Partially Quasi-Cyclic Protograph-Based LDPC Codes

Roxana Smarandache
Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182
Email: rsmarand@sciences.sdsu.edu

David G. M. Mitchell and Daniel J. Costello, Jr.
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556
Email: david.mitchell@nd.edu
costello.2@nd.edu

***Abstract*—A significant amount of the analysis of protograph-based low-density parity-check (LDPC) codes has been devoted to the subclass of quasi-cyclic (QC) LDPC codes. Despite their implementation advantages and algebraic properties that make them easy to analyze, protograph-based QC-LDPC codes have undesirable fixed upper limits on important code parameters. This implies that picking a QC code from an asymptotically good or capacity approaching ensemble is suboptimal, since long QC codes will not perform close to the ensemble asymptotic limits. Indeed, these limits can only be achieved by codes that are not QC. In this paper we present an overview together with some new results on partially-QC protograph-based LDPC codes, i.e., LDPC codes whose parity-check matrix is partially composed of circulant submatrices. We perform both a minimum Hamming distance and girth analysis of these codes. Moreover, we present explicit partially-QC LDPC code constructions with parameters that exceed the restricted QC upper bounds.**

***Index Terms*—Girth, graph cover, low-density parity-check code, low-density parity-check matrix, protograph, protomatrix, quasi-cyclic code, Tanner graph.**

I. Introduction

Protograph-based codes [1], [2] are constructed by taking r-fold graph covers [3], [4] of a given protograph, for a given positive integer r. A protograph is a Tanner graph [5] described by an $m \times n$ incidence matrix, known as a protomatrix, with non-negative integer entries a_{ij} that correspond to a_{ij} parallel edges in the graph. An r-fold graph cover of a given protograph preserves its degree distribution and is described by an $rm \times rn$ matrix obtained by replacing each non-zero entry a_{ij} by a sum of a_{ij} permutation matrices of size r and a zero entry by an $r \times r$ zero matrix.

Among the possible codes obtained by this method are quasi-cyclic (QC) low-density parity-check (LDPC) codes [6]–[8], [10]–[12]. A QC LDPC code of length rn can be described by an $rm \times rn$ parity-check matrix that is formed by an $m \times n$ array of $r \times r$ circulant matrices. Clearly, the construction of QC LDPC codes can be seen as a special case of the protograph-based construction in which the r-fold cover is obtained by restricting the edge permutations to be cyclic. Members of a protograph-based LDPC code ensemble that are QC are of great interest to code designers, since they can be encoded with low complexity using simple feedback shift-registers [13] and their structure leads to efficiencies in decoder design. However, QC codes have limitations. In particular, it is known that QC codes based on protographs have upper bounds on minimum Hamming distance independent of the size of the circulant matrix entries; therefore, an increase in the circulant size does not provide an increase in minimum distance beyond a certain limit, see, e.g., [9], [10], [14]. Similarly, the protograph itself imposes a limit on the girth of the code if the code is QC [8], [11], [14], [15]. This implies that the codes from protograph-based ensembles that have capacity approaching iterative decoding thresholds cannot be QC.

In this paper we study partially-QC LDPC codes based on a given protograph, where only some of the permutation matrices are circulants. Focusing on protographs with single edges, we show that any r-fold cover graph of a protograph is isomorphic to an r-fold cover graph that is the Tanner graph of a partially-QC LDPC code.This constitutes the main motivation for our interest in partially-QC structures. We then analyze the minimum Hamming distance and girth of such codes and compare them to QC codes. Towards this end, we give algebraic conditions on the r-permutation matrices describing the r-fold graph covers of a given protograph that ensure higher girth and minimum distance than the upper bounds for QC codes. Finally, we give examples of partially-QC codes with such parameters, which promise improved performance compared to protograph-based QC codes of the same length that are obtained from the same protograph, and we discuss their structural differences relative to QC codes.

