable cycles of length 12 [3], [4]. In other words, the girth of this QC LDPC code is less than or equal to 12. Such an inevitable cycle of length 12 is depicted in Fig. 1(a). In QC LDPC codes lifted from multiple-edge protographs, inevitable cycles can also appear. As an example, Fig. 1(b) shows an inevitable cycle of length 10, which appears in QC LDPC codes lifted from protographs with double edges. We can see that for a certain subgraph structure, inevitable cycles are always generated no matter what shift values are assigned to the edges.

III. Subgraphs of Multiple-Edge Protographs Inducing Inevitable Cycles

In order for QC LDPC codes to have large girth, their protographs should not contain subgraphs which induce short inevitable cycles in the QC LDPC codes, and thus, it is necessary to find out all such subgraphs. From now on, the terms "*an inevitable-cycle-inducing (ICI) subgraph of length* $2i$" will refer to a subgraph inducing inevitable cycles of length $2i$. In [5], ICI subgraphs of length up to 12 in single- and multiple-edge protographs were fully investigated and, in [7], all ICI subgraphs of lengths 12 to 20 in single-edge protographs were searched by a brute force method. After that, a graph-theoretical framework was provided in [16], which can be used to search all single- and multiple-edge ICI subgraphs. In this section, we will search and provide all ICI subgraphs as an extension of [5], [7], and [16].

Define $\mathcal{P}_{2i}$ as the set of all irreducible ICI subgraphs of length $2i$ satisfying the following conditions.

1) A subgraph $P \in \mathcal{P}_{2i}$ induces inevitable cycles of length $2i$ in the QC LDPC code.
2) A subgraph $P \in \mathcal{P}_{2i}$ does not contain any proper subgraph, which induces inevitable cycles of length less than or equal to $2i$.
3) The number of rows in a subgraph $P \in \mathcal{P}_{2i}$ is not larger than that of columns.
4) From each isomorphic class in $\mathcal{P}_{2i}$, only one protograph must be chosen as a representative of that class.

The conditions 1) and 2) guarantee that if a protograph does not have any subgraph $P \in \mathcal{P}_{2i'}$ for $i' < i$, the QC LDPC code appropriately lifted from this protograph has girth larger than or equal to $2i$. A subgraph $P \in \mathcal{P}_{2i}$ is irreducible because condition 2) implies that if any edge is removed from P, it cannot induce inevitable cycles of length $2i$. Conditions 3) and 4) are required to choose a unique representative for each isomorphic class of subgraphs inducing inevitable cycles of length $2i$.

For identifying $\mathcal{P}_{2i}$, we need to investigate the relationship between inevitable cycles and TNC walks. A TNC walk W of a protograph is called *abelian-forcing*[16] if for each edge in W, the number of traversals of the edge in a direction is the same as that in the opposite direction. Clearly, the shift sum of abelian-forcing TNC walks is zero regardless of the shift values of their edges. An abelian-forcing TNC walk is said to be *simple* if it does not contain any shorter abelian-forcing TNC subwalk. It is obvious that inevitable cycles of QC LDPC codes are generated from simple abelian-forcing TNC (SAF-TNC) walks in protographs.

Lemma 2: Any abelian-forcing TNC walk contains at least two different cycles. ■

Proof: Consider an abelian-forcing TNC walk $W = v_{i_0} e_{i_0} v_{i_1} \cdots v_{i_{n-1}} e_{i_{n-1}} v_{i_n}$. There exist k and l with $k \neq l$ such that $i_k = i_l$, i.e., $v_{i_k} = v_{i_l}$. Also, there exists a path $v_m e_{i_{p-1}} v_{i_p} \cdots v_{i_q} e_{i_q} v_m$ in W such that all vertices from v_{i_p} to v_{i_q} are distinct. Since W is nonreversing and tailless, that path forms a cycle, and thus, W contains at least one cycle.

Assume that W contains only one cycle. Since W is abelian-forcing, there exists a path $v_f e_g v_h e_{i_{a-1}} v_{i_a} \cdots v_{i_b} e_{i_b} v_h e_g v_f$ in

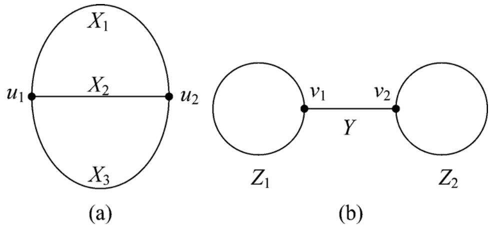


Fig. 2. Theta graph and dumbbell graph. (a) Theta graph. (b) Dumbbell graph.

W such that $v_{i_j} \neq v_h$ for all $j = a, a+1, \ldots, b$. This contradicts the assumption that W contains only one cycle because in W, a vertex cannot go back to itself without reversing. Therefore, W contains at least two different cycles.

As in [16], two classes of graphs are defined as illustrated in Fig. 2.

Definition 2 ([16]): An (x_1, x_2, x_3)*-theta graph*, denoted by $T(x_1, x_2, x_3)$, is a graph consisting of two vertices, each of degree three, that are connected to each other via three disjoint paths X_1, X_2, X_3 of length $x_1 \geq 1, x_2 \geq 1$, and $x_3 \geq 1$, respectively. A $(z_1, z_2; y)$*-dumbbell graph*, denoted by $D(z_1, z_2; y)$, is a connected graph consisting of two edge-disjoint cycles Z_1 and Z_2 of length $z_1 \geq 1$ and $z_2 \geq 1$, respectively, that are connected by a path Y of length $y \geq 0$.

Lemma 3: Connecting two different cycles always results in either a theta graph or a dumbbell graph.

Proof: Let C_1 and C_2 denote two different cycles. Then, C_1 and C_2 can be connected in only three ways: The number of common vertices in C_1 and C_2 is 1) 0, 2) 1, or 3) larger than or equal to 2. For cases 1) and 2), C_1 and C_2 form $D(z_1, z_2; y)$ with $y > 0$ or $y = 0$, respectively. In case 3), $T(x_1, x_2, x_3)$ is formed where $C_1 = X_1 \cup X_2$, $C_2 = X_2 \cup X_3$, and $x_2 + 1$ is the number of the common vertices. ■

Lemma 4: The lengths of SAF-TNC walks in $T(x_1, x_2, x_3)$ and $D(z_1, z_2; y)$ are $2(x_1 + x_2 + x_3)$ and $2(z_1 + z_2) + 4y$, respectively.

Proof: Consider $T(x_1, x_2, x_3)$ in Fig. 2(a). Let u_1 and u_2 denote the left and the right vertices of degree three, respectively, and let X_1, X_2, and X_3 be the paths from u_1 to u_2. Also, let $\bar{X}_1$, $\bar{X}_2$, and $\bar{X}_3$ denote the reverse paths of X_1, X_2, and X_3, respectively. Then, we can see that the SAF-TNC walk $X_1\bar{X}_2X_3\bar{X}_1X_2\bar{X}_3$ has the length $2(x_1+x_2+x_3)$ and any other SAF-TNC walks possibly generated in $T(x_1, x_2, x_3)$ have the same length. ■

Similarly, consider $D(z_1, z_2; y)$ in Fig. 2(b). Let v_1 and v_2 denote the left and the right vertices of degree three, respectively, and let Z_1 and Z_2 be the cycles rotating clockwise from v_1 and v_2, respectively, and let Y be the path from v_1 to v_2. Also, let $\bar{Z}_1$, $\bar{Z}_2$, and $\bar{Y}$ denote the reverse paths of Z_1, Z_2, and Y, respectively. Then, we can see that the SAF-TNC walk $Z_1YZ_2\bar{Y}\bar{Z}_1Y\bar{Z}_2\bar{Y}$ has the length $2(z_1+z_2)+4y$ and any other SAF-TNC walks possibly generated in $D(z_1, z_2; y)$ have the same length. ■

Note that if any edge is removed from $T(x_1, x_2, x_3)$ or $D(z_1, z_2; y)$, those inherent SAF-TNC walks disappear, and thus, $T(x_1, x_2, x_3)$ and $D(z_1, z_2; y)$ are of irreducible form. Now, we will check whether it is sufficient to only consider theta graphs and dumbbell graphs for $\mathcal{P}_{2i}$.

Lemma 5: Suppose that a graph G contains at least one theta graph or one dumbbell graph as its proper subgraphs. The shortest SAF-TNC walk in G occurs only in a theta graph or a dumbbell graph.

Proof: Let W denote the shortest SAF-TNC walk and assume that W traverses all edges in G. From Lemmas 2 and 3, W should contain a theta graph or a dumbbell graph. Consider the following two cases: 1) G has some theta graphs, 2) G does not have any theta graphs.

In case 1), we first note that $l(W)$ is at least twice the number of edges in G due to the definition of abelian-forcing TNC walks. The SAF-TNC walk only generated by a theta graph in G is shorter than W because the SAF-TNC walk has the length exactly twice the number of edges in the theta graph. This contradicts the assumption that W is the shortest one. In case 2), we note that a SAF-TNC walk should traverse the edge not belonging to any cycles at least four times because if the walk traverses the edge twice, the walk will include two SAF-TNC walks each of which occurs on different sides of the edge. Since cycles in G are connected with each other via only one path which does not belong to any cycles, the SAF-TNC walk only generated by a dumbbell graph in G is shorter than W. This contradicts the assumption that W is the shortest one. Therefore, W occurs only in a theta graph or a dumbbell graph. ■

In the next theorem, $\mathcal{P}_{2i}$ will be identified.

Theorem 1: $\mathcal{P}_{2i}$ is the collection of all $T(x_1, x_2, x_3)$'s with $2(x_1 + x_2 + x_3) = 2i$ and all $D(z_1, z_2; y)$'s with $2(z_1 + z_2) + 4y = 2i$.

Proof: From Lemmas 2 and 5, any subgraph $P \in \mathcal{P}_{2i}$ should be either a theta graph or a dumbbell graph. Therefore, the proof is completed by Lemma 4. ■

Remark 1: Lemmas 3 and 4 are known results from [16] and Theorem 1 is similar to Theorem 4.5 in [16]. However, in this paper, $\mathcal{P}_{2i}$ is formally defined as the set of all irreducible ICI subgraphs of length $2i$ and it is clearly shown in Theorem 1 that $\mathcal{P}_{2i}$ is equivalent to a collection of all $T(x_1, x_2, x_3)$'s with $2(x_1 + x_2 + x_3) = 2i$ and all $D(z_1, z_2; y)$'s with $2(z_1 + z_2) + 4y = 2i$. For a natural flow from the definition of $\mathcal{P}_{2i}$ to Theorem 1, we supplement Lemmas 2 and 5 which are not found in [16].

Now, we can find all single- and multiple-edge ICI subgraphs from $T(x_1, x_2, x_3)$ and $D(z_1, z_2; y)$. A representative of an isomorphic class in $\mathcal{P}_{2i}$ can be uniquely chosen by selecting parameters satisfying the following conditions.

1) $x_1 \geq x_2 \geq x_3 \geq 1$.
2) x_1, x_2, x_3 are all even or all odd.
3) $z_1 \geq z_2 \geq 2, y \geq 0$.
4) z_1 and z_2 are even.

Note that the second and the fourth conditions follow from the fact that each subgraph $P \in \mathcal{P}_{2i}$ is a bipartite graph.

According to Theorem 1, each integer solution of the equations $2(x_1 + x_2 + x_3) = 2i$ and $2(z_1 + z_2) + 4y = 2i$ yields an ICI subgraph in $\mathcal{P}_{2i}$. Note that all ICI subgraphs of any length can be easily found and $T(x_1, 1, 1)$ and $D(z_1, 2; y)$ are ICI subgraphs having multiple edges. All ICI subgraphs of length up to 20 are listed as a form of theta or dumbbell graphs in Table I

TABLE I
ALL ICI SUBGRAPHS OF LENGTH UP TO 20 (T: THETA GRAPH, D: DUMBBELL GRAPH, S: SINGLE EDGE, M: MULTIPLE EDGE)

$\mathcal{P}_{2i}$		$\mathcal{P}_6$	$\mathcal{P}_8$	$\mathcal{P}_{10}$	$\mathcal{P}_{12}$		$\mathcal{P}_{14}$		$\mathcal{P}_{16}$				$\mathcal{P}_{18}$			$\mathcal{P}_{20}$					
T	x_1	1	-	3	2	-	3	5	4	-	-	-	3	5	7	4	6	-	-	-	-
	x_2	1	-	1	2	-	3	1	2	-	-	-	3	3	1	4	2	-	-	-	-
	x_3	1	-	1	2	-	1	1	2	-	-	-	3	1	1	2	2	-	-	-	-
Type		M	-	M	S	-	S	M	S	-	-	-	S	S	M	S	S	-	-	-	-
D	z_1	-	2	-	2	4	-	-	2	4	4	6	-	-	-	2	4	4	6	6	8
	z_2	-	2	-	2	2	-	-	2	2	4	2	-	-	-	2	2	4	2	4	2
	y	-	0	-	1	0	-	-	2	1	0	0	-	-	-	3	2	1	1	0	0
Type		-	M	-	M	M	-	-	M	M	S	M	-	-	-	M	M	S	M	S	M

and all ICI subgraphs of length up to 14 are listed as a form of incidence matrices as follows:

$$\begin{aligned}
\mathcal{P}_6 &= [3]\\
\mathcal{P}_8 &= [2 \quad 2]\\
\mathcal{P}_{10} &= \begin{bmatrix} 2 & 1\\ 1 & 1 \end{bmatrix}\\
\mathcal{P}_{12} &= \begin{bmatrix} 2 & 1\\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 1\\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1\\ 1 & 1 & 1 \end{bmatrix}\\
\mathcal{P}_{14} &= \begin{bmatrix} 2 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1\\ 1 & 1 & 0\\ 1 & 0 & 1 \end{bmatrix}
\end{aligned}$$

where the single-edge ICI subgraphs in Table I were also listed in [7] and all ICI subgraphs of length up to 12 were also listed in [5]. Note that the transpose of each ICI subgraph also generates inevitable cycles of the same length, and thus, $\mathcal{P}_{2i}$ will be used to denote both the listed matrices and their transposes.

