Constructing Good QC-LDPC Codes by Pre-lifting 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, rsmarand, costello.2}@nd.edu

***Abstract*—Quasi-cyclic (QC) low-density parity-check (LDPC) codes are of great interest to code designers because of their implementation advantages and algebraic properties that facilitate their analysis. In this paper, we present some new results on QC-LDPC codes that are constructed using a two-step lifting procedure based on a protograph, and, by implementing this method instead of the usual one-step procedure, we are able to show improved minimum distance and girth properties. We also present two design rules to construct QC-LDPC codes: one uses only circulant permutation matrices at the first (pre-lifting) stage and the other uses a selection of non-commuting permutation matrices. For both techniques, we obtain a demonstrable increase in the minimum distance compared to a one-step circulant-based lifting. The expected performance improvement is verified by simulation results.**

I. Introduction

Quasi-cyclic (QC) low-density parity-check (LDPC) codes [1]–[9] are of great interest to code designers, since they can be encoded with low complexity using simple feedback shift-registers [4], [5] 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 [8], [9]. Protograph-based codes [10] are constructed by taking N-fold graph covers, or "liftings", of a given protograph, for a given positive integer N. QC-LDPC codes can be constructed from a protograph by restricting the edge permutations in the graph cover to be cyclic. 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 [2], [11].

In [12], QC-LDPC codes were constructed from so-called *pre-lifted* protographs. The procedure consists of two lifting 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. As a result of the pre-lifting, the QC ensemble associated with the pre-lifted protograph can have an increased upper bound on minimum distance compared to the QC ensemble associated with the original protograph. The first lifting step was analysed in [12] and a technique was given to choose a pre-lifted protograph based on the minimum distance characteristics of the QC-LDPC code ensemble.

In this paper, we perform a joint analysis of the two lifting steps involved in the construction. We present some new results on the minimum distance and girth of pre-lifted QC-LDPC codes, and we give two design rules for code construction: one uses only circulant permutation matrices at the first (pre-lifting) stage and the other uses a selection of non-commuting permutation matrices. For both techniques, we obtain a demonstrable increase in the minimum distance compared to a direct circulant-based lifting of the original protograph. We also show that, by a careful choice of pre-lifting, we can reduce the number of conditions on the component matrices that must be checked in order to achieve a given girth g. By reducing the number of such conditions, we are permitted more freedom to design the code, which simplifies the search for good component matrices. The expected performance improvement is verified by simulation results.

II. Quasi-cyclic protograph-based LDPC codes

In this section we describe the protograph-based construction method and, in particular, focus on QC sub-ensembles of protograph-based ensembles of LDPC codes.

A. Definitions

All the codes in this paper are binary linear codes. As usual, an $[n, k, d_{min}]$ code C of length n, dimension 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 [13] 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 σ is a one-to-one function on the set $[N] \triangleq \{0, 1, \ldots, N-1\}$. A permutation σ 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 $(i, \sigma(i)), i \in [N]$. 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

A protograph [10] is a small bipartite graph, represented by an $n_c \times n_v$ parity-check or *base* incidence matrix $\mathbf{B}$, where the entries $B_{i,j}$ are non-negative integers. 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. 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 the permutation matrices are chosen to be *circulant*. The notation $\mathbf{I}_{a,N}$ is used to denote the $N \times N$ identity matrix with each row cyclically shifted to the left by a positions, or, simply $\mathbf{I}_a$ if the size of the matrix is clear from the context. The $N \times N$ identity matrix will be denoted by $\mathbf{I}_{0,N}$ or $\mathbf{I}_0$. When applying the protograph-based construction method, by restricting the choice of permutation matrices to be circulant, the resulting parity-check matrix $\mathbf{H}$ will be QC, i.e., $\mathbf{H} \in \xi_{\mathbf{B}}^{QC}(N) \subseteq \xi_{\mathbf{B}}(N)$. We refer to this operation as a "circulant-based lifting". For example, from the 3×4 all-ones

This work was partially supported by NSF Grants CCF-0830650, CCF-1161754, DMS-0708033, and TF-0830608.

978-1-4673-0223-4/12/$31.00 ©2012 IEEE

base matrix $\mathbf{B}$, a parity-check matrix of the shortened $(3,4)$-regular $[124,33,24]$ QC Tanner code [14] with $\mathrm{girth}(\mathbf{H})=8$ can be derived as

$$\mathbf{H}=\left[\begin{array}{cccc}\mathbf{I}_0 & \mathbf{I}_0 & \mathbf{I}_0 & \mathbf{I}_0\\ \mathbf{I}_0 & \mathbf{I}_4 & \mathbf{I}_{12} & \mathbf{I}_{28}\\ \mathbf{I}_0 & \mathbf{I}_{24} & \mathbf{I}_{10} & \mathbf{I}_{13}\end{array}\right]\in\xi_{\mathbf{B}}^{QC}(N), \qquad (1)$$

where the lifting degree is $N=31$.

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 $(n_c+1)!$ [2], [11]. In [14], an improved bound is presented which, 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.

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 repeated 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 $\mathbf{P}_{i,j}$. This assumption simplifies analysis and insures that the resulting codes are amenable to low-complexity implementation. The minimum distance of any code C derived from $\mathbf{B}$, where the permutation matrices $\mathbf{P}_{i,j}$ are chosen to be circulant, is bounded above by $(n_c+1)!$ for an *arbitrarily large* lifting factor N.