The remainder of the paper is structured as follows. Section II introduces important concepts and the notation that will be used throughout the paper. Section III contains three subsections: in Section III-A we provide the necessary background on permutations and permutation matrices to be used in the following two sections; in Section III-B we present the algebraic conditions required to achieve a certain desired girth and give a lemma that significantly reduces the number of required conditions; finally, in Section III-C we review an upper bound on minimum distance for commuting permutation matrices. The main result of the paper is contained in Section IV, which shows how any protograph-based LDPC code can be transformed into an equivalent partially-QC LDPC code with the same girth and minimum distance. Section V then analyzes some specific cases of partially QC LDPC

978-1-61284-233-2/11/$26.00 ©2011 IEEE

codes. In Section V-A, we consider the case of non-QC array LDPC codes and show that these codes have the same upper bounds on girth and minimum distance as corresponding QC codes. In Section V-B we explicitly give the smallest set of girth conditions, i.e., without any redundant conditions, on the permutation matrices in the composition of a 2×3 protomatrix that are needed to construct partially-QC codes with larger girth and minimum distance than corresponding QC codes. Then, Section V-C provides a similar analysis for 3×4 protograph-based partially-QC LDPC codes. Finally, Section VI concludes the paper.

II. Definitions

This section introduces definitions and the notation that will be used throughout the paper.

We use the following sets: $\mathbb{Z}$ is the ring of integers and $\mathbb{F}_2$ is the Galois field of size 2. By $\mathbb{F}_2^n$ and $\mathbb{F}_2^{m\times n}$ we will mean, respectively, a row vector over $\mathbb{F}_2$ of length n and a matrix over $\mathbb{F}_2$ of size $m \times n$.

All codes will be binary linear codes. As usual, a code $\mathcal{C}$ of length n can be specified by a (scalar) parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{m\times n}$, i.e., $\mathcal{C} = \left\{\mathbf{c} \in \mathbb{F}_2^n \mid \mathbf{H}\cdot\mathbf{c}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}\right\}$, where $^{\mathsf{T}}$ denotes transposition. Its minimum Hamming distance will be denoted by $d_{\min}(\mathcal{C})$.

With a parity-check matrix $\mathbf{H}$ we associate a Tanner graph [5] in the usual way. The girth of a graph is then the length of the shortest cycle in the graph.

In this paper we restrict our attention to protomatrices with all entries equal to 1, i.e., regular protographs without parallel edges. Consequently, a parity-check matrix $\mathbf{H}$ of a code $\mathcal{C}$ based on such a protograph will be an $mr \times nr$ matrix with the (i,j)th entry equal to a permutation matrix P_{ij}, for all $i \in \{0,\ldots,m-1\}$, $j \in \{0,\ldots,n-1\}$. A generalization of these results to irregular protographs and protographs with parallel edges is the subject of ongoing research.

III. Protograph based codes

A. Permutations and permutation matrices

An r-permutation p is a one-to-one function on the set $\mathcal{S} \triangleq \{0,1,\ldots,r-1\}$ described as:

$$p \triangleq \begin{pmatrix} 0 & 1 & \ldots & r-1 \\ p(0) & p(1) & \ldots & p(r-1) \end{pmatrix}.$$

Any permutation p can be represented by two corresponding $r \times r$ permutation matrices P and P', where P has all entries equal to zero except for r entries equal to one at the positions $(i, p(i)), i \in \mathcal{S}$, and P' has all entries equal to zero except for r entries equal to one at the positions $(p(i), i), i \in \mathcal{S}$. Naturally, $P' = P^{\mathsf{T}} = P^{-1}$. Composing two permutations p and q on $\mathcal{S}$ gives the two permutations pq and qp, which in general are not equal. The two matrices corresponding to the permutation pq are QP and $P'Q'$, respectively. Therefore, the composition function corresponds to a product of associated matrices; however, the order of the matrices in the product differs depending on whether the row or column representation of the matrices is considered.

Example 1. Let

$$p = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \end{pmatrix}, q = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}.$$

Then

$$P = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, Q = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$P' = P^{\mathsf{T}}, Q' = Q^{\mathsf{T}}.$$

The functions

$$pq = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 2 & 1 \end{pmatrix}, qp = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 1 & 2 \end{pmatrix}$$

correspond to the products

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

Naturally, $P'Q' = (QP)^{\mathsf{T}}$ and $Q'P' = (PQ)^{\mathsf{T}}$. Therefore pq corresponds to QP and $P'Q'$, depending on whether we take the values of the function to be row indices or column indices.