IV. CONSTRUCTION OF REGULAR PROTOGRAPHS AVOIDING INEVITABLE CYCLES OF LENGTH LESS THAN 12

In this section, we will construct regular protographs that avoid inevitable cycles of length less than 12 in QC LDPC codes. Consider a regular $J \times L$ protograph of which the column- and row-weights are d_v and d_c, respectively, where $J < L$. If triple or more edges exist in the protograph, the girth of the lifted QC LDPC code is limited to 6 because of $\mathcal{P}_6 = [3]$. Therefore, only protographs with single and double edges will be considered in this paper. Let n_2 denote the number of double edges in the protograph.

Most of the considered protographs have at least two cycles, and thus, they always induce some inevitable cycles according to Lemmas 3 and 4. Note that even if a protograph is designed not to contain any $\mathcal{P}_{2i'}$ with $i' < i$ so that inevitable cycles of length less than $2i$ are avoided, this protograph may have some inevitable cycles of length larger than or equal to $2i$.

To construct protographs that do not induce inevitable cycles of length less than 10, a pair of 2's should not appear in any row or in any column of the protograph to avoid $\mathcal{P}_8$. As shown in the next lemma, the number of double edges in a protograph should be upper bounded by the number of check nodes to construct QC LDPC codes with girth larger than or equal to 10.

Lemma 6: If a $J \times L$ protograph does not induce inevitable cycles of length less than 10, then $n_2 \leq J$.

Proof: If $n_2 > J$, there always exists a row that has at least two 2's, and thus, the protograph contains $\mathcal{P}_8$. This contradicts the assumption. ■

In order for QC LDPC codes to have girth larger than or equal to 12, their protographs should not contain $\mathcal{P}_6$, $\mathcal{P}_8$, and $\mathcal{P}_{10}$. We will explain that an incidence matrix of a *balanced ternary design* (BTD) with $\rho_2 = 1$ and $\lambda = 2$ is also the incidence matrix of a regular protograph with $n_2 = J$ that does not induce inevitable cycles of length less than 12.

Definition 3 ([21]): A BTD $(v, b; \rho_1, \rho_2, r; k, \lambda)$ is an arrangement of v elements $\{1, 2, \ldots, v\}$ into b multisets, or blocks, each of cardinality k, $k \leq v$, satisfying that 1) each element appears $r = \rho_1 + 2\rho_2$ times altogether, with multiplicity one in exactly ρ_1 blocks, with multiplicity two in exactly ρ_2 blocks and 2) every pair of distinct elements appears λ times, i.e., if $m_{j,h}$ is the multiplicity of element j in the hth block, then for any elements i and j with $i \neq j$, we have $\sum_{h=1}^{b} m_{i,h} m_{j,h} = \lambda$.

Note that a $v \times b$ incidence matrix of a BTD $(v, b; \rho_1, \rho_2, r; k, \lambda)$ is simply expressed as $[m_{j,h}]$ and the column- and row-weights are k and r, respectively.

Theorem 2: A $J \times L$ incidence matrix of a BTD $(J, L; \rho_1, \rho_2, d_\mathrm{c}; d_\mathrm{v}, \lambda)$ with $\rho_2 = 1$ and $\lambda = 2$ does not contain $\mathcal{P}_6$, $\mathcal{P}_8$, and $\mathcal{P}_{10}$.

Proof: Let P_{BTD} be an incidence matrix of a BTD $(J, L; \rho_1, \rho_2, d_\mathrm{c}; d_\mathrm{v}, \lambda)$ with $\rho_2 = 1$ and $\lambda = 2$. Since every element of this BTD can have multiplicity up to two, $\mathcal{P}_6$ does

TABLE II
REGULAR PROTOGRAPHS WITH $n_2 = J$ AVOIDING INEVITABLE CYCLES OF LENGTH LESS THAN 12 CONSTRUCTED FROM BTDS FOR $d_c \leq 15$

J	6	12	9	20	12	30	42	48	42	15	60
L	12	24	27	40	48	60	63	64	84	75	100
d_v	3	4	3	5	3	6	8	9	7	3	9
d_c	6	8	9	10	12	12	12	12	14	15	15

$$\begin{bmatrix} 2&1&1&1&1&0&0&0&0&0&0&0\\ 1&0&0&0&0&2&1&1&1&0&0&0\\ 0&2&0&0&0&1&0&0&0&1&1&1\\ 0&0&2&0&0&0&1&1&0&1&1&0\\ 0&0&0&2&0&0&1&0&1&1&0&1\\ 0&0&0&0&2&0&0&1&1&0&1&1 \end{bmatrix} \qquad \begin{bmatrix} 2&0&0&0&0&1&1&0\\ 0&2&0&1&0&0&1&0\\ 0&0&2&0&1&0&1&0\\ 1&0&0&2&0&0&0&1\\ 0&1&0&0&2&0&0&1\\ 0&0&1&0&0&2&0&1 \end{bmatrix}$$

(a) (b)

Fig. 3. Two regular protographs with $d_v = 3$ and $n_2 = 6$ avoiding inevitable cycles of length less than 12. (a) 6 × 12. (b) 6 × 8.

not appear in P_{BTD}. The condition $\rho_2 = 1$ implies that 2 appears once in each row of P_{BTD} and $\lambda = 2$ implies that each column of P_{BTD} can have at most one 2. Hence, P_{BTD} does not contain $\mathcal{P}_8$. Since a pair of distinct elements will appear at least three times in this BTD if P_{BTD} has $\mathcal{P}_{10}$ as its submatrix, P_{BTD} does not contain $\mathcal{P}_{10}$. ■

All possible BTDs with $r \leq 15$ are given in [22]. Table II lists all parameters of regular protographs with $d_c \leq 15$ avoiding inevitable cycles of length less than 12 constructed from BTDs.

Example 1: An incidence matrix of BTD $(6, 12; 4, 1, 6; 3, 2)$ is shown in Fig. 3(a) and we can see that any ICI subgraph $\mathcal{P}_{2i}$ for $i \leq 5$ does not appear.

As shown in Table II, the incidence matrices of BTDs with $\rho_2 = 1$ and $\lambda = 2$ do not provide a sufficiently large number of regular protographs. In fact, the condition that every pair of distinct elements appears exactly twice is not necessary and the condition that each pair of distinct elements appears at most twice is enough for constructing regular protographs avoiding inevitable cycles of length less than 12. Besides the regular protographs listed in Table II, there are many regular protographs with $n_2 = J$ avoiding inevitable cycles of length less than 12.

Example 2: We want to find the smallest regular protograph with $d_v = 3$ and $n_2 = J$ avoiding inevitable cycles of length less than 12. We first derive a necessary condition for the existence of such a regular protograph by regarding the protograph as an incidence matrix of a block design as shown in Definition 3. There are total $\binom{J}{2}$ pairs of distinct elements in $\{1, 2, \ldots, J\}$, and, on the other hand, the number of all possible pairs of distinct elements in such a block design is $n_2 \cdot 2 + (L - n_2) \cdot \binom{3}{2}$. Since every pair of distinct elements appears at most twice, that is, $\mathcal{P}_{10}$ does not appear in the protograph, we have the necessary condition

$$2 \cdot \binom{J}{2} \geq n_2 \cdot 2 + (L - n_2) \cdot \binom{3}{2}. \tag{1}$$

For $J = 3$, due to $L \geq 4$ and $n_2 = 3$, the necessary condition (1) is not satisfied. For $J = 4$, by counting the edges in the protograph, the equality $Jd_c = d_v L$, that is, $4d_c = 3L$ holds. Since the smallest integer root of this equality is $(d_c, L) = (6, 8)$, we have $L \geq 8$ and (1) is not satisfied. Similarly, for $J = 5$, L should be larger than or equal to 10 and (1) is not satisfied either.

$$\left[\begin{array}{c|c|c} \begin{matrix} 2 & & & & \\ & 2 & & & \\ & & \ddots & & \\ & & A & & \\ & & & \ddots & \\ & & & 2 & \\ & & & & 2 \end{matrix} & B & T \\ \hline F & G & O \end{array}\right]$$

Fig. 4. Structure of regular protographs avoiding inevitable cycle of length less than 14.

For $J = 6$, from $6d_c = 3L$, the smallest possible protograph has size 6 × 8 and it satisfies (1). By first constructing a 6 × 6 regular matrix where each column and each row has one 2 and then properly adding two columns only consisting of 0's and 1's, a 6 × 8 regular protograph can be constructed as given in Fig. 3(b). This is the smallest regular protograph with $d_v = 3$ and $n_2 = J$ avoiding inevitable cycles of length less than 12.

V. CONSTRUCTION OF REGULAR PROTOGRAPHS AVOIDING INEVITABLE CYCLES OF LENGTH LESS THAN 14

Now, we will focus on the construction of regular multiple-edge protographs avoiding inevitable cycles of length less than 14. By avoiding only the third ICI subgraphs of $\mathcal{P}_{12}$, a systematic construction method of single-edge regular protographs avoiding inevitable cycles of length less than 14 was provided in [7]. Since multiple-edge protographs are considered, we have to additionally avoid $\mathcal{P}_8$, $\mathcal{P}_{10}$, and the remaining two ICI subgraphs of $\mathcal{P}_{12}$, which makes the problem more complicated. In this section, systematic construction methods for multiple-edge protographs are proposed based on various combinatorial designs.

Consider a regular $J \times L$ protograph whose column- and row-weights are d_v and d_c, respectively. We remind the reader that n_2 denotes the number of double edges in the protograph. Assume that $d_v \geq 3$ because regular QC LDPC codes with $d_v = 2$ are not used in general due to their poor performance.

Using row and column permutations, every regular protograph not inducing inevitable cycles of length less than 14 can be represented as in Fig. 4. The $n_2 \times n_2$ submatrix A has n_2 2's as its diagonal elements and the other elements of A should be zero to avoid the first ICI subgraph of $\mathcal{P}_{12}$. F is a $(J - n_2) \times n_2$ submatrix consisting of columns of weight $d_v - 2$. By appropriate column permutation of all but A and F in the protograph, all the columns whose lower parts have nonzero weight form the submatrix $[B^T | G^T]^T$, and the remaining columns form the submatrix $[T^T | O^T]^T$, where T has column-weight d_v and O is an all-zero matrix. Let G and T be $J_G \times L_G$ and $J_T \times L_T$ matrices, respectively.

By Lemma 6, n_2 cannot be larger than J. Moreover, if the regular protographs, which do not induce inevitable cycles of length less than 14, are considered for $d_v = 3$, the following theorem provides an additional condition on n_2.

Theorem 3: Assume that a regular protograph with $d_{\mathrm{v}} = 3$ and $d_{\mathrm{c}} \geq 4$ does not induce inevitable cycles of length less than 14. Then, $n_2 \leq J - 2$.

Proof: The inequality $n_2 \leq J$ holds by Lemma 6. The protograph with $n_2 = J$ should be of the form $[A|B|T]$ from Fig. 4 and the submatrix A is no longer a diagonal matrix due to $d_{\mathrm{v}} = 3$. Therefore, A should contain the first ICI subgraph of $\mathcal{P}_{12}$ because each column of A also contains exactly one 1, and hence, n_2 should be less than J.