We will show that by choosing the permutation 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 this upper bound. The 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 $\mathbf{B}=[B_{i,j}]_{n_c\times n_v}$, where m is typically small, to form a pre-lifted base matrix $\mathbf{B}'=[\mathbf{B}'_{i,j}]$, where $\mathbf{B}'_{i,j}$ is an $m\times m$ permutation matrix if $B_{i,j}=1$, or the $m\times m$ all zero matrix if $B_{i,j}=0$,
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 circulant, creating a QC code with parity-check matrix $\mathbf{H}'=[\mathbf{P}'_{i,j}]$, where $\mathbf{P}_{i,j}$ is a *block-circulant* matrix which can be described as the product

$$\mathbf{P}_{i,j}=\mathrm{diag}(\mathbf{I}_{p_{i,j,1}},\mathbf{I}_{p_{i,j,2}},\ldots,\mathbf{I}_{p_{i,j,m}})\cdot\tilde{\mathbf{B}}'_{i,j}, \qquad (2)$$

where $p_{i,j,k}\in[r-1]$, $k=1,2,\ldots,m$, $\mathbf{I}_{p_{i,j,k}}$ has size $r\times r$, and $\tilde{\mathbf{B}}'_{i,j}\triangleq\mathbf{B}'_{i,j}\otimes\mathbf{I}_0$ denotes the Kronecker product of matrices $\mathbf{B}'_{i,j}$ and $\mathbf{I}_{0,r}$.

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 may exceed $(n_c+1)!$. 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.

To demonstrate the procedure, consider the $(2,3)$-regular base matrix

$$\mathbf{B}=\left[\begin{array}{ccc}1&1&1\\1&1&1\end{array}\right].$$

We find that any code derived from $\mathbf{B}$ using a one-step circulant-based lifting has its minimum distance upper bounded by $(n_c+1)!=6$ and its girth upper bounded by 12 [15]. A pre-lifted base matrix has the form

$$\mathbf{B}'=\left[\begin{array}{ccc}\mathbf{B}'_{1,1}&\mathbf{B}'_{1,2}&\mathbf{B}'_{1,3}\\ \mathbf{B}'_{2,1}&\mathbf{B}'_{2,2}&\mathbf{B}'_{2,3}\end{array}\right]\in\xi_{\mathbf{B}}(m),$$

where $\mathbf{B}'_{i,j}$ is an $m\times m$ permutation matrix. Then a parity-check matrix $\mathbf{H}'$ of a QC code can be obtained as

$$\mathbf{H}'=\left[\begin{array}{ccc}\mathbf{P}_{1,1}&\mathbf{P}_{1,2}&\mathbf{P}_{1,3}\\ \mathbf{P}_{2,1}&\mathbf{P}_{2,2}&\mathbf{P}_{2,3}\end{array}\right]\in\xi_{\mathbf{B}'}^{QC}(r).$$

For example, consider the following pre-lifted base matrix with $m=2$

$$\mathbf{B}'=\left[\begin{array}{ccc}\mathbf{B}'_{1,1}&\mathbf{B}'_{1,2}&\mathbf{B}'_{1,3}\\ \mathbf{B}'_{2,1}&\mathbf{B}'_{2,2}&\mathbf{B}'_{2,3}\end{array}\right]=\left[\begin{array}{cc|cc|cc}1&0&1&0&1&0\\0&1&0&1&0&1\\ \hline 1&0&1&0&0&1\\0&1&0&1&1&0\end{array}\right]\in\xi_{\mathbf{B}}(2).$$

Any code drawn from the QC-LDPC code ensemble based on this pre-lifted base matrix $\mathbf{B}'$ has its minimum distance and girth bounded above by 10 and 20, respectively [12]. The following circulant-based lifting of $\mathbf{B}'$ with $r=20$,

$$\mathbf{H}'=\left[\begin{array}{ccc}\mathbf{P}'_{1,1}&\mathbf{P}'_{1,2}&\mathbf{P}'_{1,3}\\ \mathbf{P}'_{2,1}&\mathbf{P}'_{2,2}&\mathbf{P}'_{2,3}\end{array}\right]=\left[\begin{array}{cc|cc|cc}\mathbf{I}_0&\mathbf{0}&\mathbf{I}_0&\mathbf{0}&\mathbf{I}_0&\mathbf{0}\\ \mathbf{0}&\mathbf{I}_0&\mathbf{0}&\mathbf{I}_0&\mathbf{0}&\mathbf{I}_0\\ \hline \mathbf{I}_0&\mathbf{0}&\mathbf{I}_1&\mathbf{0}&\mathbf{0}&\mathbf{I}_0\\ \mathbf{0}&\mathbf{I}_0&\mathbf{0}&\mathbf{I}_9&\mathbf{I}_4&\mathbf{0}\end{array}\right],$$

$\mathbf{H}'\in\xi_{\mathbf{B}'}^{QC}(20)$, defines a $[120,41,10]$ QC code with $\mathrm{girth}(\mathbf{H}')=20$, i.e., it achieves the increased upper bounds.[1]

A. Girth conditions for a pre-lifted base matrix

Example 1. Consider the $(3,4)$-regular protograph-based ensemble defined by the all-ones base matrix $\mathbf{B}$ of size 3×4. The upper bound on the minimum distance for QC codes drawn from $\xi_{\mathbf{B}}^{QC}(N)$ is $d_{min}(C)\le24$. We can assume, without loss of generality, that any parity-check matrix derived from $\mathbf{B}$ has the form (see [15])

$$\mathbf{H}=\left[\begin{array}{cccc}\mathbf{I}_{0,N}&\mathbf{I}_{0,N}&\mathbf{I}_{0,N}&\mathbf{I}_{0,N}\\ \mathbf{I}_{0,N}&\mathbf{P}&\mathbf{R}&\mathbf{T}\\ \mathbf{I}_{0,N}&\mathbf{Q}&\mathbf{S}&\mathbf{U}\end{array}\right], \qquad (3)$$

where $\mathbf{P},\mathbf{Q},\mathbf{R},\mathbf{S},\mathbf{T}$ and $\mathbf{U}$ are $N\times N$ permutation matrices. Accordingly, without loss of generality, we can assume that a pre-lifted base matrix, used to derive $\mathbf{H}'\in\xi_{\mathbf{B}'}^{QC}(r)$, has the form

