Quasi-Cyclic LDPC Codes Based on Pre-Lifted Protographs

David G. M. Mitchell*, Roxana Smarandache†, and Daniel J. Costello, Jr.*
*Dept. of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana, USA,
{david.mitchell, costello.2}@nd.edu
†Dept. of Mathematics and Statistics, San Diego State University, San Diego, California, USA,
rsmarand@sciences.sdsu.edu

***Abstract*— Quasi-cyclic low-density parity-check (QC-LDPC) codes based on protographs are of great interest to code designers because of their implementation advantages and algebraic properties that make them easy to analyze. However, the protograph structure imposes undesirable fixed upper limits on important code parameters. In this paper, we show that the upper bound on the minimum Hamming distance of protograph-based QC codes can be improved by the careful application of a two-step lifting procedure applied to the protograph. The promised improvement is validated by constructing codes with minimum distance exceeding the upper bound for QC codes based on a particular protograph.**

I. Introduction

A *protograph* [1] is a small Tanner graph [2] described by an $n_c \times n_v$ incidence matrix $\mathbf{B}$, known as a base matrix, that consists of non-negative integers $B_{i,j}$ that correspond to $B_{i,j}$ parallel edges in the graph. A protograph-based code is obtained by taking an N-fold graph cover [3] of a given protograph and can be described by an $Nn_c \times Nn_v$ parity-check matrix obtained by replacing each non-zero entry $B_{i,j}$ by a sum of $B_{i,j}$ permutation matrices of size $N \times N$ and a zero entry by an $N \times N$ all-zero matrix. Low-density parity-check (LDPC) codes [4] based on a protograph form a subclass of multi-edge type codes that have been shown to have many desirable features, such as good iterative decoding thresholds and, for suitably-designed protographs, linear minimum distance growth, i.e., they are asymptotically good (see, e.g., [5]).

Members of the protograph-based LDPC code ensemble that are quasi-cyclic (QC) are of great interest to code designers, since they can be encoded with low complexity using simple feedback shift-registers [6] and their structure leads to efficiencies in decoder design. Moreover, QC codes can be shown to perform well compared to random codes for moderate block lengths [7], [8]. The construction of QC-LDPC codes can be seen as a special case of the protograph-based construction in which the N-fold cover is obtained by restricting the edge permutations to be cyclic and can be described by an $Nn_c \times Nn_v$ parity-check matrix formed as an $n_c \times n_v$ array of $N \times N$ circulant matrices. However, unlike typical members of an asymptotically good protograph-based LDPC code ensemble, codes from the QC sub-ensemble do not have linear distance growth. Indeed, if the protograph base matrix consists of only ones and zeros, then the minimum Hamming distance is bounded above by $(n_c + 1)!$, where n_c is the number of check nodes in the protograph [9], [10].

In [11], partially quasi-cyclic codes were introduced, where only a selection of the permutation matrices used in the protograph-based construction are chosen to be circulants. Algebraic conditions were derived for the permutation matrices describing the N-fold graph covers of a given protograph that ensure higher girth and minimum distance than the upper bounds for QC codes. In this paper, we show that it is possible to achieve a similar improvement in minimum distance by choosing $N \times N$ permutation matrices that are composed of a sub-array of $r \times r$ circulant matrices. As a result, we can achieve an increase in the girth and distance parameters of the code while maintaining the circulant-based structure facilitating efficient implementation. The procedure consists of two stages: first, a "pre-lifting" step where we take an m-fold graph cover of the protograph, where m is typically small, and second, a circulant-based lifting step where we take an r-fold graph cover of the *pre-lifted* protograph, with the permutations chosen to be cyclic.

The paper is structured as follows. In Section II, we provide the necessary background material, describe the structure of the QC sub-ensemble of protograph-based codes, and review an existing bound concerning the minimum Hamming distance of QC protograph-based codes. In Section III, we introduce the concept of pre-lifting. In Section IV-A, we demonstrate this construction technique on a simple $(2, 3)$-regular protograph, and derive circulant-based codes with minimum distance and girth exceeding the original QC bounds after pre-lifting. Section IV-B provides a similar analysis for a $(3, 4)$-regular protograph. Finally, concluding remarks are given in Section V.

II. Quasi-cyclic protograph-based LDPC codes

One of the main advantages of QC-LDPC codes is that they can be described simply, and as such are attractive for implementation purposes (see, e.g., [6]). In this section we describe the protograph construction method and, in particular, focus on the QC sub-ensembles of protograph-based ensembles of LDPC codes.