Now suppose that $n_2 = J - 1$. The protograph has the form of Fig. 4 and F is the $1 \times (J-1)$ all-1 matrix. Due to F, d_{c} cannot be less than $J - 1$. If $d_{\mathrm{c}} > J - 1$, G becomes the $1 \times (d_{\mathrm{c}} - (J-1))$ all-1 matrix and each column of B has a pair of 1's, which generates $\mathcal{P}_{10}$ in the union of A, B, F, and G. If $d_{\mathrm{c}} = J - 1$, the protograph is made up of only A, T, F, and O, and the size of T is $(J-1) \times (J-1)(J-3)/3$ because the column- and row-weights of T are 3 and $J - 3$, respectively. Since T should not have $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ as its submatrix to avoid the second and the third ICI subgraphs of $\mathcal{P}_{12}$ in the union of A, B, and T, a pair of 1's in the same column can appear at most once in T. To satisfy this condition, the number of all possible columnwise pairs of 1's should be larger than or equal to the number of actual columnwise pairs of 1's in T. Therefore, we have $\binom{J-1}{2} \geq \binom{3}{2} \cdot (J-1)(J-3)/3$, i.e., $J \leq 4$. Due to $d_{\mathrm{c}} = J - 1$, this contradicts the assumption of $d_{\mathrm{c}} \geq 4$. ■

Based on Theorem 3, the case of $d_{\mathrm{v}} = 3$ and $n_2 = J - 2$ is considered in Section V-A and the construction method of regular protographs for $d_{\mathrm{v}} = 3$ and $n_2 = J - 2$ is extended not only to the case of $d_{\mathrm{v}} = 3$ and $n_2 < J - 2$ but also to the case of $d_{\mathrm{v}} \geq 4$ in Section V-B.

A. Regular Protographs With $d_{\mathrm{v}} = 3$ *and* $n_2 = J - 2$

In this section, we elaborate the construction of regular protographs with $d_{\mathrm{v}} = 3$ and $n_2 = J - 2$. Moreover, we derive necessary conditions on d_{c} and J for the existence of regular protographs with $d_{\mathrm{v}} = 3$ and $n_2 = J - 2$ which avoid inevitable cycles of length less than 14 as follows.

Theorem 4: Assume that a regular protograph with $d_{\mathrm{v}} = 3$, $d_{\mathrm{c}} \geq 4$, and $n_2 = J - 2$ does not induce inevitable cycles of length less than 14. Then, d_{c} and J should satisfy either

1) $J \equiv 5 \bmod 6$, $J \geq 11$, and $d_{\mathrm{c}} = (J+1)/2$; or
2) $J \equiv 2 \bmod 6$, $J \geq 14$, and $d_{\mathrm{c}} = (J-2)/2$; or
3) $J \equiv 3 \bmod 6$, $J \geq 9$, and $d_{\mathrm{c}} = (J-1)/2,\ (J+1)/2$; or
4) $J \equiv 1 \bmod 6$, $J \geq 13$, and $d_{\mathrm{c}} = (J-1)/2$; or
5) $J \equiv 0 \bmod 6$, $J \geq 12$, and $d_{\mathrm{c}} = (J-2)/2,\ J/2$; or
6) $J \equiv 4 \bmod 6$, $J = 10$, and $d_{\mathrm{c}} = 6$.

Proof: By counting the edges in the protograph, we have $d_{\mathrm{c}}J = d_{\mathrm{v}}L$. Since $d_{\mathrm{v}} = 3$ and L is an integer, $d_{\mathrm{c}}J \equiv 0 \bmod 3$. Also, the submatrix F in Fig. 4 is a $2 \times (J-2)$ matrix consisting of weight-1 columns. Consider two cases: 1) F contains an all-1 row, 2) F does not contain an all-1 row.

For case 1), if $d_{\mathrm{c}} > J-2$, the ICI subgraph $\mathcal{P}_{10}$ appears in the union of A, B, F, and G. If $d_{\mathrm{c}} = J-2$, G is a $2 \times (J-2)$ matrix with an all-1 row at the complementary row position from the all-1 row of F. Then, there exist a row containing a pair of 1's in B because B has column-weight 2 and so B has a total of $2(J-2)$ 1's, which generates the second ICI subgraph of $\mathcal{P}_{12}$ in the union of A, B, and G. Therefore, case 1) is impossible.

TABLE III
ALL POSSIBLE REGULAR PROTOGRAPHS AVOIDING INEVITABLE CYCLES OF LENGTH LESS THAN 14 WHEN $d_{\mathrm{v}} = 3$ AND $n_2 = J - 2$ FOR $J \leq 26$

J	9	10	11	12	13	14	15	16	17
L	12, 15	20	22	20, 24	26	28	35, 40	–	51
d_{c}	4, 5	6	6	5, 6	6	6	7, 8	–	9
J	18	19	20	21	22	23	24	25	26
L	48, 54	57	60	70, 77	–	92	88, 96	100	104
d_{c}	8, 9	9	9	10, 11	–	12	11, 12	12	12

For case 2), if a column of G has a pair of 1's, the column including this pair in the protograph and another column in the union of A and F generate $\mathcal{P}_{10}$. Therefore, no column of F and G can have a pair of 1's. Since the number of columns in F is $J-2$ and the total number of columns in F and G is $2d_{\mathrm{c}}$, we have $(J-2)/2 \leq d_{\mathrm{c}}$, where the equality holds when B and G do not appear in the protograph. If a row of B has a pair of 1's, either $\mathcal{P}_{10}$ or the second ICI subgraph of $\mathcal{P}_{12}$ must occur in the union of A, B, F, and G. Therefore, each row of B can have at most one 1 so that the number of 1's in B cannot exceed the number of rows in B. Since the column-weight of B is 2 and B has $2(2d_{\mathrm{c}} - (J-2))$ 1's, we obtain $d_{\mathrm{c}} \leq 3(J-2)/4$ from $2(2d_{\mathrm{c}} - (J-2)) \leq J - 2$. Finally, it remains to determine the structure of T such that the submatrix $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ does not appear in the union of B and T to prevent the second ICI subgraph of $\mathcal{P}_{12}$. As in the proof of Theorem 3, by counting the number of columnwise pairs of 1's in B and T, we obtain the condition $\binom{2}{2} \cdot (2d_{\mathrm{c}} - (J-2)) + \binom{3}{2} \cdot (d_{\mathrm{c}}J/3 - 2d_{\mathrm{c}}) \leq \binom{J-2}{2}$ yielding $d_{\mathrm{c}} \leq (J-1)(J-2)/(2(J-4))$.

The aforementioned conditions on d_{c} and J are summarized as follows:

$$d_{\mathrm{c}}J \equiv 0 \bmod 3$$

$$\frac{J-2}{2} \leq d_{\mathrm{c}} \leq \min\left\{\frac{3}{4}(J-2), \frac{(J-1)(J-2)}{2(J-4)}\right\}.$$

Since d_{c} and J are integers, the aforementioned conditions reduce to simple linear relations with respect to J modulo 6 as given in the theorem statement. ■

In Theorem 4, all possible regular protographs avoiding inevitable cycles of length less than 14 are provided for $d_{\mathrm{v}} = 3$ and $n_2 = J-2$, and Table III only lists those for $J \leq 26$ among them.

Now, we focus on the existence problem and the construction of the regular protographs with the parameters found in Theorem 4. Note that the proposed protographs we will construct may not be all instances with the parameters in Theorem 4 but we provide at least one instance per each set of parameters and also note that $J_G = 2$, $L_G = 2d_{\mathrm{c}} - (J-2)$, $J_T = J - 2$, and $L_T = d_{\mathrm{c}}(J-6)/3$. For given J and d_{c}, the matrices B, T, F, and G can be constructed step by step as follows.

1. For constructing B and T at once, an incidence matrix of a combinatorial block design suitably chosen for each case in Theorem 4 is modified such that it has size $J_T \times (L_G + L_T)$, whereby the L_G columns corresponding to B have disjoint pairs of 1's (these pairs have no overlap at all), the other columns have weight 3, all rows have weight $d_c - 2$, and any columnwise pair of 1's appears at most once to avoid the second and the third ICI subgraphs of $\mathcal{P}_{12}$ in $[A|B|T]$.
2. In G, 1's are placed such that $\lfloor L_G/2 \rfloor$ columns have 1's in the first row and the other columns have 1's in the second row.
3. For constructing F, 1's are placed such that the union of A, B, F, and G does not contain $\mathcal{P}_{10}$.

Note that the placement of 1's in the third step is guaranteed by the bound $d_c \leq 3(J-2)/4$ in the proof of Theorem 4.

Since the conditions in Theorem 4 are necessary ones for the existence of T, a protograph may not exist for some parameter values. However, as we show in the Appendix, there exist protographs for all parameter values given in Theorem 4. We do this by providing explicit combinatorial design-based construction methods for the submatrices B and T of the protographs.

B. Regular Protographs With $d_V = 3$ and $n_2 < J - 2$, and With $d_V \geq 4$

Regular protographs that do not induce inevitable cycles of length less than 14 for the case of $d_v = 3$ and $n_2 < J - 2$ and the case of $d_v \geq 4$ also have the same structure as the matrix in Fig. 4 and the construction method in the previous section can be similarly applied to these cases. However, we do not elaborate on deriving necessary conditions in the same way used in the proof of Theorem 4 and providing specific construction methods for all cases because they have to be done case by case and are very lengthy. Instead, for given J, L, d_v, d_c, and n_2, we provide a general framework for checking the constructibility and for constructing each submatrix.

First, some basic conditions on the parameters J, L, d_v, d_c, and n_2 are provided to determine whether a regular protograph with the given parameters can be potentially constructed. In F, the number of all possible columnwise pairs of 1's should be larger than or equal to the number of actual columnwise pairs of 1's, that is, $\binom{J-n_2}{2} \geq n_2 \binom{d_v - 2}{2}$. Also, the last $J - n_2$ rows of the protograph must have $(J-n_2)d_c$ 1's and the matrix F must have $n_2(d_v - 2)$ 1's, and thus, we have $(J-n_2)d_c \geq n_2(d_v - 2)$.

Second, consider constructing $[B|T]$ of size $n_2 \times (L - n_2)$. The matrix $[B|T]$ has the constant row-weight $d_c - 2$ and is not allowed to have any repeated columnwise pairs of 1's in order to avoid the second and the third ICI subgraphs of $\mathcal{P}_{12}$ in $[A|B|T]$. Moreover, T has constant column-weight d_v. The matrix $[B|T]$ can be constructed from an incidence matrix of block designs such as $S(2,k,v)$, configurations (v_r, b_k), PBD (v, K), group divisible designs (GDD) [21] and so on because they do not have any repeated columnwise pairs of 1's. If an incidence matrix of an $S(2,k,v)$ or a configuration (v_r, b_k) has the desired size of $[B|T]$, it can be directly used as $[B|T]$ whereby B is an empty matrix, i.e., $L_B = 0$. Otherwise, an incidence matrix of some block designs can be used as $[B|T]$ by doing a simple modification. Note that an incidence matrix of PBDs or GDDs may not have a constant row-weight, while an incidence matrix of $S(2,k,v)$ or configurations (v_r, b_k) is always regular.

$$
\left[\begin{array}{cccccccccccc|cccccc|cccccccccccc}
2&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&2&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&2&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&2&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1\\
0&0&0&0&2&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&0&2&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1&0&0&0\\
\hline
1&1&1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&1&1&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right]
$$

Fig. 5. 15×30 regular protograph with $d_v = 3$ and $n_2 = 12$.

To obtain $[B|T]$ from an incidence matrix of different size, we may use the following modification schemes.

1) Remove some rows.
2) Remove a row and some columns incident to the row.
3) Remove some parallel classes.
4) Delete some 1's and insert some columns such that $[B|T]$ does not have any repeated columnwise pairs of 1's.
5) Insert some parallel classes such that $[B|T]$ does not have any repeated columnwise pairs of 1's.

By properly applying these modification schemes, an incidence matrix is changed into $[B|T]$ having no repeated columnwise pairs of 1's and proper size. Moreover, Schemes 1), 3), and 5) change all row-weights by the same amount and Schemes 2) and 4) flexibly control row-weights according to how the columns and the 1's are selected. Therefore, we can freely use the aforementioned modification schemes until the desired size and the constant row-weight $d_c - 2$ of $[B|T]$ are achieved.

For given J, L, d_v, d_c, and n_2, it may be possible for $[B|T]$ to take various forms, which implies that each B may have a different number of columns and a different distribution of 1's. Therefore, some bounds on L_G, or the number of columns of B, need to be satisfied in order for a matrix $[B|T]$ to exist. Since the number of 1's in G is $(J-n_2)d_c - n_2(d_v-2)$ and each column in G can have weight from 1 to d_v, we have $L_G \leq (J - n_2)d_c - n_2(d_v - 2) \leq d_v L_G$ which yields $\{(J-n_2)d_c - n_2(d_v - 2)\}/d_v \leq L_G \leq (J-n_2)d_c - n_2(d_v - 2)$. Therefore, when $[B|T]$ is constructed by selecting and modifying an incidence matrix of a block design, the aforementioned bound on L_G must be considered.