□

Conversely, to any permutation matrix P we can associate two permutation functions p and p' on $\mathcal{S}$, such that $p(i)$ equals the column index of the entry equal to 1 in the ith row of P and $p'(i)$ equals the row index of the entry equal to 1 in the ith column of P. Naturally, $p' = p^{-1}$.

B. Girth conditions

We will say that a (permutation) matrix has a fixed column (or row) if it overlaps with the identity matrix in at least one column (or row). The following theorem gives the algebraic conditions that are imposed by a cycle of length $2l$ in the Tanner graph of a protograph-based LDPC code with parity-check matrix $\mathbf{H} = (P_{ij})$ on the permutation matrices P_{ij}, see, e.g., [8].

Theorem 2. *Let $\mathcal{C}$ be a code described by a parity-check matrix $\mathbf{H} = (P_{i,j}) \in \mathbb{F}_2^{mr\times nr}$, where each (i,j) entry is an $r \times r$ permutation matrix $P_{i,j}$. Then the Tanner graph associated with $\mathbf{H}$ has a cycle of length $2l$ if there exist indices $i_0, i_1, \ldots, i_{l-1}$ and $j_0, j_1, \ldots j_{l-1}$ such that $i_s \neq i_{s+1}, j_s \neq j_{s+1}$ (where $s+1$ here means $s+1 \mod l$), for all $s \in 0, 1, \ldots l-1$, and such that the product of matrices*

$$P_{i_0 j_0} P_{i_1 j_0}^{\mathsf{T}} P_{i_1 j_1} P_{i_2 j_1}^{\mathsf{T}} \ldots P_{i_{l-1} j_{l-1}} P_{i_0 j_{l-1}}^{\mathsf{T}}$$

has a fixed column.

For circulant matrices, the above condition reduces to the known condition presented in [11] as follows.

Corollary 3. *Let $\mathcal{C}$ be a code described by a parity-check matrix $\mathbf{H} = (P_{i,j}) \in \mathbb{F}_2^{mr\times nr}$, where each $P_{i,j}$ is an $r \times$*

r circulant matrix $[s_{i,j}]$ (where $s_{i,j}$ denotes the number of left shifts of the identity matrix needed to obtain the circulant permutation matrix). Then the Tanner graph associated with $\mathbf{H}$ has a cycle of length $2l$ if there exist indices $i_0, i_1, \ldots, i_{l-1}$ and $j_0, j_1, \ldots j_{l-1}$ such that $i_s \neq i_{s+1}, j_s \neq j_{s+1}$ (where $s+1$ here means $s+1 \mod l$), for all $s \in 0, 1, \ldots l-1$, and such that

$$s_{i_0 j_0} - s_{i_1 j_0} + s_{i_1 j_1} - s_{i_2 j_1} + \ldots + s_{i_{l-1} j_{l-1}} - s_{i_0 j_{l-1}} = 0.$$

From Theorem 2 we obtain the following corollary.

Corollary 4. *Let $\mathcal{C}$ be a code described by a parity-check matrix $\mathbf{H}$ as in Theorem 2.*
1) A 4 cycle exists if and only if there exist sets of distinct indices $\{i_0, i_1\}$ and $\{j_0, j_1\}$ such that $P_{i_0 j_0} P_{i_1 j_0}^{\mathsf{T}} P_{i_1 j_1} P_{i_0 j_1}^{\mathsf{T}}$ has a fixed column, or equivalently, such that $P_{i_0 j_0} P_{i_1 j_0}^{\mathsf{T}}$ and $P_{i_0 j_1} P_{i_1 j_1}^{\mathsf{T}}$ have a column in common.
2) Similarly, a 6 cycle exists if and only if there exist sets of distinct indices $\{i_0, i_1, i_2\}$ and $\{j_0, j_1, j_2\}$ such that $P_{i_0 j_0} P_{i_1 j_0}^{\mathsf{T}} P_{i_1 j_1} P_{i_0 j_1}^{\mathsf{T}} P_{i_2 j_2} P_{i_1 j_2}^{\mathsf{T}}$ has a fixed column, or equivalently, such that $P_{i_0 j_0} P_{i_1 j_0}^{\mathsf{T}} P_{i_1 j_1}$ and $P_{i_1 j_2} P_{i_2 j_2}^{\mathsf{T}} P_{i_0 j_1}$ have a column in common.
3) This equivalence holds for all desired girths.