A. Definitions

All the codes in this paper will be binary linear codes. As usual, an $[n, k, d_{min}]$ code C of length n, rank k, and minimum Hamming distance d_{min} can be specified as the null space of an $(n-k) \times n$ (scalar) parity-check matrix $\mathbf{H}$. With a parity-check matrix $\mathbf{H}$ we associate a Tanner graph [2] in the usual way. The girth of a graph is the length of the shortest cycle in the graph.

B. Permutations and permutation matrices

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

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

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

A permutation p can be represented by an $N \times N$ permutation matrix $\mathbf{P}$, where $\mathbf{P}$ has all entries equal to zero except for N entries equal to one at positions $(i, p(i)), i \in \mathcal{S}$. We 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).

C. Protograph-based code construction

As described in Section I, a protograph [1] is a small bipartite graph, represented by a parity-check or *base* biadjacency matrix $\mathbf{B}$. The parity-check matrix $\mathbf{H}$ of a protograph-based LDPC block code can be created by replacing each non-zero entry in $\mathbf{B}$ by a sum of $B_{i,j}$ permutation matrices of size $N \times N$ and a zero entry by the $N \times N$ all-zero matrix, where $B_{i,j}$ is a non-negative integer. Graphically, this operation is equivalent to taking an N-fold graph cover, or "lifting", of the protograph. It is an important feature of this construction that each lifted code inherits the degree distribution and local graph neigbourhood structure of the protograph. The ensemble of protograph-based LDPC codes with block length $n = Nn_v$, denoted $\xi_{\mathbf{B}}(N)$, is defined as the set of matrices $\mathbf{H}$ that can be derived from a given base matrix $\mathbf{B}$ by all possible combinations of $N \times N$ permutation matrices.

D. Structure of QC sub-ensembles

The QC sub-ensemble of $\xi_{\mathbf{B}}(N)$, denoted $\xi_{\mathbf{B}}^{QC}(N)$, is the subset of parity-check matrices in $\xi_{\mathbf{B}}(N)$ where all of the permutation matrices are chosen to be *circulant*. The notation $\mathbf{I}_a$ is used to denote the $N \times N$ identity matrix with each row cyclically shifted to the left by a positions. The $N \times N$ identity matrix will be denoted by $\mathbf{I}_0$ or $\mathbf{I}$. The set of all such matrices comprise the circulant subset of the set of $N \times N$ permutation matrices. When applying the copy-and-permute operation, by restricting the choice of permutation matrices to come from this subset, the resulting parity-check matrix $\mathbf{H}$ will be QC, i.e., $\mathbf{H} \in \xi_{\mathbf{B}}^{QC}(N) \subseteq \xi_{\mathbf{B}}(N)$. In graphical terms, we refer to this operation as a "circulant-based lifting". For example, the shortened $(3, 4)$-regular QC Tanner code (see [12]) has a parity-check matrix, lifted from the 3×4 all-ones base matrix $\mathbf{B}$, given by

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}_1 & \mathbf{I}_2 & \mathbf{I}_4 & \mathbf{I}_8 \\ \mathbf{I}_5 & \mathbf{I}_{10} & \mathbf{I}_{20} & \mathbf{I}_9 \\ \mathbf{I}_{25} & \mathbf{I}_{19} & \mathbf{I}_7 & \mathbf{I}_{14} \end{bmatrix} \in \xi_{\mathbf{B}}^{QC}(N). \tag{1}$$

For lifting factor $N = 31$, this parity-check matrix defines a $[124, 33, 24]$ code with girth 8.

Note that the sub-ensemble $\xi_{\mathbf{B}}^{QC}(N)$ is smaller than the ensemble $\xi_{\mathbf{B}}(N)$. This follows since there are only N out of $N!$ permutations that are circulant, i.e., the fraction of choices of permutation matrices that are circulant is $N/N! = 1/(N-1)!$, which tends to zero as $N \to \infty$. It follows that, if the base matrix $\mathbf{B}$ contains only ones and zeros, the fraction of codes in the ensemble that are circulant is $(1/(N-1)!)^t$, where t is the number of ones in $\mathbf{B}$. Repeated edges in $\mathbf{B}$ further reduce this fraction.