$$\mathbf{B}'=\left[\begin{array}{cccc}\mathbf{I}_{0,m}&\mathbf{I}_{0,m}&\mathbf{I}_{0,m}&\mathbf{I}_{0,m}\\ \mathbf{I}_{0,m}&\mathbf{B}'_P&\mathbf{B}'_R&\mathbf{B}'_T\\ \mathbf{I}_{0,m}&\mathbf{B}'_Q&\mathbf{B}'_S&\mathbf{B}'_U\end{array}\right]\in\xi_{\mathbf{B}}(m), \qquad (4)$$

where $\mathbf{B}'_P$, $\mathbf{B}'_Q$, $\mathbf{B}'_R$, $\mathbf{B}'_S$, $\mathbf{B}'_T$, and $\mathbf{B}'_U$ are $m\times m$ permutation matrices that represent base matrices for the block-circulant permutation matrices $\mathbf{P}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{S}$, $\mathbf{T}$, and $\mathbf{U}$, respectively.

In [15], a technique was presented to derive minimal conditions on the permutation matrices of a protograph-based parity-check matrix $\mathbf{H}$, derived from a binary base matrix $\mathbf{B}$, in order to achieve a certain desired girth g. We will see that by pre-lifting $\mathbf{B}$, it is possible to reduce the number of conditions that must be checked in order to achieve girth g. For example, to insure that $\mathrm{girth}(\mathbf{H})\ge8$ for any parity-check matrix in the form of (3), each member of the following set of 42 permutation matrices must not have a fixed column [15]:

$$\begin{array}{l}\{\mathbf{P},\mathbf{Q},\mathbf{R},\mathbf{S},\mathbf{T},\mathbf{U},\mathbf{P}\mathbf{R}^{\mathsf{T}},\mathbf{P}\mathbf{T}^{\mathsf{T}},\mathbf{Q}\mathbf{S}^{\mathsf{T}},\mathbf{Q}\mathbf{U}^{\mathsf{T}},\mathbf{R}\mathbf{T}^{\mathsf{T}},\mathbf{S}\mathbf{U}^{\mathsf{T}},\\ \mathbf{P}\mathbf{Q}^{\mathsf{T}},\mathbf{R}\mathbf{S}^{\mathsf{T}},\mathbf{T}\mathbf{U}^{\mathsf{T}},\mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{S}\mathbf{R}^{\mathsf{T}},\mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{U}\mathbf{T}^{\mathsf{T}},\mathbf{R}\mathbf{S}^{\mathsf{T}}\mathbf{U}\mathbf{T}^{\mathsf{T}},\mathbf{P}\mathbf{S}^{\mathsf{T}},\\ \mathbf{P}\mathbf{U}^{\mathsf{T}},\mathbf{R}\mathbf{Q}^{\mathsf{T}},\mathbf{R}\mathbf{U}^{\mathsf{T}},\mathbf{T}\mathbf{Q}^{\mathsf{T}},\mathbf{T}\mathbf{S}^{\mathsf{T}},\mathbf{P}\mathbf{S}\mathbf{R}^{\mathsf{T}},\mathbf{P}\mathbf{U}\mathbf{T}^{\mathsf{T}},\mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{S},\\ \mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{U},\mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{R}^{\mathsf{T}},\mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{T}^{\mathsf{T}},\mathbf{R}\mathbf{U}\mathbf{T}^{\mathsf{T}},\mathbf{R}\mathbf{S}^{\mathsf{T}}\mathbf{Q},\mathbf{R}\mathbf{S}^{\mathsf{T}}\mathbf{U},\mathbf{R}\mathbf{S}^{\mathsf{T}}\mathbf{T}^{\mathsf{T}},\\ \mathbf{T}\mathbf{U}^{\mathsf{T}}\mathbf{Q},\mathbf{T}\mathbf{U}^{\mathsf{T}}\mathbf{S},\mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{S}\mathbf{T}^{\mathsf{T}},\mathbf{P}\mathbf{Q}^{\mathsf{T}}\mathbf{U}\mathbf{R}^{\mathsf{T}},\mathbf{P}\mathbf{S}^{\mathsf{T}}\mathbf{U}\mathbf{T}^{\mathsf{T}},\\ \mathbf{P}\mathbf{U}^{\mathsf{T}}\mathbf{S}\mathbf{R}^{\mathsf{T}},\mathbf{R}\mathbf{Q}^{\mathsf{T}}\mathbf{U}\mathbf{T}^{\mathsf{T}},\mathbf{R}\mathbf{S}^{\mathsf{T}}\mathbf{Q}\mathbf{T}^{\mathsf{T}}\}.\end{array} \qquad (5)$$

[1] The parity-check matrix $\mathbf{H}'$ has rank 39, and hence the dimension of the code is $k=41$.

In the remainder of this section, we will establish some results on the girth of a parity-check matrix obtained from a pre-lifted base matrix $\mathbf{B}'$. These results will later be used to reduce the number of conditions that need to be checked at the circulant-based lifting step.

Lemma 1: Let $\mathbf{A}$ and $\mathbf{B}$ be two $mr \times mr$ block-circulant permutation matrices derived from $m \times m$ permutation matrices $\mathbf{B}'_A$ and $\mathbf{B}'_B$, respectively. Then the product $\mathbf{AB}$ cannot have a fixed column if $\mathbf{B}'_A\mathbf{B}'_B$ does not have a fixed column.
Proof. Omitted. Instead, we present an illustrative example.