Finally, consider constructing F of size $(J-n_2) \times n_2$ and G of size $(J - n_2) \times L_G$. If B is already constructed, the column-weights of G are also determined and 1's in G should be located to avoid the second and the third ICI subgraphs of $\mathcal{P}_{12}$ in the union of A, B, and G. Then, for a given G, $(J-n_2)d_c$ 1's in F should be located such that the union of A, F, and G does not contain the second and the third ICI subgraphs of $\mathcal{P}_{12}$, and the union of A, B, F, and G does not contain $\mathcal{P}_{10}$ while enforcing row-weights of $[F|G]$ to be d_c and column-weights of F to be $d_v - 2$.

For given parameters J, L, d_v, d_c, and n_2, a general procedure for constructing regular protographs, which avoid inevitable cycles of length less than 14, is summarized as follows.

$$\left[\begin{array}{ccccccccccccccccccccc|ccccccc|ccccccccccccccccccccc}
2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&1 & 1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&1 & 0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&1&0 & 1&0&0&0&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&1&0 & 0&1&0&0&0&1&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&0&1 & 0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&0&1&0 & 0&0&1&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&1&0&0 & 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&1&0&0 & 0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0 & 0&0&1&0&0&0&0 & 1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0 & 0&0&1&0&0&0&0 & 0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&1&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0 & 0&0&1&0&0&0&0 & 0&1&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0 & 0&0&0&0&1&0&0 & 0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0&0 & 0&0&0&1&0&0&0 & 0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&0 & 0&0&0&1&0&0&0 & 0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0 & 0&0&0&1&0&0&0 & 0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0&0 & 0&1&0&0&0&0&0 & 0&0&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0&0 & 0&1&0&0&0&0&0 & 1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0&0 & 0&1&0&0&0&0&0 & 0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0&0 & 1&0&0&0&0&0&0 & 0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&0 & 1&0&0&0&0&0&0 & 0&0&0&0&0&1&0&0&0&1&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2 & 1&0&0&0&0&0&0 & 0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&0\\
\hline
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 & 1&0&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0 & 0&1&0&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0 & 0&0&1&0&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&1&0&0&0 & 0&0&0&1&0&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&0&1&1&0 & 0&0&0&0&1&0&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&1&0&1 & 0&0&0&0&0&1&0 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&1&1 & 0&0&0&0&0&0&1 & 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right]$$

Fig. 6. 28×49 regular protograph with $d_{\mathrm{v}} = 4$ and $n_2 = 21$.

1. Check if the parameters satisfy the conditions $\binom{J-n_2}{2} \geq n_2\binom{d_{\mathrm{v}}-2}{2}$ and $(J-n_2)d_{\mathrm{c}} \geq n_2(d_{\mathrm{v}}-2)$. If the conditions are not satisfied, stop the procedure.
2. Select an L_G satisfying $\{(J-n_2)d_{\mathrm{c}} - n_2(d_{\mathrm{v}}-2)\}/d_{\mathrm{v}} \leq L_G \leq (J-n_2)d_{\mathrm{c}} - n_2(d_{\mathrm{v}}-2)$.
3. Construct $[B|T]$ from an incidence matrix of a proper block design.
4. Construct $[F|G]$ satisfying the weight constraints such that the union of A, B, F, and G does not have $\mathcal{P}_{10}$ and $\mathcal{P}_{12}$ as its subgraph.

Example 3: Consider the construction of a 15×30 regular protograph with $d_{\mathrm{v}} = 3$, $d_{\mathrm{c}} = 6$, and $n_2 = 12$. The given parameters satisfy the conditions $\binom{J-n_2}{2} \geq n_2\binom{d_{\mathrm{v}}-2}{2}$ and $(J-n_2)d_{\mathrm{c}} \geq n_2(d_{\mathrm{v}}-2)$. The 12×18 matrix $[B|T]$ has row-weight 4 and L_G satisfies $2 \leq L_G \leq 6$. An incidence matrix of a symmetric configuration 12_3 is chosen for the construction of $[B|T]$, which is constructed by removing two parallel classes from a 12×20 incidence matrix of the configuration $(12_5, 20_3)$ in Fig. 11(b). By inserting a parallel class consisting of six weight-2 columns to an incidence matrix of the symmetric configuration 12_3, $[B|T]$ with $L_G = 6$ is constructed, where any repeated columnwise pairs of 1's do not appear. Since the column-weight of B is 2, the 3×6 matrix G should have column-weight 1. Let each row of G have two 1's. Then, F should have column-weight 1 and row-weight 4, and the 1's in F can be properly distributed so that $\mathcal{P}_{10}$ and $\mathcal{P}_{12}$ do not appear in the union of A, B, F, and G. The resulting 15×30 regular protograph with $d_{\mathrm{v}} = 3$, $d_{\mathrm{c}} = 6$, and $n_2 = 12$ is shown in Fig. 5.

Example 4: Consider the construction of a 28×49 regular protograph with $d_{\mathrm{v}} = 4$, $d_{\mathrm{c}} = 7$, and $n_2 = 21$. We can check that those parameters satisfy the two necessary conditions for the construction and $2 \leq L_G \leq 7$. For constructing a matrix $[B|T]$ of size 21×28, an incidence matrix of a symmetric configuration 21_4 is considered. We can find a parallel class consisting of seven weight-3 columns such that if those seven columns are inserted to the incidence matrix, no repeated columnwise pairs of 1's appear. Thus, we obtain $[B|T]$ with $L_G = 7$. The 7×7 matrix G should have column-weight 1 and its row-weight can be set to 1. The matrix F has size 7×21, column-weight 2, and row-weight 6. Due to $\binom{7}{2} = 21$, F can be constructed not to have any repeated columnwise pairs of 1's. Also, we can choose F so that it avoids $\mathcal{P}_{10}$ in the union of A, B, F, and G. The resulting 28×49 regular protograph with $d_{\mathrm{v}} = 4$, $d_{\mathrm{c}} = 7$, and $n_2 = 21$ is shown in Fig. 6.

VI. Construction of QC LDPC Codes and Their Minimum Hamming Distances

A. Construction of QC LDPC Codes From the Proposed Protographs

To verify the effectiveness of the proposed protographs, QC LDPC codes will be constructed by determining the lift size and assigning an appropriate shift value to each edge of a protograph. Given a protograph, it is not easy to find all shift values even for a moderate lift size such that the girth of the QC LDPC code is the same as the length of the shortest inevitable cycle. Huang *et al.* [10] proposed a search algorithm for small lift size and a shift value assignment scheme to achieve the target girth based on a greedy search. This algorithm was originally designed for single-edge protographs. However, by a slight modification, this algorithm can be extended to the case of multiple-edge protographs.

Consider a $J \times L$ protograph P with the column-weight d_{v}, the row-weight d_{c}, and the lift size z. Each column of P has d_{v} shift values and let $s_{l,i}$, $i = 0, \ldots, d_{\mathrm{v}} - 1$, denote the ith shift value of the lth column in P. Our goal is to determine all shift values $\{s_{l,i}\}$ and search the minimum z when a protograph and a target girth g of QC LDPC codes are given. Let $\mathcal{W}_n$ denote the set of all TNC walks of length n in P. Then, by Lemma 1, the condition for achieving the target girth g of QC LDPC codes is that for any $W \in \mathcal{W}_n$, $n = 4, 6, \ldots, g-2$, the shift sum $s(W)$ satisfies $s(W) \neq 0 \bmod z$. However, it requires too much computational complexity to find $s_{l,i}$ and the minimum z satisfying the aforementioned condition by considering the entire search space of $s_{l,i}$ and z.

In order to reduce the search space of shift values, let $s_{l,i} = r_i m_l$ as in [10], where r_i is the $(i+1)$st element of the set $\{0, 1, 3, 7, 12, 20, \ldots\}$ which is constructed from $\{r_0 = 0\}$ by specifying r_i, $i = 1, 2, \ldots$, to be $r_i = r_{i-1} + \min_{j,k<i} [\mathbb{N} \setminus \{|r_j - r_k|\}]$. Thus, we only need to find L values of m_l instead of $d_{\text{v}} L$ values of $s_{l,i}$, and m_l is typically chosen in an interval around zero. Moreover, for further reduction of computational complexity, m_l is determined in a greedy manner, that is, shift values of the lth column in P are determined by considering only the first l columns in P. For this, let $\mathcal{W}_n^{(l)}$ denote the set of all TNC walks of length n in the matrix consisting of the first l columns of P.

For a given target girth g, if $s_{l,i}$ is already determined such that $s(W) \neq 0$ for every $W \in \mathcal{W}_n$, $n = 4, 6, \ldots, g-2$, the minimum z, denoted by $z_{\min}$, can be suboptimally determined as $z_{\min} = \max\{|s(W)| \mid W \in \mathcal{W}_n,\ n = 4, 6, \ldots, g-2\} + 1$. Note that for any $z \geq z_{\min}$, the target girth is achieved.

Algorithm 1: Greedy Search for the Minimum Lift Size and Shift Values

```
INPUT: Target girth $g$, $J \times L$ protograph, search bound $\Gamma_{\max}$
OUTPUT: $m_l$ $(0 \leq l \leq L-1)$ and $z_{\min}$
INITIALIZATION: $r_0 = 0$, $r_i = r_{i-1} + \min_{j,k<i} [\mathbb{N} \setminus \{|r_j - r_k|\}]$ for $1 \leq i \leq d_{\text{v}} - 1$
MAIN ROUTINE
for $l = 0$ to $L-1$ begin
    for $m_l = -\Gamma_{\max}$ to $\Gamma_{\max}$ begin
        Let $s_{l,i} = r_i m_l$ for $0 \leq i \leq d_{\text{v}} - 1$.
        If $s(W) \neq 0$ for every $W \in \mathcal{W}_n^{(l)}$, $n = 4, 6, \ldots, g-2$,
            $z_{\min}^{(l)}(m_l) = \max\left\{|s(W)| \mid W \in \mathcal{W}_n^{(l)},\ n = 4, 6, \ldots, g-2\right\} + 1$.
        Otherwise, $z_{\min}^{(l)}(m_l) = \infty$.
    end
    Select the minimum $z_{\min}^{(l)}(m_l)$ and save the minimum $z_{\min}^{(l)}(m_l)$ to $z_{\min}^{(l)}$ and also save the argument to $m_l$.
    If there are multiple minima, randomly pick any one.
end
$z_{\min} = z_{\min}^{(L-1)}$
```

An algorithm to construct QC LDPC codes of moderate length by determining all shift values and searching the minimum lift size, called Algorithm 1, is provided as follows. If the target girth g is set to the length of the shortest inevitable cycle, we can generate QC LDPC codes of moderate length with the maximum achievable girth from the proposed protographs. Note that the computational complexity of Algorithm 1 is the same for both single-edge protographs and multiple-edge protographs under the same parameter values.

Four QC LDPC codes are generated by using Algorithm 1. From the 9×15 protograph in Fig. 13, a $(15000, 6000)$ QC LDPC code with girth 14, denoted by Proposed Code 1, is constructed, which has $z = 1000$ and $\{m_l\} = \{-105, 36, 45, 75, -69, -303, -393, 127, -31, -199, 200, 184, 86, 200, 199\}$. From the 9×12 protograph in Fig. 17(b), a $(3600, 900)$ QC LDPC code with girth 14, denoted by Proposed Code 2, is constructed, which has $z = 300$ and $\{m_l\} = \{-12, 18, -39,\ 75, -57, 120, 15, 17, 0, -6, -8, -8\}$. From the 6×12 protograph in Fig. 3(a), a $(7200, 3600)$ QC LDPC code with girth 12, denoted by Proposed Code 3, is constructed, which has $z = 600$ and $\{m_l\} = \{-93, 7, 47, -52, -29, -192, 30, 29, 30, 3, 19, 42\}$. From the 6×8 protograph in Fig. 3(b), a $(800, 200)$ QC LDPC code with girth 12, denoted by Proposed Code 4, is constructed, which has $z = 100$ and $\{m_l\} = \{-3, 85, -18, -6, -7, 2, -5, -15\}$.

B. Upper Bounds On the Minimum Hamming Distance of the Proposed QC LDPC Codes

Smarandache and Vontobel [19] derived two upper bounds on the minimum Hamming distance of QC LDPC codes. While one bound needs the entire code specification, e.g., the structure of the protograph, the lift size, and the shift values, the other bound only requires knowledge of the protograph.