E. Minimum Hamming distance bounds for QC sub-ensembles

If the base matrix $\mathbf{B}$ contains only ones and zeros, then it is well known that the minimum distance of any code from the QC sub-ensemble of protograph-based LDPC codes can immediately be bounded above by $(n_c+1)!$ [9], [10]. In [12], Smarandache and Vontobel provided an improved bound that, in addition to giving tighter bounds for binary base matrices in many cases, can also be applied to base matrices with entries larger than one, i.e., protographs with repeated edges. Let the *permanent* of an $m \times m$ matrix $\mathbf{M}$ be defined as

$$\text{perm}(\mathbf{M}) = \sum_{p} \prod_{x=0}^{m-1} M_{x,p(x)},$$

where $M_{x,p(x)}$ is the entry in $\mathbf{M}$ at position $(x, p(x))$ and we sum over the $m!$ permutations p of the set $\{0, \ldots, m-1\}$. Then the minimum distance of a code drawn from the QC sub-ensemble can be upper bounded as follows:

Theorem 1: Let C be a code from $\xi_{\mathbf{B}}^{QC}(N)$, the QC sub-ensemble of the protograph-based ensemble of codes formed from base matrix $\mathbf{B}$. Then the minimum Hamming distance of C is bounded above as[1]

$$d_{min}(C) \leq \min_{\substack{S \subseteq \{1,\ldots,n_v\} \\ |S| = n_c+1}}{}^{*} \sum_{i \in S} \text{perm}(\mathbf{B}_{S \setminus i}), \tag{2}$$

where $\text{perm}(\mathbf{B}_{S\setminus i})$ denotes the permanent of the matrix consisting of the n_c columns of $\mathbf{B}$ in the set $S \setminus i$.

Note that, for all the protographs that we consider in this paper, the bound that we obtain on the minimum distance using (2) is at least as tight as $(n_c+1)!$, and in many cases tighter.

III. Pre-lifting a protograph

In this paper, we restrict our attention to base matrices $\mathbf{B}$ with entries no larger than 1, i.e., protographs without parallel edges. Consequently, if entry $B_{i,j}$ of $\mathbf{B}$ is equal to one, then the corresponding block of the lifted parity-check matrix consists of an $N \times N$ permutation matrix $\mathbf{P}_{i,j}$. Applying Theorem 1 to $\mathbf{B}$, we obtain a finite upper bound on the minimum distance of any code C derived from $\mathbf{B}$, where the permutation matrices $\mathbf{P}_{i,j}$ are chosen to be circulant, for an *arbitrarily large* lifting factor N.

We will show that by choosing some of the $N \times N$ permutation matrices $\mathbf{P}_{i,j}$ to be circulant, and the remaining matrices $\mathbf{P}_{i,j}$ to be composed of a sub-array of $r \times r$ smaller circulant matrices, we can derive QC codes with minimum distance exceeding the upper bound for the original protograph. This construction technique can be defined in two stages:

1) first, a "pre-lifting" step where we take a carefully chosen m-fold graph cover of the protograph with base matrix $\mathbf{B}$, where m is typically small, to form a pre-lifted base matrix $\mathbf{B}'$,
2) following this, we perform a circulant-based lifting step by taking an r-fold graph cover of the *pre-lifted protograph* associated with $\mathbf{B}'$, where the permutations are chosen to be cyclic, creating a QC code with parity-check matrix $\mathbf{H}$.

Clearly, the pre-lifted base matrix $\mathbf{B}'$ defines a code that exists in the ensemble $\xi_{\mathbf{B}}(m)$, and the QC code with parity-check matrix $\mathbf{H}$ obtained after the circulant lifting step exists in $\xi_{\mathbf{B}}(mr)$; however, $\mathbf{H}$ does not necessarily exist in $\xi_{\mathbf{B}}^{QC}(mr)$ and thus the minimum distance bound calculated for $\mathbf{B}$ using (2) may be exceeded. Note that, since $\mathbf{H} \in \xi_{\mathbf{B}}(mr)$, the resulting code preserves the local graph neigbourhood structure and degree distribution of the protograph.

[1]The $\min^*\{\cdot\}$ operator returns the smallest non-zero value from a set. In this context, if the all-zero codeword arises from a constructed matrix, this operator ensures that 0 is disregarded as an upper bound in the minimization.

IV. Constructing good circulant-based LDPC codes by pre-lifting protographs

In this section, we will demonstrate the pre-lifting technique by considering two examples. First, we consider a simple $(2,3)$-regular protograph that is useful to describe the method and is easy to analyse. Then, we consider a more practically interesting $(3,4)$-regular protograph, demonstrating the successful application of the techniques to a protograph with larger node degrees.

A. Case study: a $(2,3)$-regular protograph

We begin our study with a base matrix of column weight 2, and in particular, a 2×3 base matrix. Note that, without loss of generality, a 2×3 all-ones base matrix can be N-lifted to the following matrix (see [11])

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} \\ \mathbf{I} & \mathbf{P} & \mathbf{Q} \end{bmatrix}, \tag{3}$$

where $\mathbf{P}$ and $\mathbf{Q}$ are two permutation matrices and $\mathbf{I}$ is the identity matrix, all of size $N \times N$.