The next lemma and its corollary, which show that a product of two permutations pq with a fixed point implies the same for qp, allows us to improve Theorem 2 by significantly reducing the number of girth conditions that must be imposed on the permutation matrices in the composition of the protomatrix describing a protograph-based LDPC code.

Lemma 5. *Let p and q be two permutations on a set $\mathcal{S} = \{0, 1, \ldots, r-1\}$ such that pq has a fixed point. Then qp has a fixed point.*

Proof: Let $x \in \mathcal{S}$ be the fixed point of pq: $pq(x) = x$. Let $y \triangleq q(x)$. Then $p(y) = q^{-1}(y)$, from which $qp(y) = y$, and hence qp has a fixed point.

Corollary 6. *Let P and Q be two $r \times r$ permutation matrices such that QP has a fixed column. Then PQ has a fixed column.*

In Theorems 10 and 12, when we consider LDPC codes based on 2×3 and 3×4 protographs, respectively, we will show how Corollary 6 simplifies the search for partially-QC protograph-based codes with large girth and minimum distance.

C. Minimum distance

We now review some known facts regarding the minimum distance of protograph-based LDPC codes. Suppose that the matrices P_{ij} commute with each other, i.e., $P_{ij} P_{kl} = P_{kl} P_{ij}$ for all i, j, k, l. Note that parity-check matrices with all P_{ij} circulant (in the case of QC LDPC codes) or with all P_{ij} equal to powers of some (not necessarily circulant) permutation matrix P (in the case of array LDPC codes), satisfy this commutativity condition. These examples are not exhaustive. Let $\mathcal{S}$ be a size-$(m+1)$ subset of $\{0, 1, \ldots, n-1\}$ and let $\mathbf{c} = (c_i)_{0 \leqslant i \leqslant n-1}$ be a length-n vector in $(\mathbb{F}_2^{r \times r})^n$, in multivariables P_{ij}, defined by

$$c_i \triangleq \begin{cases} \det\left(\mathbf{H}_{\mathcal{S} \setminus i}\right) & \text{if } i \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases},$$

where the entries P_{ij} are regarded as entries in a commutative ring over which we define the determinant operator $\det$, and where $\mathbf{H}_{\mathcal{S} \setminus i}$ is the sub-matrix of $\mathbf{H}$ that contains all rows of $\mathbf{H}$ and only the columns of $\mathbf{H}$ with indices in the set $\mathcal{S} \setminus \{i\}$.

According to [10], [14], any column of $\mathbf{c}$ is a codeword in $\mathcal{C}$, since we are assuming that the matrices P_{ij} commute. Based on these codewords, the upper bound $d_{\min}(\mathbf{H}) \leqslant (m+1)!$ is easily obtained for any protograph-based code with commuting matrices P_{ij}.

If the matrices P_{ij} do not commute as it is in most cases, then it is unclear how to define such a determinant, since changing the order of the matrices in the products defining the determinant would most likely give different results. This implies, however, that the upper bound $(m+1)!$ no longer holds, so that partially-QC protograph-based codes can have minimum distance exceeding this bound, and this can happen even for codes having Tanner graphs with small girths.

IV. Partially-QC LDPC codes

Theorem 7. *Without loss of generality, any $m \times n$ all-one protomatrix can be r-lifted to the following matrix*

$$\begin{bmatrix} I & I & \ldots & I \\ I & P_{10} & \ldots & P_{1,n-2} \\ \vdots & \vdots & \ldots & \vdots \\ I & P_{m-2,0} & \ldots & P_{m-2,n-2} \end{bmatrix}, \tag{1}$$

where P_{ij} are permutation matrices for all $i \in \{0, \ldots, m-2\}$, $j \in \{0, \ldots, n-2\}$, I is the identity matrix, and all matrices are of size r.

We call the code defined by such a matrix *a partially-QC* LDPC code, because the first block row and column is formed by circulant matrices, in particular, by identity matrices.