Let

$$\mathbf{B}'_P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \mathbf{B}'_Q = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then

$$\mathbf{B}'_P(\mathbf{B}'_Q)^\mathsf{T} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \mathbf{PQ}^\mathsf{T} = \begin{bmatrix} \mathbf{0} & \mathbf{I}_{p_1}\mathbf{I}_{q_1} \\ \mathbf{I}_{p_2}\mathbf{I}_{q_2} & \mathbf{0} \end{bmatrix},$$

where $\mathbf{P} = \mathrm{diag}(\mathbf{I}_{p_1}, \mathbf{I}_{p_2}) \cdot \tilde{\mathbf{B}}'_P$, $\mathbf{Q} = \mathrm{diag}(\mathbf{I}_{q_1}, \mathbf{I}_{q_2}) \cdot \tilde{\mathbf{B}}'_Q$, $p_1, p_2, q_1, q_2 \in [r-1]$, and $\mathbf{I}_a$ has size $r \times r$. Clearly, $\mathbf{PQ}^\mathsf{T}$ does not have a fixed column for any p_1, p_2, q_1, and q_2 as a result of $\mathbf{B}'_P(\mathbf{B}'_Q)^\mathsf{T}$ not having a fixed column.

As a consequence of Lemma 1, if the permutation matrices $\mathbf{B}'_{i,j}$, $i = 1, 2, \ldots, n_c$, $j = 1, 2, \ldots, n_v$, satisfy all the necessary conditions to achieve $\mathrm{girth}(\mathbf{B}') \geq g$, then the corresponding circulant-based permutation matrices $\mathbf{P}_{i,j}$ must also satisfy these conditions. Consequently, we obtain the following theorem.

Theorem 2: If a pre-lifted base matrix $\mathbf{B}'$ satisfies $\mathrm{girth}(\mathbf{B}') \geq g$, then the girth of any code from the ensemble $\xi^{QC}_{\mathbf{B}'}(r)$ is bounded below by g, for any lifting factor r.

Often, the permutation matrices $\mathbf{B}'_{i,j}$ chosen in the first step will not satisfy all the conditions to achieve girth g. In this case, to insure that the conditions are satisfied at the second step, we must choose the component circulant matrices $\mathbf{I}_{p_{i,j,k}}$ comprising $\mathbf{P}_{i,j}$ carefully. This will be demonstrated later in Section IV-A.

B. Minimum distance properties of pre-lifted protograph-based codes

We begin by establishing a result on the commutativity of two block-circulant permutation matrices.

Lemma 3: Suppose that two block circulant permutation matrices are given as

$$\begin{aligned} \mathbf{P} &= \mathrm{diag}(\mathbf{I}_{p_1}, \mathbf{I}_{p_1}, \ldots, \mathbf{I}_{p_1}) \cdot \tilde{\mathbf{B}}'_P = \mathbf{B}'_P \otimes \mathbf{I}_{p_1}, \\ \mathbf{Q} &= \mathrm{diag}(\mathbf{I}_{q_1}, \mathbf{I}_{q_1}, \ldots, \mathbf{I}_{q_1}) \cdot \tilde{\mathbf{B}}'_Q = \mathbf{B}'_Q \otimes \mathbf{I}_{q_1}, \end{aligned}$$

where $p_1, q_1 \in [r-1]$, $\mathbf{I}_a$ has size $r \times r$, and $\mathbf{B}'_P$ and $\mathbf{B}'_Q$ are $m \times m$ permutation matrices. Then, $\mathbf{PQ} = \mathbf{QP}$ iff $\mathbf{B}'_P\mathbf{B}'_Q = \mathbf{B}'_Q\mathbf{B}'_P$.
Proof. Omitted.

In [11], MacKay and Davey established that, for an $n_c \times n_v$ grid of non-overlapping, commuting permutation matrices, the minimum distance is bounded above by $(n_c+1)!$. We now establish a similar result for a grid of non-overlapping, commuting block-circulant permutation matrices based on a pre-lifted base matrix $\mathbf{B}'$.

Theorem 4: Let $\mathbf{B}'$ be a pre-lifted base matrix derived from an $n_c \times n_v$ binary base matrix $\mathbf{B}$, and suppose $\mathbf{B}'_{i,j}\mathbf{B}'_{k,l} = \mathbf{B}'_{k,l}\mathbf{B}'_{i,j}$ $\forall i, k \in \{1, 2, \ldots, n_c\}, j, l \in \{1, 2, \ldots, n_v\}$, $(i,j) \neq (k,l)$. If $p_{i,j,1} = p_{i,j,2} = \cdots = p_{i,j,m}$ for each block circulant permutation matrix $\mathbf{P}_{i,j}$, as defined in (2), then the minimum distance of any code $C \in \xi^{QC}_{\mathbf{B}'}(r)$ is bounded above by $(n_c+1)!$.

Proof (sketch). By applying Lemma 3 to each pair of block-circulant permutation matrices $(\mathbf{P}_{i,j}, \mathbf{P}_{k,l})$ in $\mathbf{H}'$, corresponding to the pair $(\mathbf{B}'_{i,j}\mathbf{B}'_{k,l})$, we find that all of the matrices commute and thus the result of [11] holds. □

Note that, in general, if

$$\begin{aligned} \mathbf{P} &= \mathrm{diag}(\mathbf{I}_{p_1}, \mathbf{I}_{p_2}, \ldots, \mathbf{I}_{p_m}) \cdot \tilde{\mathbf{B}}'_P, \\ \mathbf{Q} &= \mathrm{diag}(\mathbf{I}_{q_1}, \mathbf{I}_{q_2}, \ldots, \mathbf{I}_{q_m}) \cdot \tilde{\mathbf{B}}'_Q, \end{aligned}$$

then

$$\mathbf{PQ} = \mathrm{diag}(\mathbf{I}_{p_1}, \ldots, \mathbf{I}_{p_m}) \cdot \tilde{\mathbf{B}}'_P \cdot \mathrm{diag}(\mathbf{I}_{q_1}, \ldots, \mathbf{I}_{q_m}) \cdot \tilde{\mathbf{B}}'_Q$$