These two upper bounds are shown in Theorems 5 and 6, and they are directly derived by finding some low-weight codewords as in Lemma 7. Let $Q_{\mathcal{S}}$ denote the submatrix of Q that contains only the columns of Q whose index appears in the set $\mathcal{S}$. Also, recall that the polynomial parity-check matrix $H(x)$ is defined as $H(x) = [h_{j,l}(x)]$, where $h_{j,l}(x) = \sum_{i=0}^{z-1} h_{j,l,i} x^i \in \mathbb{F}_2[x]/\langle x^z + 1 \rangle$, and $\text{wt}(h_{j,l}(x))$ is defined as the number of nonzero terms in $h_{j,l}(x)$.

Definition 4 ([19]): The permanent of an $m \times m$ matrix $Q = [q_{i,j}]$ over some commutative ring is defined to be

$$\text{perm}(Q) := \sum_{\sigma} \prod_{i \in \{0, \ldots, m-1\}} q_{i,\sigma(i)}$$

where the summation is over all $m!$ permutations σ on the set $\{0, \ldots, m-1\}$.

Lemma 7 ([19]): Let $\mathcal{C}$ be a binary QC LDPC code defined by a $J \times L$ polynomial matrix $H(x)$ with lift size z. Let $\mathcal{S}$ be an arbitrary size-$(J+1)$ subset of $\{0, 1, \ldots, L-1\}$ and let $c(x) = [c_0(x), c_1(x), \ldots, c_{L-1}(x)]$, where $c_i(x)$ is a polynomial over $\mathbb{F}_2(x)/\langle x^z + 1 \rangle$ defined by

$$c_i(x) = \begin{cases} \text{perm}\left(H_{\mathcal{S} \setminus \{i\}}(x)\right), & \text{if } i \in \mathcal{S} \\ 0, & \text{otherwise.} \end{cases}$$

Then, $c(x)$ is a codeword of $\mathcal{C}$.

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

(a) (b)

Fig. 7. Two single-edge regular protographs with $d_{\mathrm{v}} = 3$ avoiding inevitable cycles of length less than 14. (a) 9×15. (b) 9×12.

Theorem 5 ([19]): Let $\mathcal{C}$ be a binary QC LDPC code defined by a $J \times L$ polynomial matrix $H(x)$ with lift size z. Then, the minimum Hamming distance of $\mathcal{C}$ is upper bounded as

$$d_{\min}(\mathcal{C}) \leq \overset{*}{\min_{\substack{\mathcal{S}\subseteq\{0,\ldots,L-1\}\\ |\mathcal{S}|=J+1}}} \sum_{i\in\mathcal{S}} \mathrm{wt}\left(\mathrm{perm}\left(H_{\mathcal{S}\setminus\{i\}}(x)\right)\right) \tag{2}$$

where the operator $\overset{*}{\min}$ gives back the minimum value of all nonzero entries in a list of values.

Theorem 6 ([19]): Let $\mathcal{C}$ be a binary QC LDPC code lifted from a $J \times L$ protograph P. Then, the minimum Hamming distance of $\mathcal{C}$ is upper bounded as

$$d_{\min}(\mathcal{C}) \leq \overset{*}{\min_{\substack{\mathcal{S}\subseteq\{0,\ldots,L-1\}\\ |\mathcal{S}|=J+1}}} \sum_{i\in\mathcal{S}} \mathrm{perm}\left(P_{\mathcal{S}\setminus\{i\}}\right). \tag{3}$$

Theorems 5 and 6 imply that for given J, L, d_{v}, and d_{c}, these two upper bounds on the minimum Hamming distance of QC LDPC codes possibly increase as the number of multiple edges in the protograph increases, which is supported by examples for some regular protographs in [19]. Note that in general the upper bound in (2) approaches the upper bound in (3) for a large z and proper shift values.

Consider the (15000, 6000) Proposed Code 1. The upper bounds in (2) and (3) for this code are 246 and 256, respectively. For comparison, a QC LDPC code with the same parameter values is generated from the 9×15 single-edge regular protograph in Fig. 7(a) by using Algorithm 1. This single-edge protograph is constructed by attaching the last three columns to an incidence matrix of $S(2, 3, 9)$ to avoid inevitable cycles of length less than 14. The upper bounds in (2) and (3) for this code are 218 and 230, respectively.

Consider the (3600, 900) Proposed Code 2. The upper bounds in (2) and (3) for this code are 362 and 416, respectively. For comparison, a QC LDPC code with the same parameter values is generated from the 9×12 single-edge regular protograph in Fig. 7(b) by using Algorithm 1. By using the construction method in [7], this single-edge protograph is constructed by concatenating an incidence matrix of a $(9_2, 6_3)$ configuration and cyclically row-shifted matrix of it. The upper bounds in (2) and (3) for this code are 314 and 384, respectively.

Consider the (7200, 3600) Proposed Code 3. The upper bounds in (2) and (3) for this code are all 68. For comparison, a QC LDPC code with the same parameter values is generated from the 6×12 single-edge regular protograph in Fig. 8(a) by using Algorithm 1. This single-edge protograph is the best one of the randomly constructed protographs in the sense of upper bounds on the minimum Hamming distance. The upper bounds in (2) and (3) for this code are both 56.

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

(a) (b)

Fig. 8. Two single-edge regular protographs with $d_{\mathrm{v}} = 3$ avoiding inevitable cycles of length less than 12. (a) 6×12. (b) 6×8.

Finally, consider the (800, 200) Proposed Code 4. The upper bounds in (2) and (3) for this code are 130 and 174, respectively. For comparison, a QC LDPC code with the same parameter values is generated from the 6×8 single-edge regular protograph in Fig. 8(b) by using Algorithm 1. This single-edge protograph is the best one of the randomly constructed protographs in the sense of upper bounds on the minimum Hamming distance. The upper bounds in (2) and (3) for this code are 98 and 110, respectively.

The aforementioned results clearly show that two upper bounds (2) and (3) on the minimum Hamming distance of QC LDPC codes are affected in a positive way by using double edges in the protographs. In general, a multiple-edge protograph is more difficult to design than a single-edge protograph under the condition that they avoid the shortest inevitable cycles of the same length. However, if multiple-edge protographs are successfully constructed to avoid inevitable cycles of undesirable lengths, QC LDPC codes lifted from them can potentially give a larger upper bound on the minimum Hamming distance than those lifted from single-edge protographs. Nevertheless, note that these are just upper bounds on the minimum Hamming distance and it is plausible that the actual minimum Hamming distance behaves similarly, but need not be so.

C. Comparison of Error Correcting Performance

The performance of four proposed QC LDPC codes, that is, Proposed Codes 1–4 is compared with those of the progressive edge-growth LDPC codes, called PEG 1–4 [23] and the QC LDPC codes, called PEG QC 1–4 [24] with the same code length, code rate, and column-weight. PEG LDPC codes and PEG QC LDPC codes are well known to have good error correcting performance comparable to those of random LDPC codes. Note that the girths of such (15000, 6000), (3600, 900), (7200, 3600), and (800, 200) PEG LDPC codes and PEG QC LDPC codes are 12, 12, 12, and 10, respectively, and these codes are obtained by the PEG algorithm to have as large girth as possible.

The binary input additive white Gaussian noise (BIAWGN) channel is used for simulations. The belief propagation (BP) decoding algorithm is used and the number of maximum iterations is set to 100. The frame error rate (FER) performances of all the aforementioned LDPC codes are compared in Fig. 9 and we can see that the proposed QC LDPC codes show as good error correcting performance as the PEG LDPC codes and the PEG QC

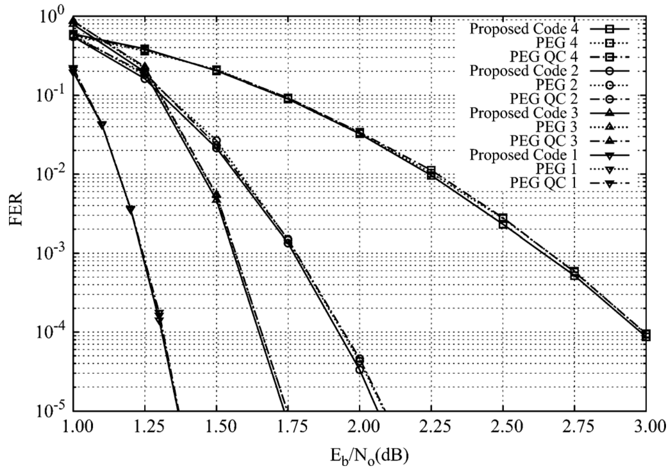


Fig. 9. Error correcting performance comparison of the proposed QC LDPC codes, the PEG LDPC codes, and the PEG QC LDPC codes.

LDPC codes. Note that the bit error rate curves behave qualitatively the same as the FER curves and they are omitted in this paper.

VII. Conclusion

The subgraphs of protographs having multiple edges, which cause inevitable cycles in the QC LDPC codes, are fully investigated by taking a graph-theoretic approach. For regular QC LDPC codes with girth larger than or equal to 12, we propose a systematic construction method of protographs that avoids inevitable cycles of length less than 12 by using BTDs. For regular QC LDPC codes with girth larger than or equal to 14, we provide construction methods of all $J \times L$ protographs with column-weight three and the number of double edges $J-2$ by using various block designs. These construction methods can be extended to construct regular protographs with double edges less than $J-2$ and with column-weight larger than three. Also, a construction algorithm of QC LDPC codes from the proposed protographs is provided based on the work in [10]. To check the validity of the proposed QC LDPC codes, we show that the proposed QC LDPC codes have larger upper bounds on the minimum Hamming distance than the QC LDPC codes lifted from single-edge protographs. However, these upper bounds only serve as a surrogate and it is an open problem to derive better upper and lower bounds on the minimum Hamming distance for the proposed codes. Finally, the error correcting performance of the proposed QC LDPC codes is compared with those of PEG LDPC codes and PEG QC LDPC codes via numerical analysis.

Appendix
Construction of B and T of the Protographs in Theorem 4

In this appendix, we show that there exist regular protographs for all parameter values given in Theorem 4 by providing explicit combinatorial design-based construction methods for the submatrices B and T of the protographs.

1) $J \equiv 5 \bmod 6$ *and* $J \geq 11$.

In this case, we have $d_c = (J+1)/2$, $L_G = 3$, and $L_T = (J+1)(J-6)/6$. We need to construct $[B|T]$ of size $(J-2) \times (J^2-5J+12)/6$ to avoid repeated columnwise pairs of 1's, i.e., the subgraph $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. For this, the following Steiner system can be used.

Definition 5 ([21]): 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 λ blocks in B. A *Steiner system* $S(t,k,v)$ is the $t-(v,k,\lambda)$ design with $\lambda = 1$.

Lemma 8 ([21]): There exists $S(2,3,v)$ only when $v \equiv 1, 3 \bmod 6$.

The number of blocks in $S(2,3,v)$ is $v(v-1)/6$. Since three columns have weight two and the other columns have weight three in the $(J-2) \times (J^2-5J+12)/6$ matrix $[B|T]$, the $(J-2) \times (J-2)(J-3)/6$ incidence matrix of $S(2,3,J-2)$ may be modified to be used as $[B|T]$ by deleting one 1 from each of well-chosen three columns and adding one column of weight three. In order for such a modified matrix to be a valid $[B|T]$, we should check whether three columnwise pairs of 1's in the weight-2 columns are disjoint, all rows have weight $(J-3)/2$, and any columnwise pair of 1's appears at most once.

Without loss of generality, let $\{v_1, v_2, v_i\}$, $\{v_2, v_3, v_j\}$, and $\{v_1, v_3, v_k\}$, $i \neq j \neq k$, be three blocks of $S(2,3,J-2)$ corresponding to three columns containing a cycle of length 6. Three disjoint blocks $\{v_2, v_i\}$, $\{v_3, v_j\}$, and $\{v_1, v_k\}$ are obtained by removing v_1, v_2, and v_3 from $\{v_1, v_2, v_i\}$, $\{v_2, v_3, v_j\}$, and $\{v_1, v_3, v_k\}$, respectively. Inserting a block $\{v_1, v_2, v_3\}$ to this modified $S(2,3,J-2)$ still makes every pair appear at most once. An incidence matrix of $S(2,3,J-2)$ has row-weight $(J-3)/2$ and the aforementioned modifications clearly keep the row-weight unchanged. Therefore, we propose a construction method of $[B|T]$ in the case of $J \equiv 5 \bmod 6$ and $J \geq 11$ as follows:

1. Permute the columns of an incidence matrix of $S(2,3,J-2)$ so that the first three columns contain a cycle of length 6.
2. Delete a 1 on the cycle of length 6 from each of the first three columns so that the resulting three columnwise pairs of 1's are disjoint.
3. Insert one column of weight three where three 1's are located in the rows traversed by the above cycle of length 6.