Proof: The most general case of an LDPC code based on an $m \times n$ all-one protomatrix is given by a parity-check matrix $\mathbf{H}$ with the (i,j)th entry equal to a permutation matrix Q_{ij}, for all $i \in \{0, \ldots, m-1\}$, $j \in \{0, \ldots, n-1\}$. This matrix can be transformed by column operations into

$$\begin{bmatrix} I & I & \ldots & I \\ Q_{10} Q_{00}^{\mathsf{T}} & Q_{11} Q_{01}^{\mathsf{T}} & \ldots & Q_{1,n-1} Q_{0,n-1}^{\mathsf{T}} \\ \vdots & \vdots & \ldots & \vdots \\ Q_{m-1,0} Q_{00}^{\mathsf{T}} & Q_{m-1,1} Q_{01}^{\mathsf{T}} & \ldots & Q_{m-1,n-1} Q_{0,n-1}^{\mathsf{T}} \end{bmatrix}, \tag{2}$$

followed by row operations to transform it into

$$\begin{bmatrix} I & I & \ldots & I \\ I & (Q_{20} Q_{00}^{\mathsf{T}})^{\mathsf{T}} Q_{21} Q_{01}^{\mathsf{T}} & \ldots & (Q_{20} Q_{00}^{\mathsf{T}})^{\mathsf{T}} Q_{2,n-1} Q_{0,n-1}^{\mathsf{T}} \\ \vdots & \vdots & \ldots & \vdots \\ I & (Q_{m-1,0} Q_{00}^{\mathsf{T}})^{\mathsf{T}} Q_{m-1,1} Q_{01}^{\mathsf{T}} & \ldots & (Q_{m-1,0} Q_{00}^{\mathsf{T}})^{\mathsf{T}} Q_{m-1,n-1} Q_{0,n-1}^{\mathsf{T}} \end{bmatrix}. \tag{3}$$

The above row and column operations do not affect the girth of the Tanner graph or the minimum distance of the code. The column operations simply imply permutations of codeword

positions, i.e., the variable nodes in the Tanner graph, given by the permutation matrices Q_{0j}, for $j = 0, 1, \ldots, n-1$. Additionally, the row operations have no effect on the code itself and, in the Tanner graph, they correspond to permutations of the check nodes. Therefore, the row and column operations result only in permuting the variable and check nodes in the Tanner graph of the parity-check matrix of the code, which does not affect the girth or minimum distance of the code or its performance under a message passing decoding algorithm, or any other decoding algorithm. In other words, any code described by an $m \times n$ protomatrix is equivalent to a code described by the protomatrix given in (1).

Our motivation in considering partially-QC LDPC codes is three-fold. First, with careful hardware design, partially-QC LDPC codes offer simplified encoding and decoding implementation due to the identity matrices in the first row and column of the protomatrix; second, the search space for good codes is reduced: instead of having to choose mn permutation matrices, we only need to choose $(m-1)(n-1)$ permutation matrices; lastly, as shown above, these structures are equivalent to the entire ensemble of protograph-based codes, so considering only partially-QC LDPC codes is by no means restrictive.

V. Case analysis for constructing good partially-QC codes

A. Non-QC array structures

When constructing codes, simple structures are attractive due to their ease of implementation and analysis. In the case of protograph-based LDPC codes, the simplest non-QC code construction is given by the case in which all the matrices P_{ij} are powers of the same permutation matrix P. However, we will see that in this case, no matter what P is chosen to be, both the girth and the minimum distance of the resulting protograph-based code are upper bounded by the same bounds that hold for QC codes. In the case of the minimum distance, this was already shown by MacKay [10]. We state this observation in the following theorem.

Theorem 8. *Let $\mathcal{C}$ be a code described by a parity-check matrix $\mathbf{H} = (P^{e_{i,j}}) \in \mathbb{F}_2^{mr \times nr}$, where $m \geqslant 2, n \geqslant 3$, $e_{i,j}$ are positive integers, $i = 0, \ldots, m-1, j = 0, \ldots, n-1$, and P is an r-permutation matrix. Then the girth of the Tanner graph associated with $\mathbf{H}$ is upper bounded by 12 and the code's minimum distance is upper bounded by $(m+1)!$.*