and

$$\tilde{\mathbf{B}}'_P \cdot \mathrm{diag}(\mathbf{I}_{q_1}, \ldots, \mathbf{I}_{q_m}) = \mathrm{diag}(\mathbf{I}_{q_{\sigma(1)}}, \ldots, \mathbf{I}_{q_{\sigma(m)}}) \cdot \tilde{\mathbf{B}}'_P,$$

where σ is the permutation associated with $\mathbf{B}'_P$. Consequently,

$$\mathbf{PQ} = \mathrm{diag}(\mathbf{I}_{p_1+q_{\sigma(1)}}, \ldots, \mathbf{I}_{p_m+q_{\sigma(m)}}) \cdot \tilde{\mathbf{B}}'_P \cdot \tilde{\mathbf{B}}'_Q, \quad (6)$$

$$\mathbf{QP} = \mathrm{diag}(\mathbf{I}_{q_1+p_{\tau(1)}}, \ldots, \mathbf{I}_{q_m+p_{\tau(m)}}) \cdot \tilde{\mathbf{B}}'_Q \cdot \tilde{\mathbf{B}}'_P, \quad (7)$$

where τ is the permutation associated with $\mathbf{B}'_Q$, and addition is performed modulo r. In addition,

$$\tilde{\mathbf{B}}'_P \cdot \tilde{\mathbf{B}}'_Q = (\mathbf{B}'_P \otimes \mathbf{I}_0) \cdot \left(\mathbf{B}'_Q \otimes \mathbf{I}_0\right) = \mathbf{B}'_P\mathbf{B}'_Q \otimes \mathbf{I}_0\mathbf{I}_0$$

by the distributive law of the Kronecker product. So $\tilde{\mathbf{B}}'_P\tilde{\mathbf{B}}'_Q = \tilde{\mathbf{B}}'_Q\tilde{\mathbf{B}}'_P$ iff $\mathbf{B}'_P\mathbf{B}'_Q = \mathbf{B}'_Q\mathbf{B}'_P$.

Consequently, if $\mathbf{B}'_P\mathbf{B}'_Q = \mathbf{B}'_Q\mathbf{B}'_P$, we must insure that the diagonal matrices in (6) and (7) are not equal in order to have $\mathbf{PQ} \neq \mathbf{QP}$. Alternatively, if $\mathbf{B}'_P\mathbf{B}'_Q \neq \mathbf{B}'_Q\mathbf{B}'_P$, then $\mathbf{PQ} \neq \mathbf{QP}$ even if the diagonal matrices are equal. In Section III-C, we will use these two cases to construct rules for constructing QC-LDPC codes based on a pre-lifted protograph.

Remark 5: By insuring that not all of the block-circulant permutation matrices $\mathbf{P}_{i,j}$ commute, we can construct pre-lifted QC-LDPC codes with minimum distance exceeding $(n_c+1)!$. This can be observed by following the proof of Theorem 2 in [11]. Instead of constructing a codeword of weight $(n_c+1)!$, we obtain an $((n_c+1)!, f)$ *near-codeword*, i.e., a binary vector of weight $(n_c+1)!$ for which $f > 0$ parity-check equations are not satisfied by the near-codeword.

C. Design rules for pre-lifted protograph-based QC-LDPC codes

In order to avoid the reduced upper bound described in Theorem 4, we provide two general rules for constructing QC-LDPC codes based on a pre-lifted protograph.

- *Rule 1: Circulant pre-lifting permutation matrices.* In this case, at Step 1, each $\mathbf{B}'_{i,j}$ is chosen to be circulant. The circulants are chosen to maximize the distance upper bound (demonstrated in [12]), and the necessary conditions to achieve a desired girth g in Step 2 are calculated. At the second step, we choose circulants that satisfy the girth conditions and, since the pre-lifting permutation matrices commute, insure that, for at least one of the pairs of block-circulant permutation matrices $(\mathbf{P}, \mathbf{Q})$, the diagonal matrices in (6) and (7) do not have an overlapping column, or, equivalently, $p_i + q_{\sigma(i)} \not\equiv q_i + p_{\tau(i)} \mod r$, $\forall i$. This can be achieved by imposing the condition that σ has no fixed point, setting $q_1 = q_2 = \cdots = q_m$, and choosing each p_i to be different.
- *Rule 2: Non-commuting pre-lifting permutation matrices.* In Step 1, we choose permutation matrices $\mathbf{B}'_{i,j}$ and insure that at least one pair of matrices does not commute. The matrices should be chosen to maximize the upper bound on the minimum Hamming distance [12], and the necessary conditions to achieve a desired girth g in Step 2 are calculated. At Step 2, we choose each component circulant to have the same shift, e.g., $p_1 = p_2 = \cdots = p_m$ in block circulant $\mathbf{P}$, such that the girth conditions are satisfied.

IV. Pre-lifting with Design Rule 1

In this section, we will focus on Design Rule 1, where the pre-lifted protograph $\mathbf{B}'$ is composed of circulant submatrices, i.e., where each of the permutation matrices $\mathbf{B}'_{i,j}$ composing $\mathbf{B}'$ are chosen to be circulant.

A. Girth conditions for circulant pre-liftings

By choosing the permutations at the pre-lifting step to be circulant, we can make use of their structure to reduce and simplify the conditions required to achieve a desired girth g. We now define some useful properties of circulant permutation matrices. Let $a, b, m \in \mathbb{Z}$, $a, b \geq 0$, $m \geq 1$.

Property 1. The $m \times m$ circulant permutation matrix $\mathbf{I}_a$ has a fixed column iff $a \equiv 0 \mod m$. In this case, $\mathbf{I}_a = \mathbf{I}_0$, and all m columns are fixed.

Property 2. The product of two $m \times m$ circulant permutation matrices $\mathbf{I}_a$ and $\mathbf{I}_b$ is given as $\mathbf{I}_a\mathbf{I}_b = \mathbf{I}_{(a+b) \mod m}$.