Remark 2: Note that in a parity-check matrix with column weight 2, any cycle corresponds to a codeword. This can be observed in the associated Tanner graph by assigning the value 1 to the variable nodes participating in the cycle and the value 0 to the remaining variable nodes.

Example 1. For parity-check matrix (3), setting $N = 3$ and choosing $\mathbf{P} = \mathbf{I}_1$ and $\mathbf{Q} = \mathbf{I}_2$, we obtain a parity-check matrix $\mathbf{H} \in \xi_{\mathbf{B}}^{QC}(3)$ with girth 8 and, correspondingly, $d_{min} = 4$. To obtain girth 12, we must increase the permutation matrix size to at least $N = 7$. By choosing circulant permutations $\mathbf{P} = \mathbf{I}_4$ and $\mathbf{Q} = \mathbf{I}_6$, $\mathbf{H} \in \xi_{\mathbf{B}}^{QC}(7)$ and the resulting code has girth 12 and, correspondingly, $d_{min} = 6$.

Thus, in order to achieve girth 8 and 12, we can choose circulant permutation matrices of small size. However, by applying Theorem 1 to the base matrix $\mathbf{B}$, we find that any code drawn from the QC sub-ensemble $\xi_{\mathbf{B}}^{QC}(N)$ has minimum distance at most 6, or equivalently, girth at most 12. In other words, we cannot exceed a girth of 12 unless we choose non-circulant permutation matrices $\mathbf{P}$ and $\mathbf{Q}$. □

In [11], a set of minimal conditions for $\mathbf{P}$ and $\mathbf{Q}$ were derived in order to guarantee girth greater than 12. We will now show that these conditions can be achieved for block-circulant permutation matrices $\mathbf{P}$ and $\mathbf{Q}$.

1) Pre-lifting a 2×3 protograph: Consider again the 2×3 all-ones base matrix $\mathbf{B}$. Suppose we set the pre-lifting factor as $m = 2$ and obtain the following lifted base matrix:

$$\mathbf{B}' = \left[\begin{array}{cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right] \in \xi_{\mathbf{B}}(2). \tag{4}$$

By applying Theorem 1, we find that a code C drawn from the QC sub-ensemble $\xi_{\mathbf{B}'}^{QC}(r)$ with base marix $\mathbf{B}'$ has its minimum distance bounded above by $d_{min}(C) \leq 10$ (and hence the girth of the parity-check matrix bounded above by $\mathrm{girth}(\mathbf{H}) \leq 20$). Note that, as $\mathbf{B}'$ is m-lifted from $\mathbf{B}$, the search space for good pre-lifted base matrices $\mathbf{B}'$ consists of, at most, only $m!^2$ parity-check matrices where m is small. How to choose the covering graph to use at the pre-lifting step will be discussed in more detail later. Using elementary row and column operations, every parity-check marix $\mathbf{H}$ from the ensemble $\xi_{\mathbf{B}'}(r)$ can be written in the form

$$\mathbf{H} = \left[\begin{array}{cc|cc|cc} \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} \\ \hline \mathbf{I} & \mathbf{0} & \mathbf{P}_1 & \mathbf{0} & \mathbf{0} & \mathbf{Q}_1 \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{P}_2 & \mathbf{Q}_2 & \mathbf{0} \end{array}\right] = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} \\ \mathbf{I} & \mathbf{P} & \mathbf{Q} \end{bmatrix}, \tag{5}$$

where permutation matrices $\mathbf{P}_1, \mathbf{P}_2, \mathbf{Q}_1$, and $\mathbf{Q}_2$ are of size $r \times r$, and $\mathbf{P}$ and $\mathbf{Q}$ are of size $N \times N = 2r \times 2r$. The QC sub-ensemble $\xi_{\mathbf{B}'}^{QC}(r)$ can then be described by the set of all parity-check matrices $\mathbf{H}$, where $\mathbf{P}_1, \mathbf{P}_2, \mathbf{Q}_1$, and $\mathbf{Q}_2$ are restricted to be circulant permutation matrices. It can easily be shown that the improvement in minimum distance and girth promised by the application of Theorem 1 can be achieved by codes from $\xi_{\mathbf{B}'}^{QC}(r)$. For example, setting $r = 9$ and choosing $\mathbf{P}_1, \mathbf{P}_2, \mathbf{Q}_1$, and $\mathbf{Q}_2$ as $\mathbf{I}_1, \mathbf{I}_2, \mathbf{I}_0$, and $\mathbf{I}_6$, respectively, gives a $[54, 19, 8]$ code with $\mathrm{girth}(\mathbf{H}) = 16$, and choosing the matrices as $\mathbf{I}_1, \mathbf{I}_9, \mathbf{I}_0$, and $\mathbf{I}_4$, respectively, with $r = 20$ gives a $[120, 41, 10]$ code with $\mathrm{girth}(\mathbf{H}) = 20$. Using this configuration, we find that $r = 9$ and $r = 20$ are the smallest possible circulant sizes that enable us to construct codes with girths 16 and 20, corresponding to minimum distances $d_{min} = 8$ and $d_{min} = 10$, respectively. There are 216 (2880) such codes in the $r = 9$ ($r = 20$) QC sub-ensembles.