Proof: Since $m \geqslant 2, n \geqslant 3$, there exists at least one 2×3 block submatrix of $\mathbf{H}$ of the form

$$\begin{bmatrix} P^{e_{0,0}} & P^{e_{0,1}} & P^{e_{0,2}} \\ P^{e_{1,0}} & P^{e_{1,1}} & P^{e_{1,2}} \end{bmatrix}.$$

The product $P^{e_{0,0}}(P^{e_{1,0}})^{\mathsf{T}} P^{e_{1,1}} (P^{e_{0,1}})^{\mathsf{T}} P^{e_{1,2}} (P^{e_{0,2}})^{\mathsf{T}} \cdot P^{e_{1,0}}(P^{e_{0,0}})^{\mathsf{T}} P^{e_{0,1}} (P^{e_{1,1}})^{\mathsf{T}} P^{e_{0,2}} (P^{e_{1,2}})^{\mathsf{T}} = I$, where I is the r-identity matrix, which implies, based on Theorem 2, the existence of a length 12 cycle, and, consequently, a girth of at most 12. Since all the permutation matrices in the composition of $\mathbf{H}$ commute as powers of the same permutation, the upper bound $(m+1)!$ [10] on the minimum distance clearly holds.

Therefore, any $m \times n$ protomatrix lifted with permutation matrices $P_{i,j}$ will have an upper bound of 12 on the girth if there exists a 2×3 or a 3×2 submatrix given by powers of the same permutation matrices.

Similarly, any $m \times n$ protomatrix lifted with permutation matrices $P_{i,j}$ will have an upper bound of $(m+1)!$ on the minimum distance if there exists an $m \times (m+1)$ submatrix of the protomatrix that is lifted with matrices that commute (hence also if lifted with powers of the same matrix), because then the upper bound $(m+1)!$ applies.

Therefore, in order to construct classes of codes that have unbounded girth and minimum distance, we need to avoid permutation matrices that commute, and in particular 2×3 substructures that include only matrices described as powers of the same permutation matrix.

B. Partially QC structures based on a 2×3 protomatrix

The next case we consider is that of column weight 2, and in particular, that of a 2×3 protomatrix. In the following we summarize the conditions that we need to impose on the permutation matrix entries of the parity-check matrices of these codes such that their girths and minimum distances exceed those of QC codes of the same length.

Remark 9. Note that in a protomatrix with column weight 2, any cycle corresponds to a codeword, which can be seen by assigning the value 1 to a variable node participating in the cycle and the value 0 to the remaining variable nodes. □

Based on Remark 9, we obtain that any Tanner graph with variable node degree equal to 2 has only cycles of length divisible by 4. Indeed, otherwise, the associated code would have codewords of odd weight, which is impossible in a code based on a protomatrix containing only 1s.

In Theorem 7 we showed that, without loss of generality, we can assume the simplified form of (1) for the parity-check matrix of a protograph-based code. In the case of a 2×3 protomatrix this reduces to

$$\mathbf{H} = \begin{bmatrix} I & I & I \\ I & P & Q \end{bmatrix}. \tag{4}$$

The following are the conditions that P and Q must satisfy in order to obtain girth larger than 12 (hence $\mathrm{girth}(\mathbf{H}) \geqslant 16$) and, equivalently, minimum distance $d_{\min}(\mathbf{H}) \geqslant 8$.

Theorem 10. *Let $\mathbf{H}$ be in the form of* (4)*. Then:*

1) $\mathrm{girth}(\mathbf{H}) > 4 \iff P, Q, PQ^{\mathsf{T}}$ *have no fixed columns.*
2) $\mathrm{girth}(\mathbf{H}) > 8 \iff P, Q, PQ^{\mathsf{T}}, PQ, P^2, Q^2, P^2Q^{\mathsf{T}}, P^{\mathsf{T}}Q^2, PQ^{\mathsf{T}}PQ^{\mathsf{T}}$ *have no fixed columns.*
3) $\mathrm{girth}(\mathbf{H}) > 12 \iff P, Q, PQ^{\mathsf{T}}, PQ, P^2, Q^2, P^2Q^{\mathsf{T}}, P^{\mathsf{T}}Q^2, PQ^{\mathsf{T}}PQ^{\mathsf{T}}, P^3, P^2Q, PQ^2, Q^3, P^3Q^{\mathsf{T}}P^2(Q^{\mathsf{T}})^2, PQ^{\mathsf{T}}PQ, PQ^{\mathsf{T}}P^{\mathsf{T}}Q^{\mathsf{T}}, QP^{\mathsf{T}}Q^{\mathsf{T}}P, P^{\mathsf{T}}Q^3, P^2Q^{\mathsf{T}}PQ^{\mathsf{T}}, P(Q^{\mathsf{T}})^2PQ^{\mathsf{T}}, QP^{\mathsf{T}}QP^{\mathsf{T}}Q, P^{\mathsf{T}}QP^{\mathsf{T}}QP^{\mathsf{T}}Q$ *have no fixed columns.*