Property 3. The transposition of an $m \times m$ circulant permutation matrix $\mathbf{I}_a$ is $\mathbf{I}_a^{\mathsf{T}} = \mathbf{I}_{(m-a) \mod m}$.

Suppose we use the technique given in [15] to generate a list of conditions on the permutation matrices comprising $\mathbf{H}$ that can be used to guarantee $\mathrm{girth}(\mathbf{H}) \geq g$. By applying Lemma 1, we can eliminate many of the conditions by checking if the corresponding products of the associated permutation matrices $\mathbf{B}'_{i,j}$ comprising $\mathbf{B}'$ have fixed columns. Choosing circulant permutation matrices is advantageous for this purpose because, using the three properties given above, we can quickly determine if a product of a number of circulant matrices has a fixed column using simple modular arithmetic (rather than costly matrix multiplication). This allows us to construct pre-lifted base matrices that minimize the number of conditions that must be checked to choose circulant permutations achieving girth g in Step 2 of the pre-lifting process.

Example 1 (cont.). In this example, we focus on achieving $\mathrm{girth}(\mathbf{H}) \geq 8$ for a parity-check matrix in the form of (3), derived from a pre-lifted base matrix, but the same principles can be applied to any protograph-based parity-check matrix derived from a binary base matrix for any desired girth. Suppose that

$$\mathbf{P} = \mathrm{diag}(\mathbf{I}_{p_1}, \mathbf{I}_{p_2}, \ldots, \mathbf{I}_{p_m}) \cdot \tilde{\mathbf{I}}_{p,m},$$

where $p \in [m-1]$, $p_i \in [r-1]$, and $\mathbf{I}_{p_i}$ has size $r \times r$. (Similar definitions apply for $\mathbf{Q}, \mathbf{R}, \mathbf{S}, \mathbf{T}$, and $\mathbf{U}$.) For pre-lifting factor $m = 5$ and any circulant-based pre-lifted base matrix $\mathbf{B}'$, the number of conditions (from the set (5)) on the permutation matrices that comprise $\mathbf{H}'$ that must be checked to guarantee $\mathrm{girth}(\mathbf{H}') \geq 8$ is in the range $[4, 42]$. Consider the following pre-lifted base matrix $\mathbf{B}'$ in the form of (4) with $m = 5$:

$$\mathbf{B}' = \begin{bmatrix} \mathbf{I}_{0,5} & \mathbf{I}_{0,5} & \mathbf{I}_{0,5} & \mathbf{I}_{0,5} \\ \mathbf{I}_{0,5} & \mathbf{I}_{0,5} & \mathbf{I}_{1,5} & \mathbf{I}_{1,5} \\ \mathbf{I}_{0,5} & \mathbf{I}_{0,5} & \mathbf{I}_{2,5} & \mathbf{I}_{4,5} \end{bmatrix}. \tag{8}$$

By choosing the permutation matrices given above at the pre-lifting step, we find that, in order to guarantee $\mathrm{girth}(\mathbf{H}') \geq 8$ in any resulting parity-check matrix $\mathbf{H}' \in \xi_{\mathbf{B}'}^{QC}(r)$, out of the 42 original conditions given in (5), we only need to check that $\mathbf{P}, \mathbf{Q}, \mathbf{P}\mathbf{Q}^{\mathsf{T}}$, and $\mathbf{R}\mathbf{T}^{\mathsf{T}}$ should not have a fixed column. Equivalently, we must insure $p_i \not\equiv 0 \mod r$, $q_i \not\equiv 0 \mod r$, $p_i + (r - q_i) \equiv p_i - q_i \not\equiv 0 \mod r$, and $r_i - t_i \not\equiv 0 \mod r$, $i = 1, 2, \ldots, 5$. Since $\mathbf{S}$ and $\mathbf{U}$ are not involved in these four conditions, the values s_i, u_i, $i = 1, \ldots, 5$ can be chosen arbitrarily.

In order to eliminate all the conditions from (5), it is necessary to increase the pre-lifting factor to $m = 9$. Then we find that it is possible to construct a circulant-based pre-lifted base matrix $\mathbf{B}'$ that has girth 8. Consequently, by Theorem 2, any $\mathbf{H}' \in \xi_{\mathbf{B}'}^{QC}(r)$ satisfies $\mathrm{girth}(\mathbf{H}') \geq 8$, i.e., there are no conditions on matrices $\mathbf{P}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{S}$, $\mathbf{T}$, and $\mathbf{U}$ that must be satisfied, so p_i, q_i, r_i, s_i, t_i, and u_i, $i = 1, 2, \ldots, 9$, can be chosen arbitrarily and we guarantee $\mathrm{girth}(\mathbf{H}') \geq 8$. The following pre-lifted base matrix is one such example:

$$\mathbf{B}' = \begin{bmatrix} \mathbf{I}_{0,9} & \mathbf{I}_{0,9} & \mathbf{I}_{0,9} & \mathbf{I}_{0,9} \\ \mathbf{I}_{0,9} & \mathbf{I}_{1,9} & \mathbf{I}_{3,9} & \mathbf{I}_{4,9} \\ \mathbf{I}_{0,9} & \mathbf{I}_{2,9} & \mathbf{I}_{6,9} & \mathbf{I}_{8,9} \end{bmatrix}. \tag{9}$$

B. Minimum distance properties

In this section, we will construct a code using Design Rule 1 and show how the minimum distance is affected if we do not follow the design criteria.