In other words, by choosing $\mathbf{P}$ and $\mathbf{Q}$ to be an array of circulants, or *block-circulant*, rather than just searching for random permutations, we obtain a significant improvement in girth and minimum distance while maintaining the desirable circulant structure facilitating simplified encoding and decoding. Moreover, the search space is greatly reduced. In searching for a code with pre-lifting factor m and circulant lifting factor r, the block-circulant permutation matrix $\mathbf{P}$ has r^m choices, whereas there are $(mr)!$ choices for a permutation matrix $\mathbf{P}$ of size mr. For example, in searching for a code with minimum distance $d_{min}(C) = 8$ with $m = 2$ and $r = 9$ there are $r^m = 81$ choices for the block-circulant permutation matrix, wheras there are $mr! = 18!$ choices for a random permutation matrix of size $mr = 18$. □

2) Choosing m-fold graph covers for pre-lifting a protograph: Not all choices of covering graph are equivalent at the pre-lifting step. For example, the possible choices for the submatrix $[\mathbf{P} \,|\, \mathbf{Q}]$ in (3) after the pre-lifting step with $m = 2$ are

$$\left[\begin{array}{cc|cc} \mathbf{P}_1 & \mathbf{0} & \mathbf{Q}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{P}_2 & \mathbf{0} & \mathbf{Q}_2 \end{array}\right], \tag{6}$$

$$\left[\begin{array}{cc|cc} \mathbf{P}_1 & \mathbf{0} & \mathbf{0} & \mathbf{Q}_1 \\ \mathbf{0} & \mathbf{P}_2 & \mathbf{Q}_2 & \mathbf{0} \end{array}\right], \tag{7}$$

$$\left[\begin{array}{cc|cc} \mathbf{0} & \mathbf{P}_1 & \mathbf{Q}_1 & \mathbf{0} \\ \mathbf{P}_2 & \mathbf{0} & \mathbf{0} & \mathbf{Q}_2 \end{array}\right], \tag{8}$$

$$\left[\begin{array}{cc|cc} \mathbf{0} & \mathbf{P}_1 & \mathbf{0} & \mathbf{Q}_1 \\ \mathbf{P}_2 & \mathbf{0} & \mathbf{Q}_2 & \mathbf{0} \end{array}\right]. \tag{9}$$

Note that choices (7), (8), and (9) are *equivalent*, i.e., they can be shown to be equal using only elementary row and column operations. Consequently, the lifted ensembles $\xi_{\mathbf{B}'}^{QC}(r)$ consist of the same set of codes, up to row and column permutations.

Applying the bound (2) to the pre-lifted configuration (6), we obtain that a code C from the QC sub-ensemble $\xi_{\mathbf{B}'}^{QC}(r)$ has its minimum distance bounded above as $d_{min}(C) \leq$

12. However, note that the Tanner graph of base matrix $\mathbf{B}'$ corresponding to (6) consists of two disconnected copies of the original protograph (or 1-cover). It follows that any lifted parity-check matrix contains the two following disjoint substructures:

$$\begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} \\ \mathbf{I} & \mathbf{P}_1 & \mathbf{Q}_1 \end{bmatrix} \text{ and } \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} \\ \mathbf{I} & \mathbf{P}_2 & \mathbf{Q}_2 \end{bmatrix},$$

and consequently has its minimum distance and girth bounded above as $d_{min}(C) \leq 6$ and $\text{girth}(\mathbf{H}) \leq 12$, respectively. Thus, in terms of maximizing minimum distance and girth, the pre-lifting configuration (7) should be chosen.