Actually, it is easy to choose three columns which contain a cycle of length 6 because an incidence matrix of $S(2,3,J-2)$ has many cycles of length 6. The following lemma shows how many cycles of length 6 exist in an incidence matrix of $S(2,3,J-2)$.

Lemma 9: An incidence matrix of $S(2,3,J-2)$ has $(J-2)(J-3)(J-5)/6$ cycles of length 6.

Proof: Consider three points $v_1, v_2, v_3 \in V$ of $S(2,3,J-2)$. Three pairs $\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_1\}$ appear in $S(2,3,J-2)$ in either of two ways: 1) one block has all the three pairs, that is, consists of v_1, v_2, v_3; or 2) each pair is contained in a block which does not have the other two pairs, that is, there are three blocks $\{v_1, v_2, v_i\}, \{v_2, v_3, v_j\}, \{v_3, v_1, v_k\}$, where $v_i, v_j, v_k \in V$ and $i \neq j \neq k$. Three pairs in case 2) form a cycle of length 6 in the incidence matrix of $S(2,3,J-2)$.

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

(a)

$$\left[\begin{array}{ccccccccc|ccc|cccccccccc} 2&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0 \\ 0&2&0&0&0&0&0&0&0&1&0&0&1&0&0&1&1&0&0&0&0&0 \\ 0&0&2&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&1&0&0 \\ 0&0&0&2&0&0&0&0&0&0&0&1&1&0&0&0&0&1&0&0&1&0 \\ 0&0&0&0&2&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&1&0 \\ 0&0&0&0&0&2&0&0&0&0&0&0&0&0&1&0&1&0&0&1&1&0 \\ 0&0&0&0&0&0&2&0&0&0&1&0&0&0&0&0&1&0&1&0&0&1 \\ 0&0&0&0&0&0&0&2&0&0&0&0&0&0&1&1&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&0&2&0&0&1&0&1&0&0&0&0&0&1&0&1 \\ \hline 1&1&1&0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0&1&1&1&0&0&0&0&0&0&0&0&0&0&0 \end{array}\right]$$

(b)

Fig. 10. Construction of an 11 × 22 regular protograph with $d_{\rm v} = 3$ and $n_2 = 9$. (a) Incidence matrix of $S(2,3,9)$. (b) 11 × 22 regular protograph with $d_{\rm v} = 3$ and $n_2 = 9$.

Hence, the number of cycles of length 6 in the incidence matrix can be enumerated by substracting the number of all blocks from the number of ways of choosing three points in V. This yields $\binom{J-2}{3} - (J-2)(J-3)/6 = (J-2)(J-3)(J-5)/6$. ■

Example 5: Fig. 10 illustrates the construction of an 11×22 protograph with $d_{\rm v} = 3$ and $n_2 = 9$. A cycle of length 6 is denoted by the circles in the incidence matrix of $S(2,3,9)$, which has been already column-wisely permuted in Fig. 10(a). To obtain $[B|T]$, three 1's marked by dotted circles are deleted and the column with 1's in the first, the second, and the fourth rows is inserted as the first column of T. Let $v_i,\ i = 1,\ldots,9$, denote the points of $S(2,3,9)$, which also denotes the ith row of $[B|T]$. We can see that every column in $[B|T]$ has none of three pairs of 1's $\{v_1,v_3\},\{v_4,v_7\},\{v_2,v_9\}$ and it is clear that three pairs $\{v_2,v_3\},\{v_1,v_7\},\{v_4,v_9\}$ in B are disjoint. The resulting 11×22 protograph with $d_{\rm v} = 3$ and $n_2 = 9$ is shown in Fig. 10(b) and we can check that $\mathcal{P}_{2i}$ with $i \leq 6$ does not appear in this protograph.

2) $J \equiv 2 \bmod 6$ and $J \geq 14$.

In this case, we have $d_{\rm c} = (J-2)/2$, $L_G = 0$, and $L_T = (J-2)(J-6)/6$. Since B and G do not appear in the protograph, T should be designed to avoid repeated columnwise pairs, where T has constant row-weight $(J-6)/2$ and column-weight 3. A configuration whose incidence matrix has column-weight 3 and the size $(J-2) \times (J-2)(J-6)/6$ can be used for T.

Definition 6 ([21]): A *configuration* (v_r, b_k) is an incidence structure of v points and b blocks such that 1) each block contains k points, 2) each point lies on r blocks, and 3) two different points are contained in at most one block. If $v = b$ and hence $r = k$, the configuration is called *symmetric* and denoted by v_k.

It is important to check the existence of the configuration with the required parameters. The following theorem shows that such configuration always exists and therefore T can be constructed.

Theorem 7: There exists a configuration (v_r, b_k) with $v = J-2, b = (J-2)(J-6)/6$, $k = 3$, and $r = (J-6)/2$ for all $J \equiv 2 \bmod 6$ and $J \geq 14$.

Proof: Necessary conditions for the existence of a (v_r, b_k) configuration [25] are given as 1) $v \leq b$ and $k \leq r$, 2) $vr = bk$, and 3) $v \geq r(k-1)+1$. We can easily check that the parameters in the theorem statement satisfy these conditions. Finally, the existence of such configurations is guaranteed by Theorem 3.1 in [25], that is, there exists a configuration with $k = 3$ if and only if the necessary conditions hold. ■

Now, a construction method of T is proposed based on the results in [25], which uses configurations with parallel classes and resolvable configurations.

Definition 7 ([21]): A *parallel class* in a design is a set of blocks that partition the point set. A *resolvable design* is a design whose blocks can be partitioned into parallel classes.

If a configuration (v_r, b_k) has at least one parallel class, for some positive integer m, we can obtain a matrix with v rows, $b - mv/k$ columns, and a constant row-weight $r - m$ by removing m parallel classes from an incidence matrix of the configuration. This property also helps to obtain T from a configuration.

For $J \equiv 2 \bmod 6$, $S(2,3,J-1)$ exists by Lemma 8. For $J \geq 20$, an incidence matrix of a resolvable configuration (v_r, b_k) with $v = J-2$, $b = (J-2)(J-4)/6$, $k = 3$, and $r = (J-4)/2$ can be constructed by removing a row and its incident columns in an incidence matrix of $S(2,3,J-1)$[25]. For $J = 14$, there is no resolvable configuration $(12_5, 20_3)$ but we can find a configuration $(12_5, 20_3)$ in the same manner as illustrated in Fig. 11(b), which contains some parallel classes from $S(2,3,13)$[25]. Since a parallel class of a configuration (v_r, b_k) with $v = J-2, b = (J-2)(J-4)/6, k = 3$, and $r = (J-4)/2$ consists of $(J-2)/3$ blocks and has all points exactly once, we obtain T by removing one parallel class from the incidence matrices of these configurations. The construction procedure of T for $J \equiv 2 \bmod 6$ and $J \geq 14$ is summarized as follows.

1) Construct $S(2,3,J-1)$.
2) Construct an incidence matrix of a resolvable configuration (v_r, b_k) with $v = J-2, b = (J-2)(J-4)/6, k = 3$, and $r = (J-4)/2$ by removing a row and its incident columns in an incidence matrix of $S(2,3,J-1)$.
3) Remove one parallel class which consists of $(J-2)/3$ columns to obtain T.

Example 6: An incidence matrix of $S(2,3,13)$ is shown in Fig. 11(a). An incidence matrix of a configuration $(12_5, 20_3)$ in Fig. 11(b) is constructed by removing the eighth row and its incident columns in the incidence matrix of $S(2,3,13)$ in Fig. 11(a). We see that the fourth, the sixth, the thirteenth, and the sixteenth columns form a parallel class. By removing these columns, an incidence matrix of a configuration $(12_4, 16_3)$ is constructed, which is used as T. The resulting 14×28 protograph with $d_{\rm v} = 3$ and $n_2 = 12$ is shown in Fig. 11(c).

3) $J \equiv 3 \bmod 6$ and $J \geq 9$:

3.1) $J \neq 9$, $d_{\rm c} = (J-1)/2$;

In this case, we have $L_G = 1$ and $L_T = (J-1)(J-6)/6$, and thus, B should have only one pair of 1's. Since $S(2,3,J-2)$ exists by Lemma 8, $[B|T]$ may be constructed by removing $J/3-1$ columns from a $(J-2) \times (J-2)(J-3)/6$ incidence matrix of $S(2,3,J-2)$ and then deleting a 1 in some other column.

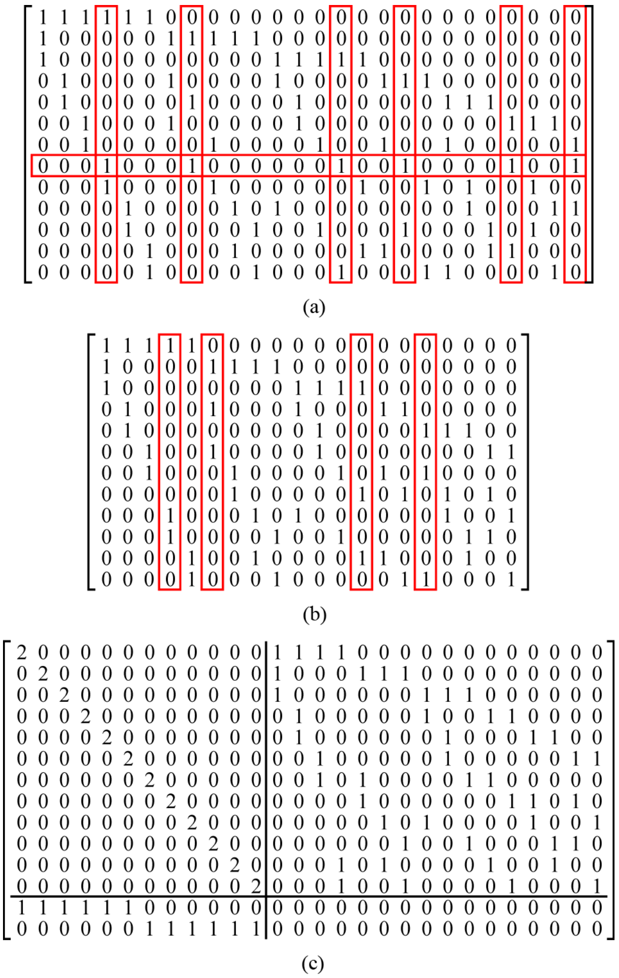


Fig. 11. Construction of a 14 × 28 regular protograph with $d_v = 3$ and $n_2 = 12$. (a) Incidence matrix of $S(2,3,13)$. (b) Incidence matrix of a configuration $(12_5, 20_3)$. (c) 14 × 28 regular protograph with $d_v = 3$ and $n_2 = 12$.

To achieve the desired row-weight $(J-5)/2$ of $[B|T]$, there should exist a submatrix consisting of $J/3$ columns satisfying that 1) two rows have weight 2 and the others have weight 1 and 2) one column has a 1 at each of these two rows of weight 2.

As seen in the case of $J \equiv 2 \bmod 6$ and $J \geq 14$, for $J \equiv 3 \bmod 6$ and $J \geq 15$, $S(2,3,J-2)$ contains as a substructure a configuration (v_r, b_k) with $v = J-3$, $b = (J-3)(J-5)/6$, $k = 3$, and $r = (J-5)/2$ which has at least one parallel class consisting of $J/3-1$ blocks. This implies that there are $J/3-1$ blocks in $S(2,3,J-2)$ which partition all but one point. Also, there always exists another block containing that point in $S(2,3,J-2)$. These $J/3$ blocks satisfy the aforementioned requirements 1) and 2) for $[B|T]$. The construction procedure of $[B|T]$ for $J \equiv 3 \bmod 6$, $J \geq 15$, and $d_c = (J-1)/2$ is summarized as follows.

1) Construct $S(2,3,J-2)$.
2) Select one row in an incidence matrix of $S(2,3,J-2)$ such that if the row and its incident columns are removed from the incidence matrix, the remaining part forms an incidence matrix of a configuration (v_r, b_k) with $v = J-3$, $b = (J-3)(J-5)/6$, $k = 3$, and $r = (J-5)/2$ including at least one parallel class.