Example 2. Consider the following circulant-based pre-lifted base matrix with $m = 2$:[2]

$$\mathbf{B}' = \begin{bmatrix} \mathbf{I}_{0,2} & \mathbf{I}_{0,2} & \mathbf{I}_{0,2} & \mathbf{I}_{0,2} \\ \mathbf{I}_{0,2} & \mathbf{I}_{0,2} & \mathbf{I}_{1,2} & \mathbf{I}_{1,2} \\ \mathbf{I}_{0,2} & \mathbf{I}_{1,2} & \mathbf{I}_{0,2} & \mathbf{I}_{0,2} \end{bmatrix}. \tag{10}$$

A resulting parity-check matrix $\mathbf{H}' \in \xi_{\mathbf{B}'}^{QC}(r)$ has the form

$$\mathbf{H}' = \left[\begin{array}{cc|cc|cc|cc} \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{0,r} \\ \hline \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{p_1,r} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{r_1,r} & \mathbf{0} & \mathbf{I}_{t_1,r} \\ \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{I}_{p_2,r} & \mathbf{I}_{r_2,r} & \mathbf{0} & \mathbf{I}_{t_2,r} & \mathbf{0} \\ \hline \mathbf{I}_{0,r} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{q_1,r} & \mathbf{I}_{s_1,r} & \mathbf{0} & \mathbf{I}_{u_1,r} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{0,r} & \mathbf{I}_{q_2,r} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{s_2,r} & \mathbf{0} & \mathbf{I}_{u_2,r} \end{array}\right].$$

Suppose that we set $p_1 = p_2 = 1$, $q_1 = q_2 = 7$, $r_1 = r_2 = 10$, $s_1 = s_2 = 11$, $t_1 = t_2 = 13$, and $u_1 = u_2 = 2$ with $r = 49$. This parity-check matrix satisfies the conditions to achieve $\mathrm{girth}(\mathbf{H}') = 10$. However, because the shift parameters in each block circulant are identical, this construction does not adhere to Design Rule 1. In fact, we have the conditions of Theorem 4, and the minimum distance is bounded above by $d_{min} \leq (n_c + 1)! = 24$. This is in fact a $[392, 100, 24]$ QC code, i.e., the upper bound is achieved.

Suppose that instead we set $p_2 = 5$ and $u_2 = 4$. Consequently, the block-circulant permutation matrices $\mathbf{P}$ and $\mathbf{U}$ are composed of two different circulant sub-matrices and the pairs of matrices no longer all commute (e.g., $\mathbf{PQ} \neq \mathbf{QP}$ for $r = 49$), satisfying Design Rule 1. The minimum distance of this code, denoted by $\mathcal{C}_1$, is increased to a range $32 \leq d_{min} \leq 56$ (determined using MAGMA) and $\mathrm{girth}(\mathbf{H}') = 10$.[3]

C. Simulation results

Simulations were performed assuming binary phase shift keyed (BPSK) modulation and an additive white Gaussian noise (AWGN) channel. The decoder was allowed a maximum of 100 iterations and employed a syndrome-check based stopping rule. In Fig. 1, we plot the simulated decoding performance for: the pre-lifted $(3, 4)$-regular QC code $\mathcal{C}_1$ with $m = 2$ from Example 2; the extended $(3, 4)$-regular QC Tanner code $\mathcal{C}_2$ defined in (1), where the circulant size is taken to be $N = 98$ so that the code length and rate are the same as for code $\mathcal{C}_1$; and the original $(3, 4)$-regular QC Tanner code $\mathcal{C}_3$ with circulant size $N = 31$. Both codes $\mathcal{C}_2$ and $\mathcal{C}_3$ achieve the upper bound $d_{min} = 24$ and have $\mathrm{girth}(\mathbf{H}) = 8$. We observe that the pre-lifted code $\mathcal{C}_1$ has significantly improved decoding performance, with a SNR gain of over 1dB at a bit error rate of 10^{-5}.

[2] Note that, for $m = 2$, we must use Design Rule 1 because all of the permutations are circulant.

[3] Due to the computational complexity, we are not able to compute the minimum distance of this example exactly. However, we conjecture that it is, in fact, equal or close to the upper bound based on 1) the results obtained for smaller values of r, and 2) the significant search time without finding any codewords of weight less than 56.

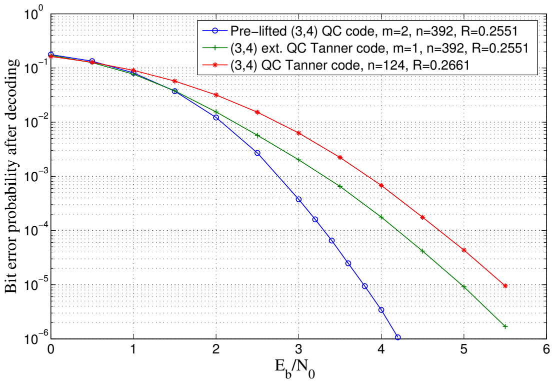

Fig. 1: Simulated decoding perfomance for the pre-lifted $(3,4)$-regular QC-LDPC code $\mathcal{C}_1$ described in Example 2, the extended $(3,4)$-regular Tanner QC-LDPC code $\mathcal{C}_2$, and the original Tanner code $\mathcal{C}_3$.

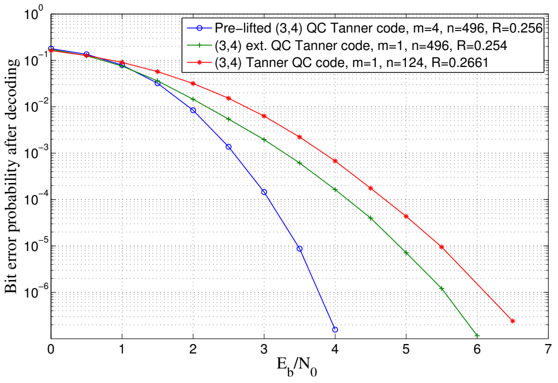

Fig. 2: Simulated decoding perfomance for the pre-lifted $(3,4)$-regular QC-LDPC code $\mathcal{C}_4$ described in Example 3, the extended $(3,4)$-regular Tanner QC-LDPC code $\mathcal{C}_5$, and the original Tanner code $\mathcal{C}_3$.