3) Larger degrees of pre-lifting: Intuitively, the larger we make the pre-lifting factor m for a fixed block length n, the more 'random-like' the QC sub-ensemble $\xi_{\mathbf{B}'}^{QC}(r)$ becomes and, as such, we would expect the maximum achievable minimum distance to increase. We saw earlier that, after a careful choice of pre-lifting with factor $m = 2$, the maximum achievable minimum distance of a circulant-based lifting increased from $d_{min}(C) \leq 6$ to $d_{min}(C) \leq 10$, and correspondingly, the maximum achievable girth increased from 12 to 20. In the remainder of this section, we describe how the minimum distance and girth is affected by increasing the pre-lifting factor to values of $m \geq 3$.

We employ the sieve principle in order to find a good covering graph to use at the pre-lifting step. Note that every 3-cover can be written in the form of (3), and as such, there are $m!^2 = 3!^2 = 36$ covering graphs to consider for $m = 3$. Of these 3-covers, we find that many are equivalent. In fact, after removing (or sieving out) the equivalent graphs, we are left with only 5 choices. Of these choices, if any contain disjoint sub-graphs of a smaller covering graph ($m = 1$ or $m = 2$ in this case), then the minimum distance cannot exceed the corresponding bound calculated for such a sub-graph. For a 3-cover, there are two such sub-graphs; either there are three copies of the 1-cover (3 disjoint copies of the original protograph), or the lifted graph consists of both a 1-cover and a 2-cover (a copy of the original protograph and a disjoint 2-cover). In both cases, a code C drawn from the QC sub-ensemble has its minimum distance bounded above as $d_{min} \leq 6$ as a result of the substructure associated with the 1-cover. For example, the only configuration of $[\mathbf{P} \,|\, \mathbf{Q}]$ that results in three copies of the 1-cover is where both $\mathbf{P}$ and $\mathbf{Q}$ have a block-identity structure, i.e., the circulants in the array occur only on the leading diagonal. There are nine (equivalent) occurences of the second limiting substructure consisting of both a 1-cover and a 2-cover. One such example is the substructure

$$\left[\begin{array}{ccc|ccc} \mathbf{P}_1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{Q}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{P}_2 & \mathbf{0} & \mathbf{Q}_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}_3 & \mathbf{0} & \mathbf{0} & \mathbf{Q}_3 \end{array}\right], \tag{10}$$

which again results in any code C drawn from $\xi_{\mathbf{B}'}^{QC}(r)$ having its minimum distance bounded above as $d_{min}(C) \leq 6$ for arbitrarily large circulant size r.

Note that applying (2) to base matrices containing these two harmful substructures gives the loose upper bounds $d_{min}(C) \leq 24$ and $d_{min}(C) \leq 12$, respectively, and so it is necessary to sieve these choices at this stage. After sieving the covering graphs containing these limiting substructures, we are left with 3 candidates for the pre-lifted base matrix $\mathbf{B}'$. Applying (2) to the remaining choices results in one candidate that bounds the minimum distance of circulant-based codes drawn from the ensemble as $d_{min}(C) \leq 10$ and two (non-equivalent) candidates with bound $d_{min}(C) \leq 12$. Note that $d_{min}(C) \leq 10$ is achievable by a 2-cover, so this choice is sieved out, leaving only two remaining choices for the pre-lifted graph. One of the remaining choices is the 3-cover given by

$$\left[\begin{array}{ccc|ccc} \mathbf{P}_1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{Q}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{P}_2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{Q}_2 \\ \mathbf{0} & \mathbf{0} & \mathbf{P}_3 & \mathbf{Q}_3 & \mathbf{0} & \mathbf{0} \end{array}\right], \tag{11}$$

and we find that the corresponding bound is indeed tight. Choosing circulants $\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3, \mathbf{Q}_1, \mathbf{Q}_2$, and $\mathbf{Q}_3$ as $\mathbf{I}_1, \mathbf{I}_5, \mathbf{I}_{25}, \mathbf{I}_4, \mathbf{I}_7$, and $\mathbf{I}_{28}$, respectively, with $r = 46$ results in a code C with minimum distance $d_{min}(C) = 12$ and $\text{girth}(\mathbf{H}) = 24$.

The procedure can be repeated for $m \geq 4$. Applying the sieve technique to the $4!^2$ candidate covering graphs for $m = 4$, we are left with 5 candidates with $d_{min}(C) \leq 14$. This bound is also found to be tight by constructing codes achieving a minimum distance that is equal to 14. Table I summarizes the results we have obtained as a result of pre-lifting the 2×3 all-ones base matrix $\mathbf{B}$.

pre-lifting factor m	d_{min}	girth
1	6	12
2	10	20
3	12	24
4	14	28

TABLE I: Largest possible values of the minimum Hamming distance and girth that are achievable given a particular pre-lifting factor m.