Example 11. Consider the representation (4) of a 2×3 protograph. The smallest size required for the permutation matrices P and Q to satisfy the conditions in 1) is $r = 3$. Now let $[a]$ denote a circulant corresponding to a shifts to the left of the identity matrix. By setting $P = [1]$ and $Q = [2]$, we then obtain a parity-check matrix with girth 8 and, correspondingly, minimum Hamming distance 4. (Note that $PQ = I$ has fixed columns, so the conditions in 2) imply that the girth is not larger than 8.)

To satisfy the conditions in 2), we must increase the permutation matrix size to at least $r = 7$. There are many choices of P and Q that satisfy these conditions. In particular, by choosing circulant permutations $P = [4]$ and $Q = [6]$ the conditions in 2) are satisfied and we obtain a parity-check matrix with girth 12 and, correspondingly, minimum Hamming distance 6. (However $P^2Q = I$ has fixed columns, so condition 3) implies that the girth is not larger than 12.)

Therefore, to achieve girth 8 and 12 we can simply choose circulant permutation matrices of small size. However, according to the discussion following Theorem 8, we cannot exceed a girth of 12 and satisfy the conditions in 3) unless we choose non-circulant permutation matrices P and Q with size larger than $r = 7$. In order to exceed this upper bound, we would need to choose non-circulant permutation matrices P, Q of order r that generate different permutation groups $< P >$ and $< Q >$. Choosing these matrices in an efficient way is the subject of ongoing research. □

C. Partially-QC structures based on a 3×4 protomatrix

According to Theorem 7, we can assume, without loss of generality, that a 3×4 protograph has the form

$$\mathbf{H} = \begin{bmatrix} I & I & I & I \\ I & P & Q & R \\ I & S & T & U \end{bmatrix}. \tag{5}$$

The following conditions are needed to obtain girth larger than 6. Note that similar conditions can be obtained to guarantee girth greater than $8, 10, \ldots$, but these are omitted here.

Theorem 12. *Let* $\mathbf{H}$ *be in the form of* (5)*. Then:*

1) $\mathrm{girth}(\mathbf{H}) > 4 \iff P, Q, R, S, T, U, PQ^{\mathsf{T}}, PR^{\mathsf{T}}, ST^{\mathsf{T}}, SU^{\mathsf{T}}, QR^{\mathsf{T}}, TU^{\mathsf{T}}, PS^{\mathsf{T}}, QT^{\mathsf{T}}, RU^{\mathsf{T}}, PS^{\mathsf{T}}TQ^{\mathsf{T}}, PS^{\mathsf{T}}UR^{\mathsf{T}}, QT^{\mathsf{T}}UR^{\mathsf{T}}$ *have no fixed columns .*
2) $\mathrm{girth}(\mathbf{H}) > 6 \iff PT^{\mathsf{T}}, PU^{\mathsf{T}}, QS^{\mathsf{T}}, QU^{\mathsf{T}}, RS^{\mathsf{T}}, RT^{\mathsf{T}}, PTQ^{\mathsf{T}}, PUR^{\mathsf{T}}, PS^{\mathsf{T}}T, PS^{\mathsf{T}}U, PS^{\mathsf{T}}Q^{\mathsf{T}}, PS^{\mathsf{T}}R^{\mathsf{T}}, QUR^{\mathsf{T}}, QT^{\mathsf{T}}S, QT^{\mathsf{T}}U, QT^{\mathsf{T}}R^{\mathsf{T}}, RU^{\mathsf{T}}S, RU^{\mathsf{T}}T, PS^{\mathsf{T}}TR^{\mathsf{T}}, PS^{\mathsf{T}}UQ^{\mathsf{T}}, PT^{\mathsf{T}}UR^{\mathsf{T}}, PU^{\mathsf{T}}TQ^{\mathsf{T}}, QS^{\mathsf{T}}UR^{\mathsf{T}}, QT^{\mathsf{T}}SR^{\mathsf{T}}$, *together with the matrices listed in condition* 1) *have no fixed columns.*