V. Pre-lifting with Design Rule 2

In this section, we construct a pre-lifted QC-LDPC code following Design Rule 2.

Example 3. We construct a parity-check matrix $\mathbf{H}'$ derived from a pre-lifted base matrix $\mathbf{B}'$ defined in (4) with $m = 4$. This matrix has the general form of (3), where, in this example, $\mathbf{I} = \mathbf{I}_{0,m} \otimes \mathbf{I}_{0,r}$ and the submatrix

$$\begin{bmatrix} \mathbf{P} & \mathbf{R} & \mathbf{T} \\ \mathbf{Q} & \mathbf{S} & \mathbf{U} \end{bmatrix} = \begin{bmatrix} \mathbf{B}'_P \otimes \mathbf{I}_{4,r} & \mathbf{B}'_R \otimes \mathbf{I}_{12,r} & \mathbf{B}'_T \otimes \mathbf{I}_{28,r} \\ \mathbf{B}'_Q \otimes \mathbf{I}_{24,r} & \mathbf{B}'_S \otimes \mathbf{I}_{10,r} & \mathbf{B}'_U \otimes \mathbf{I}_{13,r} \end{bmatrix} =$$

$$\left[\begin{array}{cccc|cccc|cccc} \mathbf{0} & \mathbf{I}_4 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{12} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{28} & \mathbf{0} & \mathbf{0} \\ \mathbf{I}_4 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{12} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{28} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_4 & \mathbf{I}_{12} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{28} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_4 & \mathbf{0} & \mathbf{0} & \mathbf{I}_{12} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{28} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{I}_{24} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{10} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{13} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{24} & \mathbf{I}_{10} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{13} \\ \mathbf{0} & \mathbf{I}_{24} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{10} & \mathbf{I}_{13} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{I}_{24} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{10} & \mathbf{0} & \mathbf{0} & \mathbf{I}_{13} & \mathbf{0} & \mathbf{0} \end{array}\right].$$

Note that the pre-lifting permutation matrices $\mathbf{B}'_P$, $\mathbf{B}'_Q$, $\mathbf{B}'_R$, $\mathbf{B}'_S$, $\mathbf{B}'_T$, and $\mathbf{B}'_U$ have been chosen so that several of the permutations do not commute, yet $\mathbf{B}'_T$ and $\mathbf{B}'_U$ are, in fact, circulant. These pre-lifting permutations were chosen in pairs following the techniques in [12] in order to give large upper bounds on the minimum distance. Also, note that the same shift parameter is used in each block-circulant; these parameters were chosen from the Tanner code with parity-check matrix given in (1). The Tanner graph associated with $\mathbf{H}'$ can be considered as a 4-fold graph cover of the original Tanner graph associated with (1).

For $r = 14$, we obtain a $[224, 59, 36]$ QC-LDPC code with $\mathrm{girth}(\mathbf{H}') = 8$. As we increase r, the minimum distance generally improves, but it becomes hard to verify the value exactly as the code length increases. For $r = 31$, we obtain a $[496, 126]$ QC-LDPC code $\mathcal{C}_4$ with $\mathrm{girth}(\mathbf{H}') = 8$ and $28 \leq d_{min} \leq 68$ (again, we conjecture that the minimum distance is, in fact, close to 68).

In Fig. 2, we simulate the decoding performance of $\mathcal{C}_4$ and the two $(3,4)$-regular QC Tanner codes (that $\mathcal{C}_4$ is based upon): the extended $(3,4)$-regular QC Tanner code $\mathcal{C}_5$ defined in (1), where the circulant size is taken to be $N = 124$ so that the code length is equal, and the rate is approximately equal to that of $\mathcal{C}_4$; and the $(3,4)$-regular QC Tanner code $\mathcal{C}_3$. Again, we observe significantly improved decoding performance for the pre-lifted QC code.

Design Rule 2 is particularly useful, because we can employ the theory presented here to design a good pre-lifting matrix and use state-of-the-art QC codes to choose the circulants at Step 2 of the pre-lifting procedure. We expect there to be large gains in decoding performance made possible by pre-lifting a 'good' code. In this paper, we have used the Tanner code as a model, but the same procedure can be applied to any array-based QC code.

VI. Conclusions

In this paper, we have extended the results of our previous work and analysed a two-step lifting procedure to create new QC-LDPC codes with improved minimum distance and girth properties. We presented two design rules: one uses circulant permutation matrices at the first (pre-lifting) stage and the other uses a selection of non-commuting permutation matrices. For both techniques, we showed that simplified conditions can be obtained to achieve a desired girth g, and we provided examples showing a demonstrable increase in minimum distance compared to a direct circulant-based lifting of the original protograph. The expected performance improvement was verified by simulation results.

References

[1] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

[2] 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, 2004.

[3] H. Tang, J. Xu, S. Lin, and K. A. S. Abdel-Ghaffar, "Codes on finite geometries," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 572–596, 2005.

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

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

[6] L. Zhang, Q. Huang, S. Lin, K. Abdel-Ghaffar, and I. F. Blake, "Quasi-cyclic LDPC codes: An algebraic construction, rank analysis, and codes on latin squares," *IEEE Trans. Comm.*, vol. 58, no. 11, pp. 3126–3139, Nov. 2010.

[7] L. Zhang, S. Lin, K. Abdel-Ghaffar, Z. Ding, and B. Zhou, "Quasi-cyclic LDPC codes on cyclic subgroups of finite fields," *IEEE Trans. on Comm.*, vol. 59, no. 9, pp. 2330–2336, Sept. 2011.

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

[9] 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. Inf. Theory*, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

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

[11] 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.

[12] D. G. M. Mitchell, R. Smarandache, and D. J. Costello, Jr., "Quasi-cyclic LDPC codes based on pre-lifted protographs," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011.

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

[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. Inf. Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.

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