Note that the minimum distance is not growing very fast in this example, but this is expected for $(2, 3)$-regular codes (see [4]). It does, however, demonstrate an observable improvement in minimum distance and girth by pre-lifting the protograph. In the next section we will see more pronounced improvements by considering a protograph with increased node degrees.

B. Case study: a $(3, 4)$-regular protograph

We consider the $(3, 4)$-regular protograph-based ensemble defined by the all-ones base matrix $\mathbf{B}$ of sixe 3×4. The upper bound on the minimum distance for QC codes drawn from $\xi_{\mathbf{B}}^{QC}(N)$ is $d_{min}(C) \leq 24$. The $[124, 33, 24]$ QC Tanner code (1) is an example of a code achieving this bound. We can assume, without loss of generality, that any parity-check matrix derived from $\mathbf{B}$ has the form (see [11])

$$\mathbf{H} = \begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \mathbf{I} \\ \mathbf{I} & \mathbf{P} & \mathbf{Q} & \mathbf{R} \\ \mathbf{I} & \mathbf{S} & \mathbf{T} & \mathbf{U} \end{bmatrix}, \tag{12}$$

where $\mathbf{P}, \mathbf{Q}, \mathbf{R}, \mathbf{S}, \mathbf{T}$ and $\mathbf{U}$ are permutation matrices.

Remark 3: Unlike the 2×3 structure considered in Section IV-A, the 3×4 base matrix $\mathbf{B}$ 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 implies the existence of a codeword with Hamming weight smaller than the upper bound on the minimum distance for matrices that commute, i.e., $d_{min} < (n_c + 1)! = 24$ (see [12]). However, if we allow general permutation matrices, or block circulant permutation matrices, this is not necessarily true.

In the remainder of this section, we will show that by pre-lifting this 3×4 base matrix $\mathbf{B}$ we can construct circulant-based codes with minimum distance exceeding the existing upper bound, $d_{min}(C) \leq 24$, for QC codes drawn from $\xi_{\mathbf{B}}^{QC}(N)$, even if a 6-cycle exists in the matrix. Moreover, we observe further improvements by ensuring that the girth of $\mathbf{H}$ is larger than 6.

There are $m^6 = 64$ possible 2-covers of $\mathbf{B}$ that can be considered as candidates $\mathbf{B}'$ for the pre-lifting step. After sieving out equivalent covering graphs (the 2-covers that are equal after re-labeling the vertices) there are 5 candidates left. Note that the only harmful substructure to avoid in a 2-cover is the one occurence of two disjoint 1-covers, where $\mathbf{P}, \mathbf{Q}, \mathbf{R}, \mathbf{S}, \mathbf{T}$, and $\mathbf{U}$ all have a block-identity structure. Any code C drawn from this QC sub-ensemble $\xi_{\mathbf{B}'}^{QC}(r)$ will have minimum distance bounded above by $d_{min}(C) \leq 24$ for arbitrarily large r. After sieving out this 2-cover, we have only 4 remaining candidates. Of these candidates, 2 give $d_{min}(C) \leq 120$ and 2 give $d_{min}(C) \leq 116$, all significantly larger than the bound for the 1-cover, $d_{min}(C) \leq 24$.

Example 2. Consider the following 2-cover of $\mathbf{B}$

$$\mathbf{B}' = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}\right], \qquad (13)$$

from which, without loss of generality, any lifted code in the ensemble $\xi_{\mathbf{B}'}(r)$ has the parity-check matrix

$$\mathbf{H} = \left[\begin{array}{cc|cc|cc|cc} \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{I} \\ \hline \mathbf{I} & \mathbf{0} & \mathbf{P}_1 & \mathbf{0} & \mathbf{0} & \mathbf{Q}_1 & \mathbf{0} & \mathbf{R}_1 \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{P}_2 & \mathbf{Q}_2 & \mathbf{0} & \mathbf{R}_2 & \mathbf{0} \\ \hline \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{S}_1 & \mathbf{T}_1 & \mathbf{0} & \mathbf{U}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{S}_2 & \mathbf{0} & \mathbf{0} & \mathbf{T}_2 & \mathbf{0} & \mathbf{U}_2 \end{array}\right], \qquad (14)$$