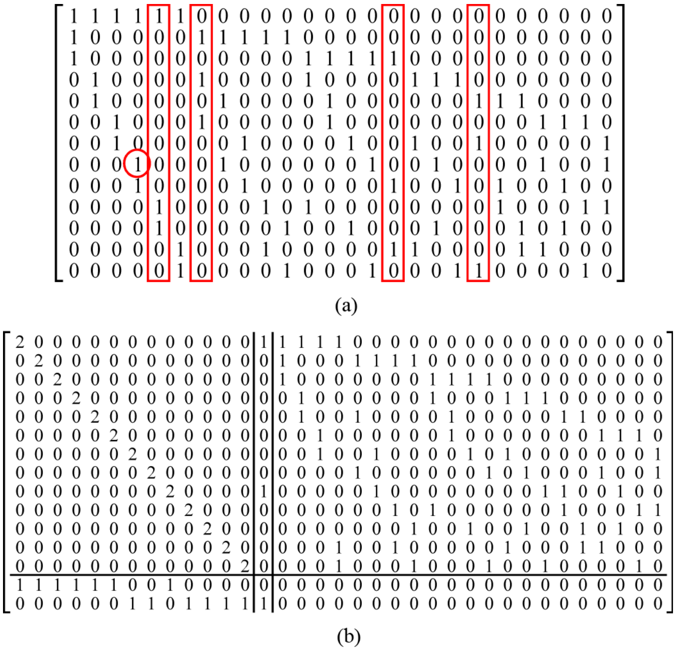


Fig. 12. Construction of a 15 × 35 regular protograph with $d_v = 3$ and $n_2 = 13$. (a) Incidence matrix of $S(2,3,13)$. (b) 15 × 35 regular protograph with $d_v = 3$ and $n_2 = 13$.

3) Find $J/3-1$ columns that form one parallel class in the aforementioned configuration.
4) In the incidence matrix of $S(2,3,J-2)$, delete a 1 in the selected row in Step 2 and remove the $J/3-1$ columns obtained in Step 3.
5) Move the column which had the deleted 1 in Step 4 to the leftmost to obtain $[B|T]$.

Note that the aforementioned construction method cannot be applied to the case of $J = 9$ and $d_c = 4$ because the configuration $(6_2, 4_3)$ does not have any parallel class. The case of $J = 9$ and $d_c = 4$ will be covered in the last part of this section.

Example 7: Fig. 12 illustrates the construction of a 15 × 35 regular protograph with $d_v = 3$ and $n_2 = 13$. In an incidence matrix of $S(2,3,13)$ in Fig. 12(a), the fifth, the seventh, the 16th, and the 20th columns partition the set of row indices except for the index of the eighth row. Also, we can see that the fourth column has a 1 in the eighth row. Thus, the 1 in the fourth column and the eighth row is deleted and the four boxed columns are removed from the incidence matrix. Then, the resulting column of weight 2 is moved to the far left and a 15 × 35 protograph with $d_v = 3$ and $n_2 = 13$ is shown in Fig. 12(b).

3.2) $d_c = (J+1)/2$;

In this case, we have $L_G = 3$ and $L_T = (J+1)(J-6)/6$, and there are three columnwise pairs of 1's in B. Since $S(2,3,J-2)$ exists for $J \equiv 3 \bmod 6$ and $J \geq 9$ by Lemma 8, the construction method for $J \equiv 5 \bmod 6$ and $J \geq 11$ can also be applied to this case in the same way. As an example, a 9 × 15 regular protograph with $d_v = 3$ and $n_2 = 7$ is shown in Fig. 13.

4) $J \equiv 1 \bmod 6$ and $J \geq 13$:

In this case, we have $d_c = (J-1)/2$, $L_G = 1$, and $L_T = (J-1)(J-6)/6$. To construct $[B|T]$, start with $S(2,3,J)$ which always exists by Lemma 8. Similar to the case of $J \equiv 2 \bmod 6$ and $J \geq 14$, a configuration (v_r, b_k) with $v = J-1$,

$$\left[\begin{array}{ccccccc|ccc|ccccc}
2&0&0&0&0&0&0&1&0&0&1&0&0&1&0\\
0&2&0&0&0&0&0&1&0&0&0&0&1&0&1\\
0&0&2&0&0&0&0&0&1&0&1&0&0&0&1\\
0&0&0&2&0&0&0&0&1&0&0&1&1&0&0\\
0&0&0&0&2&0&0&0&0&1&1&1&0&0&0\\
0&0&0&0&0&2&0&0&0&1&0&0&1&1&0\\
0&0&0&0&0&0&2&0&0&0&0&1&0&1&1\\
\hline
1&1&1&1&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&1&1&1&1&1&0&0&0&0&0&0
\end{array}\right]$$

Fig. 13. 9×15 regular protograph with $d_{\mathrm{v}} = 3$ and $n_2 = 7$.

$b = (J-1)(J-3)/6$, $k = 3$, and $r = (J-3)/2$ can be constructed by removing a row and its incident columns in an incidence matrix of $S(2,3,J)$. Any $(J-3)/2$ blocks sharing a common point in the configuration partition all points except the common point and another point. Therefore, by removing any row and its incident columns in an incidence matrix of the configuration, a $(J-2) \times (J-3)(J-4)/6$ matrix with $J-3$ rows of weight $(J-5)/2$ and a row of weight $(J-3)/2$ is obtained. Removing a 1 in the row of weight $(J-3)/2$ results in a matrix which has the desired row-weight $(J-5)/2$ and exactly one column of weight 2. Clearly, this matrix can be used as $[B|T]$. The construction procedure of $[B|T]$ for $J \equiv 1 \bmod 6$ and $J \geq 13$ is summarized as follows.

1) Construct a configuration (v_r, b_k) with $v = J-1$, $b = (J-1)(J-3)/6$, $k = 3$, and $r = (J-3)/2$ from $S(2,3,J)$ similar to the case of $J \equiv 2 \bmod 6$ and $J \geq 14$.
2) Obtain a matrix of size $(J-2) \times (J-3)(J-4)/6$ by removing a row and its incident columns.
3) Delete a 1 in the row of weight $(J-3)/2$ and move the column having the deleted 1 to the leftmost to obtain $[B|T]$.

Example 8: An incidence matrix of a configuration $(12_5, 20_3)$ is given in Fig. 11(b). By removing the first row and its incident columns, we obtain an 11×15 matrix shown in Fig. 14(a), where the seventh row has weight 5 and the others have weight 4. Then, the 1 in the seventh row is deleted from the second column and the second column is moved to the far left. The resulting 13×26 protograph with $d_{\mathrm{v}} = 3$ and $n_2 = 11$ is shown in Fig. 14(b).

5) $J \equiv 0 \bmod 6$ and $J \geq 12$:

5.1) $d_{\mathrm{c}} = (J-2)/2$;

In this case, we have $L_G = 0$ and $L_T = (J-2)(J-6)/6$. Similar to the case of $J \equiv 2 \bmod 6$ and $J \geq 14$, an incidence matrix of a configuration (v_r, b_k) with $v = J-2$, $b = (J-2)(J-6)/6$, $k = 3$, and $r = (J-6)/2$ can be used as T. Such configuration can be constructed by using difference triangle set (DTS).

Definition 8 ([21]): An (n,m)-*difference triangle set*, or (n,m)-DTS, is a set $\mathcal{U} = \{U_1, \ldots, U_n\}$, where for $1 \leq i \leq n$, $U_i = \{a_{i0}, a_{i1}, \ldots, a_{im}\}$ with a_{ij} an integer satisfying $0 = a_{i0} < a_{i1} < \cdots < a_{im}$, and the differences $a_{il} - a_{ij}$ over the integers for all i, j, l, $1 \leq i \leq n$, $0 \leq l \neq j \leq m$, are all distinct and nonzero.

Theorem 8 ([25]): If there is an $(n,2)$-DTS, a configuration (v_r, b_k) for $v \geq 6n+3$, $b = nv$, $k = 3$, and $r = nk$ can be constructed from this DTS.

For $J \equiv 0 \bmod 6$ and $J \geq 12$, a configuration (v_r, b_k) with $v = J-2$, $b = (J-2)(J-6)/6$, $k = 3$, and $r = (J-6)/2$ can be constructed from $((J-6)/6, 2)$-DTS by Theorem 8.

$$\left[\begin{array}{ccccccccccccccc}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&1&1&0&0\\
1&0&0&0&0&1&0&0&0&0&0&0&0&1&1\\
0&1&0&0&0&0&1&0&1&0&1&0&0&0&0\\
0&\textcircled{1}&0&0&0&0&0&1&0&1&0&1&0&1&0\\
0&0&1&0&1&0&0&0&0&0&0&1&0&0&1\\
0&0&0&1&0&0&1&0&0&0&0&0&1&1&0\\
0&0&1&0&0&0&0&1&1&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&1&1&0&0&0&1
\end{array}\right]$$

(a)

$$\left[\begin{array}{ccccccccccc|c|cccccccccccccc}
2&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&2&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0\\
0&0&2&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&0&0&0&0&0\\
0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&0&0\\
0&0&0&0&2&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&2&0&0&0&0&0&1&0&0&0&0&0&1&0&1&0&1&0&0&0&0\\
0&0&0&0&0&0&2&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0\\
0&0&0&0&0&0&0&2&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&1&0&0&1&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&1&0&0&0&0&1&1&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&2&0&0&0&1&0&0&0&0&0&1&1&0&0&0&1\\
\hline
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right]$$

(b)

Fig. 14. Construction of a 13×26 regular protograph with $d_{\mathrm{v}} = 3$ and $n_2 = 11$. (a) 11×15 modified matrix. (b) 13×26 regular protograph with $d_{\mathrm{v}} = 3$ and $n_2 = 11$.

$$\left[\begin{array}{cccccccccc|cccccccccc}
2&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1\\
0&2&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0\\
0&0&2&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1\\
0&0&0&2&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0\\
0&0&0&0&2&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0\\
0&0&0&0&0&2&0&0&0&0&0&0&1&0&1&1&0&0&0&0\\
0&0&0&0&0&0&2&0&0&0&0&0&0&1&0&1&1&0&0&0\\
0&0&0&0&0&0&0&2&0&0&0&0&0&0&1&0&1&1&0&0\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&1&0&1&1&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&0&0&1&0&1&1\\
\hline
1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0
\end{array}\right]$$

Fig. 15. 12×20 regular protograph with $d_{\mathrm{v}} = 3$ and $n_2 = 10$.

According to [25], the construction procedure of T is provided as follows.

1. Construct a $((J-6)/6, 2)$-DTS with $U_i = \{a_{i0}, a_{i1}, a_{i2}\}$, $i = 1, \ldots, (J-6)/6$.
2. For each U_i, $i = 1, \ldots, (J-6)/6$, construct a column of length $J-2$ denoted by C_i, which has a 1 at the $(a_{i0}+1)$st, the $(a_{i1}+1)$st, and the $(a_{i2}+1)$st rows and 0 at other rows.
3. For each i, construct a $(J-2) \times (J-2)$ matrix whose jth column, $j = 1, \ldots, J-2$, is obtained by cyclically shifting C_i downward $j-1$ times.
4. Concatenate $(J-6)/6$ matrices in Step 3 to obtain T.

Note that we can easily construct a $((J-6)/6, 2)$-DTS from the DTS lists in [26] for $J \equiv 0 \bmod 6$ and $J \geq 12$. Fig. 15 shows a 12×20 regular protograph with $d_{\mathrm{v}} = 3$ and $n_2 = 10$ constructed from $(1,2)$-DTS.

5.2) $d_{\mathrm{c}} = J/2$;

In this case, we have $L_G = 2$ and $L_T = J(J-6)/6$. Pairwise balanced designs (PBDs) can be used to construct $[B|T]$.

Definition 9 ([21]): Let K be a subset of positive integers and let λ be a positive integer. A PBD of order v with block sizes from K, denoted by PBD $(v, K; \lambda)$, is a pair $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a point set of cardinality v and $\mathcal{B}$ is a family of blocks of $\mathcal{V}$ which satisfy 1) if $B \in \mathcal{B}$, then $|B| \in K$ and 2) every pair of distinct elements of $\mathcal{V}$ occurs in exactly λ blocks of $\mathcal{B}$.

Let PBD (v, K) denote a PBD $(v, K; \lambda)$ with $\lambda = 1$ and use PBD $(v, K \cup \{k^\star\})$ to denote a PBD containing only one block of size k in the PBD, where $k \notin K$ is a positive integer. For $J \equiv 0 \bmod 6$, it was shown in [27] that PBD $(J-1, \{3, 5^\star\})$ always exists. Note that five rows sharing a 1 with the column of weight 5 have weight $(J-4)/2$ and the other rows have weight $(J-2)/2$ in a $(J-1) \times (J^2 - 3J - 12)/6$ incidence matrix of PBD $(J-1, \{3, 5^\star\})$.

Theorem 9: Removing a row of weight $(J-4)/2$ and its incident columns except the weight-5 column from an incidence matrix of PBD $(J-1, \{3, 5^\star\})$ makes a $(J-2) \times (J^2 - 6J + 6)/6$ matrix of constant row-weight $(J-4)/2$.