Remark 13. Unlike the 2×3 structure in Section V-B, the 3×4 protomatrix considered here does not imply the same relation between girth and minimum distance of the corresponding protograph-based LDPC code. In the case of permutation matrices that commute, and therefore also in the case of circulant matrices, a 4 or 6 cycle would automatically imply a codeword of weight smaller than the corresponding upper bound on the minimum Hamming distance $(m + 1)! = 24$ valid for matrices that commute, as shown in [10]. However, if we allow general permutation matrices, this is not necessarily true. Using the reduced search space implied by (5), we can find codes with minimum distance $26, 28, 30, 32, \ldots$ for girths $4, 6, 8$ as we increase the permutation size r. □

VI. Conclusions

In this paper we have performed a study of partially-QC LDPC codes based on a given protograph. We showed that any r-fold cover graph of a protograph with single edges is isomorphic to an r-fold cover graph of a partially-QC LDPC code. Using this structure, we presented simplified algebraic conditions on the r-permutation matrices describing the r-fold graph covers of a given protograph that guarantee higher girth and minimum distance than the upper bounds for QC codes.

Acknowledgements

This work was partially supported by NSF Grants CCF-0830650, DMS-0708033, CCF-0830608, and NASA Grant NNX-09AI66G.

References

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

[2] J. Thorpe, K. Andrews, and S. Dolinar, "Methodologies for designing LDPC codes using protographs and circulants," in *Proc. IEEE Intern. Symp. on Inform. Theory*, Chicago, IL, USA, June 2004, p. 238.

[3] W. S. Massey, *Algebraic Topology: an Introduction*. New York: Springer-Verlag, 1977, reprint of the 1967 edition, Graduate Texts in Mathematics, Vol. 56.

[4] H. M. Stark and A. A. Terras, "Zeta functions of finite graphs and coverings," *Adv. Math.*, vol. 121, no. 1, pp. 124–165, 1996.

[5] R. M. Tanner, "A recursive approach to low-complexity codes," *IEEE Trans. on Inform. Theory*, vol. IT–27, pp. 533–547, Sept. 1981.

[6] R. G. Gallager, *Low-Density Parity-Check Codes*. M.I.T. Press, Cambridge, MA, 1963, available online under http://web.mit.edu/gallager/www/pages/ldpc.pdf.

[7] R. M. Tanner, "On quasi-cyclic repeat-accumulate codes," in *Proc. 37th Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, Sept. 1999, pp. 249–259.

[8] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc. 2nd Intern. Conf. on Turbo Codes and Related Topics*, Brest, France, Sept. 2000.

[9] T. Mittelholzer, "Efficient encoding and minimum distance bounds of Reed-Solomon-type array codes," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, p. 282, June 2002.

[10] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *IMA Volumes in Mathematics and its Applications, Vol. 123: Codes, Systems, and Graphical Models*. Springer-Verlag, 2001, pp. 113–130.

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

[12] O. Milenkovic, K. Prakash, and B. Vasic, "Regular and irregular low-density parity-check codes for iterative decoding based on cycle-invariant difference sets," in *Proc. 41st Allerton Conf. on Communication, Control, and Computing*, Monticello, IL, USA, Oct. 2003.

[13] Z. Li, L. Chen, L. Zeng, S. Lin, and W. H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," *IEEE Trans. on Comm.*, vol. 54, no. 1, pp. 71–81, Jan. 2006.

[14] R. Smarandache and P. O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto and Tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Trans. on Inform. Theory*, accepted for publication. See also http://arxiv.org/abs/0901.4129.

[15] R. M. Tanner, D. Sridhara, and T. Fuja, "A class of group-structured LDPC codes," in *Proc. Intern. Symp. on Comm. Theory and App.*, Ambleside, England, 2001.