where $\mathbf{P}_i, \mathbf{Q}_i, \mathbf{R}_i, \mathbf{S}_i, \mathbf{T}_i$, and $\mathbf{U}_i$, $i = 1, 2$, are permutation matrices of size $r \times r$. Note that, by restricting these permutation matrices to be circulant, codes drawn from $\xi_{\mathbf{B}'}^{QC}(r)$ have their minimum distance bounded above by $d_{min}(C) \leq 116$. Choosing the permutation matrices $\mathbf{P}_1, \mathbf{P}_2, \mathbf{Q}_1, \mathbf{Q}_2, \mathbf{R}_1, \mathbf{R}_2, \mathbf{S}_1, \mathbf{S}_2, \mathbf{T}_1, \mathbf{T}_2, \mathbf{U}_1$, and $\mathbf{U}_2$ as circulant matrices $\mathbf{I}_1, \mathbf{I}_5, \mathbf{I}_2, \mathbf{I}_{10}, \mathbf{I}_4, \mathbf{I}_{20}, \mathbf{I}_7, \mathbf{I}_3, \mathbf{I}_{14}, \mathbf{I}_6, \mathbf{I}_{28}$, and $\mathbf{I}_9$, respectively, results in block-circulant permutation matrices $\mathbf{P}, \mathbf{Q}, \mathbf{R}, \mathbf{S}, \mathbf{T}$, and $\mathbf{U}$ that give $\mathrm{girth}(\mathbf{H}) > 4$ for $r \geq 31$. For $r = 31$, we find that $d_{min} = 36$ and $\mathrm{girth}(\mathbf{H}) = 6$. By increasing the circulant size to $r = 41$, we find that $\mathrm{girth}(\mathbf{H}) = 6$ and can determine that the minimum distance is bounded by $38 \leq d_{min} \leq 48$ using MAGMA [13]. Recall that circulant liftings of $\mathbf{B}$ have minimum distance bounded above as $d_{min} \leq 24$ for arbitrarily large circulant size, and a cycle of length 6 implies $d_{min} < 24$ (see [12]).

Choosing the circulant permutation matrices to be $\mathbf{I}_1, \mathbf{I}_5, \mathbf{I}_{10}, \mathbf{I}_{10}, \mathbf{I}_{13}, \mathbf{I}_{13}, \mathbf{I}_7, \mathbf{I}_7, \mathbf{I}_{11}, \mathbf{I}_{11}, \mathbf{I}_2$, and $\mathbf{I}_4$, respectively, gives $\mathrm{girth}(\mathbf{H}) > 6$ for $r \geq 20$. In fact, for only $r = 17$, we obtain a $[136, 36, 26]$ code with $\mathrm{girth}(\mathbf{H}) = 8$. By increasing the circulant size to $r = 49$, the code has $\mathrm{girth}(\mathbf{H}) = 10$ and we can determine that the minimum distance is bounded by $32 \leq d_{min} \leq 56$ using MAGMA. □

In this section, we have successfully applied the techniques of pre-lifting to a $(3, 4)$-regular protograph. We observed a large increase in the minimum distance of QC codes lifted from a 2-cover and we expect this to improve further for larger pre-lifting factors m.

V. Conclusions

To realize efficient encoder and decoder implementation, code designers are interested in the members of a protograph-based ensemble that are QC. However, direct circulant-based liftings of a protograph often result in small upper bounds on the minimum Hamming distance. In this paper we have shown that these bounds can be increased by applying a two-step lifting procedure to the protograph. The techniques were presented in detail for a simple $(2, 3)$-regular protograph and then successfully applied to a more practically interesting $(3, 4)$-regular protograph. For these ensembles, QC codes were constructed that demonstrate achievable increases in minimum distance and girth. Due to space limitations, we have only presented results for pre-lifting $(2, 3)$- and $(3, 4)$-regular protographs with single edges; however, the construction technique can be applied to an arbitrary protograph.

References

[1] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," Jet Propulsion Laboratory, Pasadena, CA, INP Progress Report 42-154, Aug. 2003.

[2] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sept. 1981.

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

[4] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.

[5] D. Divsalar, S. Dolinar, C. Jones, and K. Andrews, "Capacity-approaching protograph codes," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 6, pp. 876–888, Aug. 2009.

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

[7] L. Chen, J. Xu, I. Djurdjevic, and S. Lin, "Near-Shannon-limit quasi-cyclic low-density parity-check codes," *IEEE Trans. Communications*, vol. 52, no. 7, pp. 1038–1042, July 2004.

[8] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, Jr., "LDPC block and convolutional codes based on circulant matrices," *IEEE Trans. on Inf. Theory*, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

[9] 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.

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

[11] R. Smarandache, D. G. M. Mitchell, and D. J. Costello, Jr., "Partially quasi-cyclic protograph-based LDPC codes," in *Proc. IEEE Int. Conf. on Communications*, Kyoto, Japan, June 2011.

[12] 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. Inf. Theory*, to appear, 2011. Available: http://arxiv.org/abs/0901.4129

[13] W. Bosma, J. Cannon, and C. Playoust "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.