Proof: Without loss of generality, assume that the first column has 1's at the first five rows in an incidence matrix of PBD $(J-1, \{3, 5^\star\})$. Consider the $(J-1) \times (J-4)/2$ submatrix which consists of the columns incident to the first row. Except the first row, each row of this submatrix has only one 1 because every columnwise pair of 1's should appear exactly once in an incidence matrix of this PBD. Thus, the $(J-2) \times (J-6)/2$ submatrix obtained by removing the first row and the first column from the $(J-1) \times (J-4)/2$ submatrix does not have 1 in the first four rows and each of the other rows has only one 1. After removing the first row and the $(J-2) \times (J-6)/2$ submatrix from the incidence matrix of PBD $(J-1, \{3, 5^\star\})$, the remainder forms the $(J-2) \times (J^2 - 6J + 6)/6$ matrix of row-weight $(J-4)/2$. ■

The matrix constructed in Theorem 9 cannot be directly used as $[B|T]$ due to the improper number of columns and the weight-4 column, but it can be easily modified to meet the requirements for $[B|T]$ by splitting the weight-4 column into two weight-2 columns. The construction procedure of $[B|T]$ for $J \equiv 0 \bmod 6$, $J \geq 12$, and $d_\text{c} = J/2$ is summarized as follows.

1. Construct PBD $(J-1, \{3, 5^\star\})$.
2. Remove a row of weight $(J-4)/2$ and its incident columns except the weight-5 column from an incidence matrix of PBD $(J-1, \{3, 5^\star\})$.
3. Split the weight-4 column into two weight-2 columns and move them to the leftmost to obtain $[B|T]$.

Example 9: The construction process for a 12×24 regular protograph with $d_\text{v} = 3$ and $n_2 = 10$ is illustrated in Fig. 16. An incidence matrix of PBD $(11, \{3, 5^\star\})$ is shown in Fig. 16(a). We can see that the submatrix consisting of the columns incident to the first row has exactly one 1 in each row except the first row. By removing the first row and the second, the third, and the fourth columns and splitting the weight-4 column into two weight-2 column, $[B|T]$ is obtained. The resulting 12×24 regular protograph with $d_\text{v} = 3$ and $n_2 = 10$ is shown in Fig. 16(b).

6) $J = 9$, $d_\text{c} = 4$ and $J = 10$, $d_\text{c} = 6$.

Only two cases of Theorem 4 remain for which we need to provide construction methods. When $J = 9$ and $d_\text{c} = 4$, we have $L_G = 1$ and $L_T = 4$, and $[B|T]$ is a 7×5 matrix with row-weight 2. Although the construction method of $[B|T]$ for $J \equiv 3 \bmod 6$ and $d_\text{c} = (J-1)/2$ cannot be directly used, we can construct $[B|T]$ from an incidence matrix of $S(2,3,7)$ in Fig. 17(a). Since any two columns of an incidence matrix of $S(2,3,7)$ have a common 1, removing the first two columns from an incidence matrix results in a 7×5 matrix where one row has weight 1, four rows have weight 2, and the remaining two rows have weight 3 as shown in Fig. 17(a). To obtain $[B|T]$, first delete 1 from each of two rows of weight 3 in the 7×5 matrix such that two deleted 1's do not belong to the same column and the columns containing two deleted 1's do not have 1 in the row of weight 1. These two deleted 1's are marked by circle in Fig. 17(a). Then, by replacing a 0 at the row of weight 1 and one

$$\left[\begin{array}{c|c|c|c|ccccccccccc}
1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\ \hline
1&0&0&0&1&1&1&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&1&1&1&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&1&1&1&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0\\
0&1&0&0&0&1&0&0&1&0&0&1&0&0&1&0\\
0&0&1&0&1&0&0&0&0&1&0&1&0&0&0&1\\
0&0&0&1&0&1&0&1&0&0&0&0&1&0&0&1\\
0&0&0&1&0&0&1&0&0&1&1&0&0&0&1&0\\
0&0&1&0&0&0&1&0&1&0&0&0&1&1&0&0
\end{array}\right]$$

(a)

$$\left[\begin{array}{cccccccccc|cc|cccccccccccc}
2&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0&0&0&0\\
0&2&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&0&0&0\\
0&0&2&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&0&0\\
0&0&0&2&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&2&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&1&0&0\\
0&0&0&0&0&2&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&1&0\\
0&0&0&0&0&0&2&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&1\\
0&0&0&0&0&0&0&2&0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&1\\
0&0&0&0&0&0&0&0&2&0&0&0&0&0&1&0&0&1&1&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&2&0&0&0&0&1&0&1&0&0&0&1&1&0&0\\ \hline
1&1&0&0&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{array}\right]$$

(b)

Fig. 16. Construction of a 12×24 regular protograph with $d_\text{v} = 3$ and $n_2 = 10$. (a) Incidence matrix of PBD $(11, \{3, 5^\star\})$. (b) 12×24 regular protograph with $d_\text{v} = 3$ and $n_2 = 10$.

$$\left[\begin{array}{c|c|ccccc}
1&0&0&0&1&0&1\\
1&1&0&\textcircled{0}&0&1&0\\
0&1&1&0&0&0&1\\
1&0&1&1&0&0&0\\
0&1&0&1&1&0&0\\
0&0&\textcircled{1}&0&1&1&0\\
0&0&0&\textcircled{1}&0&1&1
\end{array}\right]$$

(a)

$$\left[\begin{array}{ccccccc|c|cccc}
2&0&0&0&0&0&0&0&0&1&0&1\\
0&2&0&0&0&0&0&0&1&0&1&0\\
0&0&2&0&0&0&0&1&0&0&0&1\\
0&0&0&2&0&0&0&1&1&0&0&0\\
0&0&0&0&2&0&0&0&1&1&0&0\\
0&0&0&0&0&2&0&0&0&1&1&0\\
0&0&0&0&0&0&2&0&0&0&1&1\\ \hline
1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0
\end{array}\right]$$

(b)

Fig. 17. Construction of a 9×12 regular protograph with $d_\text{v} = 3$ and $n_2 = 7$. (a) Incidence matrix of $S(2,3,7)$. (b) 9×12 regular protograph with $d_\text{v} = 3$ and $n_2 = 7$.

$$\left[\begin{array}{cccccccc|cccc|cccccccc}
2&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&0&0\\
0&2&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&0\\
0&0&2&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&1&0\\
0&0&0&2&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&1\\
0&0&0&0&2&0&0&0&0&0&1&0&1&0&0&0&0&1&1&0\\
0&0&0&0&0&2&0&0&0&0&1&0&0&0&1&1&0&0&0&1\\
0&0&0&0&0&0&2&0&0&0&0&1&0&1&0&1&0&0&1&0\\
0&0&0&0&0&0&0&2&0&0&0&1&1&0&0&0&1&0&0&1\\ \hline
1&1&1&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0
\end{array}\right]$$

Fig. 18. 10×20 regular protograph with $d_\text{v} = 3$ and $n_2 = 8$.

of the columns containing the deleted 1's with a 1, $[B|T]$ is constructed and the resulting 9×12 regular protograph is shown in Fig. 17(b).

When $J = 10$ and $d_{\mathrm{c}} = 6$, we have $L_G = 4$ and $L_T = 8$, and B has disjoint four columnwise pairs of 1's. An incidence matrix of a symmetric configuration 8_3 can be used as T, which does not have disjoint four columnwise pairs of 1's. A 10×20 regular protograph with $d_{\mathrm{v}} = 3$ and $n_2 = 8$ is shown in Fig. 18.

ACKNOWLEDGMENT

The authors are very grateful to anonymous reviewers and especially the associate editor for a number of very helpful comments including several technical corrections and suggestions, which substantially improved the paper.

REFERENCES

[1] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA, USA: MIT Press, 1963.

[2] J. Thorpe, Low-density parity-check (LDPC) codes constructed from protograph Jet Propulsion Laboratory, Pasadena, CA, USA, 2003, IPN Progr. Rep. 42-154.

[3] R. M. Tanner, D. Sridhara, and T. Fuja, "A class of group-structured LDPC codes," presented at the Int. Symp. Commun. Theory Appl., Ambleside, U.K., 2001.

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

[5] M. E. O'Sullivan, "Algebraic construction of sparse matrices with large girth," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 718–727, Feb. 2006.

[6] O. Milenkovic, N. Kashyap, and D. Leyba, "Shortened array codes of large girth," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3707–3722, Aug. 2006.

[7] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, "Quasi-cyclic low-density parity-check codes with girth larger than 12," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2885–2891, Aug. 2007.

[8] Y. Wang, J. S. Yedidia, and S. C. Draper, "Construction of high-girth QC-LDPC codes," in *Proc. 5th Int. Symp. Turbo Codes Related Top.*, Sep. 2008, pp. 180–185.

[9] M. Esmaeili and M. Gholami, "Structured quasi-cyclic LDPC codes with girth 18 and column-weight $J \geq 3$," *J. Electron. Commun.*, vol. 64, no. 3, pp. 202–217, Mar. 2010.

[10] J. Huang, L. Liu, W. Zhou, and S. Zhou, "Large-girth nonbinary QC-LDPC codes of various lengths," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3436–3447, Dec. 2010.

[11] X. Jiang, Y. Yan, and M. H. Lee, "Construction of multiple-rate quasi-cyclic LDPC codes via the hyperplane decomposing," *J. Commun. Netw.*, vol. 13, no. 3, pp. 205–210, Jun. 2011.

[12] I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov, and R. V. Satyukov, "Searching for voltage graph-based LDPC tailbiting codes with large girth," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2265–2279, Apr. 2012.

[13] S. J. Johnson and S. R. Weller, "Quasi-cyclic LDPC codes from difference families," presented at the 3rd Australian Commun. Theory Workshop, Canberra, Australia, Feb. 2002.

[14] 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.

[15] 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.

[16] C. A. Kelley and J. L. Walker, "LDPC codes from voltage graphs," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 792–796.

[17] R. Koetter and P. O. Vontobel, "Graph-covers and iterative decoding of finite length codes," in *Proc. 3rd Int. Symp. Turbo Codes Related Top.*, Brest, France, Sep. 2003, pp. 75–82.

[18] C. A. Kelley and D. Sridhara, "Pseudocodewords of Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4013–4038, Nov. 2007.

[19] P. O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto- and Tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.

[20] B. K. Butler and P. H. Siegel, "Bounds on the minimum distance of punctured quasi-cyclic LDPC codes," IEEE Trans. Inf. Theory [Online]. Available: http://arxiv.org/abs/1201.2386

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

[22] E. J. Billington and P. Robinson, "A list of balanced ternary designs with $R \leq 15$, and some necessary existence conditions," *Ars Combin.*, vol. 16, pp. 235–258, 1983.

[23] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.

[24] Z. Li and B. V. K. V. Kumar, "A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph," in *Proc. 38th Asilomar Conf. Sig. Syst. Comput.*, Nov. 2004, pp. 1990–1994.

[25] H. Gropp, "Nonsymmetric configurations with natural index," *Discr. Math.*, vol. 124, pp. 87–98, 1994.

[26] [Online]. Available: http://www.research.ibm.com/people/s/shearer/dtsopt.html

[27] S. Kucukcifci, "The intersection problem for $\mathrm{PBD}(5^*, 3)$s," *Discr. Math.*, vol. 308, pp. 382–385, 2008.

Hosung Park received the B.S., M.S., and Ph.D. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 2007, 2009, and 2013, respectively. He is currently a postdoctoral researcher working with Prof. Jong-Seon No and Prof. Young-Han Kim at Institute of New Media and Communications in Seoul National University, Seoul, Korea, since March 2013. From September 2013, he will work with Prof. Young-Han Kim as a postdoctoral researcher in Department of Electrical and Computer Engineering, University of California, San Diego, USA. His research interests include low-density parity-check codes, coding theory, coding for memory, compressed sensing, network information theory, and network coding.

Seokbeom Hong received the B.S. degree in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 2007, where he is currently pursuing the Ph.D. degree in electrical engineering and computer science. His area of research interests includes compressed sensing, error-correcting codes, and communications theory.

Jong-Seon No (S'80–M'88–SM'10–F'12) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, from September 1990 to July 1999. He joined the Faculty of the Department of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently a Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-time codes, LDPC codes, and wireless communication systems.

Dong-Joon Shin (S'96–M'99–SM'09) received the B.S. degree in electronics engineering from Seoul National University, Seoul, Korea, the M.S. degree in electrical engineering from Northwestern University, Evanston, USA, and the Ph.D. degree in electrical engineering from University of Southern California, Los Angeles, USA. From 1999 to 2000, he was a member of technical staff in Wireless Network Division and Satellite Network Division, Hughes Network Systems, Maryland, USA. Since September 2000, he has been a Professor in the Department of Electronic Engineering at Hanyang University, Seoul, Korea. His current research interests include error correcting codes, sequences, and wireless/mobile communication systems.